Berner
Fachhochschule

Semesterarbeit

Telemetrie von Desktop-Webbrowser

Studiengang	CAS Security Incident Management
Autor	Mauro Guadagnini
Experte	Daniel Röthlisberger

Version 1.0 vom 24. März 2024

Abstract

Diese Arbeit behandelt automatische Kommunikationen der Desktop-Webbrowser in Form von Telemetrie. Im Fokus liegen die Browser Google Chrome, Microsoft Edge und Mozilla Firefox sowie der Tor Browser unter dem Betriebssystem Windows 11. Analysen erfolgen zu Anwendungsfällen wie dem ersten Start des Browsers, dem Besuch von statischen Webseiten und Webshops sowie dem Verwenden des entsprechenden Privat-Modus. Das Vertrauen, das viele Benutzerinnen und Benutzer in den Webbrowser legen, wird hiermit hinterfragt.

Eine nachvollziehbar dokumentierte Laborumgebung bietet jedem Browser eine dedizierte virtuelle Maschine und forciert die Kommunikation über einen zentralen Proxy-Server. Auf diesem Proxy-Server wird die gegebenenfalls verschlüsselte Kommunikation aufgebrochen und aufgezeichnet. Parallel erfolgt auf der entsprechenden virtuellen Maschine eine Aufzeichnung der Prozess-Verhalten. Mittels Skript werden Aufzeichnungen standardisiert gestartet und zur Analyse-Station kopiert. Dort finden Auswertungen statt, in welchen unter anderem die Kommunikationen mit Prozessen in Verbindung gebracht, aufgezeigt und interpretiert werden.

Zum Tor Browser wurde keine Telemetrie festgestellt. Die restlichen der betrachteten Browser senden Informationen zur verwendeten Hardware und Betriebssystem zu dessen Hersteller. Weiter senden diese Browser Eingaben in die Adressleiste vor dem Absenden an die hinterlegte Suchmaschine. Im entsprechenden Privat-Modus werden die Eingaben erst beim Versand (zum Beispiel per Enter-Taste) übermittelt. Hersteller wie Google und Microsoft erwähnen, dass deren Browser sensitive Daten erkennen und nicht senden kann, gehen jedoch nicht genauer darauf ein. Microsoft Edge erzeugt durch Verwendung weiterer Funktionalitäten wie zum Beispiel dessen Shopping-Services weitere Telemetrie. Anhand welcher Webseiten bei Edge die Shopping-Funktion ausgelöst wird, kann der Herstellerdokumentation nicht entnommen werden.

Stammen der Browser und die Suchmaschine vom selben Hersteller, ist von einer Verschmelzung der Browser-Telemetrie und des Suchmaschinen-Trackings auszugehen. Google nutzt bei Chrome dessen Suchmaschine, bei Microsoft Edge wird die hauseigene Suchmaschine Bing verwendet. Im Falle dieser Arbeit stammt das verwendete Betriebssystem ebenfalls von Microsoft.

Titelbild: *Basel, Zollreportage* (Krebs 1983) [1]

Inhaltsverzeichnis

1. Einleitung

Dieses Dokument behandelt die Untersuchung der Telemetrie von Desktop-Webbrowsern[1]. Ziel ist es, die Kommunikationen der Webbrowser mit dessen Hersteller zu unterschiedlichen Zeitpunkten bzw. Anwendungsfällen aufzuzeigen. Diese Arbeit richtet sich an Personen mit Kenntnissen in Netzwerk- und Betriebssystem-Prozess-Analysen, der Internet-Kommunikation mit Protokollen wie DNS und HTTP sowie Tor.

Hierbei handelt es sich um eine Semesterarbeit im CAS Security Incident Management (2023 HS) an der Berner Fachhochschule gemäss einem selbst gewählten und bewilligten Projektantrag. Ausgangslage und Zielsetzung sind entsprechend Vorgaben und Vorstellungen des Autors definiert.

1.1. Ausgangslage

Die Wahl des Webbrowsers erfolgt bei vielen Benutzerinnen und Benutzern unter anderem aufgrund Bequemlichkeit, Gewohnheit oder Überzeugung. Egal welcher Webbrowser genutzt wird, über ihn wird unter anderem mit dem Internet interagiert sowie Infrastrukturen verwaltet. Dadurch wird ein Vertrauen in den Webbrowser gelegt, das mit dieser Arbeit hinterfragt wird.

Es gilt automatische Kommunikationen folgender Webbrowser zu ermitteln[2]:

- Google Chrome [2]
- Microsoft Edge [3]
- Mozilla Firefox [4]
- Tor Browser [5]

Diese Webbrowser-Auswahl ergibt sich aufgrund diverser Browser-Statistiken [6][7][8] und gegebenen Mitteln[3]. Der Tor Browser basiert auf Firefox [11] und kommt in besagten Browser-Statistiken nicht explizit vor. In der Praxis wird der Tor Browser in den Bereichen Cyber Security sowie zur Wahrung der Anonymität und Privatsphäre als ein Werkzeug verwendet, in das noch mehr Vertrauen als die breiter angewendeten Browser gelegt wird. Aus diesem Grund wird der Tor Browser ebenfalls betrachtet.

[1] Die Begriffe „Webbrowser“ und „Browser“ sind in dieser Arbeit als Synonyme zu betrachten
[2] Die Namen der Webbrowser werden zukünftig auch ohne Herstellernamen aufgeführt (zum Beispiel „Chrome“)
[3] Die aktuellste Version des Browsers „Safari“ von Apple für ein Microsoft-Windows-Betriebssystem wurde 2012 veröffentlicht [9][10]. In der aktuellen Version ist Safari nur auf Apple-Betriebssystemen installierbar [9]

1.2. Zielsetzung

Die Prüfung der Browser in der jeweils aktuellen Version erfolgt mittels Blackbox-Ansatz. Dazu werden sie in dedizierte Virtuelle Maschinen („VMs“) installiert und so im Netzwerk eingebunden, dass sie zur Kommunikation mit dem Internet über einen Proxy-Server verkehren müssen. Auf diesem Proxy-Server, der als MITM (Man-in-the-Middle) fungiert und der Browser-VM werden die Verhalten aufgezeichnet und gegebenenfalls so weit wie möglich aufgeschlüsselt. Zusätzlich verschlüsselte, nicht einsehbare Inhalte werden gegebenenfalls aufgezeigt und bestmöglich interpretiert.

Aus dieser Zielsetzung ergeben sich folgende Punkte als zu erreichende Ziele:

- Aufbau der Analyse-Umgebung inklusive
  - Installation der Webbrowser und Aufzeichnungs-Tools
  - Konfiguration des Proxy-Servers als MITM mit allfälliger Aufschlüsselung
  - Aufzeichnung auf Netzwerk- und Betriebssystem-Ebene
- Untersuchung der Browser auf mögliche Telemetrie-Trigger
- Analysen der Webbrowser-Telemetrie zu u. a. folgenden Zeitpunkten
  - Neuinstallation ohne Browser-Start
  - Erster Start des Webbrowsers
  - Schliessen des Browsers
  - Besuch einer statischen Webseite
  - Besuch eines Webshops
- Untersuchung des Telemetrie-Verhaltens im allfällig verfügbaren Privat-Modus des Browsers („Incognito Mode“, „InPrivate Browsing“, etc.)

Nachweisbare Aussagen zur Telemetrie (Kommunikation und Inhalt) der aufgeführten Desktop-Webbrowser sind das Ergebnis dieser Arbeit. Die dafür verwendete Infrastruktur sowie dessen Aufbau ist nachvollziehbar und reproduzierbar dokumentiert[4].

Jeder der hier behandelten Webbrowser kann auf den Betriebssystemen „Microsoft Windows“, „Apple macOS“ und „Linux“ installiert werden [11][12][13][14]. Der Fokus dieser Arbeit liegt auf den Webbrowser unter dem Betriebssystem „Microsoft Windows 11“ in der aktuellsten Version. Grund dafür ist, dass Windows das am weitesten verbreitete Desktop-Betriebssystem ist [15][16], womit diese Arbeit eine grössere Zielmenge erreichen kann.

[4] Im Rahmen dieser Arbeit werden Betriebssysteme in Virtuellen Maschinen („VMs“) betrieben.

2. Planung

Dieses Kapitel beschreibt das Vorgehen und entsprechende Massnahmen zur Zielerarbeitung dieser Arbeit.

2.1. Vorgehen

Der Aufbau dieser Arbeit entspricht folgendem Vorgehen:

1. Start
    a) Ausgangslage etablieren
    b) Ziele definieren
2. Planung
    a) Überblick über zur Verfügung stehende Mittel inkl. Beschaffung zusätzlicher Komponenten
    b) Definition Massnahmen zur Zielerarbeitung
    c) Kontrolle Planung gemäss Zielsetzung
3. Recherche
    a) Bestehende Arbeiten
    b) Aussagen der Browser-Hersteller zu deren Telemetrie
    c) Aufzeichnungs- und Analyse-Werkzeuge auf Netzwerk- und Betriebssystem-Ebene
4. Aufbau
    a) Installation und Konfiguration der Windows-VM
        i. Umgang mit dem Browser Edge auf Windows (wird mitgeliefert)
        ii. Implementation und Vorbereitung der Aufzeichnungs- und Analyse-Tools
        iii. Ermittlung allfälliger Kommunikation von Windows ohne Browser („Grundrauschen“)
        iv. Snapshots der VM mindestens vor der Browser-Installation
    b) Installation und Konfiguration des Proxy-Servers als MITM
    inklusive Implementation und Vorbereitung der Aufzeichnungs- und Analyse-Tools
    c) Verifikation und Test der Laborumgebung inklusive Aufzeichnungs- und Analyse-Möglichkeiten
5. Analyse
    a) Untersuchung der Browser auf Telemetrie-Trigger
    b) Analyse der Webbrowser-Telemetrie zu den Zeitpunkten gemäss der Liste in Kapitel 1.2
    c) Verifikation ermittelter Werte
6. Interpretation
    a) Ergebnisse aufzeigen sowie interpretieren (inkl. allfällig verschlüsselter Inhalte)
7. Abschluss
    a) Fazit, Rückblick und Ausblick definieren
    b) Dokumentation finalisieren

Zur Ermöglichung der Reproduktion sind zugehörige Befunde und Vorgehen dokumentiert.

2.2. Verfügbare Komponenten

Folgende Komponenten stehen für diese Arbeit zur Verfügung[5]:

Komponente	Hersteller	Bezeichnung	Version	Datum	Quelle
Hypervisor	Oracle	VirtualBox	7.0.12	12.10.2023	[17]
Betriebssystem	Microsoft	Windows 11	23H2	31.10.2023	[18]
Betriebssystem	Software in the Public Interest (SPI) und andere	Debian	12.4.0	10.12.2023	[19]
Browser	Google	Chrome	121.0.6167.140	30.01.2024	[2]
Browser	Microsoft	Edge	120.0.2210.144	17.01.2024	[3]
Browser	Mozilla	Firefox	122.0.1	06.02.2024	[20]
Browser	The Tor Project, Inc.	Tor Browser	13.0.8	20.01.2024	[21]
Analyse Netzwerk	Battelle Energy Alliance LLC and CISA	Malcolm	23.12.1	20.12.2023	[22]
Analyse Netzwerk	Mitmproxy Project	mitmproxy	10.2.1	06.01.2024	[23]
Analyse Netzwerk	Wireshark Foundation	Wireshark	4.2.2	01.01.2024	[24]
Analyse Windows	Mark Russinovich	AutoRuns	14.1	27.06.2023	[25]
Abhängigkeit	Python Software Found.	Python	3.12.1	08.12.2023	[26]
Analyse Windows	Brian Baskin	Noriben	2.0	09.08.2023	[27]
Abhängigkeit	Microsoft	Microsoft Visual C++ Redistributable	14.38.33130	18.11.2017	[28]
Abhängigkeit	The Graphviz Authors	Graphviz	9.0.0	08.12.2023	[26]
Analyse Windows	Christian Wojner	ProcDOT	1.22.57	28.08.2018	[29]
Analyse Windows	Mark Russinovich	Process Explorer	17.05	26.07.2023	[30]
Analyse Windows	WJ32	Process Hacker	2.39	29.03.2016	[31]
Analyse Windows	Mark Russinovich	Process Monitor	3.96	29.09.2023	[32]

Tabelle 2.1.: Verfügbare Komponenten

2.3. Massnahmen zur Zielerarbeitung

Entsprechend der Zielsetzung aus Kapitel 1.2 und dem Vorgehen aus Kapitel 2.1 ergeben sich folgende Massnahmen zur Zielerarbeitung:

1. Finden und Nachvollziehen bestehender Arbeiten und Herstellerdokumentationen
2. Erörtern zu verwendender Werkzeuge zur Aufzeichnung und Analyse auf Netzwerk- und Betriebssystem-Ebene
3. Aufbau und Verifikation Laborumgebung
4. Allfällige Telemetrie-Trigger der Webbrowser ermitteln
5. Erarbeitung von Testfällen zur Telemetrie-Ermittlung bei unterschiedlichen Zeitpunkten, Trigger und „Privat-Modi“ („Incognito Modus“, etc.)
6. Aufzeichnung, Analyse und Verifikation der Desktop-Webbrowser-Telemetrie
7. Interpretation der Ergebnisse

[5] Begründung der Analyse-Werkzeugwahl in Kapitel 3.5

3. Recherche

Dieses Kapitel zeigt in dieser Arbeit verwendete Begriffe auf und geht auf bestehende Arbeiten sowie die Herstellerdokumentationen ein. Die verwendeten Komponenten für die entsprechende Labor-Infrastruktur werden ebenfalls aufgezeigt.

3.1. Tracking versus Telemetrie

Um den Fokus dieser Arbeit hervorzuheben folgt eine Erläuterung des Unterschieds zwischen Telemetrie und Tracking („Verfolgen“) mittels u. a. Cookies und Browser-Fingerprints.

Je nach besuchter Webseite gibt es Elemente, die zu weiteren Anfragen des Webbrowsers an Dritte führen [33]. Diese Anfragen beinhalten Informationen über den Browser sowie die anwendende Person, die anhand von Cookies und Browser-Fingerprinting über mehrere Webseiten hinweg verknüpft werden können. Durch diese Verknüpfungen ergibt sich ein detailliertes Benutzerprofil [33]. Cookies speichern Informationen von einer Webseite im Browser und das Fingerprinting sammelt Charakteristiken, die zusammen eindeutig einer Benutzerin oder einem Benutzer, Browser und Hardware-Setup zuordenbar sind (Bildschirmauflösung, Schriftarten, Geolocation, etc.) [33].

Somit ist das **Tracking für Webseiten und damit verbundene Dritt-Parteien** wie z.B. Werbe-Netzwerken von Bedeutung, wobei die hier behandelte **Telemetrie für den Hersteller der Software** (in diesem Fall ein Webbrowser) eine Rolle spielt.

Unter der Telemetrie versteht man das Sammeln, Messen und Übertragen von Daten von einer entfernten Quelle zu einem zentralen Knoten [34]. Von diesem Knoten aus werden die Daten analysiert und interpretiert [34]. Oftmals wird Telemetrie bei einem Produkt eingesetzt, um mehr Informationen über u. a. dessen Verwendung einzuholen und das Produkt entsprechend zu verbessern [34]. Der Inhalt übertragener Telemetrie-Daten, die Informationen zur eigenen Infrastruktur oder Privatsphäre preisgeben könnten, stellt ein Risiko und Hauptaspekt dieser Arbeit dar.

3.2. Proxy-Server (Transparent versus Non-Transparent)

Dieser Abschnitt dient zur groben Darstellung der Unterschiede zwischen „transparenten“ und „nicht-transparenten“ Proxy-Servern. Einer der grössten Unterschiede liegt darin, dass ein Client bei einem transparenten Proxy-Server nicht von dessen Existenz wissen muss, damit dessen Kommunikation über diesen Proxy verläuft [35][36]. Ein weiteres Merkmal transparenter Proxy-Server im Gegensatz zu nicht-transparenten Proxy-Server ist, dass diese den Inhalt des Verkehrs nicht modifizieren [35][36].

Diese Eigenschaften transparenter Proxy-Server machen diese zu geeigneten Komponenten für diese Arbeit, da keine weiteren Modifikationen an den Clients für dessen Einsatz nötig sind. Somit ergibt sich ein Client-Verhalten, das näher an der Praxis der meisten Internetnutzer liegt. Hierbei handelt es sich gemäss Erfahrungen des Autors um ein Verhalten, bei welchem möglichst wenige Anpassungen am Client vorgenommen werden.

3.3. Bestehende Arbeiten

Um möglichst relevante Arbeiten aufzuzeigen, gilt es den Zeitraum entsprechend einzugrenzen. Die Browser Edge und Firefox (und somit auch der darauf aufbauende Tor Browser [11]) wurden in den letzten Jahren komplett neu aufgebaut oder generalüberholt. Edge existiert in der Neubau-Version auf Chromium-Basis seit Beginn 2020 [37][38]. Firefox existiert mit der Bezeichnung „Firefox Quantum“ und Versionsnummer 57 als generalüberholte Version seit November 2017 [39][40][41]. Als Extended Support Release (ESR)[6] Version mit Nummer 60.0esr gibt es „Firefox Quantum“ seit Mitte 2018 [43]. Der Tor Browser baut in der Stable-Version mit Nummer 8.0 vom September 2018 auf Firefox 60.0esr auf [44].

Diese Veröffentlichungszeitpunkte bewegen zur Annahme, dass die Aussagen allfällig gefundener Dokumente vor diesen Zeitpunkten mittlerweile weniger anwendbar sind. Bei bestehenden Arbeiten ist daher auf die Aktualität sowie ausgewiesene Browser-Versionsnummern zu achten.

Die bisher aktuellste und am weitesten verbreitete Arbeit ist von **Leith** mit dem Titel “Web Browser Privacy: What Do Browsers Say When They Phone Home?” aus 2020 [46], mit aktualisierter Version im Journal „IEEE Access“ im Jahr 2021 [45]. Diese Arbeit hat einige Artikel auf Webseiten zum Thema Cyber Security, IT und Technologie ausgelöst, die oft den Browser Edge mit am meisten Eingriffe in die Privatsphäre hervorheben [47][48][49][50]. Zudem beinhaltet die Arbeit die Aussage, dass nach Kenntnis der Autoren keine vorgängigen und systematischen Analysen zum Inhalt zwischen Browsern und deren zugehörigen Servern gemeldet sind [45].

Es werden u. a. zu den Webbrowsern Chrome, Edge und Firefox gemeldet, dass diese Details besuchter Webseiten mit ihren „Backend-Server“[7] teilen und langlebige Identifikatoren verwenden [45]. Eine Zusammenfassung der ermittelten Daten, die Browser mit ihren Server teilen, ist der folgenden Tabelle zu entnehmen.

Browser	Instanz-Identifikator Durch Neuinstallation änderbar	Hardware-Identifikator Nicht durch Benutzer anpassbar	Cookie	Telemetrie	URL Somit auch Webseiten-History
Chrome Version 80.0.3987.87 vom 4. Feb. 2020 [51]	ENRU		ER		NU
Edge Version 80.0.361.48 vom 7. Feb. 2020 [52]	ER	ER	EN	ER	NU
Firefox Version 73.0 vom 11. Feb. 2020 [53]	ER			ER	U

E = Erster Start des Browsers N = Seiten-Navigation R = „Restart“ (Neustart) des Browsers U = Eingabe URL

Tabelle 3.1.: Zusammenfassung der Daten, die Desktop-Browser mit ihren Backend-Server teilen gemäss der Arbeit von Leith [45]

[6] Ein Firefox ESR Release nimmt jeweils eine bestimmte Firefox Version und wartet diese für über ein Jahr, sodass diese Versionen weniger oft neue Funktionen, jedoch die neusten Sicherheits-Patches erhalten [42]

[7] Diese Backend-Server werden beispielsweise für Updates, Checks von Phishing- oder Malware-Webseiten („Safe-Browsing-Service“) oder Telemetrie verwendet [45]

Diese Erkenntnisse erzielte der Autor unter den Betriebssystemen macOS und Windows 10[8] durch Einsatz einer MITM-Proxy-Software „mitmdump“ [54][45]. Diese Software fungierte hierbei als transparenter Proxy-Server mit entsprechend hinterlegtem Zertifikat auf den Clients zur Aufschlüsselung [45]. Leith konnte bei keinem der betrachteten Browsern blockierten Verbindungen aufgrund von Certificate Pinning feststellen, bei welchen Verbindungen aufgrund des Proxy-Zertifikats nicht aufgebaut wurden [45]. Wie bei dieser Arbeit wird der Fokus auf die Standardausführung der Webbrowser gelegt, da diese die Mehrheit an Benutzern betrifft und diese Standardeinstellungen von den Entwicklern mit hoher Sicherheit nicht willkürlich festgelegt wurden [45].

Zu den „Privat-Modi“ der Browser schreibt Leith, dass sich diese hauptsächlich auf das Speichern der Browser-History und Cookies beziehen [45]. Nach Beendigung des Privat-Modus verwirft der Browser im Privat-Modus die Cookies und History [45]. Bezüglich den IP-Adressen vermerkt der Autor, dass durch diese eine ungefähre Standort-Bestimmung des Benutzers möglich ist, die durch die Frequenz der gesendeten Daten (z.B. täglich oder alle 15 Minuten) entsprechend genauer wird[9] [45].

Der Artikel von **sizeof(cat)** mit dem Titel „*Web Browser telemetry*“ von 2021 [55] listet die Verbindungen diverser Webbrowser (in Form von Domain-Namen oder IP-Adressen mit Ports) nach einer Neuinstallation unter macOS auf. Verwendet wurde dafür die Host-basierte Firewall-Software „Little Snitch“, die unter macOS ausgehende Verbindungen von Applikationen mit dem Internet überwacht und blockieren lässt [56][55].

Die in dieser Arbeit betrachteten Browser erzielten dabei folgende Anzahl an Verbindungen[10] [55]:

- Chrome, Version 96.0.4664.110 vom 13. Dez. 2021 [57]: 9
- Edge, Version 96.0.1054.62 vom 17. Dez. 2021 [58]: 21
- Firefox, Version 95.0.1 vom 16. Dez. 2021 [59]: 15
- Tor Browser, Version 11.0.2 vom 8. Dez. 2021 [60]: 0

Dass der Tor Browser keine Verbindungen aufbaut, erklärt sich dadurch, dass dieser beim Browser-Start nicht automatisch eine Verbindung mit dem Tor Netzwerk herstellt. Stattdessen muss diese Verbindung manuell initiiert werden (siehe Abbildung 3.1). Eine Verbindung zum Tor Netzwerk über einen Entry Guard tritt als TCP-Verbindung auf und würde daher ebenfalls von „Little Snitch“ aufgezeigt werden [61].

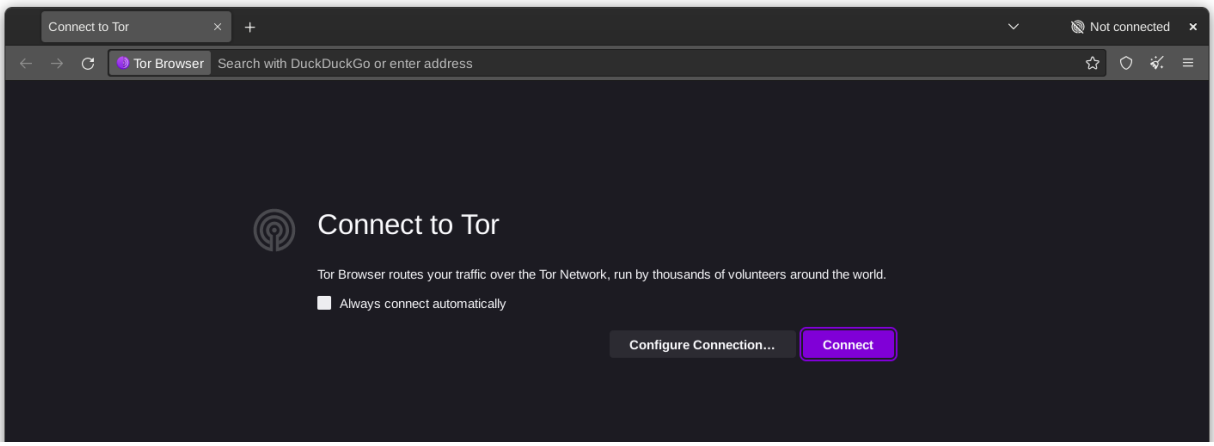


Abbildung 3.1.: Tor Browser: Dialog zum Tor-Verbindungsaufbau beim Start des Browsers

[8] Die ermittelten Verbindungen der Browser sind unter beiden Betriebssystemen ähnlich, wobei Edge unter Windows zusätzliche Kommunikationen tätigt [45]

[9] Die Arbeit von Leith betrachtet auch Browser auf Smartphones, jedoch kann ein Laptop ebenfalls unterwegs verwendet werden

[10] Domain bzw. IP-Adresse und Port zählt hierbei als eine Verbindung

Der Autor weist darauf hin, dass diese Verbindungen nicht direkt mit Telemetrie im Zusammenhang stehen, sondern auch von Vorschlägen eines neuen Browser-Tabs stammen können [55]. Bei diesen Vorschlägen handelt es sich jedoch auch um ungewollte Kommunikationen [55].

Der Artikel „*Best Privacy Web Browser to Stay Private in 2023*“ von der Webseite **privacytools.io** listet Firefox und den Tor Browser als Software zur Wahrung der Privatsphäre auf [62]. Die Seite vermerkt bei Firefox, dass bei dessen Download ein eindeutiger „Download-Token“ mitgegeben wird, der bei dessen Telemetrie gesendet wird [62]. Dies wird durch einen Artikel von Brinkmann [63] zusätzlich aufgezeigt, wobei dies auch auf der Support-Webseite von Firefox ausgewiesen wird [64]. Die Firefox-Support-Webseite merkt an, dass nicht jeder Firefox-Installer mit einem solchen Token versehen ist [64]. Chrome verwendet für dessen Windows-Installation ebenfalls einen solchen Token, löscht diesen jedoch nach dem ersten Start und Update-Check [65].

3.4. Herstellerdokumentation

Dieser Abschnitt dient als Übersicht der Herstellerdokumentationen (primär „Privacy Whitepapers“ der Hersteller von Chrome, Edge und Firefox). Zusätzlich hebt der Abschnitt die für diese Arbeit relevantesten Informationen und Standardeinstellungen der Browser vor. Auf den Aufbau der Browser selber wird aus Zeitgründen nicht eingegangen. Der Fokus liegt bei den Daten, die der Browser laut Hersteller mit ihm teilt.

3.4.1. Google Chrome

Der Hersteller von Chrome (Google) hat ein Whitepaper zur Privatsphäre im Bezug auf dessen Browser (Desktop- und Smartphone-Versionen) veröffentlicht[11] [65]. Es beschreibt die Funktionen in Chrome, die mit Google oder Dritten (z.B. je nach Suchmaschinen-Wahl[12]) kommunizieren und vermerkt auch welche Einstellungen entsprechend zu setzen sind [65].

Abbildung 3.2.: Chrome Logo [66]

Bei der Eingabe in die **Adressleiste** oder der Markierung dieser wird die hinterlegte Suchmaschine kontaktiert, wobei auch die IP-Adresse und bestimmte Cookies mitgesendet werden[13] [65]. Im „Incognito-Modus“ (dem Privat-Modus von Chrome) verwendet Chrome die Ressourcen auf dem Gerät und kontaktiert erst bei der Auswahl eines Suchmaschinen-Vorschlags die Suchmaschine [65]. Der Browser kann entscheiden, ob die Information im Feld sensitive Informationen enthält und geht dann wie im Incognito-Modus vor [65]. Bei aktiver Synchronisation der Browser-History mit einem Google-Konto und Google als Suchmaschine wird zudem die URL der aktiven HTTP(S)-Webseite geteilt, um kontextuell relevante Suchvorschläge erzielen zu können [65]. Bei der Eingabe eines einzelnen Wortes kann der Browser dieses als DNS-Anfrage verwenden und zu diesem Host navigieren [65].

Anhand der IP-Adresse wird das Land oder die Region bestimmt und entsprechende Vorschläge auf der **„New Tab“-Seite** angezeigt [65]. Diese Seite erscheint beim Öffnen eines neuen Tabs, in welchem noch nicht zu einer Ressource navigiert wurde [65]. Für neue Vorschläge wird ebenfalls die Browser-History verwendet [65]. Wird ein Vorschlag auf der Seite eines neuen Tabs angepasst, werden keine neuen Vorschläge mehr vom Browser angezeigt [65].

[11] Die letzte Änderung war am 4. Feb. 2021, wobei ein „Lite Mode“ (Option für die Smartphone-Version zur Minimierung des Datenvolumen-Verbrauchs) erwähnt wird, der 2022 von Google ausser Betrieb genommen wurde [67]. Gleiches gilt für das „Chrome Cleanup Tool“, das unter Windows das System nach „ungewollter“ Software geprüft hat und mittlerweile ebenfalls entfernt wurde [68]. Des Weiteren sind im Whitepaper Links aufgeführt, die nicht mehr zu ihrem ursprünglichen Ziel führen. Im Verlauf dieser Arbeit wurde dieses Whitepaper aktualisiert (siehe Kapitel 6.1.1)

[12] Bei einer Suchmaschine, die nicht Google ist, werden die Anfragen gemäss dessen Richtlinien verarbeitet [65]

[13] Chrome kann vorgängig eine Verbindung zur Suchmaschine aufbauen, um schneller Ergebnisse zu erzielen („Preload“) [65]

Das **„Safe Browsing“-Feature** lädt von Google regelmässig eine Liste von unsicheren Webseiten herunter, die mit Phishing, Malware, Social Engineering oder ähnlichem in Verbindung stehen [65]. Jede installierte Browser-Erweiterung, URL oder Datei wird gegen diese Liste geprüft [65]. Bei einem Treffer wird ein Teil des Hashes der URL zur Verifikation an Google gesendet [65]. Bei der Anfrage einer Webseite nach einer potentiell gefährlichen Berechtigung sendet Chrome ebenfalls ein Teil des Hashes der URL [65]. Sollte eine Webseite verdächtig erscheinen[14], werden Begriffe, die wahrscheinlich Phishing oder Social Engineering zuordenbar sind an Google gesendet [65]. Sieht eine Login-Seite einer auf der Liste hinterlegten Seite ähnlich, wird die URL und der zutreffende Listeneintrag ebenfalls an Google gesendet [65]. Für weitere Informationen zu Safe Browsing wird auf eine separate Webseite [69] verwiesen.

Weitere Kommunikationen sind ebenfalls dem Whitepaper zu entnehmen, wobei hier eine kleine, stichwortartige Liste folgt [65]:

- Aktualisierung von Chrome sowie dessen Erweiterungen (u. a. aus dem Chrome Web Store [70]) mit der Anwendung „Google Update“
- Verwendung von NTP zur Verifikation von SSL-Zertifikaten
- Wurde der Browser über eine entsprechende Werbekampagne heruntergeladen und installiert, wird dessen Tag bei der Suche mit Google mitgegeben („RLZ String“, wird nicht bei der Installation über die Hauptseite [2] verwendet)
- Die „Autofill“-Funktion sendet bei Formularen u. a. dessen Struktur und Felder-Namen zu Google, jedoch nicht die eingetragenen Werte

Bestimmte Funktionen wie das Voraussagen benötigter Ressourcen und Webseiten, das URLs der aktiven Seite an Google sendet, sind nicht in der Standardausführung aktiviert (in diesem Beispiel wäre es die Option „Make Searches and Browsing Better“) [65]. Weitere Funktionen und Daten werden in Anspruch genommen, wenn ein Google-Konto mit dem Chrome-Browser verknüpft ist [65]. Hierbei ist zu beachten, dass beim Login bei einem Google Service der Browser automatisch mit dem Login verknüpft wird, dies jedoch mit der Option „Allow Chrome sign-in“ deaktiviert werden kann [65].

Zum Incognito-Modus ist zusätzlich zu erwähnen, dass dieser keine Push-Meldungen erlaubt sowie darin entstandene Browser-History und Cookies am Ende der Sitzung entfernt [65].

[14] Wie das ermittelt wird, wird im Whitepaper nicht beschrieben

3.4.2. Microsoft Edge

Abbildung 3.3.: Edge Logo [71]

Microsoft hat im Zusammenhang mit ihrem Browser Edge ebenfalls ein Privatsphäre-Whitepaper mit Fokus auf die Desktop-Version herausgegeben [38].

Wie auch bei Chrome wird die Suchmaschine bei einer Eingabe in die **Adressleiste** oder dessen Fokussierung kontaktiert [38]. Wird die Microsoft-eigene Suchmaschine „Bing“ verwendet, wird zusätzlich ein eindeutiger, zurücksetzbarer Identifikator gesendet [38]. Ebenfalls wie bei Chrome wird beim Erkennen sensitiver Informationen die Eingabe nicht an die Suchmaschine gesendet (ausser man sendet die Eingabe als Suchanfrage ab) [38]. Eingegebene Zeichen und besuchte Webseiten werden pro Profil lokal gespeichert [38]. Der Privat-Modus von Edge („InPrivate“) sendet wie Chrome ebenfalls keine Eingaben an die Suchmaschine, sondern kontaktiert diese erst bei der Wahl eines lokal erzeugten Vorschlags oder dem Absenden einer Suchanfrage [38].

Edge sammelt je nach Einstellung mehr oder weniger **Diagnose-Daten**, wobei das Minimum als Standardeinstellung die Geräte-Konnektivität, Konfiguration, Software-Setup und Inventar beinhaltet [38]. Auf Windows-Geräten werden die Diagnose-Daten zusammen mit einem, dem Gerät eindeutig zuweisbaren Identifikator übermittelt, wobei das Whitepaper zusätzlich auf die Anwendung „Diagnostic Data Viewer“ zur eigenen Analyse unter Windows verweist [38].

Heruntergeladene Dateien und besuchte Webseiten werden mittels **Microsoft Defender SmartScreen** geprüft [38]. Dieser Verkehr wird dabei in 3 Kategorien geteilt: „Top Traffic“, Gefährlich und Unbekannt [38]. Dabei wird die URL gegen eine lokale, regelmässig aktualisierte Liste geprüft und alle URLs, die nicht zum „Top Traffic“ zählen, werden zusammen mit weiteren Webseiten-Infos, allgemeinen Standortdaten und einem Hardware-Identifikator zum SmartScreen-Dienst via HTTPS gesendet [38]. Heruntergeladene Dateien werden anhand ihrer Binärdaten während dem Download synchron gescannt und vor Download-Abschluss durch Senden des Datei-Hashes, -Namens, Download-URI und des Hardware-Identifikators an den SmartScreen-Dienst geprüft [38].

Die **„New Tab“-Seite** von Edge enthält eine Textbox, mit welcher Suchen auf Bing durchgeführt werden können [38]. Zudem werden dort mittels „Microsoft News“ Inhalte entsprechend der öffentlichen IP-Adresse[15] angezeigt [38].

[15] Diese IP-Adresse wird in einer geschnittenen Version mit Microsoft geteilt [38]

Es folgt eine nicht abschliessende Liste weiterer Kommunikationen von Edge [38]:

- Aktualisierung von Edge sowie dessen Erweiterungen mit der Anwendung „Microsoft Edge Update Service“
- Copilot, ein im Browser integrierter Assistent mit künstlicher Intelligenz [72], sendet je nach Anfrage mehr oder weniger Daten (u. a. zur offenen Webseite) an Microsoft
- Edge kontaktiert auch Google-Dienste wie z.B. den Chrome Web Store [70] bei entsprechenden Browser-Erweiterungen[16] oder für Kopierschutzmechanismen bei der Wiedergabe von Medien
- Die „Autofill“-Funktion sendet bei Formularen u. a. dessen Struktur und Felder-Namen zu Microsoft, jedoch nicht die eingetragenen Werte
- Bei einer Suche auf der Webseite (z.B. mit der Tastenkombination „Ctrl+F“ werden für das Miteinbeziehen von ähnlichen Bezeichnungen, Synonymen oder anderen Schreibweisen der Inhalt der Webseite sowie die Suchbegriffe an Microsoft gesendet)
- Soll über den Browser ein Standort mitgeteilt werden, wobei die Standort-Funktion des Geräts ausgeschaltet ist, sendet Edge lokale Netzwerkinformationen inklusive allfälliger WLAN-Access-Points zur ungefähren Standortermittlung an Microsoft
- Verwendung von NTP zur Verifikation von SSL-Zertifikaten
- „Guest-Mode“, der temporäre Instanzen eines frischen Browser-Profils verwendet, wobei die Sammlung von Diagnose-Daten der Browser-Einstellungen vom Start-Profil abhängt [38]
- „Shopping“- und „Travel“-Funktionen (Einkaufen und Reisen), die bei zutreffenden Webseiten weitere Daten wie Shopping-Produktinformationen oder Flugdaten (ohne einer Person zuweisbarer Daten) mit Microsoft teilen [38]
- Wird ein Arbeits-Profil, z.B. „user@firma.ch“ verwendet, kann die Firma sämtliche URLs, Dateien für Down- und Upload sowie Copy-Paste- und Druck-Operationen einsehen [38]

Weitere Funktionen und Daten werden in Anspruch genommen, wenn ein Microsoft-Konto mit dem Edge-Browser verknüpft ist [38]. Edge versucht anhand des hinterlegten Kontos im Windows-Betriebssystem sich ebenfalls mit diesem Account im Browser einzuloggen. Zusätzliche, nicht standardmässig aktivierte Optionen im Browser ermöglichen das Teilen weiterer Information mit dem Hersteller [38].

[16] Es existiert zudem eine Webseite mit Browser-Erweiterungen für Edge unter dem Namen „Microsoft Edge Add-ons“ [73]

3.4.3. Mozilla Firefox

Abbildung 3.4.: Firefox Logo [74]

Mozilla, der Hersteller von Firefox, hat für besagten Browser ebenfalls Privatsphäre-Notizen[17] veröffentlicht [75]. Bearbeitete Daten teilt das Dokument in 2 Kategorien auf: Standardmässig geteilte Informationen und zusätzliche Funktionalitäten [75]. Dieser Abschnitt behandelt nur die per Standardausführung aktivierten Optionen.

Im Vergleich zu den zwei zuvor erwähnten Webbrowsern ist Firefox **„Open Source“**, was bedeutet, dass dessen Quellcode frei zugänglich ist [76]. Dadurch ist jeder eingeladen, an der Entwicklung des Browsers mitzuwirken, weshalb weitere Dokumente wie z.B. zur Entwicklung [77] und internen Prozessen zur Daten-Sammlung [78] im Internet verfügbar sind. Mozilla schreibt vor, dass die Anwender jeweils die Möglichkeit haben müssen, die Daten-Sammlung auszuschalten [78].

Mozilla teilt zu sammelnde Daten in **4 Kategorien** ein [78]:

Kategorie 1 **Technische Daten**
Hard- und Software-Info, bei welcher kein oder kaum das Risiko einer persönlichen Identifizierung besteht
Beispiele: Versionsnummern, Ergebnisse automatisierter Prozesse (z.B. Updates), Benutzereinstellungen
Daten dieser Kategorie dürfen in einer „Release-Version“ (nicht Beta oder ähnlichem) standardmässig gesammelt werden

Kategorie 2 **Interaktion-Daten**
Direkte Benutzerinteraktionen, bei welcher kein oder kaum das Risiko einer persönlichen Identifizierung besteht
Beispiele: Anzahl synchronisierter Geräte, Maus-Klicks, Scroll-Position
Daten dieser Kategorie dürfen in einer „Release-Version“ standardmässig gesammelt werden

Kategorie 3 **Gespeicherte Inhalte und Kommunikationen**
Informationen zum Inhalt von Synchronisationen und Kommunikationen oder Verbindungsziele
Beispiele: Browser-History sowie gespeicherte URLs, Tags, Notizen oder Passwörter
Daten dieser Kategorie dürfen in einer „Release-Version“ zur mit der Zustimmung der Benutzerin oder des Benutzers gesammelt werden, wobei Einzelfälle je nach Risikoeinschätzung in der Standardausführung aktiv sein dürfen

Kategorie 4 **Hoch-sensitive und eindeutig einer Person zuweisbare Daten**
Informationen, die eine Person direkt oder in Kombination mit anderen Daten identifizierbar machen
Beispiele: Benutzerkonten (Name, Passwort, E-Mail-Adresse), Zahlungsdaten, Kontaktdaten
Kann zudem Daten anderer Kategorien beinhalten, die in Kombination eine Person identifizieren können
Beispiele: Log-Daten aus Kategorie 1 in Kombination mit URLs aus Kategorie 3, Biometrische Daten
Daten dieser Kategorie dürfen in einer „Release-Version“ nie standardmässig gesammelt werden

Der Firefox Browser sendet zu dessen Verbesserung Daten der ersten zwei Kategorien (Technische Daten und Interaktion-Daten) wie Version, Sprache, Hardware-Konfiguration und Fehlerinformationen (Kategorie 1) sowie die Anzahl offener Tabs und Fenster, Anzahl und Typen installierter Erweiterungen (Kategorie 2) [75].

[17] Der Begriff Whitepaper wird hier nicht aufgeführt, stattdessen wird dem Dokument der Titel „Privacy Notice“ verliehen

Betreffend **Suchfunktionalität** wird die IP-Adresse zur Bestimmung der länderspezifischen Suchmaschine verwendet[18] [75]. Zur Generierung von Suchvorschlägen wird auch in Firefox während der Eingabe der Inhalt zur entsprechenden Suchmaschine gesendet [75]. Um Vorschläge für u. a. Erweiterungen und Webseiten anzuzeigen, wird wieder die IP-Adresse zur Länder-Ermittlung verwendet sowie die Interaktion mit diesen Vorschlägen (Anzahl Darstellungen und Klicks) an Mozilla übermittelt [75]. Bei gesponserten Einträgen werden Regionaldaten mit der Uhrzeit an die Plattform „AdMarketplace“ gesendet [75].

Verbindungen zu Mozilla werden zur Überprüfung und entsprechender **Aktualisierung des Browsers und dessen Erweiterungen** gesendet [75]. Wie bei Chrome verwendet Firefox ebenfalls den „Safe Browsing“-Service von Google (siehe Kapitel 3.4.1) für besuchte Webseiten und Downloads.

Daten, die dem **Firefox-Installationsprogramm** je nach Download beigefügt wurden, werden ebenfalls an Mozilla gesendet, um die Download-Webseite oder Werbekampagne des Browser-Downloads zu ermitteln [75]. Auf alternative Quellen zum Browser-Download sowie Anweisungen zur Telemetrie-Deaktivierung wird in der „Privacy Notice“ verwiesen [75][64].

Zusätzliche Funktionalitäten und Daten werden verwendet, sobald ein Mozilla-Account mit Firefox verknüpft wird [75]. Je nach Land, in dem Firefox verwendet wird, können unterschiedliche Optionen aktiv sein (z.B. ist „DNS over HTTPS“ bereits in den USA, Kanada, Russland und der Ukraine ausgerollt [79]) [75].

3.4.4. Tor Browser

Zum Tor Browser gibt es vom Hersteller keine expliziten Privacy-Artikel, jedoch wird auf dessen Support-Seite [11] u. a. auf Fragen zur Anonymität und zur Einsicht der Daten durch Externe eingegangen[19]. Zur Ermittlung der Benutzerzahlen wird ausgewiesen, dass diese nicht direkt, sondern über die Anzahl Anfragen an Verzeichnisse mit Tor-Relays indirekt geschätzt wird [82]. Anhand der IP-Adresse wird bei der Verzeichnisanfrage das Herkunftsland ermittelt [82]. Bemerkt wird, dass nicht jedes dieser Verzeichnisse Verbindungsstatistiken preisgibt, jedoch von den verfügbaren Angaben aus hochgerechnet wird (inklusive Rechenweg) [82].

Abbildung 3.5.: Tor Browser Logo [80]

Der Tor Browser basiert auf Firefox ESR (Extended Support Release) und ist wie Firefox auch **„Open Source“** [83].

Wie andere Browser hat der Tor Browser ebenfalls eine **Suchmaschine** hinterlegt [11]. Diese trägt den Namen „DuckDuckGo“, betreibt kein Benutzer-Tracking und speichert keine Daten zu Suchanfragen [11][84].

[18] Im Gegensatz zu Google Chrome und Microsoft Edge bieten die Hersteller von Firefox keine eigene Suchmaschine an [65][38][75]
[19] Dies wird auf besagter Webseite mit Unterschieden zur Kommunikation mit und ohne HTTPS und/oder Tor veranschaulicht [81]

3.5. Aufzeichnung und Analyse

Dieser Abschnitt zeigt Applikationen zur Aufzeichnung und Analyse der genannten Webbrowser und daraus entstehendem Netzwerkverkehr auf. Die Wahl einiger Tools gründet darauf, dass diese im zu dieser Arbeit zugehörigen Unterricht des CAS Security Incident Management der Berner Fachhochschule verwendet werden. Somit wird der im Unterricht behandelte Stoff vertieft.

3.5.1. Netzwerk-Ebene

Ein Werkzeug zur Aufzeichnung und Analyse des Netzwerkverkehrs dieser Arbeit ist die Software von **„Wireshark“**[20] [24]. Diese ermöglicht Speichern der Aufzeichnungen als PCAP-Dateien [24]. Gemäss Erfahrung des Autors kann die Menge an Daten bei Aufzeichnungen mit Wireshark umfangreich ausfallen, weshalb es zur Unterstützung der PCAP-Analyse weitere Werkzeuge zu Rate ziehen gilt.

Das SANS Institut, das u. a. Cyber-Security-Kurse anbietet, listet für dessen erweiterten Netzwerk-Forensik-Kurs („FOR572“) eine Auswahl an dort behandelter Software auf [85]. Darunter liegen die Anwendungen “SOF-ELK“, “Arkime“, “Zeek“ und Wireshark [85]. Die Plattform SOF-ELK wurde ursprünglich für besagten Kurs entwickelt und bietet eine virtuelle Maschine an, die unterschiedliche Log-Typen und NetFlow einlesen und visualisieren kann [86]. NetFlow-Infos können aus PCAP-Dateien in SOF-ELK eingelesen werden, jedoch empfiehlt der Software-Autor[21] zur PCAP-Analyse die Software Arkime [88]. Mittels **Arkime** kann Netzwerkverkehr aufgezeichnet, aber auch bestehende PCAP-Dateien importiert und entsprechende Daten indexiert werden [89]. Zeek ist ein Netzwerk-Überwachungs-Tool, das Metadaten aus dem Netzwerkverkehr extrahiert, veranschaulicht und in einem eigenen Log-Format ablegt [85][90]. Zeek scheint keine tiefere Analyse von PCAP-Dateien zu erlauben, da dessen Dokumentation eine ganzheitliche Übersicht auf einem hohen Level beschreibt [91].

Die CISA (Cybersecurity and Infrastructure Security Agency, eine Bundesbehörde der USA [92]) bietet mit **„Malcolm“** eine Software-Suite an, die zuvor genannte Anwendungen Arkime und Zeek mit einer Vielzahl weiterer Software[22] vereint [96][22]. PCAP-Dateien können offline importiert und analysiert werden[23] [97].

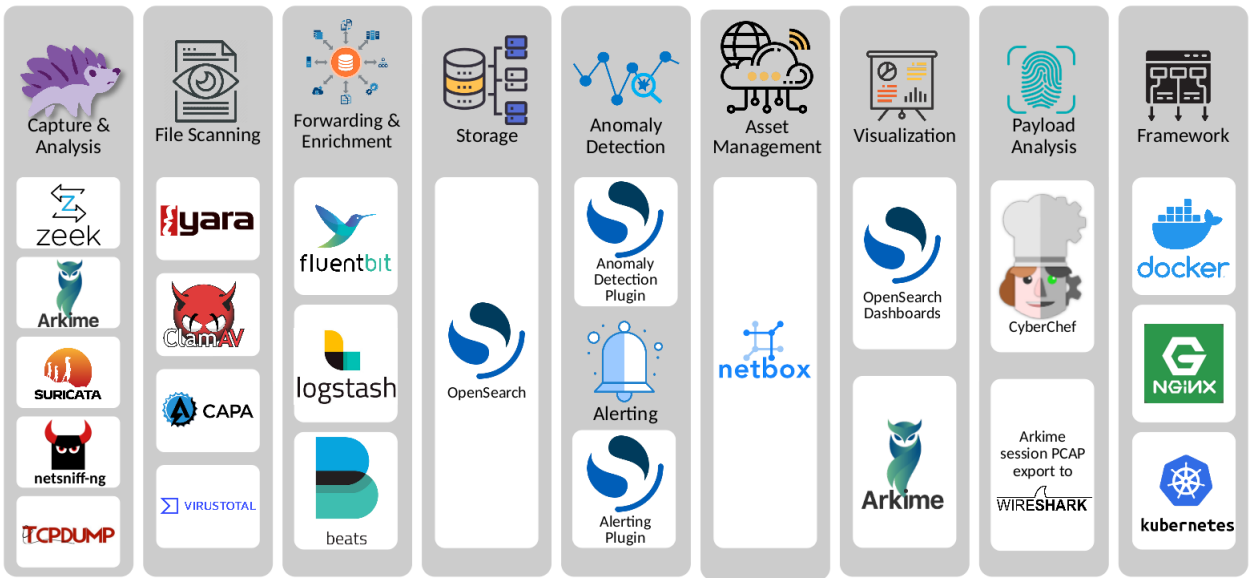


Abbildung 3.6.: Komponenten von Malcolm [96]

[20] Hierbei handelt es sich um Software aus dem Unterricht (mehr dazu siehe Beginn von Kapitel 3.5)
[21] Besagter SANS-Kurs und SOF-ELK stammen beide vom selben Autor (Philip Hagen) [86][85][87]
[22] u. a. das Intrusion Detection System „Suricata“ [93], die Such- und Analyse-Engine „OpenSearch“ [94], die AntiVirus-Engine „ClamAV“ [95] und viele mehr [96]
[23] Zum Aufbau von Malcolm ist eine Internetverbindung notwendig, jedoch nicht für dessen Betrieb [22]

In der Arbeit von Douglas J. Leith (siehe Kapitel 3.3) wird ein transparenter Proxy-Server inklusive Abhören von SSL/TLS-Verbindungen mit der Software-Suite **„mitmproxy“** [23] eingesetzt [45]. Davon unabhängig empfiehlt der Experte dieser Semesterarbeit (Daniel Röthlisberger) dem Autor dieselbe Software für den gleichen Verwendungszweck. „PolarProxy“ bietet u. a. dieselbe Funktionalität wie mitmproxy mit dem Zusatz, dass der entschlüsselte Verkehr direkt in eine PCAP-Datei gespeichert wird[24] [99]. PolarProxy ist im Vergleich zu mitmproxy auf einem älteren Software-Stand und nicht Open Source [99][23]. Aus diesen Gründen fällt die Wahl auf mitmproxy als Proxy-Server.

3.5.2. Windows-Betriebssystem-Ebene

Zur Aufzeichnung und Analyse von Interaktionen auf Windows-Betriebssystem-Ebene werden primär Anwendungen verwendet, die aus dem CAS Security Incident Management stammen. Diese Tools zur Analyse lokaler Interaktionen werden neben dem entsprechenden Unterricht auch von anderen Quellen wie einem Malware-Analyse-Kursleiter des SANS Institute [101][102] oder diversen Cyber-Security-Blogs [103][104] hervorgehoben. Zusätzlich wird auf diese Weise der im Unterricht behandelte Stoff vertieft und Zeit zum Erlernen neuer Werkzeuge eingespart.

Diese Anwendungen werden zur Analyse von Malware verwendet, sind jedoch auch auf andere Prozesse wie in diesem Falle Webbrowser anwendbar.

Folgende Software wird zur Analyse der Webbrowser-Interaktionen mit dem Windows-Betriebssystem mit Fokus auf Telemetrie verwendet[20]:

- **„Autoruns“**
  Übersicht automatisch startender Anwendungen [25]
- **„Process Explorer“**
  Liefert Informationen zu von Prozessen geladenen oder geöffneten Handles und DLLs [30]
- **„Process Hacker“**
  Alternative zum Process Explorer mit zusätzlichen Funktionen [30]
- **„Process Monitor“** (auch bekannt als „Procmon“)
  Überwachung der Aktivität zu Dateisystemen, Windows-Registry sowie Prozesse/Threads in Echtzeit [32]
- **„Noriben“**
  Zeichnet das Verhalten einer Anwendung auf (verwendet dazu Procmon) [27]
- **„ProcDOT“**
  Bietet die Korrelation von mit z.B. Noriben aufgezeichneten Procmon-Daten mit PCAP-Aufzeichnungen und visualisiert die Interaktionen als Graph [29]

[24] mitmproxy und PolarProxy sind auch in der Linux-Distribution „REMnux“ für Reverse-Engineering und Malware-Analysen [98] vorzufinden [99][100]

4. Aufbau Laborumgebung

Dieses Kapitel behandelt den Aufbau der Laborumgebung zur Analyse der Webbrowser-Telemetrie. Der Aufbau erfolgt auf einem Laptop mit virtuellen Maschinen in VirtualBox mit Software gemäss Tabelle 2.1 aus Kapitel 2.2 in jeweils englischer Sprachausgabe.

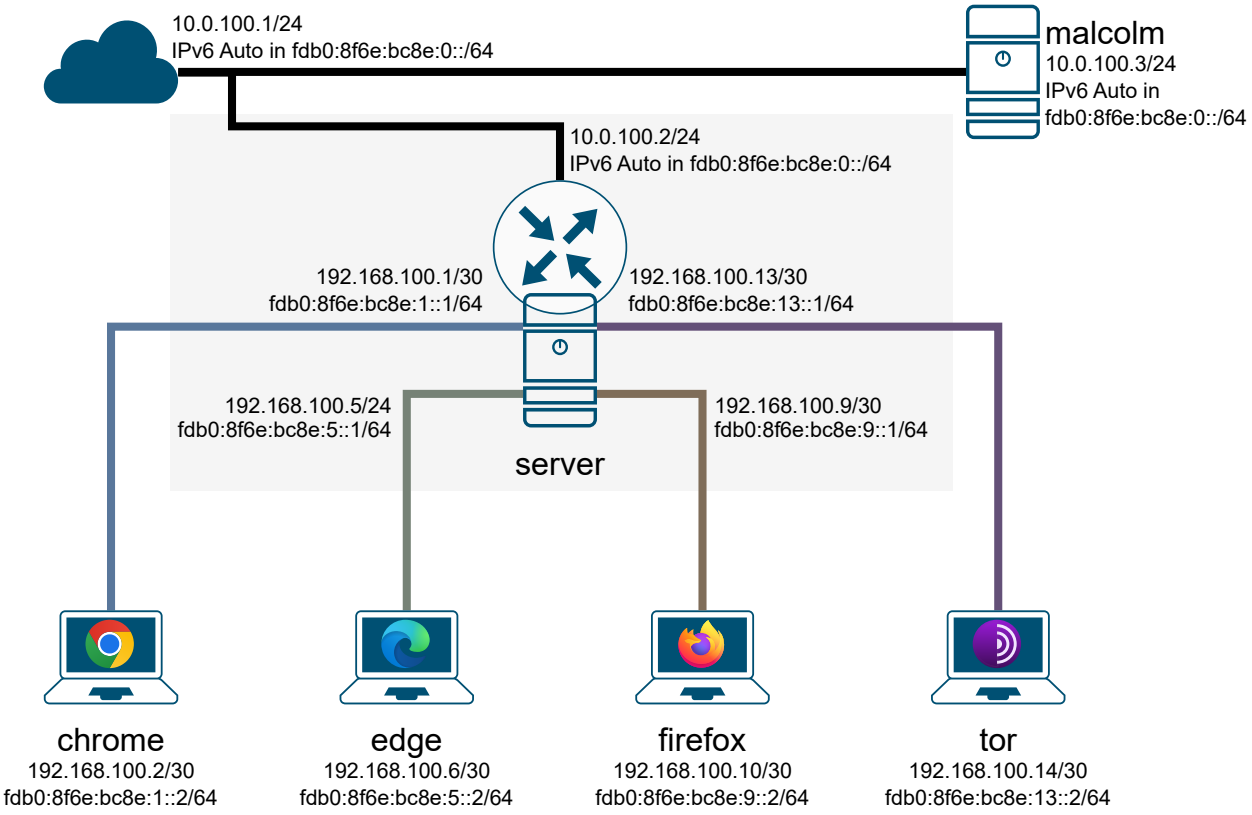


Abbildung 4.1.: Laborumgebung [66][71][74][80]

Hostname	Beschreibung
chrome.lab.internal	Windows Client mit Chrome Browser
edge.lab.internal	Windows Client mit Edge Browser
firefox.lab.internal	Windows Client mit Firefox Browser
tor.lab.internal	Windows Client mit Tor Browser
server.lab.internal	Proxy-Server, DNS-Forwarder, Firewall und Router
malcolm.lab.internal	Malcolm Analysis Software Suite

Tabelle 4.1.: Virtuelle Maschinen in der Laborumgebung (IP-Adressen siehe Abbildung 4.1)

Die Windows-Clients basieren auf einer Virtuellen Maschine, die als Vorlage aufgebaut wird und dann als Quell-VM für „Linked Clones“ agiert[25]. Diese VM wird fortan als „Windows-Template“ bezeichnet.

Um eine Kommunikation der Windows-Clients untereinander zu vermeiden, werden diese in einzelne Subnetze gelegt und über eine Firewall voneinander isoliert.

Unter VirtualBox erfolgen über die Netzwerkverwaltung unter „Tools“ → „Network“ folgende NAT-Netzwerk-Einstellungen:

- Name: `natbrowser`
  IPv4 Prefix: 10.0.100.0/24
  Enable DHCP: Deaktiviert
  Enable IPv6: Aktiviert
  IPv6 Prefix: fdb0:8f6e:bc8e:0::/64[26]
  Advertise Default IPv6 Route: Aktiviert
- Port Forwarding IPv4 (Nur für den Zugang auf die Server `server` und `malcolm` via HTTPS und SSH benötigt)
  - Name: `server-http`
    Protocol: TCP
    Host Port: 28081
    Guest IP: 10.0.100.2
    Guest Port: 8081
  - Name: `server-ssh`
    Protocol: TCP
    Host Port: 22221
    Guest IP: 10.0.100.2
    Guest Port: 22
  - Name: `malcolm-https`
    Protocol: TCP
    Host Port: 22443
    Guest IP: 10.0.100.3
    Guest Port: 443
  - Name: `malcolm-ssh`
    Protocol: TCP
    Host Port: 22222
    Guest IP: 10.0.100.3
    Guest Port: 22
  - Name: `template-ssh`
    Protocol: TCP
    Host Port: 22223
    Guest IP: 10.0.100.4
    Guest Port: 22

Die Gateway-IPv4-Adresse für Komponenten dieses NAT-Netzwerks lautet 10.0.100.1/24. Dies ist auf dem VirtualBox-Host mittels Befehl `vboxmanage natnetwork list natbrowser` verifizierbar.

[25] Bei „Linked Clones“ wird anstelle eines „Full Clones“ ein Delta des Disk-Abbildes basierend auf dem Abbild der Quell-VM angelegt [105]
[26] Generierte Unique Local IPv6 Unicast Addresse [106][107]

4.1. Zentraler Server und Firewall

Damit der Aufbau der Laborumgebung möglichst klein ausfällt, werden Firewall, Routing, Proxy-Server und DNS-Forwarder auf einem Server vereint (`server.lab.internal`). Sämtliche Befehle werden, sofern nicht anders vermerkt, als Benutzerkonto `root` oder `user` via `sudo` ausgeführt.

Dieser Server wird als VM mit Namen `server.lab.internal`, Betriebssystem Debian und folgenden Merkmalen installiert:

- VM-Ausstattung
  - Arbeitsspeicher: 2048 MB
  - Anzahl Prozessoren: 2 CPUs
  - Speicherplatz: 80 GB
  - Optisches Laufwerk: `debian-12.4.0-amd64-netinst.iso`
  - Netzwerkadapter:

    NIC1 Angeschlossen an NAT-Netzwerk `natbrowser` mittels folgendem Befehl
    ```
    vboxmanage modifyvm server.lab.internal \
     --nic1 natnetwork --nat-network1=natbrowser
    ```

    NIC2 Angeschlossen an internem Netzwerk `chrome` mittels folgendem Befehl
    ```
    vboxmanage modifyvm server.lab.internal \
     --nic2 intnet --intnet2=chrome
    ```

    NIC3 Angeschlossen an internem Netzwerk `edge` mittels folgendem Befehl
    ```
    vboxmanage modifyvm server.lab.internal \
     --nic3 intnet --intnet3=edge
    ```

    NIC4 Angeschlossen an internem Netzwerk `firefox` mittels folgendem Befehl
    ```
    vboxmanage modifyvm server.lab.internal \
     --nic4 intnet --intnet4=firefox
    ```

    NIC5 Angeschlossen an internem Netzwerk `tor` mittels folgendem Befehl
    ```
    vboxmanage modifyvm server.lab.internal \
     --nic5 intnet --intnet5=tor
    ```

- Installation[27]
  - Sprache: `English`
  - Ort: `Switzerland`
  - Locale: `en_US.UTF-8`
  - Tastatur-Layout: `Swiss German`
  - Netzwerk-Konfiguration für primäres Interface mit statischer IP-Adresse `enp0s3`: 10.0.100.2/24 (Gateway- und Nameserver-Adresse 10.0.100.1)
  - Hostname: `server.lab.internal`
  - Benutzerkonto: `user`
  - Software-Auswahl: Alles abwählen und `SSH server` wählen
  - GRUB-Bootloader-Install: `/dev/sda`

[27] Bei nicht erwähnten Einstellungen wurde jeweils die Standard-Option übernommen

- Konfiguration im Betriebssystem
  - Installation von `sudo` und Konfiguration für Benutzerkonto `user`
    `apt install sudo && usermod -a -G sudo user`
  - Netzwerk-Konfiguration durch editieren von `/etc/network/interfaces` gemäss Quelltext A.3 in Kapitel A.1.3 und ausführen von `systemctl restart networking` [28]
  - Installation notwendiger Basis-Software[29]
    `apt install curl iptables-persistent tcpdump tshark`
  - tshark für nicht privilegierte Benutzerkonten erlauben
    `setcap cap_net_raw,cap_net_admin=ep $(which dumpcap)`
  - DNS-Forwarder [109]
    - `apt install bind9 bind9utils`
    - Datei `/etc/bind/named.conf.options` so anpassen, dass der VirtualBox-Host als Forwarder eingetragen ist:
      `forwarders { 10.0.100.1; };`
    - Konfiguration übernehmen und Service neu starten mit `systemctl restart bind9`
  - Routing-/Firewall-Konfiguration
    - Blockieren der Kommunikation zwischen den Subnetzen mit Windows-Clients bzw. Paket-Weiterleitungen nur von und zum Anschluss mit Internetverbindung (`enp0s3`) erlauben
    - Whitelisting der Kommunikation der Windows-Client-Subnetze zu den Ports 80 und 443 via TCP
      - mitmproxy bietet noch keinen Support für QUIC und HTTP/3 (bisher gibt es dazu lediglich eine Reverse-Proxy-Funktion, bei welchem Verkehr an einen einzelnen Server analysiert werden kann) [110]
      - Da das QUIC-Protokoll UDP verwendet, wird dessen Nutzung durch Blockierung der entsprechenden UDP-Ports unterbunden [111][112]
    - Konfiguration siehe Quelltext A.1 in Kapitel A.1.1 und Quelltext A.2 in Kapitel A.1.2, wobei die iptables-Rules wie folgt geladen werden können:
      ```
      iptables-restore < /etc/iptables/rules.v4
      ip6tables-restore < /etc/iptables/rules.v6
      ```
    - Konfiguration speichern mittels
      ```
      sudo iptables-save | sudo tee /etc/iptables/rules.v4
      sudo ip6tables-save | sudo tee /etc/iptables/rules.v6
      ```
  - SSH-Public-Key des Users auf dem VirtualBox-Host[30] für die Analysen-Automatisierung in Kapitel 4.5 unter `~/.ssh/authorized_keys` hinzufügen und dessen Berechtigungen mittels `chmod 600 ~/.ssh/authorized_keys` sicherstellen

[28] Die Bezeichnung entsprechender Netzwerk-Interfaces kann je nach vorhandener Hardware variieren [108]

[29] `curl` wird verwendet, um Dateien von Webservern zu laden und `iptables-persistent` dient zum permanenten Anlegen von Paketfilter- und NAT-Regeln. Mit `tcpdump` kann Netzwerkverkehr aufgezeichnet werden, wobei `tshark` dies auch kann, aber auch Tools zum Editieren von PCAP-Dateien mit sich bringt

[30] Meistens unter `~/.ssh/id_ed25519.pub` bei der Verwendung des Algorithmus Ed25519

Die Installation von mitmproxy als transparenter Proxy-Server erfolgt gemäss folgenden Befehlen [113]:

- mitmproxy herunterladen und installieren
  - `curl -O \`
    `https://downloads.mitmproxy.org/10.2.1/mitmproxy-10.2.1-linux-x86_64.tar.gz`
  - `tar -xf mitmproxy-10.2.1-linux-x86_64.tar.gz -C /usr/local/bin`
- IP-Forwarding aktivieren und ICMP Redirects deaktivieren durch ablegen des folgenden Inhaltes unter `/etc/sysctl.d/mitmproxy.conf`
  ```
  net.ipv4.ip_forward=1
  net.ipv6.conf.all.forwarding=1
  net.ipv4.conf.all.send_redirects=0
  ```
- Laden der neu hinterlegten Systemvariablen mittels `sysctl --system`
- Anpassen des iptables-Rulesets, um den HTTP- und HTTPS-Verkehr der Windows-Client-Subnetze über mitmproxy zu leiten
  Siehe Quelltext A.1 in Kapitel A.1.1 und Quelltext A.2 in Kapitel A.1.2, wobei die iptables-Rules wie folgt geladen werden können:
  ```
  iptables-restore < /etc/iptables/rules.v4
  ip6tables-restore < /etc/iptables/rules.v6
  ```
- Der HTTP-Verkehr auf TCP-Port 80 und HTTPS-Verkehr auf TCP-Port 443 wird nun auf den lokalen TCP-Port 8080 weitergeleitet, auf welchen mitmproxy hört
- mitmproxy ist nun mit Benutzerkonto `user` mittels folgendem Befehl zu starten [114]:
  ```
  SSLKEYLOGFILE="~/.mitmproxy/sslkeylogfile.txt" \
   mitmproxy --mode transparent --showhost
  ```
- Die Anwendung ist wieder zu beenden und das CA-Zertifikat dieser mitmproxy-Instanz unter `~/.mitmproxy/mitmproxy-ca-cert.pem` für den Einsatz auf den Clients zu exportieren [115]

Diese Arbeit verwendet mitmproxy in Form mit einer Web-basierten, grafischen Oberfläche mit dem Namen „mitmweb“. mitmproxy kann in folgenden 3 Ausführungen verwendet werden [54]:

- mitmproxy interaktive Oberfläche in der Kommandozeile/Konsole
- mitmweb interaktive Oberfläche, mittels Webbrowser aufrufbar
- mitmdump Kommandozeilen-Version ohne interaktive Oberfläche

4.2. Vermerk zu Online-Konten

Die Webbrowser werden ohne zugehörige Online-Konten verknüpft, da gemäss der Recherche in Kapitel 3.4 bei einer solchen Verknüpfung weitere Daten bearbeitet werden. Der Fokus dieser Arbeit liegt aus Übersichts- und Zeitgründen auf der Telemetrie der Browser ohne Online-Konto.

Beim Login einer oder Benutzerin oder eines Benutzers mit einem Online-Konto bei einem Browser liegt die Vermutung nahe, dass dieser Browser seine Daten über mehrere Geräte möglichst synchron behalten möchte und somit gewillt ist, zugehörige Informationen mit dem Hersteller zu teilen. Die in dieser Arbeit untersuchten Telemetrie stellt den Zustand einer Standard-Installation ohne Online-Kontoverknüpfungen dar. Bei dieser Konstellation könnte ein Anwender davon ausgehen, dass möglichst viele Informationen offline auf dem Gerät bleiben und nicht mit dem Hersteller geteilt werden.

4.3. Windows-Template

Windows 11 wird aufgrund der Gründe im vorherigen Kapitel 4.2 ohne einen Microsoft-Account installiert. Dies weil Microsoft Edge sich versucht mit dem Account des Betriebssystems zu verknüpfen[31] [38] und für jeden zu untersuchenden Browser die gleichen Voraussetzungen gegeben sein sollen.

Zur Analyse wird jeder Browser in einer eigenen VM betrieben, die sich zusätzlich in einem eigenen Subnetz befindet. Auf Betriebssystem-Ebene sind jedoch für jede VM dieselben Voraussetzungen sicherzustellen, weshalb eine VM als Vorlage („Template“) erstellt wird.

- VM-Ausstattung
  - Arbeitsspeicher: 4096 MB
  - Anzahl Prozessoren: 2 CPUs
  - Speicherplatz: 80 GB
  - Optisches Laufwerk: `Win11_23H2_EnglishInternational_x64v2.iso`
  - Skip Unattended Installation: Aktiv (Windows wird manuell installiert)
  - Netzwerkadapter: Angeschlossen an NAT-Netzwerk `natbrowser`[32]
  - Grafik-Einstellungen: Enable 3D Acceleration: Aktiviert
- Installation[33]
  - Bei der Sprachauswahl mit der Tastenkombination Shift+F10 die Kommandozeile starten und den Registry-Editor mit `regedit` öffnen[34] [116]
    - Unter `HKEY_LOCAL_MACHINE\SYSTEM\Setup` einen neuen Schlüssel mit Namen `LabConfig` anlegen
    - Unter `LabConfig` folgende 3 DWORD-Einträge anlegen:
      - `BypassTPMCheck` / `1`
      - `BypassSecureBootCheck` / `1`
      - `BypassRAMCheck` / `1`
    - Registry-Editor und Kommanozeilenfenster schliessen
  - Sprache: `English (United Kingdom)`
  - Regionalformat: `German (Switzerland)`
  - Tastatur-Layout: `Swiss German`
  - Product-Key wird keiner angegeben
  - Betriebssystem-Version: `Windows 11 Home`[35]
  - „Customized“ Installation nach `Drive 0`

[31] siehe am Ende des Kapitels 3.4.2
[32] wird beim Klonen dieser VM für die Browser-VMs angepasst
[33] Bei nicht erwähnten Einstellungen wurde jeweils die Standard-Option übernommen
[34] Diese Einstellungen sind nötig, um Windows 11 in einer VirtualBox-VM installieren zu können. Ansonsten würde die Installation aufgrund nicht erfüllter Anforderungen verweigert werden
[35] Die am weitesten verbreitete Windows-Edition [117]

- Initial-Konfiguration
  - Netzwerk-Verbindung trennen, VM neu starten und Initial-Konfiguration nochmals starten
  - Land: `Switzerland`
  - Tastatur-Layout: `Swiss German`
  - Mit der Tastenkombination Shift+F10 die Kommandozeile starten und folgenden Befehl eingeben, um das Setup ohne Internetverbindung fortzufahren [118]: `oobe\bypassnro` Daraufhin startet die VM neu und nach erneuter Auswahl von Land und Tastatur-Layout kann man nun die Optionen `I don't have internet` und `Continue with limited setup` auswählen
  - Benutzername: `user`
  - Sämtliche Fragen zur Standort-Nutzung und Diagnose-Daten werden mit `Yes` oder der ersten Option beantwortet, da diese Einfluss auf den Browser Edge haben können [38] und gemäss Praxiserfahrung bei vielen Endanwendern so hinterlegt sind
- Konfiguration
  - Netzwerkverbindung wieder aktivieren und Konfiguration der IPv4-Adresse des Netzwerk-Interfaces durchführen:

IPv4:	10.0.100.4
Subnetzmaske:	255.255.255.0
Default Gateway:	10.0.100.1
DNS Server:	10.0.100.1

  - Deaktivieren der Datei-Explorer-Option `Hide extensions for known file types`
  - Installation der VirtualBox Guest Additions durch Anfügen der ISO-Datei via `Devices` → `Insert Guest Additions CD image...` und Ausführen von `VBoxWindowsAdditions.exe` vom geladenen Image (Reboot wird nach der Installation ausgeführt) [119]
  - Wenn nötig Image mit Guest Additions von Windows auswerfen
  - OpenSSH-Server [120]
    - Installation des Services mittels Powershell als Administrator:

```
Get-WindowsCapability -Online | Where-Object Name -like 'OpenSSH.
    Server*' | Add-WindowsCapability -Online
```

Quelltext 4.1: Installation OpenSSH-Server unter Windows [120]

    - Neustart des Betriebssystems ausführen
    - SSH-Public-Key des Users auf dem VirtualBox-Host[36] für die Analysen-Automatisierung in Kapitel 4.5 hinzufügen [121]

```
Add-Content -Force -Path C:\ProgramData\ssh\
    administrators_authorized_keys -Value 'ssh-ed25519
    AAAAC3NzaC1lZDI1NTE5AAA...NCOoCSQ2xzxz2VzVry0w5y usr@debian';
    icacls.exe "C:\ProgramData\ssh\administrators_authorized_keys"
     /inheritance:r /grant "Administrators:F" /grant "SYSTEM:F"
```

Quelltext 4.2: Hinzufügen eines Ed25519-Public-Keys für Administratoren-Konten für OpenSSH-Server unter Windows [121]

[36] Meistens unter `~/.ssh/id_ed25519.pub` bei der Verwendung des Algorithmus Ed25519

- Service starten, automatisches Ausführen beim Systemstart konfigurieren und Firewall-Rule hinterlegen durch folgende Powershell-Befehle als Administrator:

```
# Start the sshd service
Start-Service sshd

# OPTIONAL but recommended:
Set-Service -Name sshd -StartupType 'Automatic'

# Confirm the Firewall rule is configured. It should be created automatically by setup. Run the following to verify
if (!(Get-NetFirewallRule -Name "OpenSSH-Server-In-TCP" -ErrorAction SilentlyContinue | Select-Object Name, Enabled)) {
        Write-Output "Firewall Rule 'OpenSSH-Server-In-TCP' does not exist, creating it..."
        New-NetFirewallRule -Name 'OpenSSH-Server-In-TCP' -DisplayName 'OpenSSH Server (sshd)' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22
} else {
        Write-Output "Firewall rule 'OpenSSH-Server-In-TCP' has been created and exists."
}
```

Quelltext 4.3: Konfiguration OpenSSH-Server unter Windows [120]

- Ordner `C:\tools` anlegen und folgende Software dort ablegen und entpacken[37]:
  - Autoruns [25]
    Zip-Datei extrahiert nach `C:\tools\Autoruns`, Anwendung direkt in diesem Ordner
  - Process Explorer [30]
    Zip-Datei extrahiert nach `C:\tools\ProcessExplorer`, Anwendung direkt in diesem Ordner
  - Process Hacker [31]
    Zip-Datei extrahiert nach `C:\tools\processhacker`, Anwendung in Unterordner `x64`
  - Process Monitor [32]
    Zip-Datei extrahiert nach `C:\tools\ProcessMonitor`, Anwendung direkt in diesem Ordner
  - Python [26]
    Python wird installiert durch Öffnen des Installers und wählen von `Customize installation` → `for all users...` → `Next` → `Install Python 3.12 for all users` → `Install` (restliche Optionen werden nicht angepasst)
  - Noriben [27]
    Zip-Datei extrahiert nach `C:\tools`, Anwendung in Unterordner `Noriben-2.0`
    Die EXE-Dateien von Process Monitor werden zusätzlich in diesen Unterordner neben `Noriben.py` kopiert
  - ProcDOT [29]
    Zip-Datei mit Password „procdot“ extrahiert nach `C:\tools\procdot`, Anwendung in Unterordner `win64`
  - Visual C++ Redistributable [28]
    Wird durch ausführen von `VC_redist.x86.exe` installiert
  - Graphviz [122]
    Zip-Datei extrahiert nach `C:\tools`, Anwendung in Unterordner `Graphviz\bin`

[37] Versionen und Quellen siehe Tabelle 2.1 in Kapitel 2.2

- Neues Benutzerkonto `browser` mit folgenden Powershell-Befehlen als Administrator anlegen und der Administratoren-Gruppe hinzufügen[38]:

```
New-LocalUser -Name 'browser'
Add-LocalGroupMember -Group 'Administrators' -Member 'browser'
```

Quelltext 4.4: Windows-Template: Neues Benutzerkonto inkl. Zuweisung zur Administratoren-Gruppe

- Das mitmproxy-CA-Zertifikat `mitmproxy-ca-cert.pem`, das in Kapitel 4.1 aus der Server-VM exportiert wurde, wird in diese VM nach `C:\tools\` importiert
  Z.B. vom VirtualBox-Host aus mittels folgendem Befehl:
  `scp -P 22223 mitmproxy-ca-cert.pem user@192.168.0.208:C:/tools/`
- Das Zertifikat wird als Administrator in der Kommandozeile mittels folgendem Befehl importiert[39] [115]: `certutil -addstore root C:\tools\mitmproxy-ca-cert.cer`
- Die Installationspakete der Webbrowser dieser Arbeit werden mittels Edge-Browser des Templates mittels Download-Button ohne Anpassungen nach `C:\Users\user\Downloads` heruntergeladen und nach `C:\tools` verschoben, aber nicht installiert[40]
  - Chrome von `https://www.google.com/chrome/` [2]
    - Dateiname: `ChromeSetup.exe`
    - Dateigrösse: 1.31 MB
    - SHA-256-Hash[41]: `A94BA6555A12C0D290D0A5D035966F6D 2B12D1861D20E82A084F278A75EB4317`
  - Edge ist im Windows-11-Betriebssystem bereits enthalten
  - Firefox von `https://www.mozilla.org/firefox/download/` [20]
    - Dateiname: `Firefox Installer.exe`
    - Dateigrösse: 341 KB
    - SHA-256-Hash[41]: `FEE78EF6EFC1B7CC6BD385C073DDC21E 3A5407340775C58BCFAC6A98749EC8E8`
  - Tor Browser von `https://torproject.org/download` [21]
    - Dateiname: `tor-browser-windows-x86_64-portable-13.0.8.exe`
    - Dateigrösse: 96.9 MB
    - SHA-256-Hash[41]: `6C28F95F6485C8DD771F9290B1ED0495 23F4C41D8FB1594AEEFC8A515388D30C`
- Windows Updates werden über die Windows-Einstellungen heruntergeladen und installiert, wobei wenn nötig ein Neustart ausgeführt und die Updates nochmals geprüft werden bis das System aktuell ist
- VM herunterfahren und Snapshot erstellen, z.B. mit Namen `template ready`
- Die Browser-VMs werden nun wie zu Beginn von Kapitel 4 erwähnt als Linked-Clones erstellt, mit ihrem Netzwerkadapter an das entsprechende interne Netzwerk angeschlossen und gemäss Abbildung 4.1 mit IPv4- und IPv6-Adressen konfiguriert[42]
  Diese Konfiguration verläuft auf der VM mit dem Benutzerkonto `user`, wobei zur Analyse das Benutzerkonto `browser` verwendet wird

[38] Hierbei handelt es sich um das zukünftig zu verwendende Test-Benutzerkonto. Dieses wird der Administratoren-Gruppe hinzugefügt, da gemäss Praxiserfahrung oft das einzige Benutzerkonto auf dem System Administrator-Rechte hat und zum Surfen verwendet wird. Zudem können so die Aufzeichnungs- und Analyse-Tools unter diesem Benutzerkonto ausgeführt werden

[39] Das Zertifikat befindet sich danach im Zertifikats-Store `Trusted Root Certification Authorities` des lokalen Computers

[40] Die Installationspaket-Grössen bewegen zur Annahme, dass nur beim Tor Browser die effektive Browser-Anwendung enthalten ist

[41] Ausgerechnet mittels Powershell-Befehl `Get-FileHash -Algorithm SHA256 DATEIPFAD`

[42] Die IP-Adresse des DNS-Servers und Standard-Gateways entspricht deren des zentralen Servers im selben lokalen Subnetz, die Einstellung `DNS over HTTPS` bleibt ausgeschaltet

4.4. Malcolm

Für die Installation von Malcolm wird ein ISO-Image gemäss der Herstellerdokumentation [123] auf dem VirtualBox-Host mit Debian Linux entsprechend nachfolgenden Befehlen generiert.

```
# install tools and vagrant plugins
sudo apt install git live-build vagrant
vagrant plugin install vagrant-sshfs vagrant-reload vagrant-vbguest

# install docker
curl -fsSL https://download.docker.com/linux/debian/gpg | sudo gpg --dearmor -o /etc/apt/keyrings/docker.gpg
sudo chmod a+r /etc/apt/keyrings/docker.gpg
echo \
"deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.gpg] https://download.docker.com/linux/debian \
$(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \
sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt update
sudo apt install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
```

Quelltext 4.5: Vorbereitung des Debian Linux Hosts zur Malcolm-ISO-Generierung [123][124][125]

```
# clone malcolm repository
git clone git@github.com:cisagov/Malcolm.git
cd Malcolm
# start building ISO
./malcolm-iso/build.sh
ls -lh malcolm-24.01.0.iso
```

Quelltext 4.6: Generierung des ISO-Images der Malcolm Software Suite unter Linux [123][124]

Die erstelle ISO-Datei `malcolm-24.01.0.iso` wird einer neuen VM mit Namen `malcolm.lab.internal` angehängt, die wie folgt installiert wird:

- VM-Ausstattung
  - Arbeitsspeicher: 8192 MB
  - Anzahl Prozessoren: 2 CPUs
  - Speicherplatz: 80 GB
  - Optisches Laufwerk: `malcolm-24.01.0.iso`
  - Skip Unattended Installation: Aktiv (Betriebssystem manuell installieren)
  - Netzwerkadapter: Angeschlossen an NAT-Netzwerk `natbrowser`
- Installation starten durch wählen von `Install Malcolm` → `Virtual Machine Single Partition Quick Install` im Bootloader [43] [123]
  - Netzwerk-Konfiguration:
    Name server: 10.0.100.1
    Disable IPv6: `No`
  - Hostname: `malcolm.lab.internal`
  - Benutzerkonto: `user`
  - SSH Password Authentication: `Yes`
  - VM startet neu und ein Einrichtungsassistent erscheint

[43] Bei nicht erwähnten Einstellungen wurde jeweils die Standard-Option übernommen

- Netzwerk-Konfiguration:
  Als `root` den Befehl `nmtui` ausführen und die Verbindungseinstellungen von `Wired connection 1` editieren:
  - IPv4 Configuration: Manual
  - Addresses: 10.0.100.3/24
  - Gateway: 10.0.100.1
  - DNS servers: 10.0.100.1
  - Einstellungen speichern und Verbindung deaktivieren und wieder aktivieren, um Konfiguration zu übernehmen
- Terminal öffnen und Authentication Setup ausführen:
  `cd ~/Malcolm && ./scripts/auth_setup`
  Administrator username: `malcolm`
  Rest mit Standardauswahl beantworten
- Docker Images herunterladen
  `cd ~/Malcolm && docker compose --profile malcolm pull`
- Configuration Setup ausführen:
  `cd ~/Malcolm && ./scripts/configure`
  Alle Fragen mit Standardauswahl beantworten, ausser `Restart Malcolm upon system or Docker daemon restart` mit `Yes` und dann `unless-stopped` [126]
- `Start Malcolm` Programm-Verknüpfung öffnen und warten, bis die Applikation gestartet ist und sich das automatisch geöffnete Log-Fenster schliesst [124]
- Firefox öffnen, nach `https://localhost` oder `https://VIRTUALBOX-HOST-IP:22443`[44] navigieren und mit dem Benutzerkonto `malcolm` einloggen

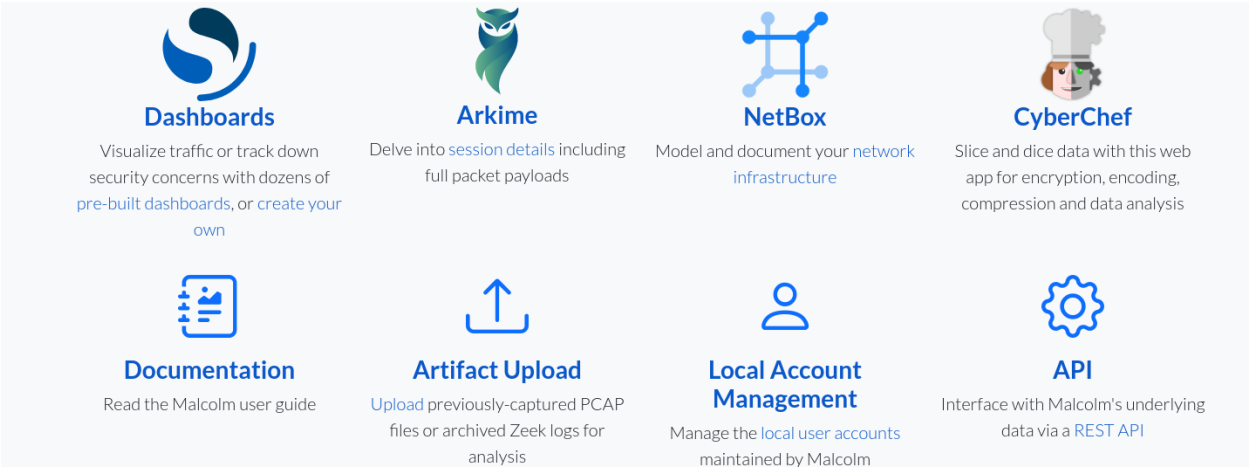


Abbildung 4.2.: Malcolm Weboberfläche nach Login

Nun können PCAP-Dateien mittels `Artifact Upload` hochgeladen und in den Dashboards sowie Arkime analysiert werden.

[44] gemäss Port Forwarding zu Beginn von Kapitel 4

4.5. Analysen-Automatisierung

In den vorherigen Kapiteln wurde auf dem zentralen Server sowie den Windows-Templates ein SSH-Serverdienst installiert und auf dem VirtualBox-Host Port Forwarding eingerichtet. Dies dient dazu, diese VMs vom VirtualBox-Host aus via SSH ansteuern zu können, um Messungen möglichst einfach und standardisiert starten und stoppen zu können.

Hierzu wurde ein Bash-Skript entwickelt, das mittels `start`-Parameter auf dem Server mitmproxy und in der Browser-VM Noriben mit entsprechenden Parametern zur Ablage der TLS-Schlüssel [114] startet. Der `stop`-Parameter kontrolliert und wartet bis Noriben auf der Browser-VM gestoppt ist (muss manuell getätigt werden[45]), stoppt mitmproxy auf dem Server und kopiert sämtliche Aufzeichnungen auf den VirtualBox-Host. Zusätzlich werden die bei mitmproxy entstandenen TLS-Schlüssel vor dem Kopiervorgang in die PCAP-Datei integriert.

Das Skript ist im Anhang als Quelltext B.1 in Kapitel B.1 einsehbar. Die Kommunikation via SSH verläuft mit dem Server, wobei dieser auch als Jumphost zur Kommunikation mit den Browser-VMs verwendet wird[46]. In den nachfolgenden Abschnitten wird dieses Skript unter anderem als „Lab-Control"-Skript bezeichnet. Während der Durchführung kann auf dem VirtualBox-Host unter dem Port der Port-Forwarding-Einstellung `server-http` zu Beginn von Kapitel 4 via Webbrowser die mitmweb-Oberfläche von mitmproxy geöffnet und der Verkehr live eingesehen werden. Das Skript legt auch eine Datei ab, die in mitmproxy eingelesen und z.B. via mitmweb-Option `-r DATEI` eingesehen werden kann [128].

```
$ ./src/lab_control.sh start chrome
########################################
LAB CONTROL
########################################
starting lab
acquiring lock at /var/lock/lab-chrome.lock
...
registered scheduled task lab-chrome-noriben
started mitmweb lab-chrome
started tshark lab-chrome
lab started, to stop execute: ./src/lab_control.sh stop chrome
$ ./src/lab_control.sh stop chrome
########################################
LAB CONTROL
########################################
stopping lab for lab-chrome
Scheduled Task lab-chrome-noriben running, please stop in browser host with Ctrl+C
checking again in 10s
waiting 60s for files to be generated
stopped mitmweb
stopped tshark
tshark:
injected tls secrets from keylogfile to new pcap
copied new mitm lab-chrome-20240128-1257.mitm to .../data/lab-chrome/20240128-1300
copied new pcap lab-chrome-20240128-1257.tlsdecrypted.pcap to .../data/lab-chrome
    /20240128-1300
lab lab-chrome stopped, check .../data/lab-chrome/20240128-1300
removing lock at /var/lock/lab-chrome.lock
$ ls data/lab-chrome/20240128-1300
lab-chrome-20240128-1257.mitm                Noriben_28_Jan_24__12_58_733454.csv
    Noriben_28_Jan_24__12_58_733454_timeline.csv
lab-chrome-20240128-1257.tlsdecrypted.pcap   Noriben_28_Jan_24__12_58_733454.pml
    Noriben_28_Jan_24__12_58_733454.txt
```

Quelltext 4.7: Beispiel-Ausführung des Skripts zur Analysen-Automatisierung (Quelltext B.1 in Kapitel B.1)

[45] Beim Ausführen und Beenden von Noriben bzw. Process Monitor muss ein „User Account Control"-Dialog bestätigt werden

[46] Mehr zu SSH, dessen Verwendung sowie Absicherung ist in der entsprechenden Semesterarbeit des Autors zu finden [127]

5. Analyse

Zur Analyse wird jeweils eine Browser-VM mit dem Aufbau gemäss Kapitel 4.3 verwendet. Für jeden Webbrowser wird eine eigene VM verwendet, die nach dem Namen des Browsers benannt ist. Die VM verfügt jeweils über die korrekte Netzwerkkonfiguration und befindet sich im ausgeschalteten Zustand (siehe Abbildung 4.1 in Kapitel 4). Dieser Stand wird in der VM mit einem Snapshot (z.B. mit dem Namen `prepared`) festgehalten, falls zukünftig eine entsprechende Wiederherstellung nötig ist. Sollte dies der Fall oder weitere Anpassungen vor einer Analyse nötig sein, wird dies entsprechend erwähnt.

Zu Beginn der Analyse wird jeweils die entsprechende VM gestartet und der Login mit dem Benutzerkonto `browser` durchgeführt[47]. Daraufhin wird das Lab-Control-Skript aus Kapitel 4.5 gestartet und die zugehörige Analyse durchgeführt (z.B. `./lab_control.sh start chrome`).

Nach Abschluss der Analyse-Schritte wird der Durchlauf gemäss Kapitel 4.5 beendet (z.B. mittels `./lab_control.sh stop chrome`), woraufhin diverse Dateien zur Analyse vorliegen:

- mitmproxy-Datei
  Zur Einsicht wird hierzu mitmweb auf dem Server wie folgt ausgeführt:
  `mitmweb --web-host 10.0.100.2 --web-port 8081 -r DATEI`
  Daraufhin ist die mitmweb-Oberfläche bzw. der aufgezeichnete Inhalt auf dem VirtualBox-Host mit Port Forwarding via Webbrowser unter Port 28081 via HTTPS einsehbar
- Noriben-Dateien
  Können in einer Windows-VM mit ProcDOT und Process Monitor analysiert werden
- PCAP mit entschlüsseltem TLS-Verkehr
  Wird mittels Wireshark/tshark ausgewertet und in die Malcolm-VM (siehe Kapitel 4.4) zur Analyse hochgeladen

Ein Analyse-Fall läuft demzufolge entsprechend folgenden Schritten ab:

1. Server- und Browser-VM starten (falls nicht bereits gestartet)
2. In Browser-VM mit Benutzerkonto `browser` einloggen
3. Aufzeichnung mittels Lab-Control-Bash-Skript mit Browser-Namen als Parameter von VirtualBox-Host aus starten
   a) Auf Server wird mitmproxy und tshark gestartet
   b) In Browser-VM wird Noriben gestartet
4. Fall in Browser-VM durchspielen
5. Noriben in Browser-VM manuell beenden
6. Aufzeichnung mittels Lab-Control-Bash-Skript mit Browser-Namen als Parameter von VirtualBox-Host aus stoppen
   a) Auf Server wird mitmproxy und tshark gestoppt
   b) Von mitmproxy zwischengespeicherte TLS-Schlüssel werden mit tshark-Aufzeichnung in eine neue PCAP-Datei mit entschlüsseltem TLS-Verkehr gespeichert
   c) Aufzeichnungen werden auf VirtualBox-Host kopiert[48]
7. Aufzeichnungen werden analysiert und Befunde dokumentiert

[47] Der Initial-Login des `browser`-Benutzerkontos nimmt einige Minuten in Anspruch, wobei die Fragen zu Standort-Nutzung, Diagnose-Daten, etc. gleich wie in Kapitel 4.3 bei Benutzerkonto `user` beantwortet werden (`Yes` oder erste Option)

[48] Das Lab-Control-Skript entfernt zur Übersicht und aus Speicherplatzgründen die Aufzeichnungen von den Hosts. Somit müssen die Aufzeichnungen zur Analyse wieder auf die entsprechende Maschine kopiert werden

Es wird grossen Wert darauf gelegt, dass mit den aufgeführten Tätigkeiten die festgestellten Ergebnisse reproduziert und zusätzlich zu betrachtende Aspekte mit demselben Analyse-Vorgehen gemessen werden können. Weicht ein Fall vom zuvor aufgelisteten Vorgehen ab, wird dies explizit erwähnt, ansonsten wird besagter Ablauf durchgeführt.

Um einen übersichtlicheren Vergleich zwischen den Webbrowsern zu ermöglichen, werden die Analyse-Ergebnisse entsprechend den betrachteten Anwendungsfällen gegliedert und in Kapitel 5.5 zusammengefasst. Zusätzlich wird dazu zum entsprechenden Browser dessen Logo aus Kapitel 3.4 aufgeführt[49].

Ausführlichere Analyse-Ausgaben sind im Anhang vorzufinden und entsprechend referenziert. Zusätzlich sind dieser Arbeit sämtliche Aufzeichnungen als Dateien beigelegt (siehe Kapitel C).

5.1. Abgrenzungen

Aufgrund der gegebenen Zeit zur Durchführung dieser Arbeit entstehen Abgrenzungen, an welchen für zukünftige Arbeiten weiter angesetzt werden könnte. Webbrowser wie Apple Safari [129] oder Brave [130] sowie Ausführungen bereits beinhalteter Browser unter anderen Betriebssystemen als Windows könnten betrachtet werden.

Des Weiteren werden **Verknüpfungen von Benutzerkonten mit den Browsern ausgeklammert**, da hierzu weitere Vereinbarungen zwischen Benutzerinnen und Benutzer mit dem Browser-Hersteller entstehen. Hinzu kommt, dass einem Anwender das Teilen von Daten mit dem Hersteller bei der Nutzung eines Benutzerkontos mehr oder weniger bewusst ist (Beispielsweise müssen zur Synchronisation von Lesezeichen diese zentral abgelegt werden, damit der Browser auf einem anderen Gerät diese einlesen kann).

Zur **Konfiguration der Browser** ist zu erwähnen, dass diese zur Analyse hier **nicht weiter angepasst** wird. Somit wird der Einfluss von Browser-Konfigurationen und der Einsatz von Erweiterungen nicht beachtet. Mit der Aktualisierung eines Webbrowsers könnte es vorkommen, dass neue Funktionalitäten eingeführt werden, die neue Standardeinstellungen zur Telemetrie beitragen. Dies würde bedeuten, dass ein Browser-Anwender mit Bedarf an möglichst geringer Telemetrie nach jedem Update die komplette Konfiguration kontrollieren müsste. Hinzu kommt, dass gemäss Praxiserfahrung nicht jede Funktionalität über eine grafische Oberfläche angepasst werden kann, sondern tieferes Wissen über den Browser bedingt.

Das **QUIC-Protokoll** wird aufgrund der fehlenden Unterstützung von mitmproxy [110] gemäss Kapitel 4.1 **nicht verwendet**.

Im Fokus liegen der Besuch von statischen Seiten sowie Webshops und der Nutzung des Privat-Modus des Browsers. Zusätzliche Funktionen oder Modi wie zum Beispiel „Copilot“ [72], der „Guest Mode“ oder der „Kids Mode“ von Edge [38] werden nicht betrachtet. Das **Konsumieren von Inhalten mit Kopierschutz-Mechanismen wird** aus Zeitgründen ebenfalls **weggelassen**, wobei diese zur Vermeidung deren Umgehung gemäss Erfahrung ihr Verhalten nicht offen legen.

Es besteht eine **Wahrscheinlichkeit, dass nicht sämtliche Kommunikationen identifiziert und ermittelt werden können**. Dies kann unter anderem aus Zeitgründen sein, hat aber auch mit der Menge an aufgezeichneten Daten zu tun. Eine zeitlich uneingeschränkte Analyse mit weiteren Teilnehmern und mehreren Durchläufen könnte zusätzliche Ergebnisse erzielen. Es kann somit nicht ausgeschlossen werden, dass gewisse Telemetrie übersehen wird.

Spezifische Aussagen zur Analyse des Tor Browsers sind Kapitel 5.3.2 zu entnehmen.

[49] Hierbei wird aus Übersichtsgründen auf eine Abbildungsbeschreibung verzichtet und auf die entsprechenden Bezeichnungen und Quellen auf die Abbildungen 3.2 (Chrome), 3.3 (Edge), 3.4 (Firefox) und 3.5 (Tor Browser) verwiesen

5.2. Windows-Kommunikation („Grundrauschen“)

Windows 11 betreibt ebenfalls Telemetrie [131]. Diese kann aus Zeitgründen nicht auf einem tiefen Level ermittelt werden, soll jedoch den Zusammenhang zwischen Prozessen und deren Kommunikation aufzeigen. Dieses Kapitel dient als Einführung, um zukünftig angewandte Analyse-Schritte besser nachvollziehen zu können. Eine tiefere Auseinandersetzung mit der Windows-Telemetrie sowie dessen automatisch ausgeführten Diensten wird in dieser Arbeit nicht durchgeführt.

Zur groben „Grundrauschen“-Analyse wird die Chrome-Browser-VM und eine Aufzeichnung mit dem Lab-Control-Skript gestartet, wobei keine Applikation installiert oder ein Webbrowser ausgeführt wird. Folgende Schritte werden vor dem Anhalten der Aufzeichnung getätigt:

1. Öffnen des Datei Explorers
2. Navigieren nach `C:\tools`
3. Ausführen von `Autoruns\Autoruns.exe`
4. Lizenzvereinbarung akzeptieren
5. Warten bis Anwendung die Autorun-Einträge gescannt hat (Status im Fenster links unten wechselt auf `Ready`)
6. Anwendung schliessen
7. Datei Explorer schliessen

Diese Analyse startet 15 Minuten nach dem Erstlogin mit dem Windows-Benutzerkonto `browser`. Während der Wartezeit vor dem Start wird der Desktop ohne weitere Interaktion angezeigt.

Folgende Prozesse mit TCP-Verbindungen sind aus dem Noriben-Bericht auszulesen:

```
$ grep -F "\"TCP" Noriben_03_Feb_24__17_12_955129.csv | sed 's,\",,g' | awk -F
    ',' '{if ($7 == "Length: 0") next; print $2" ("$3"):&    "$5}' | sort |
    uniq | sed 's,\&,\n,g'
msedge.exe (5004):
    192.168.100.2:50274 -> 13.107.21.239:443
OneDrive.exe (5732):
    192.168.100.2:50265 -> 192.229.221.185:443
OneDrive.exe (5732):
    192.168.100.2:50270 -> 52.113.194.132:443
svchost.exe (6576):
    192.168.100.2:50268 -> 68.219.88.225:443
svchost.exe (6576):
    192.168.100.2:50269 -> 23.212.193.84:443
svchost.exe (6576):
    192.168.100.2:50275 -> 2.21.22.184:80
```

Quelltext 5.1: Analyse Windows-Kommunikation („Grundrauschen“): Prozesse und TCP-Verbindungen aus Noriben CSV-Bericht

OneDrive lädt im Hintergrund Javascript- und CSS-Dateien sowie Konfigurationen im JSON-Format (siehe Quelltext D.1). Der Prozess mit der ID 6576 lädt ein OneDrive-Update sowie dessen Initialkonfiguration herunter (siehe Quelltext D.2). Microsoft Edge startet automatisch und sendet bereits regelmässig Informationen zu dessen Hersteller.

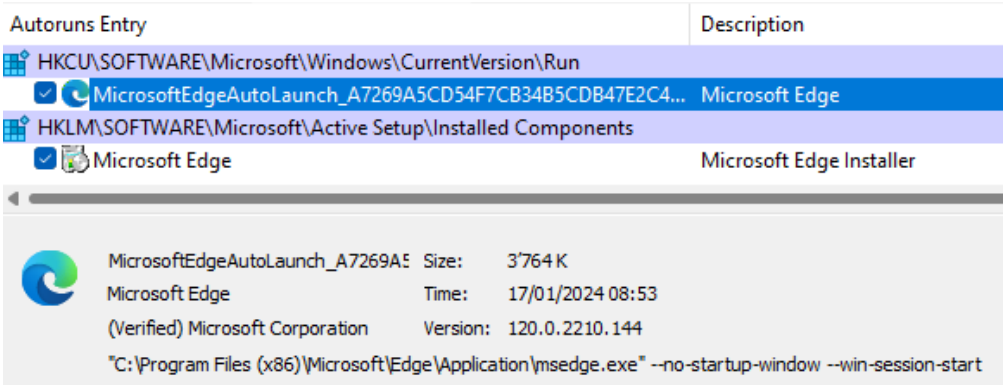


Abbildung 5.1.: Analyse Windows-Kommunikation („Grundrauschen"): Autorun-Eintrag zu Microsoft Edge

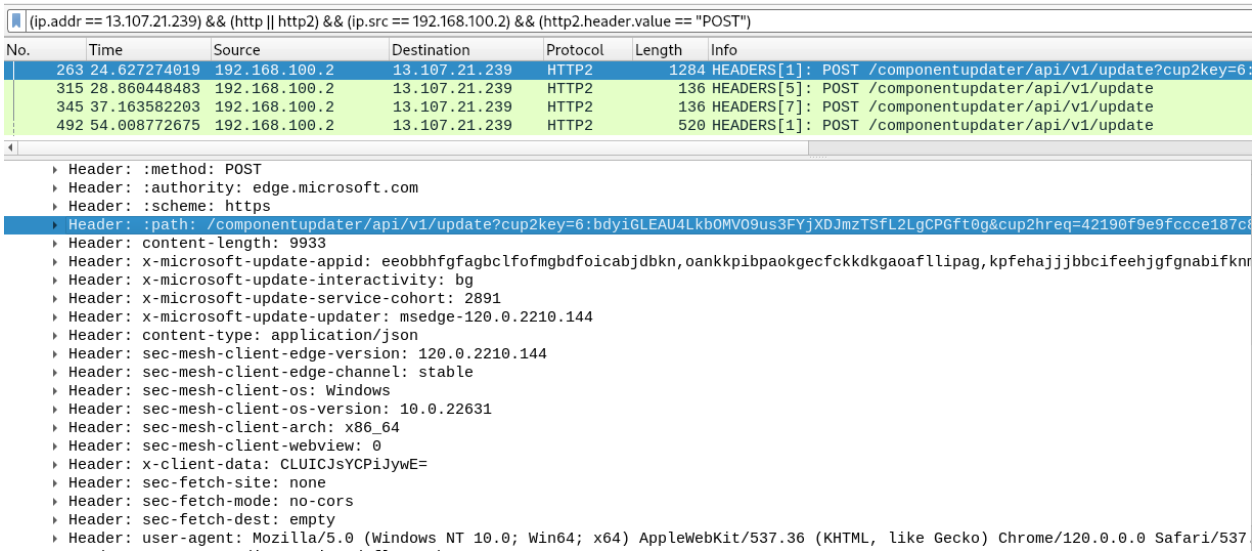


Abbildung 5.2.: Analyse Windows-Kommunikation („Grundrauschen"): Kommunikation von Microsoft Edge

Durch Kombination von Betriebssystem- und Netzwerk-Analyse kann ermittelt werden, welcher Prozess welche Netzwerkkommunikation erzeugt. Dies erlaubt ein nachvollziehbares Filtern der Netzwerk-Aufzeichnungen. Ein direkter Zusammenhang zwischen den ausgeführten Tätigkeiten und der ausgelesenen Kommunikation kann nicht hergestellt werden.

Die Noriben-Berichte enthalten von den Prozessen initiierte Netzwerkverbindungen inklusive Ziel-IP-Adresse und Port. Sofern diese Kombination nicht bei einem weiteren Eintrag mit anderer Prozess-ID vorkommt, ist die Kommunikation eindeutig einem Prozess zuweisbar. Entsprechend konstruierte Wireshark-Filter ermöglichen das Auslesen der Pakete inklusive Inhalt aus dessen entschlüsselter Netzwerk-Aufzeichnung.

Microsoft Edge kann durch dessen automatischen Start abhängig von dessen Verwendung als Windows-Grundrauschen betrachtet werden. Dieser Fall zeigt die Verschmelzung von Windows mit Edge auf. Dass eine Kommunikation von Windows zukünftig als Edge-Kommunikation interpretiert werden könnte, ist aus Zeitgründen nicht komplett auszuschliessen. Bei Analysen, die nicht Edge

betreffen, wird dessen Prozess bei der Kommunikation ausgeklammert.

Während weiterer Analysen sind weitere Prozesse aufgetaucht, die zum Windows-Betriebssystem oder dessen mitgelieferten Diensten gehören:

- `MsMpEng.exe`: Microsoft Defender Antivirus service [132]
  Pfad auf System: `C:\Program Files\Windows Defender\`
- `MpCmdRun.exe`: Microsoft Defender Antivirus command-line tool [133]
  Pfad auf System: `C:\Program Files\Windows Defender\`
- `mpam-fe_bd.exe`: Updates Microsoft Defender Antivirus & andere Microsoft antimalware [134]
  Pfad auf System: Hier gefunden unter `C:\Windows\SystemTemp` in einem generierten Unterverzeichnis
- `OneDrive.exe`, `OneDriveSetup.exe`: Microsoft Datei-Hosting-Dienst OneDrive
  Pfad auf System: `C:\Users\browser\AppData\Local\Microsoft\OneDrive\Update`
- `svchost.exe`: Generischer Service Host Prozess [135]
  Pfad auf System: `C:\Windows\System32\`
  Muss individuell betrachtet werden, da hierbei ein relevanter Prozess ausgeführt werden könnte. Dieser Prozess wird wenn möglich erst nach entsprechender Analyse ausgeklammert
- `SystemSettings.exe`: Windows Settings [136]
  Pfad auf System: `C:\Windows\ImmersiveControlPanel\`

5.3. Anwendungsfälle

5.3.1. Installation und erster Start

Die Installationsprogramme aus Kapitel 4.3 werden in der jeweiligen VM ausgeführt und die Browser mit Standardparameter installiert.

Während der Installation von Google Chrome werden die Optionen `Don't sign in` und `Set as default` gewählt. Somit wird kein Google-Konto mit dem Browser verknüpft und Chrome als Standard-Webbrowser hinterlegt.

Der Chrome-Installer lädt einen neuen Chrome-Installer herunter, der Chrome auf dem System installiert.

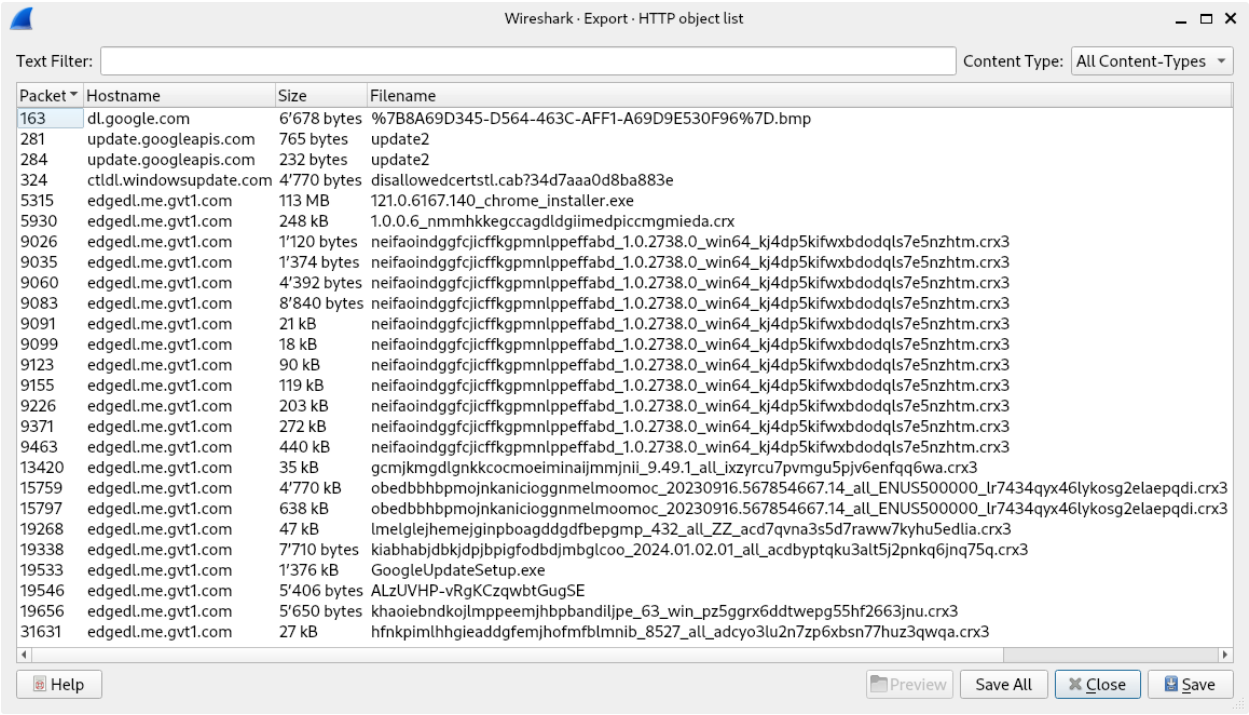


Abbildung 5.3.: Analyse Installation und erster Start: Mit HTTP aufgerufene Dateien

`GoogleUpdate.exe` führt sich mit dem Parameter `/ping` und einem mit Base64 encodierten Argument aus (siehe Quelltext D.3). Dieses Argument enthält u. a. den Wert `userid="6C7488BD-B56B-42D8-B2CB-5F6F6A3A9EAB"`. Minuten nach der Installation wird ein HTTP-GET-Request an `clients2.google.com` ausgelöst, der `userid=%7B6C7488BD-B56B-42D8-B2CB-5F6F6A3A9EAB%7D` enthält.

Chrome lädt Erweiterungen und verwendet dabei in dessen Kommunikation dieselbe Session-ID (siehe Quelltext D.5). Danach öffnet sich Chrome automatisch nach der Installation und zeigt das `New Tab`-Fenster an. Im Hintergrund prüft Chrome auf Updates und lädt für dessen SafeBrowsing-Feature dessen Liste mit Bedrohungen (siehe Ende von Quelltext D.6).

Ein HTTP-POST-Request an `https://clientservices.googleapis.com/uma/v2` (UMA steht für „User Metrics Analysis“ [137]) beinhaltet u. a. Chrome- und Windows-Version sowie ein Zeitstempel und eine UUID, dessen Verknüpfung derzeit unklar ist.

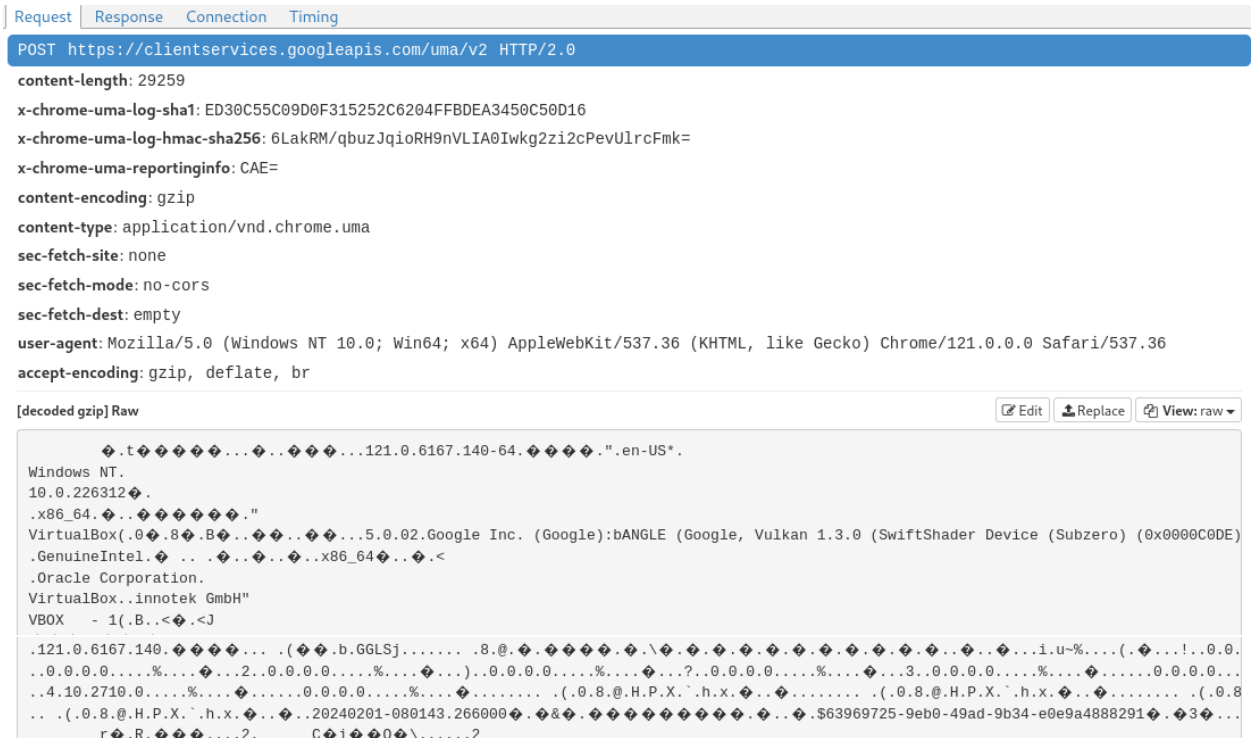


Abbildung 5.4.: Analyse Installation und erster Start: POST-Request an „User Metrics Analysis“-URI

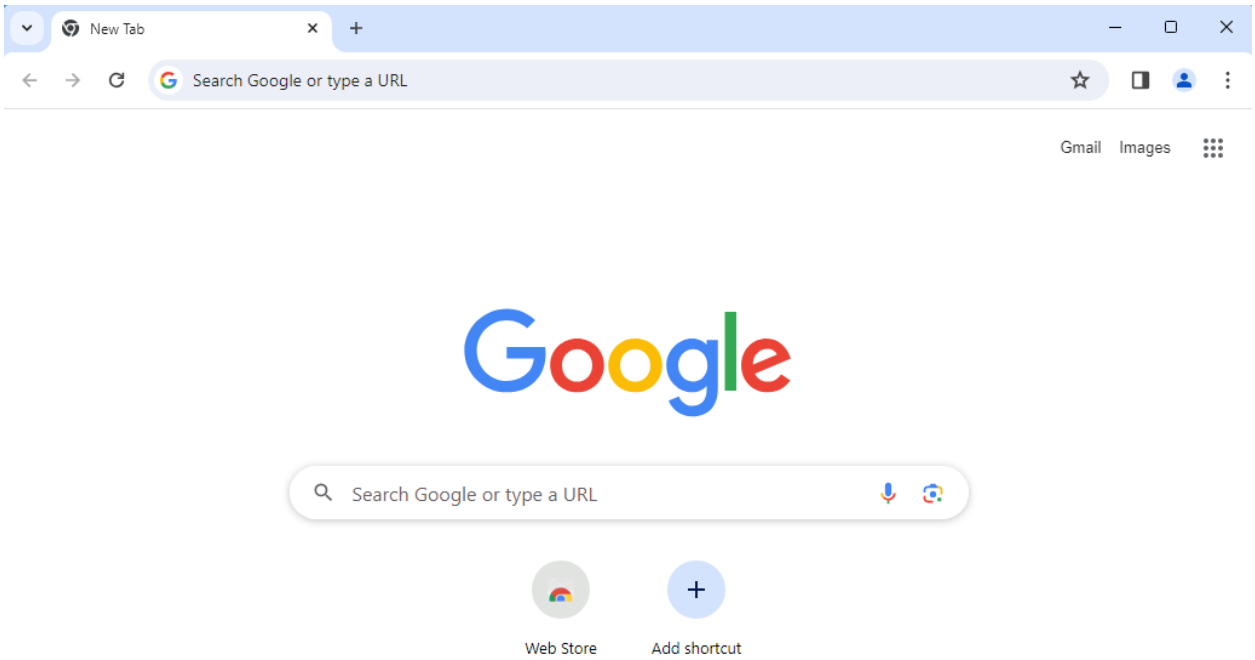


Abbildung 5.5.: Analyse Installation und erster Start: Chrome nach Initial-Start

Bei Microsoft Edge entfällt die Installation, da der Browser mit dem Windows-Betriebssystem in diesem Fall mitgeliefert wird.

Der erste Start von Edge in einem neuen Benutzerprofil beinhaltet das Durchlaufen von Fragen zur Einrichtung. Dabei wird `Start without your data` gewählt und die Fragen zum Browser-Daten-Import abgelehnt. Eine Frage, ob Microsoft die Aktivitätsdaten speichern darf, erscheint. Würde diese Aktivitätsspeicherung erlaubt werden, würden Daten aktiv geteilt werden. Zur Unterscheidung dieser Daten zwischen der Telemetrie anhand der restlichen Standardeinstellungen wird die Anfrage abgelehnt. Der Assistent zur Darstellungsanpassung wird mit `Next` und `Finish` durchlaufen.

Die „New Tab“-Seite mit einer Anfrage zu Cookies erscheint, welche ebenfalls nicht akzeptiert wird. Obwohl das Betriebssystem in englischer Sprachausgabe installiert ist, wird die „New Tab“-Seite in deutscher Sprachausgabe angezeigt.

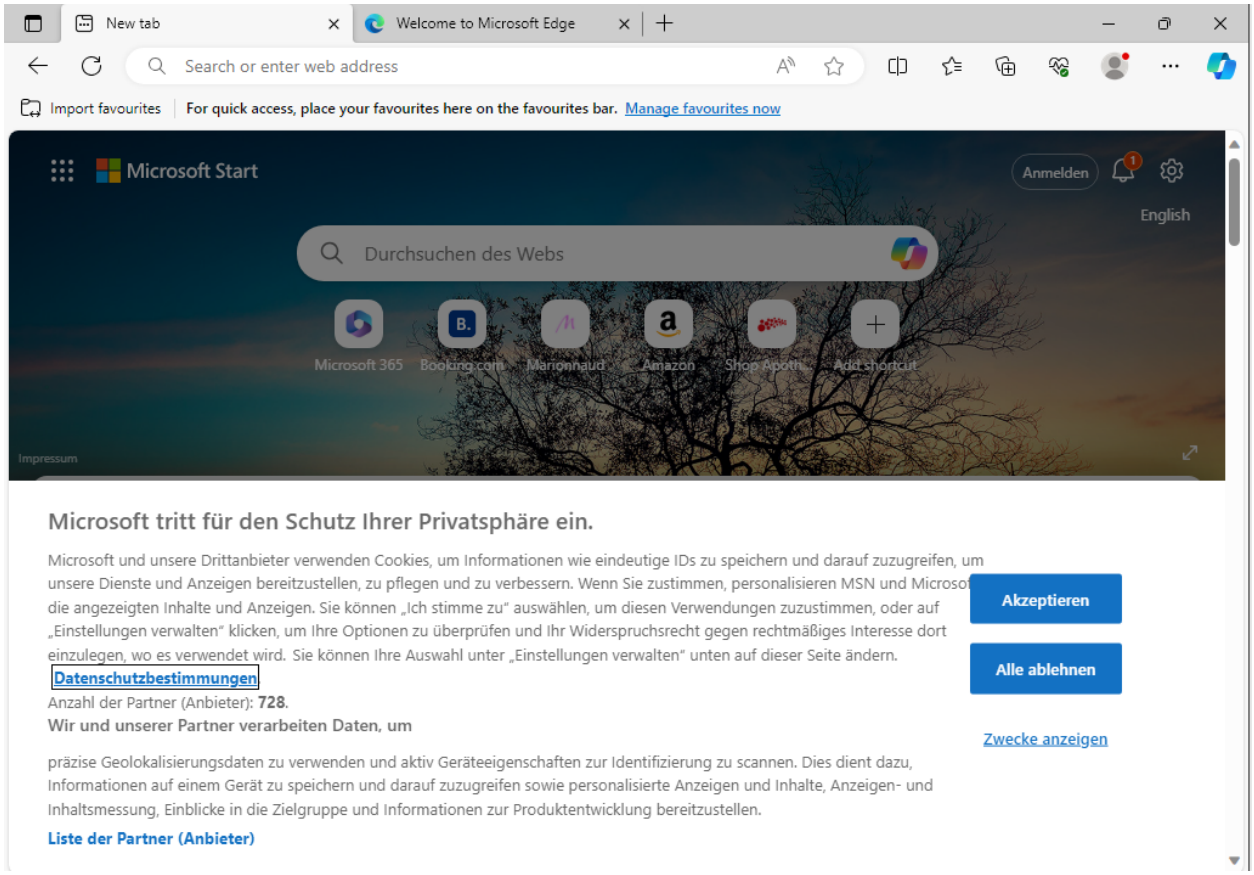


Abbildung 5.6.: Analyse Installation und erster Start: Edge nach Initial-Start

Während dem Initial-Start von Edge und dessen Ersteinrichtung werden unter anderem HTTP-Requests (siehe Quelltext D.9) mit folgenden URLs ausgeführt:

- `https://data-edge.smartscreen.microsoft.com/api/browser/edge/data/toptraffic/3`
  `https://data-edge.smartscreen.microsoft.com/api/browser/edge/data/settings/3`
- `https://edgeservices.bing.com/rp/5f8STjRzdjQ-8jgF3Ho7ptcTR94.br.js`
  Weitere Requests zum selben FQDN mit ähnlichen Anfragen sind ebenfalls vorzufinden
- `https://inference.location.live.net/inferenceservice/v21/pox/GetLocationUsingFingerprint`

- `https://browser.events.data.msn.com/OneCollector/1.0?cors=true&content-type=application/x-json-stream&client-id=NO_AUTH&client-version=1DS-Web-JS-3.2.8&apikey=0ded60c75e44443aa3484c42c1c43fe8-9fc57d3f-...-b927-75eafe60192e-7279&upload-time=1708248688667&w=0&anoncknm=app_anon&NoResponseBody=true`
  - Diese URL mit unterschiedlichem `upload_time`-Wert kommt in einem Grossteil der POST-Requests vor
  - Dabei sind Header wie `x-client-data` oder `x-edge-shopping-flag` ersichtlich
  - Cookies mit Benutzerdaten und Daten zur Verhaltensanalyse mit dem Tool `Clarity` [138] sind ebenfalls ersichtlich [139]
    `USRLOC=CLOC=LAT=47.4635|LON=8.3874|A=49239|TS=240218093052|SRC=I, MUID=196F9BEA1E01692C1C168FC31F5A68F5,_EDGE_S=F=1&SID=38B83CC1B2136D2731B628E8B3D36C7B,_EDGE_V=1, OptanonConsent=isGpcEnabled=0&datestamp=Sun+Feb+18+2024+10%3A30%3A49+...&version=202310.2.0&browserGpcFlag=0&isIABGlobal=false&hosts=&landingPath=https%3A%2F%2Fntp.msn.com%2Fedge%2Fntp%3Flocale...`
    Das `MUID`-Cookie wird dabei zur eindeutigen Identifizierung von Webbrowser für Microsoft-Seiten verwendet [139]
- `https://nw-umwatson.events.data.microsoft.com/Telemetry.Request`
  - Hier werden Informationen u. a. zum Betriebssystem und der Hardware mitgegeben (siehe Qualltext D.10)
  - Die ID `df037cfb-6deb-5b17-aa71-67af033ccb01`, die hier mit den Hardware-Daten mitgesendet wird, wird von der Anwendung `compattelrunner.exe` gesetzt (siehe Quelltext 5.2). Diese Anwendung gehört zum „Microsoft Customer Experience Improvement Program“ [140]. Der Ort, an dem die ID gesetzt wird, ist der Amcache, welcher Informationen zu ausgeführten Anwendungen und Dateien in Windows speichert [141]. „Plug and play“ (PnP) Geräte werden auch dort gepflegt [142]
  - Die Dokumentation von Microsoft nennt der hier verwendete FQDN unter `Windows Error Reporting` [131]
- `https://edge.microsoft.com/componentupdater/api/v1/update`
- `https://deff.nelreports.net/api/report`
  - Diese Adresse wird von Microsoft für das „Network Error Logging“ (NEL) verwendet [143]
  - Einer der zugehörigen POST-Requests beinhaltet u. a. URLs zu Microsoft-Diensten, YouTube oder Facebook, angereichert mit entsprechenden Auswertungen (siehe Quelltext D.11)

```
1 Noriben_18_Feb_24__10_30_984540.csv:"10:34:52.0191906","compattelrunner.exe","8856","
    RegSetValue","\REGISTRY\A\{0800e185-cc23-ba2d-a591-85bf7686c110}\Root\
    InventoryDevicePnp\{df037cfb-6deb-5b17-aa71-67af033ccb01}\(Default)","SUCCESS","
    Type: REG_DWORD, Length: 4, Data: 1","8012","C:\Windows\system32\compattelrunner.
    exe"
```

Quelltext 5.2: Analyse Installation und erster Start: Hardware-ID beim Edge Initial-Start

Die Anwendung für Updates von Edge verhält sich hierbei ähnlich zur Anwendung `GoogleUpdate.exe` von Chrome , bei welcher `MicrosoftEdgeUpdate.exe` ebenfalls mit einem `/ping` Parameter und Base64 encodierten Argument mit ähnlichem Inhalt ausgeführt wird (`userid`, etc.).

Die Installation von Mozilla Firefox erfolgt mittels Ausführen von `Firefox Installer.exe`, ohne weitere Anpassungen. Daraufhin startet Firefox mit Fragen zur Einrichtung und zum Browser-Daten-Import, die nicht akzeptiert und übersprungen werden. Nach dem Klick auf `Start Browsing` erscheint die „New Tab“-Seite von Firefox.

Die Firefox-Installationsanwendung lädt einen neuen Firefox Installer herunter, welcher den „Mozilla Maintenance Service“ und damit den Firefox Browser installiert (siehe Quelltext D.13). Während der Installation werden unter anderem folgende Dateien heruntergeladen:

- Effektives Firefox-Installationsprogramm von
  `https://download-installer.cdn.mozilla.net/pub/firefox/releases/122.0.1/win64/en-GB/Firefox%20Setup%20122.0.1.exe`
  Dateigrösse: 61 MB
- Video-Decodierungs-Prorgrammbibliothek `OpenH264` von
  `http://ciscobinary.openh264.org/openh264-win64-31c4d2e4a037526fd30d4e5c39f60885986cf865.zip`
  Dateigrösse: 491 KB
- Media-Kopierschutz-System `Widevine` [144]
  `https://r2---sn-1gieen7e.gvt1.com/edgedl/widevine-cdm/4.10.2710.0-win-x64.zip?cms_redirect=yes&mh=R8&mip=31.10.XXX.234&mm=28&mn=sn-1gieen7e&ms=nvh&mt=1708258344&mv=m&mvi=2&pl=18&shardbypass=sd`[50]
  Dateigrösse: 14 MB

Während der Installation und dem Initial-Start von Firefox sowie dessen Ersteinrichtung werden unter anderem HTTP-Requests mit folgenden URLs ausgeführt:

- `http://download-stats.mozilla.org/stub/v8/release/release/en-GB/1/1/10/0/22631/0/0/0/2/0/61161104/61161104/0/0/23/19/3/4/28/1/0/0/0/0/0/122.0.1/20240205133611/1/1/0/1/34.117.35.28/campaign%3D%2528not%2Bset%2529%26content%3D%2528not%2Bset%2529%26dlsource%3Dmozorg%26dltoken%3D57909725-d4cd-4e98-8918-ded4b042003f%26experiment%3D%2528not%2Bset%2529%26medium%3Dreferral%26source%3Dwww.bing.com%26ua%3Dedge%26variation%3D%2528not%2Bset%2529/0/0`
  Hier sind Download-Token, -Info und Kampagnen-Info aus u. a. Kapitel 3.4.3 ersichtlich.
- `https://incoming.telemetry.mozilla.org/submit/firefox-desktop/first-startup/1/0d8a62f2-ecb3-4227-a116-4fc848d3f0c6`
  Betriebssystem- und Hardware-Informationen werden auch hier an den Hersteller gesendet (siehe Quelltexte D.15 und D.16)

[50] Hier ist zusätzlich zu sehen, dass die öffentliche IPv4-Adresse als Parameter mitgegeben wird. Die Domain `gvt1.com` und `Widevine` gehören Google [144]

5.3.2. Tor Browser

Der Tor Browser wird mit der Installationsanwendung und Standardangaben in das Desktop-Verzeichnis des Benutzers installiert. Daraufhin erscheint der Tor Browser mit der Option zum Tor Netzwerk zu verbinden.

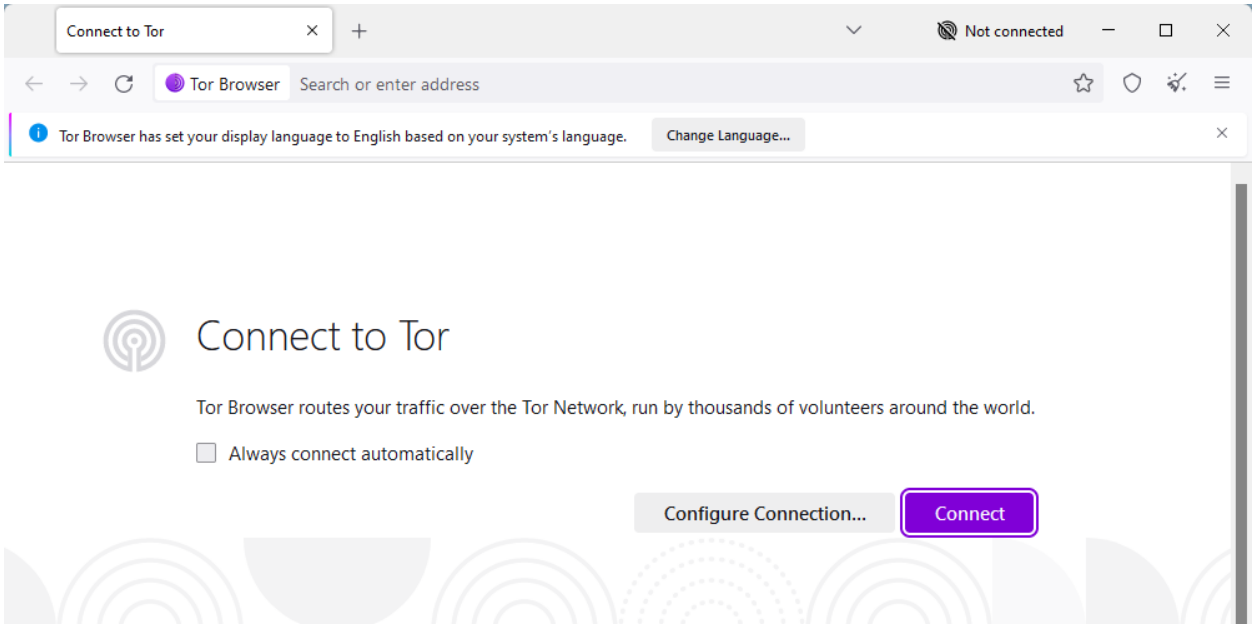


Abbildung 5.7.: Analyse Tor Browser: Tor Browser nach Initial-Start

Ausgelöste Netzwerkverbindungen konnten nur mit der Localhost-Adresse `127.0.0.1` festgestellt werden (siehe Quelltext D.20). Gemäss Quelltext D.19 hat die Installationsanwendung lediglich den Tor Browser in das Desktop-Verzeichnis platziert und gestartet. Die Anwendung des Browsers lautet `firefox.exe`, wobei `tor.exe` der Dienst zur Verbindung zum Tor Netzwerk darstellt.

Startet man eine Verbindung über den Browser zum Tor Netzwerk, versucht dieser Tor-Relays via TCP-Port 443 (HTTPS) zu erreichen. Zusätzlich werden POST-Requests an `https://moat.torproject.org.global.prod.fastly.net` gesendet. `moat` dient dazu, Bridges für Tor zu laden [145]. Eine Bridge ist hierbei wie ein übliches Tor-Relay mit folgendem Unterschied: Bridges sind nicht öffentlich gelistet und somit schwieriger als solche zu identifizieren.

Mit dem Testaufbau gemäss Kapitel 4 kann keine Verbindung zu Tor hergestellt werden. Je nach Relay wird ein Port verwendet, der nicht freigegeben ist [146][147]. Eine Teilmenge der Tor-Relays hört auf TCP-Port 443 [146][147], jedoch sind auch dorthin die Verbindungsversuche erfolglos[51].

Folgende Zeilen sind in der iptables-Konfiguration für IPv4 (siehe Quelltext A.1) in der FORWARD-Kette hinzuzufügen:

```
1 -A FORWARD -i enp0s3 -o enp0s16 -p tcp --sport 80 -j ACCEPT
2 -A FORWARD -i enp0s3 -o enp0s16 -p tcp --sport 443 -j ACCEPT
```

Quelltext 5.3: iptables-Ruleset-Zusatz für Tor (`/etc/iptables/rules.v4` auf `server.lab.internal`)

Die Zeilen mit `PREROUTING -i enp0s16` sind zu entfernen.

Nach Anwendung der neuen Konfiguration mittels
`sudo iptables-restore < /etc/iptables/rules.v4`
kann der Tor Browser eine Verbindung mit Tor nach einigen Versuchen herstellen.

[51] Dies führt zur Annahme, dass für Tor-Relay-Verbindungen ein Certificate Pinning durchgeführt werden könnte

Es werden nur die TCP-Ports 80 und 443 in dieser Umgebung zugelassen, wobei wie erwähnt nicht jeder Relay unter diesen Ports kommuniziert [146][147]. Daher benötigt der Client einige Verbindungsversuche bis er einen Relay oder eine Bridge mit passendem Port findet.

Es besteht zusätzlich die Vermutung, dass mitmproxy nicht mit der Tor-Kommunikation umgehen kann. Einträge sind im mitmproxy als TCP-Verbindung ohne HTTP-Interpretation ersichtlich. Aufgrund des Aufbaus von Tor wird der Paket-Inhalt verschlüsselt, sodass die Interpretation als HTTP ebenfalls nicht möglich ist [148]. Aus Zeitgründen wird auf die konkrete Erörterung des Problems bzw. eine Tor-Kommunikation über mitmproxy verzichtet.

Sobald eine Tor-Kommunikation aufgebaut ist, ist der Paketinhalt in diesem Laboraufbau nicht mehr einsehbar [149].

Bis auf die POST-Requests zu `https://moat.torproject.org.global.prod.fastly.net` konnte beim Tor Browser keine Telemetrie festgestellt werden. Dies auch bei zusätzlichen Tätigkeiten im Tor Browser wie dem Verwenden der Suchmaschine „DuckDuckGo“ oder dem Besuchen von Webseiten mit und ohne Tor (bzw. mit und ohne `.onion`-Adresse). **Daher wird der Tor Browser im Zusammenhang mit dessen Telemetrie im Rahmen dieser Arbeit nicht weiter betrachtet.**

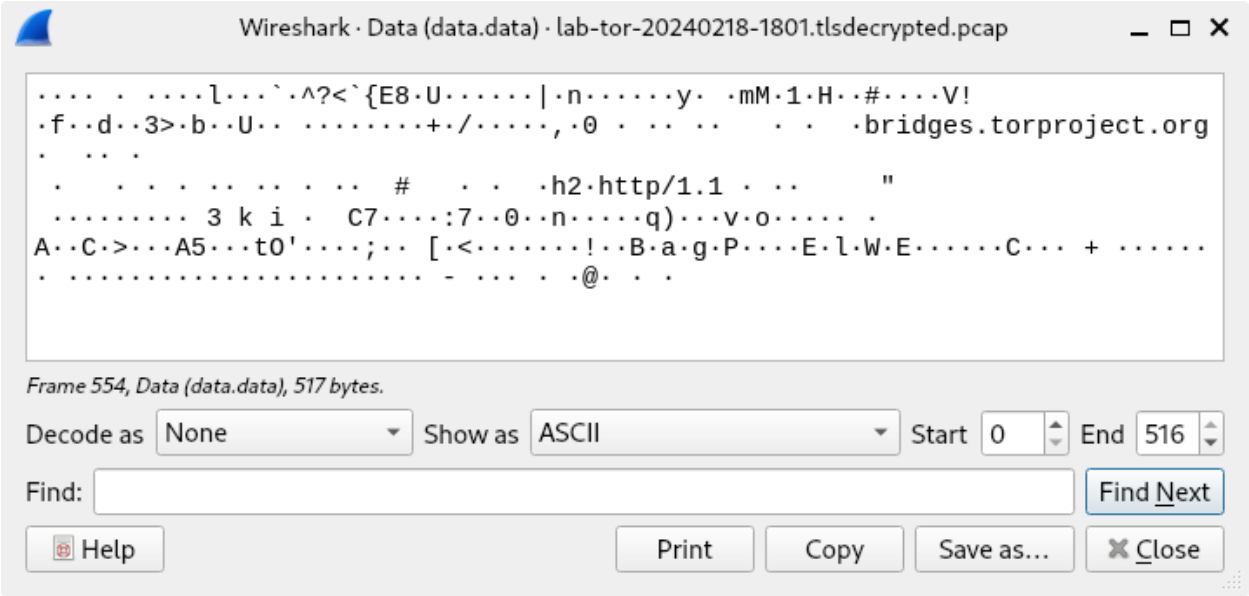


Abbildung 5.8.: Analyse Tor Browser: Inhalt HTTP-POST-Request von Tor Browser an `moat.torproject.org.global.prod.fastly.net`

5.3.3. Privat-Modus

Dieser Anwendungsfall betrachtet die Browser-Telemetrie beim Start des Privat-Modus, Besuch der Webseite `www.bfh.ch` und Schliessen des gesamten Browsers.

Das Tracking[52] der Webseite ist bei jedem Browser ersichtlich.

In Google Chrome wird mit geöffneter „New Tab“-Seite ein „Incognito“-Fenster mittels Tastenkombination `Ctrl+Shift+N` geöffnet. Hierbei wurde keine Telemetrie festgestellt. Für die „Safe Browsing“-Funktionalität aus Kapitel 3.4.1 wird die aktuelle Liste mit gefährlichen Seiten geladen (siehe Quelltexte D.7 und D.8).

Bei Edge wird mit derselben Tastenkombination ein „InPrivate“-Fenster geöffnet, `www.bfh.ch` besucht und der gesamte Browser geschlossen. Edge sendet dabei die Adresse der Webseite an dessen SmartScreen-Dienst[53].

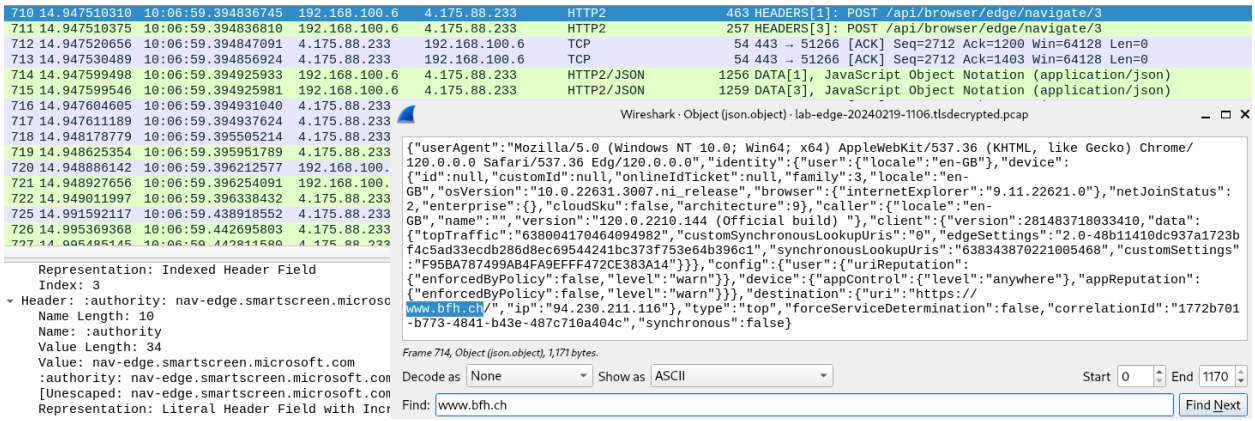


Abbildung 5.9.: Analyse Privat-Modus: Übermittlung der Webseitenadresse von Edge an `https://nav-edge.smartscreen.microsoft.com/api/browser/edge/navigate/3` im InPrivate-Modus

Für Firefox wird dessen „Private“-Fenster mittels `Ctrl+Shift+P` geöffnet. Daraufhin wird die Webseite `www.bfh.ch` besucht und der gesamte Browser geschlossen. Telemetrie konnte hier keine ermittelt werden.

[52] siehe Kapitel 3.1
[53] siehe Kapitel 3.4.2

5.3.4. Untersuchung auf Telemetrie-Trigger

Dieses Kapitel deckt neben dem Besuch von statischen Webseiten und Webshops sowie das Schliessen des Browsers auch das Untersuchen auf Telemetrie-Trigger ab. Folgende Tätigkeiten werden u. a. aufgrund der Herstellerdokumentation in Kapitel 3.4 in den Browsern unternommen:

1. Snapshot der Browser-VM erstellen
2. Analyse starten (siehe Kapitel 4.5)
3. Browser öffnen
4. BFH-Wikipedia-Eintrag suchen und öffnen
   a) Suchbegriff `Fachhochschule Bern` in der Adressleiste eingeben
   b) `Enter`-Taste drücken
   c) Auf Suchergebnis für den Wikipedia-Eintrag der BFH klicken
   `https://de.wikipedia.org/wiki/Berner_Fachhochschule`
   oder
   `https://en.wikipedia.org/wiki/Bern_University_of_Applied_Sciences`
5. Auf Amazon Bluetooth-Lautsprecher anschauen
   a) Suchbegriff `amazon` in der Adressleiste eingeben
   b) `Enter`-Taste drücken
   c) Auf Suchergebnis für `amazon.de` klicken
   d) In Suchleiste auf Amazon nach `bluetooth lautsprecher` suchen
   e) Artikel, der den ersten Treffer ist, anklicken
   f) Versuch, den Artikel zum Warenkorb hinzuzufügen und zur Kasse gehen → Login-Maske erscheint
   g) Text `Einkaufen!24` in die Adressleiste des Browsers eingeben und wieder mit der `Backspace`-Taste löschen
   Hiermit soll ein schwaches Passwort „aus Versehen“ in die Adressleiste eingegeben werden
   h) Mit persönlichem Amazon-Konto einloggen[54]
6. Flüge nach Kanada anschauen
   a) Suchbegriff `flug kanada` in der Adressleiste eingeben
   b) Treffer für „Air Canada“ anklicken
   c) Hin- und Rückflug von Zürich ZRH nach Toronto YYZ mit Abflugdatum in einer Woche und Rückflugdatum in 2 Wochen suchen
   d) Economy-Ticket in der billigsten Variante von erstem Treffer auswählen bis die Reiseüberprüfung angezeigt wird
7. Malware-Triggerseite aufrufen
   a) Adresse `http://malware.testing.google.test/testing/malware/*` in die Adressleiste kopieren [150]
   b) `Enter`-Taste drücken
   c) Malware-Warnung des Browsers wird angezeigt
8. Fenster schliessen
9. Analyse stoppen (siehe Kapitel 4.5)
10. Browser-VM auf Snapshot zurückspielen
11. Dasselbe nochmals mit dem Privat-Modus des Browsers durchspielen

[54] Das Konto-Passwort wird am Ende der Arbeit neu angepasst, womit in den Aufzeichnungen gegebenenfalls ein unbrauchbares Passwort vorzufinden ist

Cookie-Anfragen der Webseiten, die optisch fast die ganze Webseite überdecken, werden abgelehnt (Amazon und Google). Restliche Cookie-Anfragen werden ignoriert und weder akzeptiert noch abgelehnt. Edge zeigt Coupons bei Amazon an und findet die versuchte Malware-Seite mittels DNS nicht. Unter Firefox konnte Air Canada die Anfrage nicht verarbeiten (siehe Abbildung 5.11).

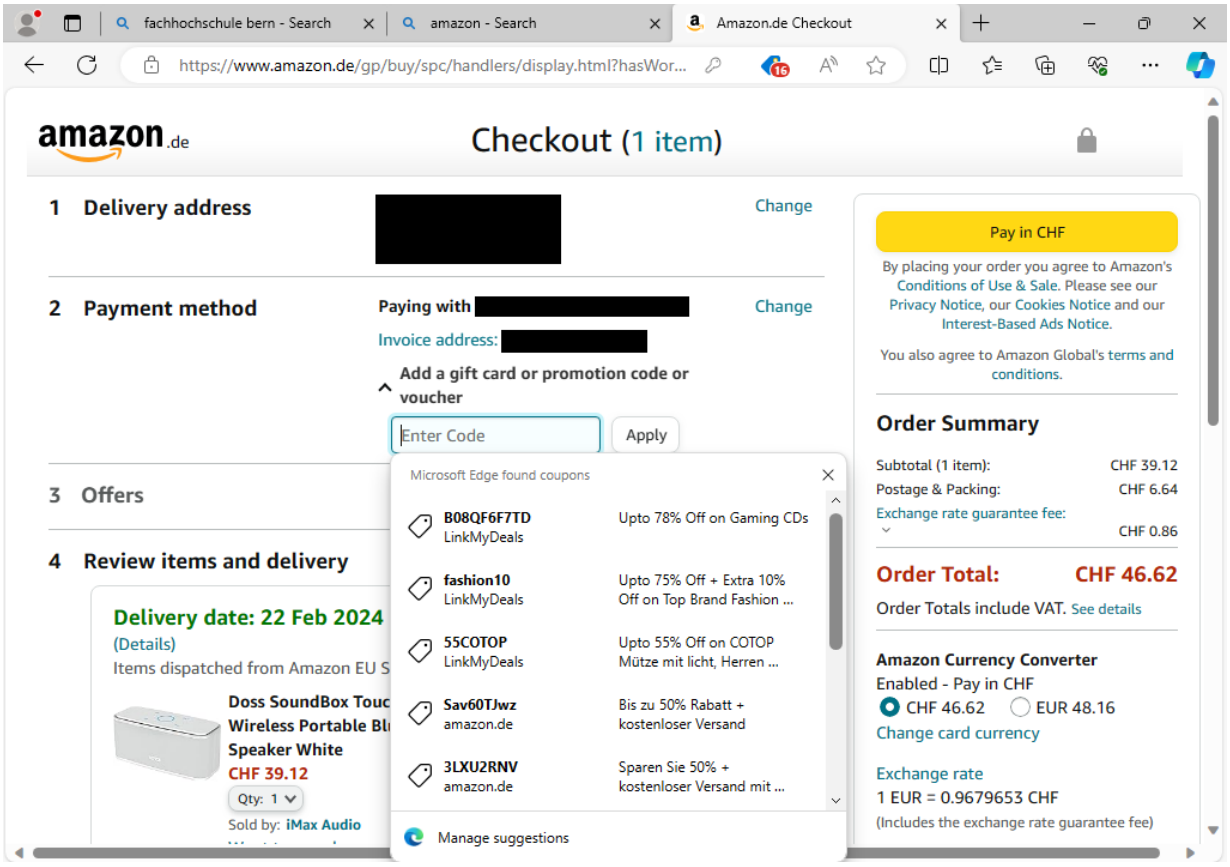


Abbildung 5.10.: Analyse Untersuchung auf Telemetrie-Trigger: Anzeige von Coupons mit Edge auf Amazon

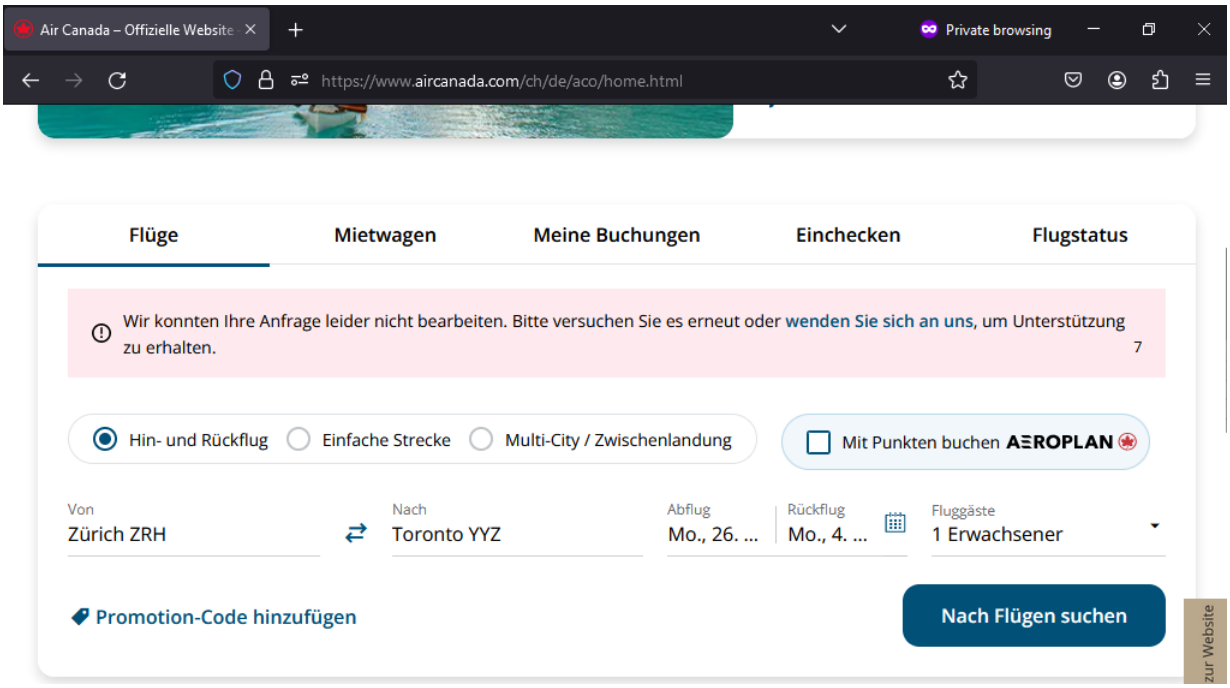


Abbildung 5.11.: Analyse Untersuchung auf Telemetrie-Trigger: Air Canada Fehler mit Firefox

Nicht abgesetzte Suchanfragen werden bei Chrome , Edge und Firefox gesendet, jedoch nicht im privaten Modus.

```
$ tshark -r lab-chrome-20240219-1449.tlsdecrypted.pcap -Y "($(grep -F TCP
    Noriben_19_Feb_24__14_49_538916.csv | grep -F chrome.exe | awk -F',' '{print $5}' |
     sort | uniq | sed 's,.*->\ \([^"]*\):443",ip.dst\ ==\ \1\ ||\ ,g' | sed 's,ip\.dst
    \ ==\ \([^:]*:\),ipv6.dst\ ==\ \1,g' | sed -z 's,\n,,g' | sed 's,\ ||\ $,,g') && (
    http || http2))" -T fields -e ipv6.src -e ipv6.dst -e ip.src -e ip.dst -e http.
    request.full_uri -e http2.request.full_uri -e frame.len  | awk '{if ($4 == "") next
     ;print $1" "$2" "$4" bytes "$3}' | grep "Einkaufen\!24"
192.168.100.2 216.58.215.228 236 bytes https://www.google.com/complete/search?client=
    chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=Einkaufen!24&oit=4&cp=12&pgcl=4&gs_rn
    =42&psi=3NI3jaoMsOKd21VW&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw

$ tshark -r lab-edge-20240219-1504.tlsdecrypted.pcap -Y "($(grep -F TCP
    Noriben_19_Feb_24__15_04_289858.csv | grep -E "(msedge\.exe|msedgewebview2\.exe)" |
     awk -F',' '{print $5}' | sort | uniq | sed 's,.*->\ \([^"]*\):443",ip.dst\ ==\ \1\
     ||\ ,g' | sed 's,ip\.dst\ ==\ \([^:]*:\),ipv6.dst\ ==\ \1,g' | sed -z 's,\n,,g' |
    sed 's,\ ||\ $,,g') && (http || http2))" -T fields -e ipv6.src -e ipv6.dst -e ip.
    src -e ip.dst -e http.request.full_uri -e http2.request.full_uri -e frame.len  |
    awk '{if ($4 == "") next ;print $1" "$2" "$4" bytes "$3}' | grep "Einkaufen\!24"
192.168.100.6 23.0.174.90 212 bytes https://www.bing.com/qbox?query=Einkaufen!24&
    language=en-GB&pt=EdgBox&cvid=1b63489aa23d4c869ef2e7203e1ea9a3&oit=4&cp=12&pgcl=4&
    richanswersentity=1

$ tshark -r lab-firefox-20240219-1535.tlsdecrypted.pcap  -Y "($(grep -F TCP
    Noriben_19_Feb_24__15_35_760334.csv | grep -F firefox.exe | awk -F',' '{print $5}'
    | sort | uniq | sed 's,.*->\ \([^"]*\):443",ip.dst\ ==\ \1\ ||\ ,g' | sed 's,.*->\
    \([^"]*\):80",ip.dst\ ==\ \1\ ||\ ,g' | grep -Fv "127.0.0.1" | sed 's,ip\.dst\ ==\
    \([^:]*:\),ipv6.dst\ ==\ \1,g' | sed -z 's,\n,,g' | sed 's,\ ||\ $,,g') && (http ||
     http2))" -T fields -e ipv6.src -e ipv6.dst -e ip.src -e ip.dst -e http.request.
    full_uri -e http2.request.full_uri -e frame.len  | awk '{if ($4 == "") next ;print
    $1" "$2" "$4" bytes "$3}' | grep "Einkaufen"
192.168.100.10 216.58.215.228 153 bytes https://www.google.com/complete/search?client=
    firefox&q=Einkaufen&channel=fen
192.168.100.10 216.58.215.228 155 bytes https://www.google.com/complete/search?client=
    firefox&q=Einkaufen%21&channel=fen
192.168.100.10 216.58.215.228 156 bytes https://www.google.com/complete/search?client=
    firefox&q=Einkaufen%212&channel=fen
192.168.100.10 216.58.215.228 157 bytes https://www.google.com/complete/search?client=
    firefox&q=Einkaufen%2124&channel=fen
192.168.100.10 216.58.215.228 157 bytes https://www.google.com/complete/search?client=
    firefox&q=Einkaufen%2124&channel=fen
```

Quelltext 5.4: Analyse Untersuchung auf Telemetrie-Trigger: Suchanfrage von Chrome, Edge und Firefox bei Eingabe ins Adressfeld ohne aktives Absenden

Während der Eingabe des Suchbegriffs im Adressfeld wird dieses bereits abgesendet, zur frühzeitigen Generierung der Suchvorschläge (Chrome und Firefox mit Google, Edge mit Bing). Im Privaten Modus wird jeweils erst die Anfrage an die Suchmaschinen gesendet sobald der Suchbegriff abgesendet wird.

Bei Edge wird beobachtet wie die Domain `amazon.de` an `https://www.bing.com/api/shopping/v1/telemetry` gesendet wird. Daten zur Webseite von Air Canada werden ebenfalls übermittelt. Dieselben Verhalten sind bei Edge im InPrivate-Fenster ebenfalls zu sehen.

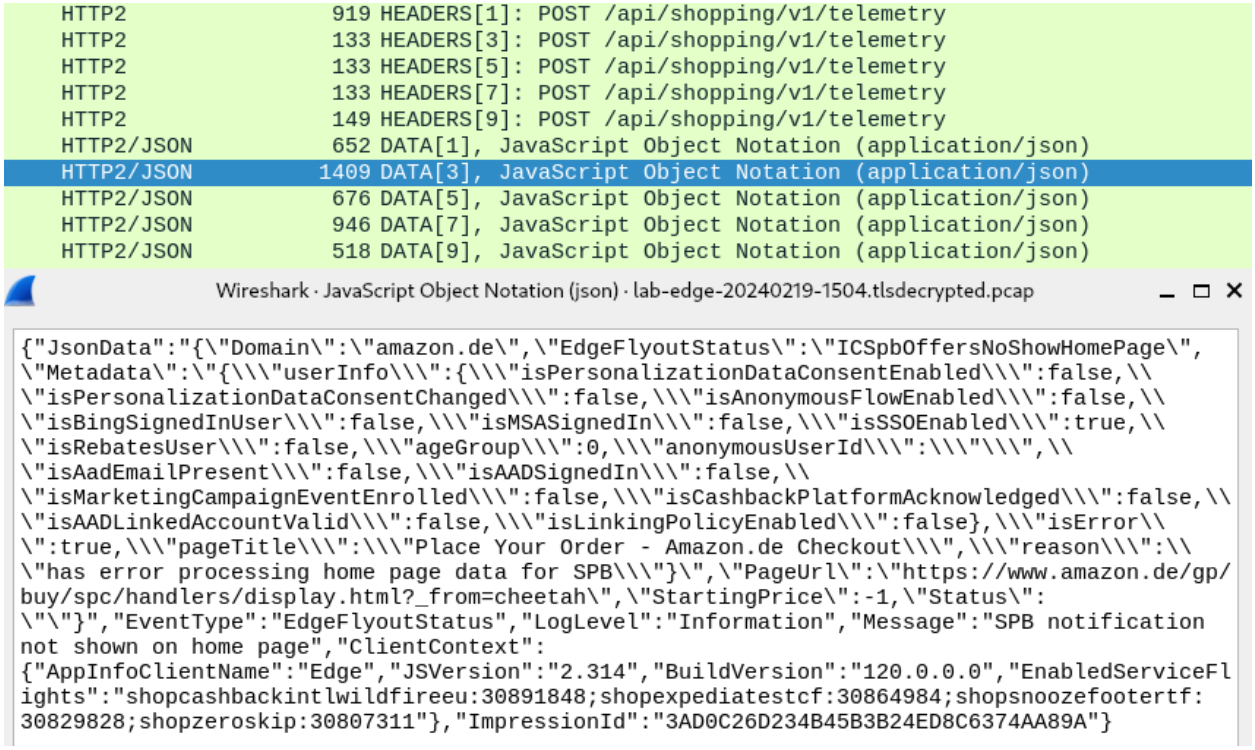


Abbildung 5.12.: Analyse Untersuchung auf Telemetrie-Trigger: Bing-Shopping-Telemetrie von Edge

Bei Firefox konnte Telemetrie beim Schliessen des Browsers festgestellt werden.

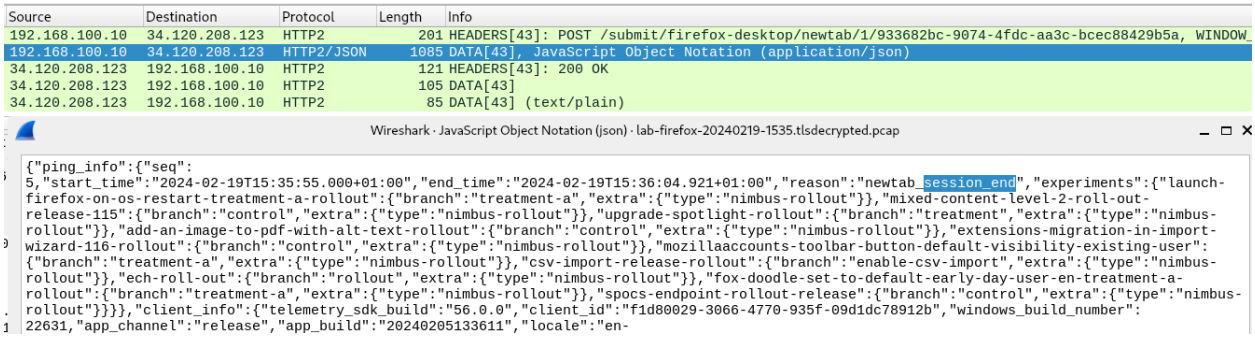


Abbildung 5.13.: Analyse Untersuchung auf Telemetrie-Trigger: Telemetrie von Firefox beim Schliessen des Browsers

5.3.5. Besuch Statische Webseite

Dieser Anwendungsfall behandelt das Besuchen einer statischen Webseite mit den Browsern Chrome , Edge und Firefox jeweils im „normalen“ und im privaten Modus. Als statische Webseite wird `info.cern.ch` [151] gewählt. Grund dafür ist der überschaubare Quellcode der Webseite (siehe Quelltext 5.5), bei welchem Tracking ausgeschlossen werden kann. Bei den Webseiten des vorherigen Kapitels ist Tracking nicht komplett auszuschliessen.

```
<html><head></head><body><header>
<title>http://info.cern.ch</title>
</header>

<h1>http://info.cern.ch - home of the first website</h1>
<p>From here you can:</p>
<ul>
<li><a href="http://info.cern.ch/hypertext/WWW/TheProject.html">Browse the first
    website</a></li>
<li><a href="http://line-mode.cern.ch/www/hypertext/WWW/TheProject.html">Browse the
    first website using the line-mode browser simulator</a></li>
<li><a href="http://home.web.cern.ch/topics/birth-web">Learn about the birth of the
    web</a></li>
<li><a href="http://home.web.cern.ch/about">Learn about CERN, the physics laboratory
    where the web was born</a></li>
</ul>
</body></html>
```

Quelltext 5.5: Analyse Besuch Statische Webseite: Quellcode der Webseite info.cern.ch [151]

Das Verhalten äussert sich wie zu dem aus vorherigem Kapitel: Bei der Eingabe der Adresse im Webbrowser (mit und ohne `http://`-Präfix), wird die Eingabe der Suchmaschine übergeben. Im Privat-Modus des jeweiligen Browsers wird keine Suchanfrage gestellt, da die Webseite direkt aufgerufen wird.

5.3.6. Besuch Webshop

Der Besuch eines Webshops wird in Kapitel 5.3.4 behandelt.

5.3.7. Schliessen Browser

Das Schliessen des Browsers wird am Ende von Kapitel 5.3.4 betrachtet.

5.4. Extrahierung von GUIDs

Das Auswertungs-Skript (siehe Kapitel B.2) extrahiert aus den Aufzeichnungen anhand regulären Ausdrücken (englisch „regular expression“ oder „RegEx“) mögliche GUIDs mit allfälligen Bezeichnungen. Dazu werden IP-Adressen aus den Noriben-Aufzeichnungen, die durch die Browser-Prozesse entstanden sind, als Filter auf die PCAP-Dateien angewendet und entsprechende Inhalte von HTTP-Paketen entnommen. Diese Werte werden in folgenden Fassungen auf GUIDs überprüft:

- Roh-Fassung, wie sie im PCAP vorhanden sind
- Mittels Befehl `strings`, welches nur darstellbare Zeichen ausgibt, jeweils mit Standard- und 16-Bit-Little-Endian-Codierung (`strings -el`) [152]
- Dekomprimiert mittels `gzip` und wieder mit `strings` und beiden Codierungen

Daraus extrahierte GUIDs werden pro Browser gezählt und jeweils die häufigsten Einträge betrachtet. Die Ergebnisse sind in Quelltext D.22 und D.23 einzusehen. Folgend wird auf die IDs mit Parameter eingegangen, wobei lediglich die ID-Werte mit den häufigsten Vorkommnissen betrachtet werden:

- `_abck`, `_uetsid`, `_uetvid`, `_cls_s`, `_cls_v`, `ak_bmsc`, `bm_sv`, `bm_sz`, `gbCookie`, `MCMID`, `x=session`[55]: Werden in jedem Browser ausschliesslich bei der Webseite `aircanada.com` aus Kapitel 5.3.4 verwendet. Diese Parameter werden aus der Zählung ausgefiltert, was zur Auflistung der Angaben in Quelltext D.23 führt
  - Die überbleibenden Werte in Quelltext D.23 sind besonders bei Chrome und Firefox ohne Parameter-Bezeichnung und könnten Werte sein, die keine GUIDs repräsentieren
- Edge
  - `GUID` wird beim Kontaktieren der Domain `bing.com` und dessen Subdomains wie `edgeservices.bing.com` und `th.bing.com` verwendet
    - `GUID=3D9C6AE06E2842B59D414EDA507D52AB` erscheint in jeder PCAP-Aufzeichnung, ausser bei der Analyse des Browsers im Privat-Modus (siehe Quelltext D.24)
    - Der `GUID`-Parameter taucht in Kapitel 5.3.1 in derselben Anfrage mit dem `MUID`-Parameter auf. Eine Beschreibung des Parameters ist in der gegebenen Zeit nicht auffindbar
  - `MUID` wird ähnlich wie `GUID` verwendet, neben denselben Subdomänen für `bing.com` werden mit diesem Parameter zusätzlich `c.bing.com`, `c.clarity.ms`, `c.msn.com`, `www.clarity.ms` und `www.msn.com` kontaktiert (siehe Quelltext D.25)
    - Der Parameter erscheint in jeder Aufzeichnung von Edge , auch in einer mit Privat Modus. In der Aufzeichnung zum Besuch einer statischen Webseite im Privat Modus erscheint der `MUID`-Wert nicht[56]
    - Derselbe Wert für ein `MUID`-Parameter wurde auch für ein `MUIDB`-Parameter beobachtet (siehe Quelltexte 5.6 und D.22)
    - Der `MUID`-Parameter wird, wie bereits in Kapitel 5.3.1 erwähnt, zur eindeutigen Identifizierung von Webbrowser für Microsoft-Seiten verwendet [139]

[55] Der komplette Parametername vor der GUID lautet `mbox=session#`

[56] In einer anderen Aufzeichnung mit Privat Modus erschien der `MUID`-Wert. Dass in der entsprechenden Aufzeichnung kein solcher Wert gefunden wurde kann mit der verhältnismässig kleinen Grösse der Aufzeichnung zusammenhängen (siehe Quelltext D.21)

- SID taucht mit unterschiedlichen Werten in jeweils einer einzelnen Aufzeichnung auf und wird ebenfalls bei der Kontaktaufnahme zu bing.com verwendet
  - ⋆ Der SID-Parameter taucht ebenfalls in Kapitel 5.3.1 in derselben Anfrage mit dem MUID-Parameter auf. Eine Beschreibung des Parameters ist in der gegebenen Zeit nicht auffindbar

```
1 20240228-0942-stat-tshark-http.txt:1211 281 192.168.100.6
    23.0.174.89 https://edgeservices.bing.
    com/rp/wua3_gB3vbVTArfn8C89Tc4iifk.br.js GET GET,edgeservices.bing.com,
    https,/rp/wua3_gB3vbVTArfn8C89Tc4iifk.br.js,"Not_A Brand";v="8", "Chromium";v
    ="120", "Microsoft Edge";v="120",https://edgeservices.bing.com,?0,Mozilla/5.0 (
    Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/120.0.0.0 Mobile Safari/537.36 Edg/120.0.0.0,"Windows",*/*,1,5
    ED043D49FB987DE7...oiZGVza3RvcCJ9,same-origin,cors,script,https://edgeservices.bing
    .com/edgesvc/chat?udsframed=1&form=SHORUN&clientscopes=chat,noheader,udsedgeshop,
    channelstable,wincopilot,ntpquery,devtoolsapi,udsinwin11,udsdlpconsent,&shellsig
    =303a2cdef685a44beb50c449e085d350a44dc6c3&setlang=en-GB&lightschemeovr=1,gzip,
    deflate, br,en-GB,en;q=0.9,en-US;q=0.8,CUID=S
    -1-5-21-657352131-1967444620-1008359691-1002,USRLOC=HS=1&CLOC=LAT=47.4635|LON
    =8.3874|A=49239|TS=240218093052|SRC=I,SRCHD=AF=SHORUN,SRCHUID=V=2&
    GUID=3D9C6AE06E2842B59D414EDA507D52AB&dmnchg=1,SRCHUSR=DOB=20240218,EDGSRVCPERSIST=,
    SRCHHPGUSR=SRCHLANG=en&DM=0,EDGSRCHHPGUSR=CIBV=1.1579.2,
    MUID=14B4264737A06A3F04C3326E360C6B18,MUIDB=14B4264737A06A3F04C3326E360C6B18,_EDGE_S=
    SID=16ED1A554EB86D1429750E664F026CC7,_SS=SID=16ED1A554EB86D1429750E664F026CC7,EDGSRVC=
    lightschemeovr=displaytheme=edgeservices&EN=language=edgeservices,EDGSRVCSCEN=shell
    =clientscopes=noheader-coauthor-chat-visibilitypm-devtoolsapi-udsedgeshop-
    wincopilot-udsinwin11-ntpquery-udsdlpconsent-docvisibility-channelstable&chat=
    clientscopes=chat-noheader-udsedgeshop-channelstable-wincopilot-ntpquery-
    devtoolsapi-udsinwin11-udsdlpconsent
```

Quelltext 5.6: Analyse Extrahierung von GUIDs: Beispiel einer Anfrage mit GUID-, MUID- und SID-Parameter in Edge-Aufzeichnungen mit dem Auswertungsskript aus Kapitel B.2

Das Ergebnis dieser GUID-Auswertung zeigt deren Verwendung beim Tracking von Edge mit Bing auf, weist jedoch bei Chrome und Firefox lediglich auf das Tracking von aircanada.com hin.

Es kann nicht ausgeschlossen werden, dass Identifikatoren in einem anderen Format als GUIDs verwendet werden. Die Auswertung solcher Identifikatoren liegt, sofern nicht in einem anderen Kapitel erfolgt, aufgrund der gegebenen Zeit ausserhalb dieser Arbeit.

5.5. Übersicht Ergebnisse

Es folgt eine Zusammenfassung zuvor ermittelter Ergebnisse. Bemerkungen zu Abgrenzungen und Vollständigkeit sind Kapitel 5.1 zu entnehmen.

Feststellung	Chrome	Edge	Firefox	Tor Browser
Sendet Infos zur Hardware	❗	❗	❗	⛔
Sendet Infos zum Betriebssystem	❗	❗	❗	⛔
Sendet Webseitenadresse im Privat-Modus	⛔	❗	⛔	Kein Privat-Modus
Überträgt Text an Suchmaschine während Eingabe	❗	❗	❗	⛔
Überträgt Text an Suchmaschine während Eingabe im privaten Modus	⛔	⛔	⛔	Kein Privat-Modus
Kontaktiert eigene Shopping-API mit Infos zu besuchter Shopping-Seite	⛔	❗	⛔	⛔
Telemetrie beim Schliessen des Browsers	⛔	⛔	❗	⛔
GUID erscheint mit gleichem Wert in fast jeder Aufzeichnung	⛔	❗	⛔	⛔

Tabelle 5.1.: Übersicht Ergebnisse (❗ Telemetrie entdeckt, ⛔ Telemetrie nicht entdeckt)

6. Interpretation

Diese Kapitel betrachtet die Ergebnisse der Analyse aus Kapitel 5 und interpretiert diese gegebenenfalls.

Bei einer Interpretation ohne konkrete Fakten wird die Zuversicht des Autors gemäss folgender Wertung mit dem entsprechenden Symbol angefügt:

- **Sicher**, dass die Interpretation der Tatsache entspricht. Es ist kaum Spielraum für weitere Interpretationen offen, die stark abweichen
- **Eher sicher**, dass die Interpretation stimmt. Es bestehen einzelne Indizien für dessen Richtigkeit
- **Unsicher** über die Korrektheit der Interpretation. Indizien sind keine oder kaum vorhanden

Die Interpretationen sind als Erkenntnisse zuvor durchgeführter und dokumentierter Analysen zu betrachten. Je nach Browser ist dessen Quellcode einsehbar und könnte somit genauer verifiziert werden, jedoch wird dies aus Zeitgründen unterlassen. Es besteht die Wahrscheinlichkeit, dass wesentliche Informationen in den Aufzeichnungen nicht zum Vorschein gekommen sind, die Einfluss auf die folgenden Interpretationen haben könnten.

Der Tor Browser ist in diesem Kapitel, sofern nicht explizit erwähnt, auszuklammern. Dies weil er gemäss Kapitel 5.3.2 als einziger Browser dieser Arbeit keine Telemetrie aufgezeigt hat.

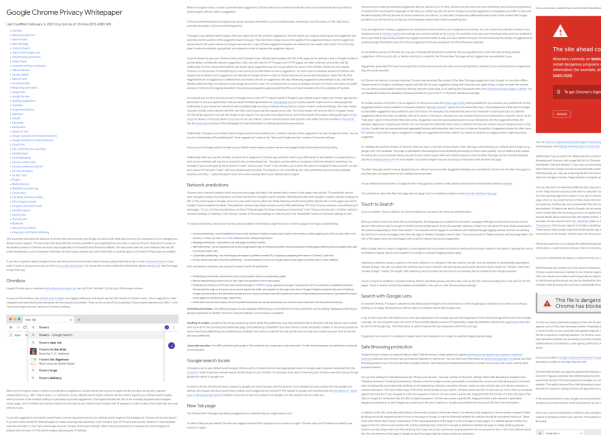
6.1. Vergleich mit Herstellerdokumentation

Allgemein gilt für jeden untersuchten Browser die Aussage, dass dieser dessen Telemetrie gemäss Herstellerdokumentation betreibt.

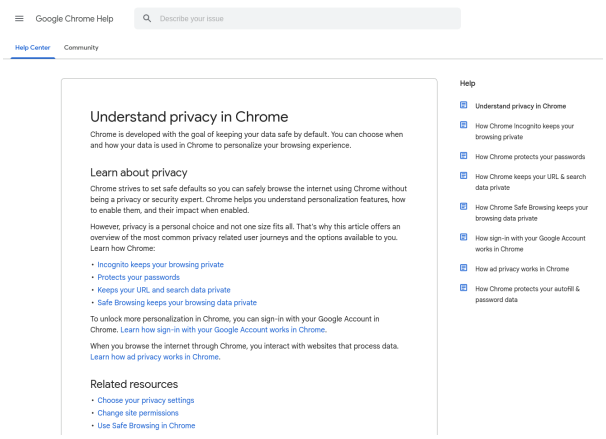
Die Hersteller lassen sich genügend Spielraum in den Dokumentationen, indem konkrete Ausführungen unterlassen werden. Dadurch leidet die Transparenz der betriebenen Telemetrie, was zur Annahme führt, dass u. a. die Adressen besuchter Webseiten mit dem jeweiligen Browser-Hersteller geteilt werden. Das Verwenden zahlreicher Identifikatoren sowie kurzen und undurchsichtigen Bezeichnungen erschweren die Analyse der Browser-Kommunikationen.

6.1.1. Aktualität Chrome Privacy Whitepaper

Google hat dessen Privatsphären-Whitepaper zu Chrome im Jahr 2024 aktualisiert, wobei es Ende 2023 noch den Modifikations-Zeitstempel vom Februar 2021 zeigte [153]. Die alte Version zeigte sämtlichen Inhalt auf einer Webseite, wobei die neue Version diverse Aspekte in einzelne Seiten unterteilt und verlinkt. Die Recherche in Kapitel 3.4 beruht auf der alten Version. Es folgen Screenshots beider Versionen[57]:



(a) Chrome Privacy Whitepaper von Ende 2023 [153]



(b) Chrome Privacy Page von März 2024 [154]

Abbildung 6.1.: Screenshots der Adresse `https://www.google.com/chrome/privacy/whitepaper.html`

Zu Beginn dieser Arbeit wurde das Privacy Whitepaper von Chrome über 2 Jahre lang nicht modifiziert [153]. Dies zeigt, dass sich die Aussagen der Hersteller jederzeit ändern können.

6.1.2. Sensitive Daten in Adressleiste

Google und Microsoft erwähnen jeweils, dass die Eingabe sensitiver Daten wie Passwörter oder lokale Dateinamen in deren Adresszeile erkannt werden können und diese dann nicht senden [155][38]. In der Analyse in Kapitel 5.3.4 wird mit Listenpunkt 5g eine solche Detektion mit einem einfachen Passwort („Einkaufen!24“) geprüft. Diese Eingabe wurde bei der Analyse ohne aktives Absenden (z.B. mittels Enter-Taste) an die hinterlegte Suchmaschine gesendet (siehe Quelltext 5.4).

Betreibt man Chrome , Edge oder Firefox im jeweiligen Privat-Modus, werden gemäss Kapitel 5.3.4 Eingaben in die Adressleiste erst nach aktivem Absenden der Suchmaschine mitgeteilt. Dies wird von den Herstellern auch so in ihrer Dokumentation ausgeführt.

[57] Der Screenshot der alten Seite wurde so editiert, sodass Text unten rechts weitergeführt wird. Weiterer Text wurde abgeschnitten. Von der aktuellen Seite ist bis auf die Fusszeile und dem Feedback-Button sämtlicher Inhalt ersichtlich

Es ist davon auszugehen, dass sämtliche Eingaben in der Adressleiste der zuvor genannten Browser an die hinterlegte Suchmaschine gesendet werden. Ausnahme bildet hierbei das Betreiben des Browsers in dessen Privat Modus. Wie die Detektion sensitiver Eingaben erfolgt ist derzeit unklar. Die Wahrscheinlichkeit, dass ein nicht technischer Benutzer ein Passwort verwendet, das nicht als solches detektiert wird, ist gemäss Praxiserfahrung sehr hoch.

Gibt man zum Beispiel ein einfaches Passwort ein, kann dies der Suchmaschine übertragen werden. Kombiniert mit der Information über die derzeit besuchende Seite könnten somit der Suchmaschine brauchbare Zugangsdaten zugespielt werden. Bestenfalls ist man in der Suchmaschine mit dem Konto eingeloggt, dessen E-Mail-Adresse zum eingegebenen Passwort gehört.

6.1.3. Edge und dessen Services

Der Shopping Service von Edge betreibt gemäss Analyse und Herstellerdokumentation Telemetrie. Gemäss Edge Privacy Whitepaper werden hierbei Produktinformationen und Informationen zu Edge und das Betriebssystem mit zufälligen Identifikatoren und Cookies (falls erlaubt) gesendet [38]. Zusätzlich benötigt dieses Feature gemäss Hersteller das Teilen von Informationen zu Cookies mit Bing [38]. Das Privacy Whitepaper beschreibt, dass Edge eine Liste mit Shopping-Domains herunterlädt und anhand dieser lokal über das Verwenden des Shopping-Services entscheidet [38]. Die Liste der Domains konnte in dieser Arbeit nicht ermittelt werden[58]. Bei Analysen wurde die Shopping-Telemetrie für die Webseiten `amazon.de` und `aircanada.com` ausgeführt.

Download einzelner Shopping-Gutscheine beim Initial-Start von Edge konnten ausgelesen werden, jedoch ist eine konkrete Liste in der gegebenen Zeit nicht auffindbar. Bestehende Aufzeichnungen wurden zusätzlich zusammen mit `aircanada.com` durchsucht, da dafür in Kapitel 5.3.4 Shopping-Telemetrie betrieben wurde, jedoch erfolglos.

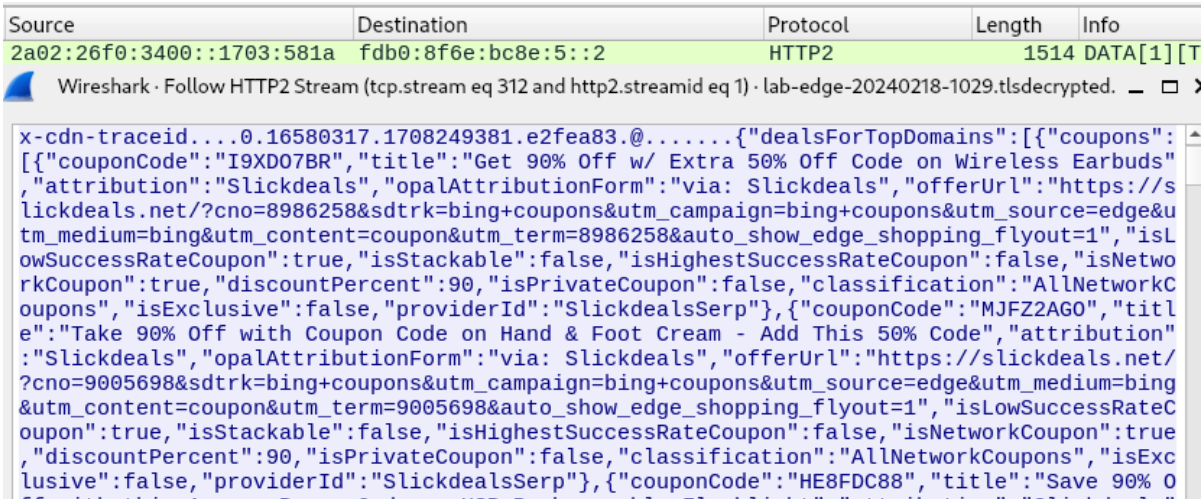


Abbildung 6.2.: Edge Shopping Gutschein Download beim Initial-Start von Edge

Edge teilt mit Microsoft Informationen über unser Einkaufsverhalten. Die Liste an Shopping-Domains zur Telemetrie der Shopping-Funktion wird nicht transparent geführt. Dies führt zur Annahme, dass potentiell jede Webseite mit einer Kauf-Funktion betroffen ist und andere Webseiten fälschlicherweise als Shopping-Webseite betrachtet werden könnten.

Zur Funktion mit künstlicher Intelligenz (Copilot) entscheidet gemäss Microsoft der Edge Browser anhand der Anfragen und Zustimmungen, welche Informationen geteilt werden [38].

[58] Hierfür wurden Online-Recherchen sowie Durchsuchungen der Aufzeichnungen betrieben

6.2. Verschmelzung von Telemetrie, Tracking und weiteren Diensten

Obwohl in Kapitel 3.1 zwischen Telemetrie und Tracking unterschieden wird, verwenden Chrome und Edge in deren Standardausführung Suchmaschinen desselben Herstellers.

Die Kombination der Telemetrie zusammen mit dem Tracking der Suchmaschinen und dem sofortigen Absenden von Eingaben im Adressfeld erlauben die Erstellung eines detaillierten Profils der anwendenden Person. Chrome und Edge verwenden für das Tracking und die Telemetrie u. a. dieselben Domänen. Dies macht das Auseinanderhalten von Tracking und Telemetrie schwieriger.

Das Windows-Betriebssystem scheint in den Aufzeichnungen ebenfalls Telemetrie zu betreiben. **Windows, Edge und Bing stammen alle von Microsoft**, womit sämtliche zugehörige Kommunikation mit Microsoft erfolgt. Eine **Korrelation der geteilten Informationen bei Microsoft kann derzeit nicht ausgeschlossen werden**. Gleiche Annahmen können auf üblichen Smartphones mit Android-Betriebssystem[59] und deren Chrome Browser zusammen mit der Google-Suchmaschine getroffen werden.

Microsoft hat eine Geschichte, in welcher sie unter anderem Edge in Windows hervorheben und Links je nach Anwendung automatisch damit öffnen [157][158][159].

Google und Microsoft haben zudem beide Werbe-Plattformen zum Aufschalten von Werbe-Anzeigen („Google Ads“ [160] und „Microsoft Advertising“ [161]), welche in weiteren Webseiten verankert sind. **Tracking-Informationen aus diesen Plattformen könnten mit Daten anderer Produkte des gleichen Herstellers kombiniert werden.** Der Hersteller von Firefox (Mozilla) bietet aktuell keine eigene Suchmaschine oder Betriebssystem an, dafür eine Werbe-Plattform [162].

Gemäss diverser Browser-Statistiken [6][7][8] verfügen Chrome, Edge und Firefox über folgende Marktanteile:

Browser	Marktanteil
Chrome	69.2
Edge	7
Firefox	3.4

Tabelle 6.2.: Marktanteile zu Beginn des Jahres 2024 der Browser Chrome, Edge und Firefox (Mittelwerte der Quellen) [6][7][8]

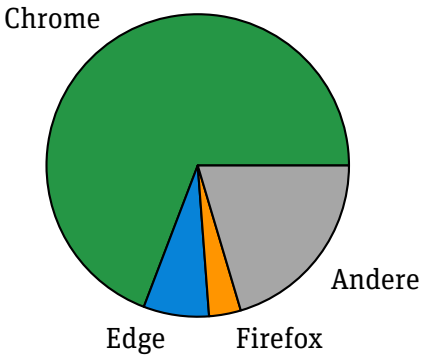


Abbildung 6.3.: Grafische Darstellung der Marktanteile aus Tabelle 6.2

Gemäss den Zahlen von W3Schools [7] wächst seit 2020 der Marktanteil von Edge , während die Anteile von Firefox und Chrome sinken [7].

Der geringe Marktanteil von Firefox wird wahrscheinlich dazu führen, dass weniger Webseiten ihren Inhalt dafür optimieren. Firefox ist unter den drei besagten Browsern der Einzige, der nicht auf Chromium aufbaut [163][39]. Je weniger Webdienste unter Firefox reibungslos genutzt werden können, umso schneller wird dessen Verwendung weniger verbreitet. **Chromium-basierte Webbrowser bilden so gut wie eine Quasimonopol-Stellung**, wogegen u. a. Firefox und Apple Safari[60] [129] ankämpfen.

[59] Android wird zu einem Grossteil von Google entwickelt [156]
[60] Das Apple-Logo stammt aus dem LaTeX-Paket `fontawesome` [164][165]

Zusätzlich zu beachten gilt, dass Google, Microsoft und Mozilla Unternehmen aus den Vereinigten Staaten von Amerika (USA) sind [166][167][168]. Eine Statistik aus Malcolm (siehe Kapitel 4.4) zeigt, dass die meisten Ziel-Adressen für SSL/TLS-Kommunikationen aus den USA stammen. Diese Auswertung beinhaltet sämtliche Aufzeichnungen dieser Arbeit mit jedem der erwähnten Browser.

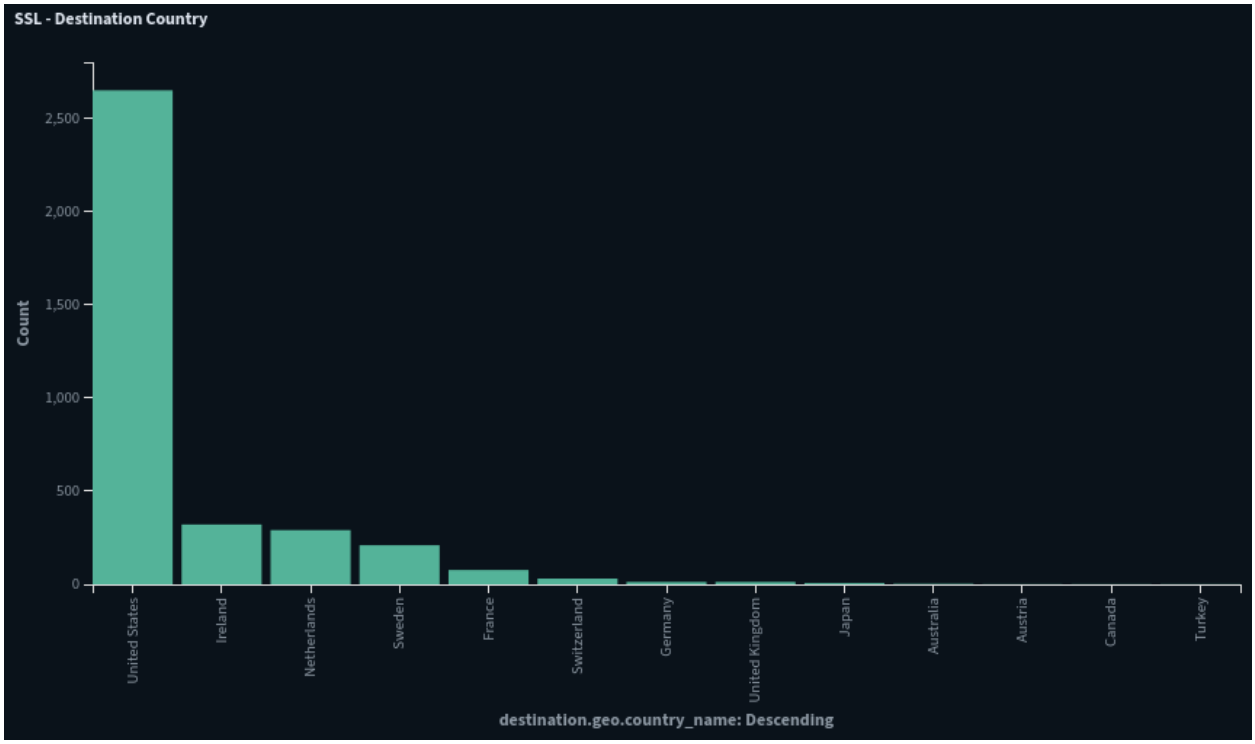


Abbildung 6.4.: Länder der Ziel-Adressen von SSL/TLS-Kommunikationen aus Malcolm gemäss importierter PCAP-Aufzeichnungen

Je weniger ein Dienst benutzt wird, umso weniger Daten können zu dessen Hersteller fliessen. **Hersteller wie Google oder Microsoft versuchen Benutzerinnen und Benutzer weitere ihrer Produkte zu vermitteln, sodass möglichst alles aus einer Hand genutzt wird. Die Kombination solcher Produkte kann die Benutzerfreundlichkeit erhöhen, jedoch auch ziemlich sicher die Menge an Telemetrie- und Tracking-Daten.** Zusätzliche Verknüpfungen mit Online-Profilen heben das Besagte mit hoher Wahrscheinlichkeit auf eine grössere Datenmenge.

7. Abschluss

7.1. Fazit

Kommunikation und Inhalt zur Telemetrie von Desktop-Webbrowser sind **nach Analyse der Browser-Verhalten und Aufzeichnungen nachvollziehbarer**. Der dokumentierte Aufbau der **Analyse-Umgebung mit einem Proxy-Server als MITM (Man-in-the-Middle) sowie der Prozess-Protokollierung** beim Browser ermöglichen eine tiefe Auseinandersetzung mit der Browser-Kommunikation.

Ein Skript zur Durchführung von Aufzeichnungen sorgt für ein effizientes sowie standardisiertes Vorgehen, das jeden Anwendungsfall und Browser gleich behandelt. Ein weiteres Skript zur Auswertung besagter Aufzeichnungen prüft diese auf mögliche Identifikatoren in Form von GUIDs.

Die Hersteller der Browser Chrome , Edge und Firefox erhalten Informationen mit unter anderem **Inhalten zur verwendeten Hardware und dem Betriebssystem**. Diese Browser **senden Eingaben in ihre Adressleisten bereits während der Eingabe an ihre hinterlegten Suchmaschinen**. Während der Nutzung eines entsprechenden **Privat-Modus** wird die Eingabe **erst beim Absenden** (zum Beispiel mit der Enter-Taste) an die Suchmaschine übermittelt. Chrome und Edge verwenden mit Google und Bing jeweils die hauseigene Suchmaschine, womit die **Grenzen zwischen Tracking und Telemetrie verschwimmen**.

Hersteller-Dokumentationen zu ihrer Browser-Telemetrie existieren, nennen jedoch **bestenfalls ungefähre Angaben oder Informationsbeschreibungen**. Diese Ausführungen können sich jederzeit ändern, was auch die Telemetrie-Verhalten der Browser betrifft.

Microsoft **Edge** generiert durch zusätzliche Shopping-Funktionen und einem Assistent mit künstlicher Intelligenz weitere Daten, die an dessen Hersteller übermittelt werden. Die **Shopping-Telemetrie wird** gemäss Hersteller bei bestimmten Webseiten **anhand einer Liste betrieben, die nicht transparent einsehbar ist**. Zudem wird bei Edge als einziger Browser ein **Identifikator** (GUID) festgestellt, dessen **Wert über mehrere Aufzeichnungen gleich** ausfällt. Zwischen einigen Aufzeichnungen wurden zugehörige Browser-Fenster jeweils geschlossen.

Der Tor Browser verhält sich bis zur Verbindung mit dem Tor Netzwerk still, ist jedoch danach aufgrund des Tor-Aufbaus undurchsichtig.

Zusammenfassend zeigt diese Arbeit allfällige Telemetrie der Desktop-Webbrowser Chrome , Edge , Firefox sowie des Tor Browsers in ihrer Standardkonfiguration auf. Hierbei wurden Anwendungsfälle wie die Installation, den ersten Browser-Start, das Besuchen von statischen Seiten und Webshops sowie deren Besuch im allfälligen Privat-Modus des Browsers behandelt. Die in dieser Arbeit erstellte Laborumgebung, zugehörige Skripts und Dokumentation ermöglichen das Nachvollziehen besagter Fälle sowie das standardisierte Analysieren weiterer Fälle.

7.2. Rückblick

Die Arbeit erzielte eine umfängliche Analyse der Telemetrie von Desktop-Webbrowser, wobei **viel gelernt und erarbeitet** werden konnte.

Die grösste Herausforderung dieser Arbeit war die gegebene Zeit. Durch die Vielzahl an Konfigurationsmöglichkeiten der Webbrowser mussten zu Beginn der Analyse **klare Abgrenzungen** definiert werden. Während der Analyse wurde nach Anhaltspunkten gesucht, deren Form und Existenz zuvor unklar war. Beispielsweise sind viele Bezeichnungen kurz gehalten und deren Zweck somit nicht rasch ersichtlich. Dies resultierte in **zeitintensiven, manuellen Analysen, die teils** zu Gunsten eines weiteren Anwendungsfalles **nicht auf das letzte Datenpaket durchleuchtet werden konnten.**

Die **Trennung zwischen Tracking und Telemetrie verschwamm** im Laufe der Arbeit. Dass Google und Microsoft für beide Typen teils dieselben Domänen verwenden, macht die Analyse zwar undurchsichtiger, könnte dafür ein Indiz zur Daten-Korrelation beim Hersteller sein.

Diese zuvor erwähnten Faktoren ergaben weniger detaillierte Einblicke in die Kommunikation der hier betrachteten Webbrowser. Die **Analysen könnten weiter vertieft werden, indem der Fokus auf einen einzelnen Browser gelegt** und zusätzlich so weit wie möglich dessen Aufbau inklusive Quellcode betrachtet wird. Aus dem Quellcode wären die teils schwer interpretierbaren Bezeichnungen konkret ermittelbar, sofern Einsicht in den Quellcode möglich ist. Mit dem Ansatz dieser Arbeit konnte hingegen ein Vergleich zwischen den Browsern erzielt werden.

Durch den nachvollziehbaren Aufbau der Laborumgebung sowie der Skripts in Kapitel B wurde eine Basis geschaffen, mit welcher zukünftige Kommunikationen von Anwendungen auf Windows 11 betrachtet werden können. Die Ressourcen-Anforderungen an die Hardware zur Betreibung der Virtuellen Maschinen (VMs) ist nicht zu unterschätzen. Es konnten aufgrund des gegebenen Arbeitsspeichers nicht sämtliche VMs parallel betrieben werden, was jedoch kein wirkliches Hindernis war.

Insgesamt bin ich mit der Arbeit sehr zufrieden und kann mir gut vorstellen, das hier erworbene Wissen weiter verwenden zu können.

An dieser Stelle möchte ich mich bei meinem Experten Daniel Röthlisberger für das Lesen vorgängiger Versionen und Besprechungen zu dieser Arbeit bedanken.

7.3. Ausblick

Die in dieser Arbeit betriebene Analyse der Browser-Telemetrie bietet trotz zeitintensiver Auseinandersetzung weitere Gebiete, die betrachtet werden können.

Konfigurationsparameter der Browser bieten teilweise gemäss Hersteller die Möglichkeit, die Menge an Telemetrie zu verringern, was verifiziert werden könnte. Die **Telemetrie von Windows 11** und dessen mitgelieferten Diensten sowie möglichen Anpassungs-Parametern wäre mit den hier gelieferten Mitteln ebenfalls analysierbar. Hierbei gilt es auch zu betrachten, ob die entsprechenden Anpassungen jeweils nach zugehörigen Aktualisierungen bestehen bleiben.

Wo möglich könnte das Verhalten der Webbrowser zusätzlich auf Basis ihres **Quellcodes** betrachtet werden. Hierfür wären aus den Browsern dieser Arbeit lediglich Firefox und der Tor Browser potenzielle Kandidaten [77][83]. Die Chromium-Basis der Browser Chrome und Edge wäre ebenfalls eine mögliche Option [163][169].

Das **QUIC-Protokoll sowie HTTP/3** werden zum Zeitpunkt dieser Arbeit von der Software mitmproxy noch nicht für dessen Proxy-Server-Funktionalität unterstützt[61]. Dies bewegt zur Annahme, dass weitere Anwendungen mit Handhabungen von HTTP(S)-Verkehr dies ebenfalls noch zu implementieren haben. Bestehende Infrastrukturen müssen dies berücksichtigen, um zukünftig einen reibungslosen Übergang zwischen den verwendeten Protokollen erzielen zu können. Je nach Implementierung der Komponenten und Umgebungen kann dies entsprechend als Herausforderung erscheinen.

[61] siehe Kapitel 4.1

Abbildungsverzeichnis

Tabellenverzeichnis

Quelltextverzeichnis

Glossar

Certificate Pinning

Sicherheitstechnik, bei welcher nur authorisierte („pinned“) Zertifikate für den Verbindungsaufbau einer sicheren Sitzung akzeptiert werden [170]. 7, 38

Chromium

Open-Source Webbrowser, der u.a. als Basis für die Browser Chrome und Edge dient [171]. 6, 52, 56

Cookies

Informationen, die Webseiten im Browser abspeichern (Login-Info, Online-Shopping-Warenkorb, etc.), aber auch fürs Tracking missbraucht werden können [33]. 5–9, 35, 36, 51

Curve25519

Spezifische elliptische Kurve. 61

DLL (Dynamic-Link Libraries)

Modul mit Funktionen und Daten, die von anderen Modulen (Anwendungen oder DLLs) verwendet werden können. Somit können Applikationen modularisiert und Funktionen einfacher wiederverwendet werden [172]. 15

Ed25519

EdDSA mit SHA-512 und Curve25519 [173]. 19, 22, 59

EdDSA (Edwards-curve Digital Signature Algorithm)

Variante der Schnorr-Signatur (Verfahren mit Beziehung zum Diskreten Logarithmus) auf Basis von „twisted Edwards Kurven“ (Familie von Ellipitischen Kurven) [173]. 61

Entry Guard

Mitglied des Tor Netzwerks (Relay), das als zufällig gewählter Eintrittspunkt ins Tor Netzwerk fungiert und jeweils nur für diesen ersten „Hop“ verwendet wird (Tor übermittelt durch mindestens 3 Relays bevor die Übertragung zum Ziel gesendet wird) [148]. 7

Fingerprint (Webbrowser)

Liste von Charakteristiken, die zusammen eindeutig Benutzerinnen und Benutzer, Browser und Hardware-Setup zuordenbar sind (Bildschirmauflösung, Schriftarten, Geolocation, etc.) [33]. 5

FQDN (Fully Qualified Domain Name)

Absoluter Name einer Domain in der Baum-Hierarchie des Domain Name Systems (DNS). 35, 36

GUID (Globally Unique IDentifier)

Universally Unique IDentifier, auch bekannt als GUID (Globally Unique IDentifier), ist ein Identifikator, der garantiert eindeutig ist [174]. 46–48, 54, 59, *siehe* UUID (Universally Unique IDentifier)

Handle

Erlaubt den Zugriff auf ein Objekt (Objektdaten oder Systemressource), was z.B. eine Datei, Thread oder Grafikbild darstellen kann [175]. 15

Hypervisor

Software, Firmware oder Hardware, die Virtuelle Maschinen (VMs) erzeugt und betreibt. 4

MITM (Man-in-the-Middle)

Angriffstechnik, bei dem der Angreifer sich physisch oder logisch zwischen zwei Komunikationspartnern befindet und somit die Kontrolle über den entsprechenden Datenverkehr hat [176]. 2, 3, 7, 54

NetFlow

Protokoll zur Sammlung von Daten zu Verkehrsflüssen in einem Netzwerk [177]. 14

PCAP

„Packet Capture“ - Dateiformat zur Ablage von Netzwerkpaket-Daten, die von einem Netwerk-Interface aufgezeichnet wurden [178]. 14, 15, 19, 26–28, 46, 53, 57

Proxy-Server

Server-Anwendung, über welche Anfragen von einem Client zum Ziel-Server geleitet werden. Der Proxy kann die Anfrage dann filtern oder verändern [179]. ii, 2, 3, 5, 7, 15, 16, 18, 20, 54, 56, 74

QUIC

Auf UDP basierendes Transportprotokoll, das u. a. für HTTP/3 [180] verwendet wird und in diversen Webbrowsern bereits im Einsatz ist [181][182][183][184]. 19, 29, 56

SHA-256 (Secure Hash Algorithm 2 mit 256-Bits)

Hash-Funktion. 24

SHA-512 (Secure Hash Algorithm 2 mit 512-Bits)

Hash-Funktion. 61

SSH (Secure Shell)

Protokoll für sicheren Fernzugriff und andere sichere Netzwerkdienste über ein unsicheres Netzwerk [185]. 17–19, 22, 27

Telemetrie

Fernmessung oder auch Übertragung von Messwerten [186]. ii, 1–6, 8, 13, 15, 16, 20, 29, 30, 35, 39–41, 44, 48–58, 74

Tor

„The onion routing network“ dient als Methode, das Internet mit so viel Privatsphäre wie möglich zu benuzten, wobei der Verkehr über mehrere Server / „Relays“ geleitet und bei jedem Schritt auf dem Weg verschlüsselt wird [187]. 1, 7, 13, 38, 39, 54, 57, 59, 63, 74, *siehe* Tor Netzwerk

Tor Browser

Webbrowser auf Basis von Firefox, der einen Zugang zu Tor ermöglicht [148]. ii, 1, 4, 6–8, 13, 16, 24, 29, 38, 39, 48, 49, 54, 56, 57, 60, 74, 78, 126, 127, *siehe* Tor

Tor Netzwerk

Verteiltes Netzwerk mit Mitgliedern („Relays“) auf der ganzen Welt, das beim Abhören der Internetverbindung das Auffinden besuchter Webseiten verhindert und die Webseiten daran hindert, den physischen Standort zu ermitteln [148]. 7, 38, 54, 61

UUID (Universally Unique IDentifier)

Universally Unique IDentifier, auch bekannt als GUID (Globally Unique IDentifier), ist ein Identifikator, der garantiert eindeutig ist [174]. 33, 59, 100, *siehe* GUID (Globally Unique IDentifier)

VirtualBox

Virtualisierungssoftware der Firma Oracle. 4, 16, 17, 19, 21, 22, 24, 25, 27, 28

Whitepaper

Dokument mit detaillierten Produktinformationen, technischen Spezifikationen u. a., das meist für eine gründliche Studie von Produkten und Dienstleistungen erstellt wurde [188]. 8–10, 12, 50, 51, 74

Literaturverzeichnis

[1] Hans Krebs. *Basel, Zollreportage. Com_L32-0104-0002-0001*. 16. März 1983. DOI: 10.3932/ethz-a-001383292. URL: https://ba.e-pics.ethz.ch/catalog/ETHBIB.Bildarchiv/r/1676412 (besucht am 22. 12. 2023).

[2] Google. *Google Chome - The Fast & Secure Web Browser Built to be Yours*. URL: https://www.google.com/chrome/ (besucht am 31. 12. 2023).

[3] Microsoft. *Get to Know Microsoft Edge*. URL: https://www.microsoft.com/edge (besucht am 31. 12. 2023).

[4] Mozilla Corporation und individual mozilla.org contributors. *Get Firefox for Desktop*. URL: https://www.mozilla.org/en-US/firefox/new/ (besucht am 31. 12. 2023).

[5] The Tor Project Inc. *Tor Project. Download Tor Browser*. URL: https://www.torproject.org/download/ (besucht am 31. 12. 2023).

[6] StatCounter. *Statcounter GlobalStats. Browser Market Share Worldwide*. URL: https://gs.statcounter.com/ (besucht am 06. 03. 2024).

[7] Refsnes Data. *Browser Statistics. The Most Popular Browsers*. URL: https://www.w3schools.com/browsers/ (besucht am 06. 03. 2024).

[8] Similarweb. *similarweb. Top Browsers Market Share*. URL: https://www.similarweb.com/browsers/ (besucht am 06. 03. 2024).

[9] Apple Inc. *Update to the latest version of Safari*. 17. Nov. 2023. URL: https://support.apple.com/en-us/102665 (besucht am 26. 12. 2023).

[10] Topher Kessler. *Apple releases Safari 5.1.7, Snow Leopard updates, and more*. 9. Mai 2012. URL: https://www.cnet.com/tech/computing/apple-releases-safari-5-1-7-snow-leopard-updates-and-more/ (besucht am 26. 12. 2023).

[11] The Tor Project Inc. *Tor Project. Support*. URL: https://support.torproject.org/ (besucht am 26. 12. 2023).

[12] Google. *Chrome browser system requirements*. URL: https://support.google.com/chrome/a/answer/7100626 (besucht am 26. 12. 2023).

[13] Dan Wesley u. a. *Microsoft Edge supported Operating Systems*. 19. Sep. 2023. URL: https://github.com/MicrosoftDocs/Edge-Enterprise/blob/public/edgeenterprise/microsoft-edge-supported-operating-systems.md (besucht am 26. 12. 2023).

[14] Mozilla Corporation und individual mozilla.org contributors. *Firefox System Requirements. Firefox 121.0*. URL: https://www.mozilla.org/en-US/firefox/121.0/system-requirements/ (besucht am 26. 12. 2023).

[15] StatCounter. *Statcounter GlobalStats. Desktop Operating System Market Share Worldwide*. URL: https://gs.statcounter.com/os-market-share/desktop/worldwide (besucht am 26. 12. 2023).

[16] Statista Research Department. *Market share held by the leading computer (desktop/tablet/console) operating systems worldwide from January 2012 to June 2023*. 5. Sep. 2023. URL: https://www.statista.com/statistics/268237/global-market-share-held-by-operating-systems-since-2009/ (besucht am 26. 12. 2023).

[17] Oracle. *Oracle VM VirtualBox*. URL: https://www.oracle.com/virtualization/technologies/vm/downloads/virtualbox-downloads.html (besucht am 26. 12. 2023).

[18] Microsoft. *Download Windows 11 (Current release: Windows 11 2023 Update | Version 23H2)*. URL: https://www.microsoft.com/software-download/windows11 (besucht am 14. 01. 2024).

[19] Software in the Public Interest (SPI). *debian - The universal operating system*. URL: https://www.debian.org/ (besucht am 13. 01. 2024).

[20] Mozilla Corporation und individual mozilla.org contributors. *Download Firefox*. URL: https://www.mozilla.org/firefox/download/ (besucht am 20. 01. 2024).

[21] The Tor Project Inc. *Tor Project. Download*. URL: https://torproject.org/download (besucht am 20. 01. 2024).
[22] Battelle Energy Alliance LLC, Cybersecurity und Infrastructure Security Agency. *Malcolm*. 20. Dez. 2023. URL: https://github.com/cisagov/Malcolm (besucht am 06. 01. 2024).
[23] Mitmproxy Project. *mitmproxy - An interactive HTTPS proxy*. URL: https://mitmproxy.org/ (besucht am 06. 01. 2024).
[24] Wireshark Foundation. *Wireshark - Go Deep*. URL: https://www.wireshark.org/ (besucht am 06. 01. 2024).
[25] Mark Russinovich. *Autoruns for Windows v14.1*. 7. Juni 2023. URL: https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns (besucht am 13. 01. 2024).
[26] Python Software Foundation. *Python 3.12.1*. URL: https://www.python.org/downloads/release/python-3121/ (besucht am 20. 01. 2024).
[27] Brian Baskin. *Noriben Malware Analysis Sandbox*. 9. Aug. 2023. URL: https://github.com/Rurik/Noriben (besucht am 13. 01. 2024).
[28] Mahmoud Saleh, Colin Robertson, Matin Sasanpour u. a. *Microsoft Visual C++ Redistributable latest supported downloads*. URL: https://learn.microsoft.com/en-us/cpp/windows/latest-supported-vc-redist (besucht am 20. 01. 2024).
[29] Christian Wojner. *ProcDOT - Visual Malware Analysis*. URL: https://procdot.com/ (besucht am 13. 01. 2024).
[30] Mark Russinovich. *Process Explorer v17.05*. 30. März 2023. URL: https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer (besucht am 13. 01. 2024).
[31] WJ32. *Process Hacker*. URL: https://processhacker.sourceforge.io/ (besucht am 13. 01. 2024).
[32] Mark Russinovich. *Process Monitor v3.96*. 9. März 2023. URL: https://learn.microsoft.com/en-us/sysinternals/downloads/procmon (besucht am 13. 01. 2024).
[33] Electronic Frontier Foundation. *Cover Your Tracks. How do trackers work?* URL: https://coveryourtracks.eff.org/learn (besucht am 27. 12. 2023).
[34] Proofpoint. *What Is Telemetry?* URL: https://www.proofpoint.com/us/threat-reference/telemetry (besucht am 28. 12. 2023).
[35] Fortinet Inc. *What Is A Transparent Proxy?* URL: https://www.fortinet.com/resources/cyberglossary/transparent-proxy (besucht am 31. 12. 2023).
[36] Jomilė Nakutavičiūtė. *What is a transparent proxy: An easy explanation*. 27. März 2019. URL: https://nordvpn.com/blog/transparent-proxy/ (besucht am 31. 12. 2023).
[37] Joe Belfiore. *New year, new browser – The new Microsoft Edge is out of preview and now available for download*. 15. Jan. 2020. URL: https://blogs.windows.com/windowsexperience/2020/01/15/new-year-new-browser-the-new-microsoft-edge-is-out-of-preview-and-now-available-for-download/ (besucht am 27. 12. 2023).
[38] Microsoft Edge Team u. a. *Microsoft Edge Privacy Whitepaper*. 14. Dez. 2023. URL: https://learn.microsoft.com/en-us/microsoft-edge/privacy-whitepaper/ (besucht am 31. 12. 2023).
[39] Mark Mayo. *Introducing the New Firefox: Firefox Quantum*. 14. Nov. 2017. URL: https://blog.mozilla.org/en/mozilla/introducing-firefox-quantum/ (besucht am 27. 12. 2023).
[40] Chelsea Novak. *The New Firefox: By the Numbers*. 14. Nov. 2017. URL: https://blog.mozilla.org/en/products/firefox/the-new-firefox-by-the-numbers/ (besucht am 27. 12. 2023).
[41] Mozilla Corporation und individual mozilla.org contributors. *Firefox Release Notes. Version 57.0, first offered to Release channel users on November 14, 2017*. 14. Nov. 2017. URL: https://www.mozilla.org/en-US/firefox/57.0/releasenotes/ (besucht am 27. 12. 2023).
[42] Alice Wyman, Lamont Gardenhire, Mozilla Corporation u. a. *Firefox ESR release cycle*. URL: https://support.mozilla.org/en-US/kb/firefox-esr-release-cycle (besucht am 06. 01. 2024).

[43] Mozilla Corporation und individual mozilla.org contributors. *Firefox ESR Release Notes. Version 60.0esr, first offered to ESR channel users on May 9, 2018*. 9. Mai 2018. URL: https://www.mozilla.org/en-US/firefox/60.0esr/releasenotes/ (besucht am 27. 12. 2023).

[44] boklm. *New Release: Tor Browser 8.0*. 5. Sep. 2018. URL: https://blog.torproject.org/new-release-tor-browser-80/ (besucht am 27. 12. 2023).

[45] Douglas J. Leith. "Web Browser Privacy: What Do Browsers Say When They Phone Home?" In: *IEEE Access* 9 (2021), S. 41615–41627. DOI: 10.1109/ACCESS.2021.3065243.

[46] Douglas J. Leith. "Web Browser Privacy: What Do Browsers Say When They Phone Home?" In: (24. Feb. 2020). URL: https://www.scss.tcd.ie/Doug.Leith/pubs/browser_privacy.pdf (besucht am 27. 12. 2023).

[47] Lindsey O'Donnell. *Microsoft Edge Shares Privacy-Busting Telemetry, Research Alleges*. 16. März 2020. URL: https://threatpost.com/microsoft-edge-privacy-busting-telemetry/153733/ (besucht am 28. 12. 2023).

[48] Mayank Parmar. *Research Finds Microsoft Edge Has Privacy-Invading Telemetry*. 14. März 2020. URL: https://www.bleepingcomputer.com/news/microsoft/research-finds-microsoft-edge-has-privacy-invading-telemetry/ (besucht am 28. 12. 2023).

[49] Catalin Cimpanu. *Brave deemed most private browser in terms of 'phoning home'*. 2. März 2020. URL: https://www.zdnet.com/article/brave-deemed-most-private-browser-in-terms-of-phoning-home/ (besucht am 28. 12. 2023).

[50] Sofia Elizabella Wyciślik-Wilson. *Microsoft Edge has more privacy-invading telemetry than other browsers*. 9. März 2020. URL: https://betanews.com/2020/03/09/microsoft-edge-privacy-telemetry/ (besucht am 28. 12. 2023).

[51] Srinivas Sista. *Chrome Releases - Release updates from the Chrome team. Stable Channel Update for Desktop*. 4. Feb. 2020. URL: https://chromereleases.googleblog.com/2020/02/stable-channel-update-for-desktop.html (besucht am 31. 12. 2023).

[52] Microsoft. *Archived release notes for Microsoft Edge Stable Channel. Version 80.0.361.48: February 7*. 7. Feb. 2020. URL: https://learn.microsoft.com/en-us/deployedge/microsoft-edge-relnote-archive-stable-channel#version-80036148-february-7 (besucht am 31. 12. 2023).

[53] Mozilla Corporation und individual mozilla.org contributors. *Firefox Release Notes. Version 73.0, first offered to Release channel users on February 11, 2020*. 11. Feb. 2020. URL: https://www.mozilla.org/en-US/firefox/73.0/releasenotes/ (besucht am 31. 12. 2023).

[54] Mitmproxy Project. *mitmproxy docs. Introduction*. 19. Juli 2023. URL: https://docs.mitmproxy.org/stable/ (besucht am 31. 12. 2023).

[55] sizeof(cat). *Web Browser telemetry*. 19. Dez. 2021. URL: https://sizeof.cat/post/web-browser-telemetry/ (besucht am 28. 12. 2023).

[56] Objective Development. *Little Snitch. Makes the invisible visible!* URL: https://www.obdev.at/products/littlesnitch/index.html (besucht am 28. 12. 2023).

[57] Srinivas Sista. *Chrome Releases - Release updates from the Chrome team. Stable Channel Update for Desktop*. 13. Dez. 2021. URL: https://chromereleases.googleblog.com/2021/12/stable-channel-update-for-desktop_13.html (besucht am 28. 12. 2023).

[58] Microsoft. *Archived release notes for Microsoft Edge Stable Channel. Version 96.0.1054.62: December 17*. 17. Dez. 2021. URL: https://learn.microsoft.com/en-us/deployedge/microsoft-edge-relnote-archive-stable-channel#version-960105462-december-17 (besucht am 28. 12. 2023).

[59] Mozilla Corporation und individual mozilla.org contributors. *Firefox Release Notes. Version 95.0.1, first offered to Release channel users on December 16, 2021*. 16. Dez. 2021. URL: https://www.mozilla.org/en-US/firefox/95.0.1/releasenotes/ (besucht am 28. 12. 2023).

[60] sysrqb. *New Release: Tor Browser 11.0.2*. 8. Dez. 2021. URL: https://blog.torproject.org/new-release-tor-browser-1102/ (besucht am 28. 12. 2023).

[61] The Tor Project Inc. *Tor Project. Technical Setup*. URL: https://community.torproject.org/relay/setup/ (besucht am 28. 12. 2023).
[62] Privacy Tools. *Best Privacy Web Browser to Stay Private in 2023*. URL: https://www.privacytools.io/private-browser (besucht am 28. 12. 2023).
[63] Martin Brinkmann. *Each Firefox download has a unique identifier*. 17. März 2022. URL: https://www.ghacks.net/2022/03/17/each-firefox-download-has-a-unique-identifier/ (besucht am 28. 12. 2023).
[64] Alice Wyman, Michele Rodaro, Mozilla Corporation u. a. *About Firefox Desktop Attribution*. URL: https://support.mozilla.org/en-US/kb/desktop-attribution-privacy (besucht am 31. 12. 2023).
[65] Google. *Google Chrome Privacy Whitepaper*. 4. Feb. 2021. URL: https://www.google.com/chrome/privacy/whitepaper.html (besucht am 31. 12. 2023).
[66] Google. *Google Chrome Logo*. URL: https://www.google.com/chrome/static/images/chrome-logo.svg (besucht am 06. 01. 2024).
[67] Babu Mohan. *Google Chrome's data-saving Lite mode is going away next month*. 23. Feb. 2022. URL: https://www.androidcentral.com/google-killing-chrome-lite-mode (besucht am 01. 01. 2024).
[68] Jasika Bawa. *Thank you and goodbye to the Chrome Cleanup Tool*. 8. März 2023. URL: https://security.googleblog.com/2023/03/thank-you-and-goodbye-to-chrome-cleanup.html (besucht am 01. 01. 2024).
[69] Google. *Safe Browsing*. URL: https://safebrowsing.google.com/ (besucht am 01. 01. 2024).
[70] Google. *chrome web store*. URL: https://chromewebstore.google.com/ (besucht am 01. 01. 2024).
[71] Microsoft. *Microsoft Edge Logo*. URL: https://commons.wikimedia.org/wiki/File:Edge_Logo_2019.svg (besucht am 06. 01. 2024).
[72] Microsoft. *Copilot*. URL: https://www.microsoft.com/en-us/edge/features/copilot (besucht am 01. 01. 2024).
[73] Microsoft. *Edge Add-ons*. URL: https://microsoftedge.microsoft.com/addons (besucht am 01. 01. 2024).
[74] Mozilla Corporation. *Mozilla Firefox Logo*. URL: https://commons.wikimedia.org/wiki/File:Firefox_logo,_2019.svg (besucht am 06. 01. 2024).
[75] Mozilla Corporation und individual mozilla.org contributors. *Firefox Privacy Notice*. 1. Nov. 2023. URL: https://www.mozilla.org/en-US/privacy/firefox/ (besucht am 31. 12. 2023).
[76] Mozilla Corporation und individual mozilla.org contributors. *Mercurial*. URL: https://hg.mozilla.org/ (besucht am 06. 01. 2024).
[77] Mozilla Corporation und individual mozilla.org contributors. *Getting Set Up To Work On The Firefox Codebase*. URL: https://firefox-source-docs.mozilla.org/setup/index.html (besucht am 06. 01. 2024).
[78] Mozilla Corporation und individual mozilla.org contributors. *MozillaWiki. Data Collection*. 4. Jan. 2024. URL: https://wiki.mozilla.org/Data_Collection (besucht am 06. 01. 2024).
[79] Alice Wyman u. a. *Firefox DNS-over-HTTPS*. URL: https://support.mozilla.org/en-US/kb/firefox-dns-over-https (besucht am 06. 01. 2024).
[80] The Tor Project Inc. *Tor Styleguide. Brand Assets*. URL: https://styleguide.torproject.org/brand-assets/ (besucht am 06. 01. 2024).
[81] The Tor Project Inc. *Tor Project. Tor Metrics*. URL: https://support.torproject.org/metrics/ (besucht am 31. 12. 2023).
[82] The Tor Project Inc. *Tor Project. About Tor*. URL: https://support.torproject.org/metrics/ (besucht am 31. 12. 2023).
[83] The Tor Project Inc. *Tor Browser Repository*. URL: https://gitlab.torproject.org/tpo/applications/tor-browser (besucht am 06. 01. 2024).
[84] DuckDuckGo. *DuckDuckGo Privacy Policy*. URL: https://duckduckgo.com/privacy (besucht am 16. 03. 2024).

[85] Philip Hagen. *Next Generation FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response*. 6. Nov. 2023. URL: https://www.sans.org/blog/next-generation-for572-advanced-network-forensics-threat-hunting-analysis-and-incident-response/ (besucht am 06. 01. 2024).
[86] Philip Hagen. *SOF-ELK*. URL: https://www.sans.org/tools/sof-elk/ (besucht am 06. 01. 2024).
[87] SANS Institute. *FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response*. URL: https://www.sans.org/cyber-security-courses/advanced-network-forensics-threat-hunting-incident-response/ (besucht am 06. 01. 2024).
[88] Philip Hagen und antmar904. *SOF-ELK. How to ingest a pcap file*. 8. Juni 2021. URL: https://github.com/philhagen/sof-elk/issues/225 (besucht am 06. 01. 2024).
[89] Andy Wick, Elyse Rinne, Nathan Bower u. a. *Arkime FAQ*. 3. Jan. 2024. URL: https://arkime.com/faq (besucht am 06. 01. 2024).
[90] The Zeek Project. *About Zeek*. URL: https://docs.zeek.org/en/master/about.html (besucht am 06. 01. 2024).
[91] The Zeek Project. *Quick Start Guide. Reading Packet Capture (pcap) Files*. URL: https://docs.zeek.org/en/master/quickstart.html#reading-packet-capture-pcap-files (besucht am 06. 01. 2024).
[92] Cybersecurity und Infrastructure Security Agency. *About CISA*. URL: https://www.cisa.gov/about (besucht am 06. 01. 2024).
[93] Open Information Security Foundation. *Suricata*. URL: https://suricata.io/ (besucht am 06. 01. 2024).
[94] OpenSearch contributors. *About OpenSearch*. URL: https://opensearch.org/about.html (besucht am 06. 01. 2024).
[95] Cisco and/or its affiliates. *ClamAV. About*. URL: https://www.clamav.net/about (besucht am 06. 01. 2024).
[96] Battelle Energy Alliance LLC, Cybersecurity und Infrastructure Security Agency. *Malcolm. Components*. 20. Dez. 2023. URL: https://github.com/cisagov/Malcolm/blob/main/docs/components.md (besucht am 06. 01. 2024).
[97] Battelle Energy Alliance LLC, Cybersecurity und Infrastructure Security Agency. *Malcolm*. 21. Dez. 2023. URL: https://github.com/cisagov/Malcolm/blob/main/docs/README.md (besucht am 06. 01. 2024).
[98] Zeltser Security Corp. *REMnux: A Linux Toolkit for Malware Analysis*. URL: https://remnux.org (besucht am 06. 01. 2024).
[99] NETRESEC. *PolarProxy*. URL: https://www.netresec.com/?page=PolarProxy (besucht am 06. 01. 2024).
[100] Zeltser Security Corp. *REMnux Documentation. Monitoring*. 30. Dez. 2021. URL: https://docs.remnux.org/discover-the-tools/explore+network+interactions/monitoring (besucht am 06. 01. 2024).
[101] Anuj Soni und Lenny Zeltser. *FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques*. URL: https://www.sans.org/cyber-security-courses/reverse-engineering-malware-malware-analysis-tools-techniques/ (besucht am 13. 01. 2024).
[102] Lenny Zeltser. *Malware Analysis Cheat Sheet*. 20. Juli 2021. URL: https://zeltser.com/media/docs/malware-analysis-cheat-sheet.pdf (besucht am 13. 01. 2024).
[103] Mossé Cyber Security Institute. *Tools to get you Started in Malware Analysis*. Juni 2022. URL: https://mcsi-library.readthedocs.io/articles/2022/06/tools-to-get-you-started-in-malware-analysis/tools-to-get-you-started-in-malware-analysis.html (besucht am 13. 01. 2024).
[104] Neil Fox. *11 Best Malware Analysis Tools and Their Features*. 3. März 2022. URL: https://www.varonis.com/blog/malware-analysis-tools (besucht am 13. 01. 2024).

[105] Oracle. *Oracle VM VirtualBox - User Guide for Release 7.0. First Steps*. URL: https://docs.oracle.com/en/virtualization/virtualbox/7.0/user/Introduction.html (besucht am 13. 01. 2024).
[106] Brian Haberman und Bob Hinden. *Unique Local IPv6 Unicast Addresses*. RFC 4193. Okt. 2005. DOI: 10.17487/RFC4193. URL: https://www.rfc-editor.org/info/rfc4193.
[107] cd34. *RFC4193 IPv6 Generator*. URL: https://cd34.com/rfc4193/ (besucht am 14. 01. 2024).
[108] systemd. *Predictable Network Interface Names*. 5. Juli 2022. URL: https://systemd.io/PREDICTABLE_INTERFACE_NAMES/ (besucht am 14. 01. 2024).
[109] M. Zinoune. *Setting Up a Forwarding DNS Server On Debian*. 22. Jan. 2016. URL: https://www.unixmen.com/setting-forwarding-dns-server-debian/ (besucht am 14. 01. 2024).
[110] Maximilian Hils. *Mitmproxy 10: First Bits of HTTP/3!* 4. Aug. 2023. URL: https://mitmproxy.org/posts/releases/mitmproxy10/ (besucht am 14. 01. 2024).
[111] adumitru. *Technical Tip : How to block/disable QUIC*. 4. Juli 2022. URL: https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-block-disable-QUIC/ta-p/191273 (besucht am 14. 01. 2024).
[112] Palo Alto Networks Inc. *How to Block QUIC Protocol*. 6. März 2023. URL: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClarCAC (besucht am 14. 01. 2024).
[113] Mitmproxy Project. *mitmproxy docs. Transparent Proxying*. 29. Apr. 2023. URL: https://docs.mitmproxy.org/stable/howto-transparent/ (besucht am 31. 12. 2023).
[114] Mitmproxy Project. *mitmproxy docs. Wireshark and SSL/TLS Master Secrets*. 23. Nov. 2022. URL: https://docs.mitmproxy.org/stable/howto-wireshark-tls/ (besucht am 14. 01. 2024).
[115] Mitmproxy Project. *mitmproxy docs. About Certificates*. 6. Sep. 2023. URL: https://docs.mitmproxy.org/stable/concepts-certificates/ (besucht am 31. 12. 2023).
[116] Simon Coter. *How to install Microsoft Windows 11 on VirtualBox*. 29. Nov. 2021. URL: https://blogs.oracle.com/virtualization/post/install-microsoft-windows-11-on-virtualbox (besucht am 14. 01. 2024).
[117] Chetan Nayak. *Windows 11 Home vs Windows 11 Pro: Which license to get for your PC*. 11. Juli 2023. URL: https://www.croma.com/unboxed/windows-11-home-vs-windows-11-pro (besucht am 14. 01. 2024).
[118] Mauro Huculak. *How to bypass internet connection to install Windows 11*. 12. Apr. 2024. URL: https://pureinfotech.com/bypass-internet-connection-install-windows-11/ (besucht am 14. 01. 2024).
[119] Oracle. *Oracle VM VirtualBox - User Manual. Guest Additions for Windows*. URL: https://www.virtualbox.org/manual/ch04.html#additions-windows (besucht am 20. 01. 2024).
[120] Robin Harwood, Kevin Kaland, Seth Manheim u. a. *Get started with OpenSSH for Windows. Install OpenSSH for Windows*. 10. Jan. 2024. URL: https://learn.microsoft.com/en-us/windows-server/administration/openssh/openssh_install_firstuse?tabs=powershell#install-openssh-for-windows (besucht am 14. 01. 2024).
[121] Robin Harwood, Danny Maertens, Seth Manheim u. a. *Key-based authentication in OpenSSH for Windows*. 5. Aug. 2022. URL: https://learn.microsoft.com/en-us/windows-server/administration/openssh/openssh_keymanagement (besucht am 21. 01. 2024).
[122] The Graphviz Authors. *Graphviz. Download*. URL: https://graphviz.org/download/ (besucht am 20. 01. 2024).
[123] Battelle Energy Alliance LLC, Cybersecurity und Infrastructure Security Agency. *Malcolm. Malcolm installer ISO*. 20. Dez. 2023. URL: https://github.com/cisagov/Malcolm/blob/main/docs/malcolm-iso.md (besucht am 20. 01. 2024).
[124] Battelle Energy Alliance LLC, Cybersecurity und Infrastructure Security Agency. *Malcolm. Quick start*. 10. Jan. 2024. URL: https://github.com/cisagov/Malcolm/blob/main/docs/quickstart.md (besucht am 20. 01. 2024).
[125] Docker Inc. *Install Docker Desktop on Debian*. URL: https://docs.docker.com/desktop/install/debian/ (besucht am 20. 01. 2024).

[126] Battelle Energy Alliance LLC, Cybersecurity und Infrastructure Security Agency. *Malcolm. End-to-end Malcolm and Hedgehog Linux ISO Installation*. 8. Jan. 2024. URL: https://github.com/cisagov/Malcolm/blob/main/docs/malcolm-hedgehog-e2e-iso-install.md#MalcolmConfig (besucht am 20. 01. 2024).
[127] Mauro Guadagnini. "Sicherer Umgang mit dem SSH-Serverdienst von OpenSSH". Semesterarbeit CAS IT Security Management. Berner Fachhochschule, 24. Sep. 2023.
[128] Mitmproxy Project. *mitmproxy docs. Options*. 8. Mai 2023. URL: https://docs.mitmproxy.org/stable/concepts-options/ (besucht am 28. 01. 2024).
[129] Apple Inc. *Safari*. URL: https://www.apple.com/safari/ (besucht am 28. 01. 2024).
[130] Brave Software Inc. *Brave - Secure, Fast, & Private Web Browser with Adblocker*. URL: https://brave.com/ (besucht am 06. 01. 2024).
[131] Dan Brown u. a. *Configure Windows diagnostic data in your organization*. 24. Juni 2023. URL: https://learn.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization (besucht am 28. 01. 2024).
[132] Denise Vangel, Jesse Esquivel, Daniel Simpson u. a. *Microsoft Defender Antivirus in Windows*. 16. Jan. 2024. URL: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-windows (besucht am 04. 02. 2024).
[133] Denise Vangel, Brit Weston, Daniel Simpson u. a. *Configure and manage Microsoft Defender Antivirus with the mpcmdrun.exe command-line tool*. 6. Juni 2023. URL: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/command-line-arguments-microsoft-defender-antivirus (besucht am 18. 02. 2024).
[134] Microsoft. *Microsoft Defender Antivirus in Windows*. URL: https://www.microsoft.com/en-us/wdsi/defenderupdates (besucht am 18. 02. 2024).
[135] Steven White u. a. *Service Programs*. 7. Jan. 2021. URL: https://learn.microsoft.com/en-us/windows/win32/services/service-programs (besucht am 04. 02. 2024).
[136] Simon Ren und Wang Haipeng. *How to setting SystemSettings.exe Process default access to Internet*. 30. Aug. 2023. URL: https://learn.microsoft.com/en-us/answers/questions/1342273/how-to-setting-systemsettings-exe-process-default (besucht am 04. 02. 2024).
[137] David Bokan. *What does UMA refer in Chrome?* 11. Sep. 2018. URL: https://stackoverflow.com/a/39045389 (besucht am 04. 02. 2024).
[138] Alekhya Sai. *Clarity Overview*. 29. Jan. 2024. URL: https://learn.microsoft.com/en-us/clarity/setup-and-installation/about-clarity (besucht am 18. 02. 2024).
[139] Alekhya Sai. *Clarity. Cookie List*. 30. Jan. 2024. URL: https://learn.microsoft.com/en-us/clarity/setup-and-installation/cookie-list (besucht am 18. 02. 2024).
[140] Kristoffer Abs. *CompatTelRunner.exe in Windows 10*. 15. Aug. 2015. URL: https://answers.microsoft.com/en-us/windows/forum/all/compattelrunnerexe-in-windows-10/b0c6abf9-df70-44d4-8343-206e07773b2d (besucht am 18. 02. 2024).
[141] Greycode Intelligence. *Unveiling the Power of Amcache: A Crucial Artifact in Digital Forensic Investigations*. 25. Juli 2023. URL: https://greycodeintelligence.com/insights/unveiling-the-power-of-amcache-a-crucial-artifact-in-digital-forensic-investigations/ (besucht am 18. 02. 2024).
[142] Eric Zimmerman. *(Am)cache still rules everything around me (part 2 of 1)*. 6. Okt. 2017. URL: https://binaryforay.blogspot.com/2017/10/amcache-still-rules-everything-around.html (besucht am 18. 02. 2024).
[143] Raj Kumar. *Microsoft Edge Making Suspicious Connection? Here's what you need to know*. 3. Jan. 2024. URL: https://allthings.how/microsoft-edge-making-suspicious-connection-heres-what-you-need-to-know/ (besucht am 18. 02. 2024).
[144] Google. *Widevine - Leading Content Protection for Media*. URL: https://widevine.com/ (besucht am 18. 02. 2024).
[145] The Tor Project Inc. *Glossary. moat*. URL: https://support.torproject.org/glossary/moat/ (besucht am 18. 02. 2024).

[146] Paul Staroch. *TorStatus. Tor Network Status*. URL: https://torstatus.rueckgr.at/ (besucht am 16. 03. 2024).
[147] Daniel Austin. *TOR Node List*. URL: https://www.dan.me.uk/tornodes (besucht am 18. 02. 2024).
[148] The Tor Project Inc. *Tor Project. About Tor*. URL: https://support.torproject.org/about/ (besucht am 28. 12. 2023).
[149] The Tor Project Inc. *Tor Project. When I'm using Tor, can eavesdroppers still see the information I share with websites, like login information and things I type into forms?* URL: https://support.torproject.org/https/https-1/ (besucht am 18. 02. 2023).
[150] Kaj Magnus. *How can I trigger a fake Malware API response from my test suites?* URL: https://github.com/google/safebrowsing/issues/96 (besucht am 19. 02. 2024).
[151] CERN (Europäische Organisation für Kernforschung). *http://info.cern.ch - home of the first website*. URL: http://info.cern.ch (besucht am 28. 02. 2024).
[152] Free Software Foundation Inc. *strings - print the sequences of printable characters in files*. 14. Jan. 2023. URL: https://manpages.debian.org/bookworm/binutils-common/strings.1.en.html (besucht am 06. 03. 2024).
[153] Google. *Wayback Machine. Google Chrome Privacy Whitepaper*. 4. Feb. 2021. URL: https://web.archive.org/web/20231128043908/https://www.google.com/chrome/privacy/whitepaper.html (besucht am 28. 11. 2023).
[154] Google. *Google Chrome Privacy Whitepaper*. URL: https://www.google.com/chrome/privacy/whitepaper.html (besucht am 06. 03. 2024).
[155] Google. *How Chrome keeps your URL & search data private*. URL: https://support.google.com/chrome/answer/13730681 (besucht am 06. 03. 2024).
[156] Bertel King. *Is Android Really Open-Source? And Does It Even Matter?* 2. Dez. 2021. URL: https://www.makeuseof.com/tag/android-really-open-source-matter/ (besucht am 06. 03. 2024).
[157] Sean Hollister, Tom Warren, Umar Shakir u. a. *Every trick Microsoft pulled to make you browse Edge instead of Chrome*. 29. Jan. 2024. URL: https://www.theverge.com/23935029/microsoft-edge-forced-windows-10-google-chrome-fight (besucht am 06. 03. 2024).
[158] Thomas Claburn. *Mozilla slams Microsoft for using dark patterns to drive Windows users toward Edge*. 2. Feb. 2024. URL: https://www.theregister.com/2024/02/02/mozilla_slams_microsoft_dark_patterns/ (besucht am 06. 03. 2024).
[159] Harry Brignull und Cennydd Bowles. *Every trick Microsoft pulled to make you browse Edge instead of Chrome*. 25. Jan. 2024. URL: https://research.mozilla.org/files/2024/01/Over-the-Edge-Report-January-2024.pdf.
[160] Google. *Google Ads*. URL: https://ads.google.com/ (besucht am 06. 03. 2024).
[161] Microsoft. *Microsoft Advertising*. URL: https://ads.microsoft.com (besucht am 06. 03. 2024).
[162] Mozilla Corporation und individual mozilla.org contributors. *Advertise with Mozilla*. URL: https://www.mozilla.org/en-US/advertising/ (besucht am 06. 03. 2024).
[163] Cornelia Möhring. *Chromium vs. Chrome - wo liegen die Unterschiede?* 23. Okt. 2019. URL: https://www.heise.de/tipps-tricks/Chromium-vs-Chrome-wo-liegen-die-Unterschiede-4566098.html (besucht am 10. 03. 2024).
[164] Marcel Krüger und Fonticons Inc. *The fontawesome5 package*. 2. Mai 2022. URL: http://mirrors.ibiblio.org/CTAN/fonts/fontawesome5/doc/fontawesome5.pdf (besucht am 10. 03. 2024).
[165] Fonticons Inc. *Font Awesome*. URL: https://fontawesome.com/ (besucht am 10. 03. 2024).
[166] Google. *From the garage to the Googleplex*. URL: https://about.google/intl/ALL_us/our-story/ (besucht am 06. 03. 2024).
[167] Microsoft. *Facts About Microsoft*. URL: https://news.microsoft.com/facts-about-microsoft/ (besucht am 06. 03. 2024).

[168] Mozilla Foundation. *Articles of Incorporation of the Mozilla Foundation*. 14. Juli 2003. URL: https://static.mozilla.com/foundation/documents/mf-articles-of-incorporation.pdf (besucht am 06. 03. 2024).
[169] Google. *Chromium Repository*. URL: https://chromium.googlesource.com/chromium/src/ (besucht am 10. 03. 2024).
[170] shlipsey3. *What is Certificate pinning?* 6. Dez. 2023. URL: https://learn.microsoft.com/en-us/azure/security/fundamentals/certificate-pinning (besucht am 31. 12. 2023).
[171] Stephen Shankland. *Google gets web allies by letting outsiders help build Chrome's foundation*. 30. Nov. 2020. URL: https://www.cnet.com/tech/mobile/google-gets-web-allies-by-letting-outsiders-help-build-chromes-foundation/ (besucht am 27. 12. 2023).
[172] Steven White u. a. *Dynamic-Link Libraries*. 31. Mai 2022. URL: https://learn.microsoft.com/en-us/windows/win32/dlls/dynamic-link-libraries (besucht am 13. 01. 2024).
[173] Simon Josefsson und Ilari Liusvaara. *Edwards-Curve Digital Signature Algorithm (EdDSA)*. RFC 8032. Jan. 2017. DOI: 10.17487/RFC8032. URL: https://www.rfc-editor.org/info/rfc8032.
[174] Paul J. Leach, Rich Salz und Michael H. Mealling. *A Universally Unique IDentifier (UUID) URN Namespace*. RFC 4122. Juli 2005. DOI: 10.17487/RFC4122. URL: https://www.rfc-editor.org/info/rfc4122.
[175] Steven White u. a. *Handles and objects*. 8. Feb. 2022. URL: https://learn.microsoft.com/en-us/windows/win32/sysinfo/handles-and-objects (besucht am 13. 01. 2024).
[176] Mohamed Abdallah Elakrat und Jae Cheon Jung. "Development of field programmable gate array–based encryption module to mitigate man-in-the-middle attack for nuclear power plant data communication network". In: *Nuclear Engineering and Technology* 50.5 (2018), S. 780–787. ISSN: 1738-5733. DOI: https://doi.org/10.1016/j.net.2018.01.018. URL: https://www.sciencedirect.com/science/article/pii/S173857331730565X.
[177] Paessler AG. *NetFlow monitoring: FAQ*. URL: https://www.paessler.com/netflow_monitoring#faq (besucht am 06. 01. 2024).
[178] Tim Keary. *PCAP: Packet Capture, what it is & what you need to know*. 29. Sep. 2023. URL: https://www.comparitech.com/net-admin/pcap-guide/ (besucht am 06. 01. 2024).
[179] Ari Luotonen und Kevin Altis. "World-Wide Web proxies". In: *Computer Networks and ISDN Systems* 27.2 (1994). Selected Papers of the First World-Wide Web Conference, S. 147–154. ISSN: 0169-7552. DOI: https://doi.org/10.1016/0169-7552(94)90128-7. URL: https://www.sciencedirect.com/science/article/pii/0169755294901287.
[180] Mike Bishop. *HTTP/3*. RFC 9114. Juni 2022. DOI: 10.17487/RFC9114. URL: https://www.rfc-editor.org/info/rfc9114.
[181] Jana Iyengar und Martin Thomson. *QUIC: A UDP-Based Multiplexed and Secure Transport*. RFC 9000. Mai 2021. DOI: 10.17487/RFC9000. URL: https://www.rfc-editor.org/info/rfc9000.
[182] Google. *Chrome is deploying HTTP/3 and IETF QUIC*. 7. Okt. 2020. URL: https://blog.chromium.org/2020/10/chrome-is-deploying-http3-and-ietf-quic.html (besucht am 14. 01. 2024).
[183] Dragana Damjanovic. *QUIC and HTTP/3 Support now in Firefox Nightly and Beta*. 16. Apr. 2021. URL: https://hacks.mozilla.org/2021/04/quic-and-http-3-support-now-in-firefox-nightly-and-beta/ (besucht am 14. 01. 2024).
[184] Kurt Mackie. *Microsoft Embracing Native QUIC in Newer Windows OSes and Edge Browser*. 26. Aug. 2021. URL: https://redmondmag.com/articles/2021/08/26/native-quic-in-windows-edge.aspx (besucht am 14. 01. 2024).
[185] Chris M. Lonvick und Tatu Ylonen. *The Secure Shell (SSH) Protocol Architecture*. RFC 4251. Jan. 2006. DOI: 10.17487/RFC4251. URL: https://www.rfc-editor.org/info/rfc4251.
[186] Cornelsen Verlag GmbH. *Telemetrie, die*. URL: https://www.duden.de/rechtschreibung/Telemetrie (besucht am 26. 12. 2023).

[187] The Tor Project Inc. *Tor Project. History*. URL: https://www.torproject.org/about/history/ (besucht am 28. 12. 2023).
[188] openPR Redaktion. *Whitepaper - Definition und Bedeutung für Ihre PR*. URL: https://www.openpr.de/wiki/whitepaper (besucht am 01. 01. 2024).
[189] Danny Maertens, Tess Gauthier, niknah u. a. *Win32-OpenSSH. my scp'ed files are getting truncated at 204800 bytes after upgrading openssh*. URL: https://github.com/PowerShell/Win32-OpenSSH/issues/2098 (besucht am 03. 02. 2024).
[190] Mohammad Shah Miran und Ashakul Islam Sowad. *4 Methods to Pass Named Parameters in a Bash Script*. 27. Nov. 2023. URL: https://linuxsimply.com/bash-scripting-tutorial/parameters/named-parameters/ (besucht am 21. 01. 2024).
[191] Microsoft. *New-ScheduledTask*. URL: https://learn.microsoft.com/en-us/powershell/module/scheduledtasks/new-scheduledtask (besucht am 21. 01. 2024).

Versionsverzeichnis

Datum	Tätigkeit	Aufwand ca.
15.11.2023	Erstellung Projektskizze Vorbereitung LaTeX Vorlage	8h
04.12.2023	Themenpräsentation Anpassung Projektskizze	1h
22.12.2023	Kickoff Meeting mit Experte (Daniel Röthlisberger)	1h
26.12.2023	Einleitung und Planung	3h
27.12.2023	Recherche zu Browser-Überarbeitungen („New Edge“, „Firefox Quantum“) und bestehenden Arbeiten	2h
28.12.2023	Recherche zu bestehenden Arbeiten, Firefox Download-Token und Tor Browser	3h
31.12.2023	Recherche zu bestehenden Arbeiten, Proxy-Server	4h
01.01.2024	Recherche Privacy Whitepapers von Chrome und Edge	5h
06.01.2024	Recherche Privacy Whitepapers von Edge und Firefox, Tor Browser sowie Aufzeichnung und Analyse auf Netzwerk-Ebene	7h
13.01.2024	Recherche Aufzeichnung und Analyse Aufbau Laborumgebung (Server)	5h
14.01.2024	Aufbau Laborumgebung (Server und Windows-Template)	7h
20.01.2024	Aufbau Laborumgebung (Windows-Template und Malcolm)	7h
21.01.2024	Aufbau Laborumgebung (Analysen-Automatisierung)	8h
28.01.2024	Ergänzungen und Testing Analysen-Automatisierung Dokumentation Analyse-Vorgehen und Abgrenzungen Klonen und Netzwerk-Konfiguration Browser-VMs	6h
03.02.2024	Text-Korrekturen nach Besuch des Moduls „Wissenschaftliches Arbeiten in der Weiterbildung“ Troubleshooting ProcDOT, Process Monitor & Win32-OpenSSH [189] Analyse Windows-Kommunikation	7h
04.02.2024	Analyse Installation und erster Start mit Chrome	6h
08.02.2024	50% Meeting mit Experte (Daniel Röthlisberger)	-
18.02.2024	Analyse Installation und erster Start mit Edge, Firefox & Tor Browser Troubleshooting Tor und Laborumgebung bzw. mitmproxy	8h
19.02.2024	Analyse Privat-Modi und Telemetrie-Trigger	7h
28.02.2024	Analyse Telemetrie-Trigger und Besuch statischer Webseite Start Interpretation und Evaluations-Skript	8h
05.03.2024	90% Meeting mit Experte (Daniel Röthlisberger)	-

Datum	Tätigkeit	Aufwand ca.
06.03.2024	Auswertung Ergebnisse des Evaluations-Skript Interpretation	9h
10.03.2024	Interpretation, Fazit, Rückblick und Ausblick Darstellungs-Anpassungen und Präsentation	6h
13.03.2024	Abstract und Präsentation	5h
16.03.2024	Review, Korrekturen und Ergänzungen	4h
24.03.2024	Review und Abgabe	3h
	Total Aufwand	130h

Tabelle 7.1.: Versionsverzeichnis

Eigenständigkeitserklärung

Hiermit erkläre ich, dass ich die hier vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Sämtliche Ausführungen, die anderen Schriften wörtlich oder sinngemäß entnommen wurden, habe ich als solche kenntlich gemacht.

Hiermit stimme ich zu, dass die vorliegende Arbeit in elektronischer Form mit entsprechender Software überprüft wird.

24. März 2024

Mauro Guadagnini

A. Konfigurationsdateien

A.1. Server `server.lab.internal`

A.1.1. iptables-Ruleset `/etc/iptables/rules.v4`

```
*filter
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
# --------------------------- DON'T ALLOW TRAFFIC BETWEEN CLIENT SUBNETS START
:FORWARD DROP [57:11514]
-A FORWARD -i enp0s3 -p tcp --dport 80 -j ACCEPT
-A FORWARD -i enp0s3 -p tcp --dport 443 -j ACCEPT
-A FORWARD -o enp0s3 -p tcp --dport 80 -j ACCEPT
-A FORWARD -o enp0s3 -p tcp --dport 443 -j ACCEPT
# --------------------------- DON'T ALLOW TRAFFIC BETWEEN CLIENT SUBNETS END
COMMIT
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
# --------------------------- MITMPROXY SETUP FOR CLIENT SUBNETS START
-A PREROUTING -i enp0s8 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 8080
-A PREROUTING -i enp0s8 -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8080
-A PREROUTING -i enp0s9 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 8080
-A PREROUTING -i enp0s9 -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8080
-A PREROUTING -i enp0s10 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 8080
-A PREROUTING -i enp0s10 -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8080
-A PREROUTING -i enp0s16 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 8080
-A PREROUTING -i enp0s16 -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8080
# --------------------------- MITMPROXY SETUP FOR CLIENT SUBNETS END
# --------------------------- NAT START
-A POSTROUTING -o enp0s3 -j MASQUERADE
# --------------------------- NAT END
COMMIT
```

Quelltext A.1: iptables-Ruleset `/etc/iptables/rules.v4` auf `server.lab.internal`

A.1.2. ip6tables-Ruleset /etc/iptables/rules.v6

```
*filter
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
# -------------------------- DON'T ALLOW TRAFFIC BETWEEN CLIENT SUBNETS START
:FORWARD DROP [0:0]
-A FORWARD -i enp0s3 -p tcp --dport 80 -j ACCEPT
-A FORWARD -i enp0s3 -p tcp --dport 443 -j ACCEPT
-A FORWARD -o enp0s3 -p tcp --dport 80 -j ACCEPT
-A FORWARD -o enp0s3 -p tcp --dport 443 -j ACCEPT
# -------------------------- DON'T ALLOW TRAFFIC BETWEEN CLIENT SUBNETS END
COMMIT
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
# -------------------------- MITMPROXY SETUP FOR CLIENT SUBNETS START
-A PREROUTING -i enp0s8 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 8080
-A PREROUTING -i enp0s8 -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8080
-A PREROUTING -i enp0s9 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 8080
-A PREROUTING -i enp0s9 -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8080
-A PREROUTING -i enp0s10 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 8080
-A PREROUTING -i enp0s10 -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8080
-A PREROUTING -i enp0s16 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 8080
-A PREROUTING -i enp0s16 -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8080
# -------------------------- MITMPROXY SETUP FOR CLIENT SUBNETS END
# -------------------------- NAT START
-A POSTROUTING -o enp0s3 -j MASQUERADE
# -------------------------- NAT END
COMMIT
```

Quelltext A.2: ip6tables-Ruleset /etc/iptables/rules.v6 auf server.lab.internal

Für den Umgebung mit dem Tor Browser ist die Konfigurations-Anpassung in Kapitel 5.3.2 zu beachten.

A.1.3. Netzwerk-Konfiguration `/etc/network/interfaces`

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
allow-hotplug enp0s3
iface enp0s3 inet static
address 10.0.100.2/24
gateway 10.0.100.1
# dns-* options are implemented by the resolvconf package, if installed
dns-nameservers 10.0.100.1
dns-search lab.internal
iface enp0s3 inet6 auto

auto enp0s8
allow-hotplug enp0s8
iface enp0s8 inet static
address 192.168.100.1/30
iface enp0s8 inet6 static
address fdb0:8f6e:bc8e:1::1/64

auto enp0s9
allow-hotplug enp0s9
iface enp0s9 inet static
address 192.168.100.5/30
iface enp0s9 inet6 static
address fdb0:8f6e:bc8e:5::1/64

auto enp0s10
allow-hotplug enp0s10
iface enp0s10 inet static
address 192.168.100.9/30
iface enp0s10 inet6 static
address fdb0:8f6e:bc8e:9::1/64

auto enp0s16
allow-hotplug enp0s16
iface enp0s16 inet static
address 192.168.100.13/30
iface enp0s16 inet6 static
address fdb0:8f6e:bc8e:13::1/64
```

Quelltext A.3: Netzwerk-Konfigurationsdatei `/etc/network/interfaces` auf `server.lab.internal`

B. Skripts

B.1. Laborumgebung-Steuerung

```
#!/bin/bash
#
# LAB CONTROL SCRIPT
# Semesterarbeit:     Telemetrie von Desktop-Webbrowser
# Studiengang:        CAS Security Incident Management
# Autor:              Mauro Guadagnini
# Version:            1.1
# Datum:              03.02.2024
#

# FUNCTIONS

function lockcheck {
        # returns false if no lock, true if lock active
        # if file exists, lock is active
        lockfilepath="${lockfilepath}/${filenameprefix}.lock"
        if [ -f ${lockfilepath} ]; then
            return 0
        else
            return 1
        fi
}

function lockset {
    echo "aquiring lock at ${lockfilepath}"
    touch ${lockfilepath}
    if [ $? -ne 0 ]; then
            echo "error at creating ${lockfilepath}, exiting script"
            exit 1
    fi
}

function lockremove {
    echo "removing lock at ${lockfilepath}"
    rm ${lockfilepath}
    if [ $? -ne 0 ]; then
            echo "error at removing ${lockfilepath}, exiting script"
            exit 1
    fi
}

function header {
        echo "########################################"
        echo "LAB CONTROL"
        echo "########################################"
}

function help {
        header
        echo "use 'start' or 'stop' and then 'chrome','edge', 'firefox' or '
           tor'"
        echo "example: $0 start edge"
```

```
52          exit
53  }
54
55  function scheduledtaskregister {
56      sshbrowsercommand='powershell␣$action␣=␣New-ScheduledTaskAction␣-Execute␣
            \"C:\tools\Noriben-2.0\Noriben.py\"␣-Argument␣\"--headless␣--output␣%
            TEMP%\";␣$settings␣=␣New-ScheduledTaskSettingsSet;␣$task␣=␣New-
            ScheduledTask␣-Action␣$action␣-Settings␣$settings;␣Register-
            ScheduledTask␣'${browsernoribenschedtask}'␣-InputObject␣$task'
57      ${sshbrowserconnection} "${sshbrowsercommand}"
58      if [ $? -ne 0 ]; then
59              echo "error␣while␣registering␣scheduled␣task␣${
                    browsernoribenschedtask},␣exiting␣script"
60              lockremove
61              exit 1
62      fi
63      echo "registered␣scheduled␣task␣${browsernoribenschedtask}"
64  }
65
66  function scheduledtaskcheck {
67      sshbrowsercommand='powershell␣$(Get-ScheduledTask␣'${
            browsernoribenschedtask}'␣-ErrorAction␣Ignore).State'
68      schedtaskstate="$(${sshbrowserconnection}␣"${sshbrowsercommand}")"
69      schedtaskstate=$(echo ${schedtaskstate} | grep -E -o "(Ready|Running)")
70      if [ "${schedtaskstate}" = "Ready" ] || [ "${schedtaskstate}" = "Running"
            ]; then
71              echo "${schedtaskstate}"
72      else
73              echo "notinstalled"
74      fi
75  }
76
77  function scheduledtaskstart {
78      taskstate="$(scheduledtaskcheck)"
79      if [ "${taskstate}" == "Running" ]; then
80              echo "Scheduled␣Task␣${browsernoribenschedtask}␣already␣running,␣
                    exiting␣script"
81              lockremove
82              exit 1
83      elif [ "${taskstate}" == "Ready" ]; then
84              sshbrowsercommand='powershell␣Start-ScheduledTask␣'${
                    browsernoribenschedtask}''
85              ${sshbrowserconnection} "${sshbrowsercommand}"
86              if [ $? -ne 0 ]; then
87                      echo "error␣when␣starting␣scheduled␣task␣${
                            browsernoribenschedtask},␣exiting␣script"
88                      lockremove
89                      exit 1
90              fi
91      elif [ "${taskstate}" == "notinstalled" ]; then
92              scheduledtaskregister
93              scheduledtaskstart
94      else
95              echo "Scheduled␣Task␣${browsernoribenschedtask}␣not␣found,␣exiting
                    ␣script"
96              lockremove
97              exit 1
98      fi
```

```
99
100 }
101
102 function startlab {
103     header
104         echo "starting␣lab"
105     if lockcheck; then
106         echo "lab␣is␣already␣running␣for␣${filenameprefix},␣doing␣nothing"
107         exit 1
108     else
109         lockset
110         # STARTING LAB
111
112         # BROWSER HOST
113         scheduledtaskstart
114         sshbrowsercommand='ipconfig␣/flushdns'
115         ${sshbrowserconnection} "${sshbrowsercommand}"
116
117         # SERVER
118         sshservercommand="pgrep␣${mitmcommand}"
119         ${sshserverconnection} ${sshservercommand} > /dev/null
120         if [ $? -eq 0 ]; then
121                 echo "${mitmcommand}␣already␣running␣at␣${sshserverconnection
                        },␣exiting␣script"
122                 lockremove
123                 exit 1
124         fi
125
126         sshservercommand="pgrep␣tshark"
127         ${sshserverconnection} ${sshservercommand} > /dev/null
128         if [ $? -eq 0 ]; then
129                 echo "tshark␣already␣running␣at␣${sshserverconnection},␣
                        exiting␣script"
130                 lockremove
131                 exit 1
132         fi
133
134         sshservercommand="SSLKEYLOGFILE=\"${mitmkeylogfile}\"␣${mitmcommand}␣
                --mode␣transparent␣--showhost␣--no-web-open-browser␣--web-host␣${
                serverhttplisten}␣--web-port␣${serverhttpport}␣-w␣${mitmfile}␣-q"
135         ${sshserverconnection} ${sshservercommand} &
136         if [ $? -ne 0 ]; then
137                 echo "error␣at␣starting␣${mitmcommand}␣at␣${
                        sshserverconnection},␣exiting␣script"
138                 lockremove
139                 exit 1
140         fi
141         echo "started␣${mitmcommand}␣${filenameprefix}"
142
143         sshservercommand="tshark␣-i␣${serverinterfacetobrowser}␣-w␣${pcapfile}
                ␣-Q"
144         ${sshserverconnection} ${sshservercommand} &
145         if [ $? -ne 0 ]; then
146                 echo "error␣at␣starting␣${mitmcommand}␣at␣${
                        sshserverconnection},␣exiting␣script"
147                 echo "PLEASE␣STOP␣${mitmcommand}␣at␣${sshserverconnection}␣
                        MANUALLY!"
148                 lockremove
```

```
149                 exit 1
150         fi
151         echo "started␣tshark␣${filenameprefix}"
152 
153         echo "lab␣started,␣to␣stop␣execute:␣$0␣stop␣$(echo␣$filenameprefix␣|␣
               awk␣-F'-'␣'{print␣$NF}')"
154 
155     fi
156 }
157 
158 function stoplab {
159     header
160     if lockcheck; then
161         echo "stopping␣lab␣for␣${filenameprefix}"
162 
163         # STOPPING LAB
164 
165         # BROWSER HOST
166         taskstate="$(scheduledtaskcheck)"
167         if [ "${taskstate}" == "Running" ]; then
168             while [ "${taskstate}" == "Running" ]; do
169                     echo "Scheduled␣Task␣${browsernoribenschedtask}␣running,␣
                           please␣stop␣in␣browser␣host␣with␣Ctrl+C"
170                     echo "checking␣again␣in␣10s"
171                     sleep 10
172                     taskstate="$(scheduledtaskcheck)"
173             done
174             echo "waiting␣60s␣for␣files␣to␣be␣generated"
175             sleep 60
176         fi
177 
178         tmpnoribenfiles="/tmp/labcontrol_$(uuidgen)"
179         noribenfolder="${noribenfolder}/${filenameprefix}/${timestamp}"
180         mkdir -p ${noribenfolder}
181         sshbrowsercommand='powershell␣"$(gci␣-path␣%TEMP%/Noriben*␣|␣Select-
               Object␣-Last␣4).FullName"'
182         ${sshbrowserconnection} "${sshbrowsercommand}" > ${tmpnoribenfiles}
183         while read -r file; do
184                 filepath="$(printf␣"%s\n"␣"${file}"␣|␣sed␣'s,\\,/,g'␣|␣strings
                       )"
185                 # buffer parameter is workaround because otherwise it would
                       only transmit 200KB (Win32-OpenSSH Issue, https://github.
                       com/PowerShell/Win32-OpenSSH/issues/2098)
186                 scp -q -X buffer=204800 -J ${serveruser}@${serverip}:${
                       serversshport} ${browseruser}@${browserip}:${filepath} ${
                       noribenfolder}/
187                 if [ $? -ne 0 ]; then
188                     echo "error␣while␣getting␣${filepath}␣from␣browser␣host,␣
                           please␣backup␣manually"
189                 fi
190         done <${tmpnoribenfiles}
191         rm ${tmpnoribenfiles}
192 
193         # SERVER
194         sshservercommand="pgrep␣${mitmcommand}"
195         ${sshserverconnection} ${sshservercommand} > /dev/null
196         if [ $? -eq 0 ]; then
197                 # kill ${mitmcommand}
```

```
198                 sshservercommand="pkill␣${mitmcommand}"
199                 ${sshserverconnection} ${sshservercommand}
200                 if [ $? -ne 0 ]; then
201                         echo "error␣at␣killing␣${mitmcommand}␣at␣${
                               sshserverconnection},␣exiting␣script"
202                         exit 1
203                 fi
204                 echo "stopped␣${mitmcommand}"
205
206                 sshservercommand="pgrep␣tshark"
207                 ${sshserverconnection} ${sshservercommand} > /dev/null
208                 if [ $? -eq 0 ]; then
209                         # kill tshark
210                         sshservercommand="pkill␣tshark"
211                         ${sshserverconnection} ${sshservercommand}
212                         if [ $? -ne 0 ]; then
213                                 echo "error␣at␣killing␣tshark␣at␣${
                                       sshserverconnection},␣exiting␣script"
214                                 exit 1
215                         fi
216                         echo "stopped␣tshark"
217                 fi
218
219                 tmppcappattern="$(dirname␣${pcapfile})/${filenameprefix}*pcap"
220                 sshservercommand="ls␣-l␣${tmppcappattern}␣2>␣/dev/null"
221                 tmppcap=$(${sshserverconnection} ${sshservercommand})
222                 if [ $? -eq 0 ]; then
223                     tmppcap="$(echo␣${tmppcap}␣|␣awk␣'{print␣$NF}'␣|␣head␣-1)"
224                 else
225                     tmppcap=""
226                 fi
227
228                 tmpmitmpattern="$(dirname␣${mitmfile})/${filenameprefix}*mitm"
229                 sshservercommand="ls␣-l␣${tmpmitmpattern}␣2>␣/dev/null"
230                 tmpmitm=$(${sshserverconnection} ${sshservercommand})
231                 if [ $? -eq 0 ]; then
232                     tmpmitm="$(echo␣${tmpmitm}␣|␣awk␣'{print␣$NF}'␣|␣head␣-1)"
233                 else
234                     tmpmitm=""
235                 fi
236
237                 tmpsslkeylogfilepattern="$(dirname␣${mitmkeylogfile})/${
                        filenameprefix}*sslkeylogfile.txt"
238                 sshservercommand="ls␣-l␣${tmpsslkeylogfilepattern}␣2>␣/dev/
                        null"
239                 tmpsslkeylogfile="$(${sshserverconnection}␣${sshservercommand
                        })"
240                 if [ $? -eq 0 ]; then
241                     tmpsslkeylogfile="$(echo␣${tmpsslkeylogfile}␣|␣awk␣'{print
                            ␣$NF}'␣|␣head␣-1)"
242                 else
243                     tmpsslkeylogfile=""
244                 fi
245
246                 if [ "${tmppcap}" != "" ] && [ "${tmpsslkeylogfile}" != "" ];
                        then
247                     tmppcapdecrypted="$(echo␣${tmppcap}␣|␣sed␣'s,\.pcap$,\.
                            tlsdecrypted\.pcap,')"
```

```
248                     sshservercommand="editcap␣--inject-secrets␣tls,${
                            tmpsslkeylogfile}␣${tmppcap}␣${tmppcapdecrypted}"
249                     ${sshserverconnection} ${sshservercommand}
250                     if [ $? -ne 0 ]; then
251                             echo "error␣at␣injecting␣${tmpsslkeylogfile}␣in␣${
                                    tmppcap}␣to␣${tmppcapdecrypted}␣on␣${
                                    sshserverconnection},␣exiting␣script"
252                             exit 1
253                     fi
254                     echo "injected␣tls␣secrets␣from␣keylogfile␣to␣new␣pcap"
255                     sshservercommand="rm␣${tmpsslkeylogfile}␣${tmppcap}␣${
                            tmppcapdecrypted}␣${tmpmitm}"
256                 elif [ "${tmppcap}" != "" ] && [ "${tmpsslkeylogfile}" == ""
                        ]; then
257                     echo "no␣sslkeylogfile␣generated,␣maybe␣no␣tls␣traffic␣
                            generated?"
258                     echo "exporting␣original␣pcap"
259                     tmppcapdecrypted="${tmppcap}"
260                     sshservercommand="rm␣${tmpsslkeylogfile}␣${tmppcap}␣${
                            tmpmitm}"
261                 else
262                     echo "error␣at␣getting␣pcap␣and␣keylogfile␣locations,␣
                            exiting␣script"
263                     exit 1
264                 fi
265
266                 mitmfolder="${mitmfolder}/${filenameprefix}/${timestamp}"
267                 mkdir -p ${mitmfolder}
268                 scp -q -P ${serversshport} ${serveruser}@${serverip}:${tmpmitm
                        } ${mitmfolder}/
269                 if [ $? -ne 0 ]; then
270                         echo "error␣at␣copying␣new␣pcap␣from␣${tmpmitm}␣on␣${
                                sshserverconnection}␣to␣${mitmfolder},␣exiting␣
                                script"
271                         exit 1
272                 fi
273                 echo "copied␣new␣mitm␣$(basename␣${tmpmitm})␣to␣${mitmfolder}"
274
275                 pcapfolder="${pcapfolder}/${filenameprefix}/${timestamp}"
276                 mkdir -p ${pcapfolder}
277                 scp -q -P ${serversshport} ${serveruser}@${serverip}:${
                        tmppcapdecrypted} ${pcapfolder}/
278                 if [ $? -ne 0 ]; then
279                         echo "error␣at␣copying␣new␣pcap␣from␣${
                                tmppcapdecrypted}␣on␣${sshserverconnection}␣to␣${
                                pcapfolder},␣exiting␣script"
280                         exit 1
281                 fi
282                 echo "copied␣new␣pcap␣$(basename␣${tmppcapdecrypted})␣to␣${
                        pcapfolder}"
283
284                 ${sshserverconnection} ${sshservercommand}
285                 if [ $? -ne 0 ]; then
286                         echo "error␣at␣removing␣tmp␣files␣on␣${
                                sshserverconnection},␣clean␣up␣manually"
287                         echo "files:␣${tmpsslkeylogfile}␣${tmppcap}␣${
                                tmppcapdecrypted}"
288                 fi
```

```
289
290                 echo "lab␣${filenameprefix}␣stopped,␣check␣${pcapfolder}"
291
292         else
293                 echo "${mitmcommand}␣not␣running␣at␣${sshserverconnection},␣
                        exiting␣script"
294                 exit 1
295         fi
296
297         lockremove
298         exit 0
299
300     else
301         echo "no␣lock␣file␣found␣at␣${lockfilepath},␣assuming␣no␣lab␣running,␣
                exiting␣script"
302         exit 1
303     fi
304 }
305
306 # VARIABLES
307 serverip="192.168.0.208"
308 serversshport="22221"
309 serverhttplisten="10.0.100.2"
310 serverhttpport="8081"
311 serveruser="user"
312 sshserverconnection="ssh␣${serveruser}@${serverip}␣-p␣${serversshport}"
313 serverinterfacetobrowser=""
314 mitmcommand="mitmweb"
315 mitmkeylogfile="/tmp"
316 mitmfile="/tmp"
317 pcapfile="/tmp"
318
319 browserip=""
320 browsersshport="22"
321 browseruser="browser"
322 sshbrowserconnection="ssh␣-J␣${serveruser}@${serverip}:${serversshport}␣${
       browseruser}@"
323
324 filenameprefix="lab"
325 lockfilepath="/var/lock"
326 timestamp=$(date +%Y%m%d-%H%M)
327 mitmfolder="/home/usr/src/BFH23_SIM/semesterarbeit/data"
328 pcapfolder="/home/usr/src/BFH23_SIM/semesterarbeit/data"
329 noribenfolder="/home/usr/src/BFH23_SIM/semesterarbeit/data"
330
331 # MAIN
332 options=$(getopt -o "" -l "start:,stop:" "$@")
333 eval set $options
334
335 if [ $# -eq 0 ]; then
336         help
337 fi
338
339 while [ $# -gt 0 ]; do
340         case $1 in
341                 start) action=1;;
342                 stop)  action=0;;
343                 *) help
```

```
        esac

        case $2 in
                chrome)
                        browserip="192.168.100.2"
                        serverinterfacetobrowser="enp0s8"
                        filenameprefix="${filenameprefix}-$2"
                        shift;;
                edge)
                        browserip="192.168.100.6"
                        serverinterfacetobrowser="enp0s9"
                        filenameprefix="${filenameprefix}-$2"
                        shift;;
                firefox)
                        browserip="192.168.100.10"
                        serverinterfacetobrowser="enp0s10"
                        filenameprefix="${filenameprefix}-$2"
                        shift;;
                tor)
                        browserip="192.168.100.14"
                        serverinterfacetobrowser="enp0s16"
                        filenameprefix="${filenameprefix}-$2"
                        shift;;
                *)      help; shift;;
        esac

        shift
done

# VARIABLES AFTER OPTION EVALUATION
mitmkeylogfile="${mitmkeylogfile}/${filenameprefix}-${timestamp}-sslkeylogfile
    .txt"
mitmfile="${mitmfile}/${filenameprefix}-${timestamp}.mitm"
pcapfile="${pcapfile}/${filenameprefix}-${timestamp}.pcap"
sshbrowserconnection="${sshbrowserconnection}${browserip}"
browsernoribenschedtask="${filenameprefix}-noriben"

if [ $action -eq 1 ]; then
        startlab
else
        stoplab
fi
```

Quelltext B.1: Steuerung der Laborumgebung `lab_control.sh` [190][191][189]

B.2. Laborumgebung-Auswertung

```
#!/bin/bash
#
# LAB EVALUATION SCRIPT
# Semesterarbeit:     Telemetrie von Desktop-Webbrowser
# Studiengang:        CAS Security Incident Management
# Autor:              Mauro Guadagnini
# Version:            1.0
# Datum:              28.02.2024
#

# MAIN
datafolder="/home/usr/src/BFH23_SIM/semesterarbeit/data"
labfolderprefix="lab-"
evaluationfolderprefix="eval"
timestamp=$(date +%Y%m%d-%H%M)

echo "########################################"
echo "LAB EVALUATE"
echo "########################################"

# for each lab folder
find ${datafolder} -type d | while read -r folder; do
pushd ${folder} > /dev/null
    # if folder contains pcap and noriben file start
    if [[ $(find . -type f -maxdepth 1 -name "*.pcap") && $(find . -type f -maxdepth 1 -name "Noriben*[0-9].csv") ]]; then
        currentlab=$(echo ${folder} | grep -o "${labfolderprefix}[^/]*")
        currentfolder=$(echo ${folder} | awk -F'/' '{print $NF}')
        currentexecontains=$(echo ${currentlab} | cut -d"-" -f2)
        if [[ ${currentexecontains} == "tor" ]]; then
                currentexecontains="firefox"
        fi
        evaluationfolder="${datafolder}/${currentlab}/${evaluationfolderprefix}-${timestamp}"
        pcaptxt="${evaluationfolder}/${currentfolder}-tshark-http.txt"
        mkdir -p ${evaluationfolder}
        echo "Evaluating ${currentlab}, folder: ${folder}, writing in ${evaluationfolder}"

        # HTTP / HTTP2
        tshark -r *.pcap -Y "($(grep -F TCP Noriben*[0-9].csv | grep -i ${currentexecontains} | awk -F',' '{print $5}' | sort | uniq | sed 's,.*->\ \([^"]*\):443",ip.dst\ ==\ \1\ ||\ ,g' | sed 's,.*->\ \([^"]*\):80",ip.dst\ ==\ \1\ ||\ ,g' | grep -Fv "127.0.0.1" | sed 's,ip\.dst\ ==\ \([^:]*:\),ipv6.dst\ ==\ \1,g' | sed -z 's,\n,,g' | sed 's,\ ||\ $,,g') && (http || http2))" -T fields -e frame.number -e frame.len -e ipv6.src -e ipv6.dst -e ip.src -e ip.dst -e http.request.full_uri -e http.chunk_data -e http.file_data -e http.request.method -e http.referer -e http2.request.full_uri -e http2.headers.method -e http2.header.unescaped -e http2.data.data -e json.member_with_value -e xml 2>&1 | awk '{if ($4 == "") next; print $0}' >> ${pcaptxt} 2>&1
        # collect all in single file for lab
        cat ${pcaptxt} >> "${evaluationfolder}/all.txt" 2>&1
        grep -Eoi "[^&;,]{3,10}[0-9a-f]{8}-?[0-9a-f]{4}-?[0-9a-f]{4}-?[0-9a-f]{4}-?[0-9a-f]{12}" ${pcaptxt} >> "${evaluationfolder}/guid.txt"
```

```
            2>&1
42
43          # try to get hex data and parse it
44          i=0
45          grep -Eio "[^a-f0-9][a-f0-9]{32}[a-f0-9]*" ${pcaptxt} | sed 's,^.,,g'
                | sort | uniq | while read -r hexstring; do
46              echo ${hexstring} | xxd -r -p > "${pcaptxt}.hexparse.${i}"
47              file "${pcaptxt}.hexparse.${i}" >> "${pcaptxt}.hexparse.txt"
48              file "${pcaptxt}.hexparse.${i}" >> "${pcaptxt}.hexparse.file.txt"
49              cat "${pcaptxt}.hexparse.${i}" >> "${pcaptxt}.hexparse.txt"
50              strings "${pcaptxt}.hexparse.${i}" >> "${pcaptxt}.hexparse.txt"
51              strings -el "${pcaptxt}.hexparse.${i}" >> "${pcaptxt}.hexparse.txt
                    "
52              gzip -cd "${pcaptxt}.hexparse.${i}" >> "${pcaptxt}.hexparse.${i}.
                    gunzip" 2>&1
53              file "${pcaptxt}.hexparse.${i}.gunzip" >> "${pcaptxt}.hexparse.txt
                    "
54              file "${pcaptxt}.hexparse.${i}.gunzip" >> "${pcaptxt}.hexparse.
                    file.txt"
55              cat "${pcaptxt}.hexparse.${i}.gunzip" >> "${pcaptxt}.hexparse.txt"
56              strings "${pcaptxt}.hexparse.${i}.gunzip" >> "${pcaptxt}.hexparse.
                    txt"
57              strings -el "${pcaptxt}.hexparse.${i}.gunzip" >> "${pcaptxt}.
                    hexparse.txt"
58              rm "${pcaptxt}.hexparse.${i}"
59              rm "${pcaptxt}.hexparse.${i}.gunzip"
60              ((i++))
61          done
62
63          # evaluate unique file types
64          cat "${pcaptxt}.hexparse.file.txt" 2> /dev/null | awk '{$1="";␣print␣
                $0}' | sort | uniq -c >> "${pcaptxt}.hexparse.file.uniq"
65          # collect all in single file for lab
66          cat "${pcaptxt}.hexparse.txt" >> "${evaluationfolder}/all.txt" 2>&1
67          grep -Eoi "[^&;,]{3,10}[0-9a-f]{8}-?[0-9a-f]{4}-?[0-9a-f]{4}-?[0-9a-f
                ]{4}-?[0-9a-f]{12}" "${pcaptxt}.hexparse.txt" >> "${
                evaluationfolder}/guid.txt" 2>&1
68
69      fi
70  popd > /dev/null
71  done
72
73  # evaluate guid.txt files with timestamp from this script
74  echo "Sorting␣and␣counting␣found␣guids␣in␣this␣evaluation␣(${timestamp})"
75  find ${datafolder} -type f -wholename "*${evaluationfolderprefix}-${timestamp
        }/guid.txt" | while read -r guidfile; do
76      cat ${guidfile} | sort | uniq -ci | sort -nr >> "${guidfile}.sorted" 2>&1
77  done
78  echo "done"
```

Quelltext B.2: Auswertung der Laborumgebung `lab_evaluate.sh`

C. Aufzeichnungen Dateiliste

Sämtliche Aufzeichnungen in entsprechenden Dateien sind dieser Arbeit ebenfalls beigelegt.
Es folgt eine Auflistung entsprechender Dateien:

```
lab-chrome/20240203-1713-windows
  6576.png (68 KB)
  lab-chrome-20240203-1712.mitm (1292 KB)
  lab-chrome-20240203-1712.tlsdecrypted.pcap (5264 KB)
  Noriben_03_Feb_24__17_12_955129.csv (1128 KB)
  Noriben_03_Feb_24__17_12_955129.pml (2540 KB)
  Noriben_03_Feb_24__17_12_955129_timeline.csv (128 KB)
  Noriben_03_Feb_24__17_12_955129.txt (116 KB)
  Screenshot from 2024-02-03 17-18-44.png (24 KB)
  Screenshot from 2024-02-03 17-19-08.png (24 KB)
  Screenshot from 2024-02-03 18-17-15.png (128 KB)

lab-chrome/20240204-1035-install
  lab-chrome-20240204-1028.mitm (147588 KB)
  lab-chrome-20240204-1028.tlsdecrypted.pcap (208324 KB)
  newtab.png (36 KB)
  Noriben_04_Feb_24__10_29_088515.csv (24668 KB)
  Noriben_04_Feb_24__10_29_088515.pml (32208 KB)
  Noriben_04_Feb_24__10_29_088515_timeline.csv (388 KB)
  Noriben_04_Feb_24__10_29_088515.txt (376 KB)
  Screenshot from 2024-02-04 12-50-35.png (188 KB)
  Screenshot from 2024-02-04 13-15-11.png (280 KB)
  Screenshot from 2024-02-04 15-32-08.png (104 KB)
  Screenshot from 2024-02-04 15-32-31.png (28 KB)

lab-chrome/20240219-1022-privatmodus
  lab-chrome-20240219-1022.mitm (10000 KB)
  lab-chrome-20240219-1022.tlsdecrypted.pcap (16316 KB)
  Noriben_19_Feb_24__10_22_069784.csv (2372 KB)
  Noriben_19_Feb_24__10_22_069784.pml (3364 KB)
  Noriben_19_Feb_24__10_22_069784_timeline.csv (24 KB)
  Noriben_19_Feb_24__10_22_069784.txt (24 KB)

lab-chrome/20240219-1453-telemetrytrigger
  lab-chrome-20240219-1449.mitm (61792 KB)
  lab-chrome-20240219-1449.tlsdecrypted.pcap (111724 KB)
  Noriben_19_Feb_24__14_49_538916.csv (24392 KB)
  Noriben_19_Feb_24__14_49_538916.pml (36616 KB)
  Noriben_19_Feb_24__14_49_538916_timeline.csv (1220 KB)
  Noriben_19_Feb_24__14_49_538916.txt (1152 KB)

lab-chrome/20240219-1501-telemetrytrigger-private
  lab-chrome-20240219-1457.mitm (58096 KB)
  lab-chrome-20240219-1457.tlsdecrypted.pcap (96616 KB)
  Noriben_19_Feb_24__14_57_592054.csv (19812 KB)
  Noriben_19_Feb_24__14_57_592054.pml (29644 KB)
  Noriben_19_Feb_24__14_57_592054_timeline.csv (976 KB)
  Noriben_19_Feb_24__14_57_592054.txt (920 KB)
```

```
lab-chrome/20240228-0925-stat
  lab-chrome-20240228-0923.mitm (4668 KB)
  lab-chrome-20240228-0923.tlsdecrypted.pcap (11032 KB)
  Noriben_28_Feb_24__09_24_331616.csv (2024 KB)
  Noriben_28_Feb_24__09_24_331616.pml (4040 KB)
  Noriben_28_Feb_24__09_24_331616_timeline.csv (104 KB)
  Noriben_28_Feb_24__09_24_331616.txt (104 KB)

lab-chrome/20240228-0925-stat-private
  lab-chrome-20240228-0925.mitm (44 KB)
  lab-chrome-20240228-0925.tlsdecrypted.pcap (2620 KB)
  Noriben_28_Feb_24__09_25_541945.csv (648 KB)
  Noriben_28_Feb_24__09_25_541945.pml (1752 KB)
  Noriben_28_Feb_24__09_25_541945_timeline.csv (20 KB)
  Noriben_28_Feb_24__09_25_541945.txt (16 KB)

lab-chrome/eval-20240228-1700
  20240203-1713-windows-tshark-http.txt (4 KB)
  20240203-1713-windows-tshark-http.txt.hexparse.file.uniq (0 KB)
  20240204-1035-install-tshark-http.txt (300 KB)
  20240204-1035-install-tshark-http.txt.hexparse.file.txt (8 KB)
  20240204-1035-install-tshark-http.txt.hexparse.file.uniq (4 KB)
  20240204-1035-install-tshark-http.txt.hexparse.txt (140 KB)
  20240219-1022-privatmodus-tshark-http.txt (208 KB)
  20240219-1022-privatmodus-tshark-http.txt.hexparse.file.txt (4 KB)
  20240219-1022-privatmodus-tshark-http.txt.hexparse.file.uniq (4 KB)
  20240219-1022-privatmodus-tshark-http.txt.hexparse.txt (108 KB)
  20240219-1453-telemetrytrigger-tshark-http.txt (6704 KB)
  20240219-1453-telemetrytrigger-tshark-http.txt.hexparse.file.txt (148 KB)
  20240219-1453-telemetrytrigger-tshark-http.txt.hexparse.file.uniq (8 KB)
  20240219-1453-telemetrytrigger-tshark-http.txt.hexparse.txt (2640 KB)
  20240219-1501-telemetrytrigger-private-tshark-http.txt (6228 KB)
  20240219-1501-telemetrytrigger-private-tshark-http.txt.hexparse.file.txt (148 KB)
  20240219-1501-telemetrytrigger-private-tshark-http.txt.hexparse.file.uniq (8 KB)
  20240219-1501-telemetrytrigger-private-tshark-http.txt.hexparse.txt (2664 KB)
  20240228-0925-stat-private-tshark-http.txt (16 KB)
  20240228-0925-stat-private-tshark-http.txt.hexparse.file.txt (4 KB)
  20240228-0925-stat-private-tshark-http.txt.hexparse.file.uniq (4 KB)
  20240228-0925-stat-private-tshark-http.txt.hexparse.txt (8 KB)
  20240228-0925-stat-tshark-http.txt (48 KB)
  20240228-0925-stat-tshark-http.txt.hexparse.file.txt (4 KB)
  20240228-0925-stat-tshark-http.txt.hexparse.file.uniq (4 KB)
  20240228-0925-stat-tshark-http.txt.hexparse.txt (8 KB)
  all.txt (19052 KB)
  guid.txt (6000 KB)
  guid.txt.sorted (4020 KB)
```

```
lab-edge/20240218-1042-firstrun
  05_edge_firstrun.png (428 KB)
  lab-edge-20240218-1029.mitm (166260 KB)
  lab-edge-20240218-1029.tlsdecrypted.pcap (371340 KB)
  Noriben_18_Feb_24__10_30_984540.csv (84368 KB)
  Noriben_18_Feb_24__10_30_984540.pml (109284 KB)
  Noriben_18_Feb_24__10_30_984540_timeline.csv (3928 KB)
  Noriben_18_Feb_24__10_30_984540.txt (3716 KB)

lab-edge/20240219-1107-privatmodus
  lab-edge-20240219-1106.mitm (3792 KB)
  lab-edge-20240219-1106.tlsdecrypted.pcap (10732 KB)
  Noriben_19_Feb_24__11_06_986655.csv (2548 KB)
  Noriben_19_Feb_24__11_06_986655.pml (4116 KB)
  Noriben_19_Feb_24__11_06_986655_timeline.csv (132 KB)
  Noriben_19_Feb_24__11_06_986655.txt (132 KB)
  smartscreen.png (200 KB)

lab-edge/20240219-1510-telemetrytrigger
  lab-edge-20240219-1504.mitm (59608 KB)
  lab-edge-20240219-1504.tlsdecrypted.pcap (166096 KB)
  Noriben_19_Feb_24__15_04_289858.csv (47576 KB)
  Noriben_19_Feb_24__15_04_289858.pml (70212 KB)
  Noriben_19_Feb_24__15_04_289858_timeline.csv (1676 KB)
  Noriben_19_Feb_24__15_04_289858.txt (1584 KB)
  Screenshot from 2024-02-19 15-07-50.png (168 KB)
  Screenshot from 2024-02-19 19-20-01.png (144 KB)

lab-edge/20240219-1523-telemetrytrigger-private
  lab-edge-20240219-1519.mitm (61724 KB)
  lab-edge-20240219-1519.tlsdecrypted.pcap (142636 KB)
  Noriben_19_Feb_24__15_20_162855.csv (38860 KB)
  Noriben_19_Feb_24__15_20_162855.pml (48516 KB)
  Noriben_19_Feb_24__15_20_162855_timeline.csv (2664 KB)
  Noriben_19_Feb_24__15_20_162855.txt (2596 KB)

lab-edge/20240228-0942-stat
  lab-edge-20240228-0941.mitm (10180 KB)
  lab-edge-20240228-0941.tlsdecrypted.pcap (28500 KB)
  Noriben_28_Feb_24__09_41_289551.csv (7068 KB)
  Noriben_28_Feb_24__09_41_289551.pml (11408 KB)
  Noriben_28_Feb_24__09_41_289551_timeline.csv (208 KB)
  Noriben_28_Feb_24__09_41_289551.txt (196 KB)

lab-edge/20240228-0943-stat-private
  lab-edge-20240228-0942.mitm (884 KB)
  lab-edge-20240228-0942.tlsdecrypted.pcap (9856 KB)
  Noriben_28_Feb_24__09_42_762524.csv (3164 KB)
  Noriben_28_Feb_24__09_42_762524.pml (5348 KB)
  Noriben_28_Feb_24__09_42_762524_timeline.csv (92 KB)
  Noriben_28_Feb_24__09_42_762524.txt (92 KB)
```

```
lab-edge/eval-20240228-1700
  20240218-1042-firstrun-tshark-http.txt (4648 KB)
  20240218-1042-firstrun-tshark-http.txt.hexparse.file.txt (64 KB)
  20240218-1042-firstrun-tshark-http.txt.hexparse.file.uniq (4 KB)
  20240218-1042-firstrun-tshark-http.txt.hexparse.txt (1132 KB)
  20240219-1107-privatmodus-tshark-http.txt (92 KB)
  20240219-1107-privatmodus-tshark-http.txt.hexparse.file.txt (4 KB)
  20240219-1107-privatmodus-tshark-http.txt.hexparse.file.uniq (4 KB)
  20240219-1107-privatmodus-tshark-http.txt.hexparse.txt (16 KB)
  20240219-1510-telemetrytrigger-tshark-http.txt (8608 KB)
  20240219-1510-telemetrytrigger-tshark-http.txt.hexparse.file.txt (216 KB)
  20240219-1510-telemetrytrigger-tshark-http.txt.hexparse.file.uniq (12 KB)
  20240219-1510-telemetrytrigger-tshark-http.txt.hexparse.txt (3292 KB)
  20240219-1523-telemetrytrigger-private-tshark-http.txt (7352 KB)
  20240219-1523-telemetrytrigger-private-tshark-http.txt.hexparse.file.txt (216 KB)
  20240219-1523-telemetrytrigger-private-tshark-http.txt.hexparse.file.uniq (8 KB)
  20240219-1523-telemetrytrigger-private-tshark-http.txt.hexparse.txt (2952 KB)
  20240228-0942-stat-tshark-http.txt (288 KB)
  20240228-0942-stat-tshark-http.txt.hexparse.file.txt (12 KB)
  20240228-0942-stat-tshark-http.txt.hexparse.file.uniq (4 KB)
  20240228-0942-stat-tshark-http.txt.hexparse.txt (80 KB)
  20240228-0943-stat-private-tshark-http.txt (28 KB)
  20240228-0943-stat-private-tshark-http.txt.hexparse.file.txt (4 KB)
  20240228-0943-stat-private-tshark-http.txt.hexparse.file.uniq (4 KB)
  20240228-0943-stat-private-tshark-http.txt.hexparse.txt (8 KB)
  all.txt (28484 KB)
  guid.txt (7564 KB)
  guid.txt.sorted (4264 KB)

lab-firefox/20240218-1322-installandfirstrun
  lab-firefox-20240218-1317.mitm (212716 KB)
  lab-firefox-20240218-1317.tlsdecrypted.pcap (449608 KB)
  Noriben_18_Feb_24__13_18_210754.csv (99332 KB)
  Noriben_18_Feb_24__13_18_210754.pml (139260 KB)
  Noriben_18_Feb_24__13_18_210754_timeline.csv (2600 KB)
  Noriben_18_Feb_24__13_18_210754.txt (2476 KB)

lab-firefox/20240219-1146-privatmodus
  lab-firefox-20240219-1145.mitm (7208 KB)
  lab-firefox-20240219-1145.tlsdecrypted.pcap (24824 KB)
  Noriben_19_Feb_24__11_45_985100.csv (6732 KB)
  Noriben_19_Feb_24__11_45_985100.pml (10508 KB)
  Noriben_19_Feb_24__11_45_985100_timeline.csv (352 KB)
  Noriben_19_Feb_24__11_45_985100.txt (336 KB)

lab-firefox/20240219-1543-telemetry
  lab-firefox-20240219-1535.mitm (53432 KB)
  lab-firefox-20240219-1535.tlsdecrypted.pcap (154992 KB)
  Noriben_19_Feb_24__15_35_760334.csv (42640 KB)
  Noriben_19_Feb_24__15_35_760334.pml (72960 KB)
  Noriben_19_Feb_24__15_35_760334_timeline.csv (1252 KB)
  Noriben_19_Feb_24__15_35_760334.txt (1208 KB)
  Screenshot from 2024-02-28 10-44-32.png (104 KB)
```

```
lab-firefox/20240219-1552-telemetrytrigger-private
  lab-firefox-20240219-1548.mitm (35652 KB)
  lab-firefox-20240219-1548.tlsdecrypted.pcap (93392 KB)
  Noriben_19_Feb_24__15_48_080209.csv (24708 KB)
  Noriben_19_Feb_24__15_48_080209.pml (40980 KB)
  Noriben_19_Feb_24__15_48_080209_timeline.csv (704 KB)
  Noriben_19_Feb_24__15_48_080209.txt (668 KB)
  Screenshot from 2024-02-19 15-51-29.png (104 KB)

lab-firefox/20240228-0947-stat
  lab-firefox-20240228-0946.mitm (20820 KB)
  lab-firefox-20240228-0946.tlsdecrypted.pcap (35512 KB)
  Noriben_28_Feb_24__09_46_382501.csv (5308 KB)
  Noriben_28_Feb_24__09_46_382501.pml (9112 KB)
  Noriben_28_Feb_24__09_46_382501_timeline.csv (96 KB)
  Noriben_28_Feb_24__09_46_382501.txt (92 KB)

lab-firefox/20240228-0948-stat-private
  lab-firefox-20240228-0947.mitm (360 KB)
  lab-firefox-20240228-0947.tlsdecrypted.pcap (2468 KB)
  Noriben_28_Feb_24__09_48_744496.csv (424 KB)
  Noriben_28_Feb_24__09_48_744496.pml (1500 KB)
  Noriben_28_Feb_24__09_48_744496_timeline.csv (20 KB)
  Noriben_28_Feb_24__09_48_744496.txt (20 KB)

lab-firefox/eval-20240228-1700
  20240218-1322-installandfirstrun-tshark-http.txt (1136 KB)
  20240218-1322-installandfirstrun-tshark-http.txt.hexparse.file.txt (8 KB)
  20240218-1322-installandfirstrun-tshark-http.txt.hexparse.file.uniq (4 KB)
  20240218-1322-installandfirstrun-tshark-http.txt.hexparse.txt (80 KB)
  20240219-1146-privatmodus-tshark-http.txt (208 KB)
  20240219-1146-privatmodus-tshark-http.txt.hexparse.file.txt (4 KB)
  20240219-1146-privatmodus-tshark-http.txt.hexparse.file.uniq (4 KB)
  20240219-1146-privatmodus-tshark-http.txt.hexparse.txt (24 KB)
  20240219-1543-telemetry-tshark-http.txt (9768 KB)
  20240219-1543-telemetry-tshark-http.txt.hexparse.file.txt (276 KB)
  20240219-1543-telemetry-tshark-http.txt.hexparse.file.uniq (12 KB)
  20240219-1543-telemetry-tshark-http.txt.hexparse.txt (4280 KB)
  20240219-1552-telemetrytrigger-private-tshark-http.txt (4336 KB)
  20240219-1552-telemetrytrigger-private-tshark-http.txt.hexparse.file.txt (108 KB)
  20240219-1552-telemetrytrigger-private-tshark-http.txt.hexparse.file.uniq (4 KB)
  20240219-1552-telemetrytrigger-private-tshark-http.txt.hexparse.txt (1948 KB)
  20240228-0947-stat-tshark-http.txt (684 KB)
  20240228-0947-stat-tshark-http.txt.hexparse.file.txt (12 KB)
  20240228-0947-stat-tshark-http.txt.hexparse.file.uniq (4 KB)
  20240228-0947-stat-tshark-http.txt.hexparse.txt (532 KB)
  20240228-0948-stat-private-tshark-http.txt (4 KB)
  20240228-0948-stat-private-tshark-http.txt.hexparse.file.uniq (0 KB)
  all.txt (22980 KB)
  guid.txt (6820 KB)
  guid.txt.sorted (4252 KB)
```

```
lab-tor
  Screenshot from 2024-02-18 18-02-46.png (44 KB)

lab-tor/20240218-1528-installandfirstrun
  lab-tor-20240218-1517.mitm (67784 KB)
  lab-tor-20240218-1517.tlsdecrypted.pcap (155168 KB)
  Noriben_18_Feb_24__15_17_568267.csv (36600 KB)
  Noriben_18_Feb_24__15_17_568267.pml (45712 KB)
  Noriben_18_Feb_24__15_17_568267_timeline.csv (1452 KB)
  Noriben_18_Feb_24__15_17_568267.txt (1364 KB)
  Screenshot from 2024-02-18 15-20-15.png (40 KB)

lab-tor/20240218-1609-torconnect-failed
  lab-tor-20240218-1553.tlsdecrypted.pcap (57520 KB)
  lab-tor-REGULAR-20240218-1553.mitm (296 KB)
  Noriben_18_Feb_24__15_53_323612.csv (15356 KB)
  Noriben_18_Feb_24__15_53_323612.pml (23716 KB)
  Noriben_18_Feb_24__15_53_323612_timeline.csv (600 KB)
  Noriben_18_Feb_24__15_53_323612.txt (564 KB)

lab-tor/20240218-1809-torconnect-failedagain
  lab-tor-20240218-1801.mitm (8552 KB)
  lab-tor-20240218-1801.tlsdecrypted.pcap (70000 KB)
  Noriben_18_Feb_24__18_01_226509.csv (12988 KB)
  Noriben_18_Feb_24__18_01_226509.pml (19056 KB)
  Noriben_18_Feb_24__18_01_226509_timeline.csv (408 KB)
  Noriben_18_Feb_24__18_01_226509.txt (392 KB)
  Screenshot from 2024-02-18 18-46-09.png (44 KB)

lab-tor/20240218-1835-connected-updated-closed
  lab-tor-20240218-1827.mitm (724 KB)
  lab-tor-20240218-1827.tlsdecrypted.pcap (229440 KB)
  Noriben_18_Feb_24__18_27_101711.csv (64784 KB)
  Noriben_18_Feb_24__18_27_101711.pml (101796 KB)
  Noriben_18_Feb_24__18_27_101711_timeline.csv (4200 KB)
  Noriben_18_Feb_24__18_27_101711.txt (3888 KB)

lab-tor/eval-20240228-1700
  20240218-1528-installandfirstrun-tshark-http.txt (4 KB)
  20240218-1528-installandfirstrun-tshark-http.txt.hexparse.file.uniq (0 KB)
  20240218-1609-torconnect-failed-tshark-http.txt (4 KB)
  20240218-1609-torconnect-failed-tshark-http.txt.hexparse.file.uniq (0 KB)
  20240218-1809-torconnect-failedagain-tshark-http.txt (4 KB)
  20240218-1809-torconnect-failedagain-tshark-http.txt.hexparse.file.uniq (0 KB)
  20240218-1835-connected-updated-closed-tshark-http.txt (4 KB)
  20240218-1835-connected-updated-closed-tshark-http.txt.hexparse.file.uniq (0 KB)
  all.txt (4 KB)
  guid.txt (4 KB)
  guid.txt.sorted (4 KB)
```

Quelltext C.1: Dateien, die dieser Arbeit digital beigelegt sind

D. Analyse-Ausschnitte

Dieses Kapitel beinhaltet Analyse-Ausschnitte zur zusätzlichen Belegung der Befunde dieser Arbeit. Die Quelltext-Beschriftungen befinden sich ab hier vor dem Inhalt.

Sämtliche Aufzeichnungen sind dieser Arbeit beigelegt (siehe Kapitel C). Entsprechend verwendete Quelldaten sind zu Beginn des entsprechenden Ausschnitts ersichtlich oder anhand der Quelltext-Beschreibung ermittelbar.

D.1. Windows-Kommunikation („Grundrauschen“)

Quelltext D.1: Analyse Windows-Kommunikation („Grundrauschen“): Kommunikation des OneDrive-Prozesses mit ID 5732

```
$ tshark -r lab-chrome-20240203-1712.tlsdecrypted.pcap -Y "(ip.addr == 192.229.221.185
    || ip.addr == 52.113.194.132) && (http || http2)" | awk '{$1=$2=""; print $0}'
192.168.100.2 → 192.229.221.185 HTTP 616 GET /16.000/Converged_v22057_mG-wAdV--
   _sq1kXms675SA2.css HTTP/1.1
192.229.221.185 → 192.168.100.2 TLSv1.3 4306 [TLS segment of a reassembled PDU]HTTP
   /1.1 200 OK (text/css)
192.168.100.2 → 192.229.221.185 HTTP 646 GET /16.000/content/js/
   ConvergedLoginPaginatedStrings.en-gb_K56Wnj7b56kCvr6wXPBBQQ2.js HTTP/1.1
192.229.221.185 → 192.168.100.2 HTTP 9913 HTTP/1.1 200 OK (application/x-javascript)
192.168.100.2 → 192.229.221.185 HTTP 634 GET /shared/1.0/content/js/
   ConvergedLogin_PCore_yZQmhMbiqPW1IsJcdAPQ0A2.js HTTP/1.1
192.229.221.185 → 192.168.100.2 TLSv1.3 35511 [TLS segment of a reassembled PDU]HTTP
   /1.1 200 OK (application/x-javascript)
192.168.100.2 → 192.229.221.185 HTTP 616 GET /shared/1.0/content/js/
   oneDs_f2e0f4a029670f10d892.js HTTP/1.1
192.229.221.185 → 192.168.100.2 TLSv1.3 14474 [TLS segment of a reassembled PDU]HTTP
   /1.1 200 OK (application/x-javascript)
192.168.100.2 → 52.113.194.132 HTTP 479 GET /config/v1/ODSP_Sync_Client
   /22.012.0117.0003?UpdateRing=Prod&OS=Win&OSVer=10.0.22631&OSSku=101&accountType=
   Consumer&clientid=941a0e7c-f373-6ed4-38f5-a17c15af4a43 HTTP/1.1
52.113.194.132 → 192.168.100.2 HTTP/JSON 425 HTTP/1.1 200 OK , JavaScript Object
   Notation (application/json)
```

Quelltext D.2: Analyse Windows-Kommunikation („Grundrauschen“): Kommunikation des Prozesses mit ID 6576

```
$ tshark -r lab-chrome-20240203-1712.tlsdecrypted.pcap -Y "(ip.addr == 68.219.88.225 || ip.addr == 23.212.193.84 || ip.addr == 2.21.22.184) && (http || http2)" | awk '{$1=$2=""; print $0}'
...
192.168.100.2 → 68.219.88.225 HTTP2 149 HEADERS[3]: GET /odclientsettings/Prod?OneDriveUpdate=57415d3812ee8426fca720b98137
68.219.88.225 → 192.168.100.2 HTTP2 117 HEADERS[3]: 302 Found
192.168.100.2 → 23.212.193.84 HTTP 381 GET /PreSignInSettings/Prod/2022-09-17-00-05-23/PreSignInSettingsConfig.json?OneDriveUpdate=57415d3812ee8426fca720b98137 HTTP/1.1
23.212.193.84 → 192.168.100.2 HTTP/JSON 2216 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
192.168.100.2 → 2.21.22.184 HTTP 407 HEAD /filestreamingservice/files/ef5f792e-9df7-4748-accf-02ec33a4a2c4?P1=1707508670&P2=404&P3=2&P4=JxXzBSOP2bhNWgzmvIStnTMQLorxbPGAmd1gJwOZzaodjyy1xw%2bs5z%2fL3R3wE81daADWnmMHzd9Pz64qtzT86w%3d%3d HTTP/1.1
2.21.22.184 → 192.168.100.2 HTTP 873 HTTP/1.1 200 OK
192.168.100.2 → 2.21.22.184 HTTP 479 GET /filestreamingservice/files/ef5f792e-9df7-4748-accf-02ec33a4a2c4?P1=1707508670&P2=404&P3=2&P4=JxXzBSOP2bhNWgzmvIStnTMQLorxbPGAmd1gJwOZzaodjyy1xw%2bs5z%2fL3R3wE81daADWnmMHzd9Pz64qtzT86w%3d%3d HTTP/1.1
2.21.22.184 → 192.168.100.2 HTTP 1174 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
...
192.168.100.2 → 2.21.22.184 HTTP 484 GET /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638?P1=1707508671&P2=404&P3=2&P4=JsgF43Gjvt4pWsPjMe6sOWKNUs2dnb4JY8GmjsOIXtZtOac1UR%2fN23q7VWfJmNhCseqO9P9puDGSZOPVAOhOYw%3d%3d HTTP/1.1
2.21.22.184 → 192.168.100.2 HTTP 42475 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
```

D.2. Google Chrome

Quelltext D.3: Analyse Installation und erster Start: Durch den Chrome-Installer gestartete Prozesse

```
$ grep -F "Process Create" Noriben_04_Feb_24__10_29_088515.csv | sed 's,\",,g' | grep -Ev "(MsMpEng|svchost|SystemSettings).exe" | awk -F',' '{print $2" ("$3") -> "$5" ("$7")£   "$8}' | sed 's,\£,\n,g'
Explorer.EXE (4304) -> C:\tools\ChromeSetup.exe (PID: 2176)
    Command line: C:\tools\ChromeSetup.exe
ChromeSetup.exe (2176) -> C:\Users\browser\AppData\Local\Temp\GUMCC97.tmp\GoogleUpdate.exe (PID: 4728)
    Command line: C:\Users\browser\AppData\Local\Temp\GUMCC97.tmp\GoogleUpdate.exe /installsource taggedmi /install appguid={8A69D345-D564-463C-AFF1-A69D9E530F96}&iid={12CD208E-FCC4-FB26-7802-40C00C706ECB}&lang=en&browser=5&usagestats=1&appname=Google%20Chrome&needsadmin=prefers&ap=x64-stable-statsdef_1&installdataindex=empty
GoogleUpdate.exe (4728) -> C:\Users\browser\AppData\Local\Temp\GUMCC97.tmp\GoogleUpdateSetup.exe (PID: 4720)
    Command line: C:\Users\browser\AppData\Local\Temp\GUMCC97.tmp\GoogleUpdateSetup.exe /installsource taggedmi /install appguid={8A69D345-D564-463C-AFF1-A69D9E530F96}&iid={12CD208E-FCC4-FB26-7802-40C00C706ECB}&lang=en&browser=5&usagestats=1&appname=Google%20Chrome&needsadmin=prefers&ap=x64-stable-statsdef_1&installdataindex=empty /installelevated /nomitag
GoogleUpdateSetup.exe (4720) -> C:\Windows\SystemTemp\GUMDB8D.tmp\GoogleUpdate.exe (PID: 1944)
    Command line: C:\Windows\SystemTemp\GUMDB8D.tmp\GoogleUpdate.exe /installsource taggedmi /install appguid={8A69D345-D564-463C-AFF1-A69D9E530F96}&iid={12CD208E-FCC4-FB26-7802-40C00C706ECB}&lang=en&browser=5&usagestats=1&appname=Google%20Chrome&needsadmin=prefers&ap=x64-stable-statsdef_1&installdataindex=empty /installelevated
GoogleUpdate.exe (1944) -> C:\Program Files (x86)\Google\Update\GoogleUpdate.exe (PID: 1452)
    Command line: C:\Program Files (x86)\Google\Update\GoogleUpdate.exe /regsvc
GoogleUpdate.exe (1944) -> C:\Program Files (x86)\Google\Update\GoogleUpdate.exe (PID: 6472)
    Command line: C:\Program Files (x86)\Google\Update\GoogleUpdate.exe /regserver
GoogleUpdate.exe (1944) -> C:\Program Files (x86)\Google\Update\GoogleUpdate.exe (PID: 5260)
    Command line: C:\Program Files (x86)\Google\Update\GoogleUpdate.exe /ping PD94bWwgdmVyc2lvbjOiMS4wIiBlbmNvZGluZzOiVV...Lz48L2FwcD48L3JlcXVlc3Q-
GoogleUpdate.exe (1944) -> C:\Program Files (x86)\Google\Update\GoogleUpdate.exe (PID: 6720)
    Command line: C:\Program Files (x86)\Google\Update\GoogleUpdate.exe /handoff appguid={8A69D345-D564-463C-AFF1-A69D9E530F96}&iid={12CD208E-FCC4-FB26-7802-40C00C706ECB}&lang=en&browser=5&usagestats=1&appname=Google%20Chrome&needsadmin=prefers&ap=x64-stable-statsdef_1&installdataindex=empty /installsource taggedmi /sessionid {6B05C4A0-DBBE-4A01-A7F0-5B250474FB7A}
...
chrome.exe (4380) -> C:\Program Files\Google\Chrome\Application\chrome.exe (PID: 3580)
    Command line: C:\Program Files\Google\Chrome\Application\chrome.exe --type=crashpad-handler --user-data-dir=C:\Users\browser\AppData\Local\Google\Chrome\User Data /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler --database=C:\Users\browser\AppData\Local\Google\Chrome\User Data\Crashpad --metrics-dir=C:\Users\browser\AppData\Local\Google\Chrome\User Data --url=https://clients2.google.com/cr/report --annotation=channel= --annotation=plat=Win64 --annotation=prod=Chrome --annotation=ver=121.0.6167.140 --initial-client-data=0x16c
...
chrome.exe (4380) -> C:\Program Files\Google\Chrome\Application\chrome.exe (PID: 1972)
    Command line: C:\Program Files\Google\Chrome\Application\chrome.exe --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --no-appcompat-clear --mojo-platform-channel-handle=2104 --field-trial-handle=1792
...
```

Quelltext D.4: Analyse Installation und erster Start: Kommunikation von Chrome nach Initial-Start

```
$ grep -F "\"TCP" Noriben_04_Feb_24__10_29_088515.csv | sed 's,\",,g' | grep -Ev "(
    msedge|MsMpEng|svchost|SystemSettings).exe" | awk -F',' '{if ($7 == "Length: 0")
    next; print $2" ("$3"):&    "$5}' | sort | uniq | sed 's,\&,\n,g'
chrome.exe (1972):
    fdb0:8f6e:bc8e:1:0:0:0:2:49952 -> 2a00:1450:4013:c1a:0:0:0:54:443
chrome.exe (1972):
    fdb0:8f6e:bc8e:1:0:0:0:2:49953 -> 2a00:1450:400a:801:0:0:0:2003:443
chrome.exe (1972):
    fdb0:8f6e:bc8e:1:0:0:0:2:49954 -> 2a00:1450:400a:800:0:0:0:200e:443
chrome.exe (1972):
    fdb0:8f6e:bc8e:1:0:0:0:2:49955 -> 2600:1900:4110:86f:0:0:0:0:80
chrome.exe (1972):
    fdb0:8f6e:bc8e:1:0:0:0:2:49956 -> 2a00:1450:400a:803:0:0:0:200a:443
chrome.exe (1972):
    fdb0:8f6e:bc8e:1:0:0:0:2:49957 -> 2a00:1450:400a:803:0:0:0:200a:443
chrome.exe (1972):
    fdb0:8f6e:bc8e:1:0:0:0:2:49958 -> 2a00:1450:400a:803:0:0:0:200a:443
chrome.exe (1972):
    fdb0:8f6e:bc8e:1:0:0:0:2:49959 -> 2a00:1450:400a:801:0:0:0:2001:443
chrome.exe (1972):
    fdb0:8f6e:bc8e:1:0:0:0:2:49960 -> 2a00:1450:400a:801:0:0:0:2001:443
chrome.exe (1972):
    fdb0:8f6e:bc8e:1:0:0:0:2:49961 -> 2a00:1450:400a:800:0:0:0:200a:443
chrome.exe (1972):
    fdb0:8f6e:bc8e:1:0:0:0:2:49962 -> 2a00:1450:400a:803:0:0:0:2004:443
chrome.exe (1972):
    fdb0:8f6e:bc8e:1:0:0:0:2:49963 -> 2a00:1450:400a:803:0:0:0:2004:443
chrome.exe (1972):
    fdb0:8f6e:bc8e:1:0:0:0:2:49964 -> 2a00:1450:400a:803:0:0:0:2004:443
chrome.exe (1972):
    fdb0:8f6e:bc8e:1:0:0:0:2:49965 -> 2a00:1450:400a:803:0:0:0:2004:443
chrome.exe (1972):
    fdb0:8f6e:bc8e:1:0:0:0:2:49966 -> 2a00:1450:400a:802:0:0:0:2003:443
chrome.exe (1972):
    fdb0:8f6e:bc8e:1:0:0:0:2:49967 -> 2a00:1450:400a:802:0:0:0:2003:443
chrome.exe (1972):
    fdb0:8f6e:bc8e:1:0:0:0:2:49968 -> 2a00:1450:400a:802:0:0:0:2003:443
chrome.exe (1972):
    fdb0:8f6e:bc8e:1:0:0:0:2:49969 -> 2a00:1450:400a:802:0:0:0:200e:443
chrome.exe (1972):
    fdb0:8f6e:bc8e:1:0:0:0:2:49971 -> 2a00:1450:400a:803:0:0:0:2003:443
chrome.exe (1972):
    fdb0:8f6e:bc8e:1:0:0:0:2:49973 -> 2a00:1450:400a:800:0:0:0:200e:443
chrome.exe (1972):
    fdb0:8f6e:bc8e:1:0:0:0:2:49974 -> 2a00:1450:400a:803:0:0:0:2003:443
```

Quelltext D.5: Analyse Installation und erster Start: Kommunikation von Chrome, gefiltert nach UUID-Format

```
$ tshark -r lab-chrome-20240204-1028.tlsdecrypted.pcap -Y "((http || http2))" -T fields -e ipv6.src -e ipv6.dst -e ip.src -e ip.dst -e http.request.full_uri -e http2.request.full_uri -e data.data -e http2.header.unescaped -e json.member_with_value | awk '{if ($3 == "") next ;print $0}' | uniq | grep -Ei "[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}"
                192.168.100.2   172.217.168.14   https://dl.google.com/update2/installers/icons/%7B8A69D345-D564-463C-AFF1-A69D9E530F96%7D.bmp

                192.168.100.2   172.217.168.67          https://update.googleapis.com/service/update2?cup2key=13:abf6NLvnPsIN-e6tXzOTRbewJfR2OF1rKG2D9ZvCoT4&cup2hreq=11cb6ca0f77c38fb3e598d5cc1f1134f5a2ccd3ece5a628cba05cef283209692
                        POST,/service/update2?cup2key=13:abf6NLvnPsIN-e6tXzOTRbewJfR2OF1rKG2D9ZvCoT4&cup2hreq=11cb6ca0f77c38fb3e598d5cc1f1134f5a2ccd3ece5a628cba05cef283209692,update.googleapis.com,https,no-cache,no-cache,Google Update/1.3.36.352;winhttp;cup-ecdsa,age=-1; cnt=1,{8A69D345-D564-463C-AFF1-A69D9E530F96},Omaha-1.3.36.352,fg,0x80072ee7,0,1,3,775
                23.50.111.27    192.168.100.2                                   200,text/xml;charset=utf-8,"4f8c244dad93567f0dca23f45adbddab",Kestrel,https://compass-ssl.microsoft.com,appId=cid-v1:cfffaf62-ab0f-4cff-bf71-cd6090101fcb,True,Accept-Encoding,gzip,2164,public, max-age=11195, Sun, 04 Feb 2024 09:32:34 GMT
fdb0:8f6e:bc8e:1::2     2a00:1450:400a:803::2003
                        @os:win,@updater:chrome,acceptformat:crx3,puff,appid:ihnlcenocehgdaegdmhbidjhnhdchfmm,brand:GGLS,enabled:true,lang:en-US,r:-2,version:0.0.0.0,appid:neifaoindggfcjicffkgpmnlppeffabd,brand:GGLS,enabled:true,lang:en-US,r:-2,version:0.0.0.0,appid:oimompecagnajdejgnnjijobebaeigek,brand:GGLS,enabled:true,lang:en-US,r:-2,version:4.10.2710.0,appid:gcmjkmgdlgnkkcocmoeiminaijmmjnii,brand:GGLS,enabled:true,lang:en-US,r:-2,version:0.0.0.0,accept_locale:ENUS500000,appid:obedbbhbpmojnkanicioggnmelmoomoc,brand:GGLS,enabled:true,lang:en-US,r:-2,version:0.0.0.0,appid:lmelglejhemejginpboagddgdfbepgmp,brand:GGLS,enabled:true,lang:en-US,r:-2,version:0.0.0.0,appid:kiabhabjdbkjdpjbpigfodbdjmbglcoo,brand:GGLS,enabled:true,lang:en-US,r:-2,version:0.0.0.0,appid:giekcmmlnklenlaomppkphknjmnnpneh,brand:GGLS,enabled:true,lang:en-US,r:-2,version:0.0.0.0,appid:khaoiebndkojlmppeemjhbpbandiljpe,brand:GGLS,enabled:true,lang:en-US,r:-2,version:0.0.0.0,appid:hfnkpimlhhgieaddgfemjhofmfblmnib,brand:GGLS,enabled:true,lang:en-US,r:-2,version:0.0.0.0,appid:llkgjffcdpffmhiakmfcdcblohccpfmo,brand:GGLS,enabled:true,lang:en-US,r:-2,version:0.0.0.0,appid:laoigpblnllgcgjnjnllmfolckpjlhki,brand:GGLS,enabled:true,lang:en-US,r:-2,version:1.0.7.1652906823,appid:ehgidpndbllacpjalkiimkbadgjfnnmc,brand:GGLS,enabled:true,lang:en-US,r:-2,version:0.0.0.0,appid:efniojlnjndmcbiieegkicadnoecjjef,brand:GGLS,enabled:true,lang:en-US,r:-2,version:0.0.0.0,appid:jflookgnkcckhobaglndicnbbgbonegd,brand:GGLS,enabled:true,lang:en-US,r:-2,version:0.0.0.0,appid:ggkkehgbnfjpeggfpleeakpidbkibbmn,brand:GGLS,enabled:true,lang:en-US,r:-2,version:0.0.0.0,appid:jamhcnnkihinmdlkakkaopbjbbcngflc,brand:GGLS,enabled:true,lang:en-US,r:-2,version:0.0.0.0,appid:ojhpjlocmbogdgmfpkhlaaeamibhnphh,brand:GGLS,enabled:true,lang:en-US,r:-2,version:0.0.0.0,appid:eeigpngbgcognadeebkilcpcaedhellh,brand:GGLS,enabled:true,lang:en-US,r:-2,version:0.0.0.0,appid:jflhchccmppkfebkiaminageehmchikm,brand:GGLS,enabled:true,lang:en-US,r:-2,version:0.0.0.0,appid:gonpemdgkjcecdgbnaabipppbmgfggbe,brand:GGLS,enabled:true,lang:en-US,r:-2,version:0.0.0.0,appid:niikhdgajlphfehepabhhblakbdgeefj,brand:GGLS,enabled:true,lang:en-US,r:-2,version:0.0.0.0,arch:x64,dedup:cr,domainjoined:false,avx:true,physmemory:4,sse:true,sse2:true,sse3:true,sse41:true,sse42:true,ssse3:true,ismachine:true,nacl_arch:x86-64,arch:x86_64,platform:Windows,version:10.0.22631.3007,prodversion:121.0.6167.140,protocol:3.1,requestid:{c91d3005-9465-4a75-a8be-13e4ce9698f2},sessionid:{53b83130-6d26-440e-9304-281e7ac59370},autoupdatecheckenabled:true,ismachine:true,name:Omaha,updatepolicy:-1,version:1.3.36.352,updaterversion:121.0.6167.140
fdb0:8f6e:bc8e:1::2     2a00:1450:400a:803::2003
                        @os:win,@updater:chrome,acceptformat:crx3,puff,appid:neifaoindggfcjicffkgpmnlppeffabd,brand:GGLS,cohort:1:1299:,cohortname:Auto,enabled:true,download_time_ms:16131,downloaded:1181927,downloader:bits,eventresult:1,
```

```
    eventtype:14,nextversion:1.0.2738.0,previousversion:0.0.0.0,total:1181927,url:http
    ://edgedl.me.gvt1.com/edgedl/release2/chrome_component/imoffpf67hel7kbknqflao2oo4_1
    .0.2738.0/neifaoindggfcjicffkgpmnlppeffabd_1.0.2738.0
    _win64_kj4dp5kifwxbdodqls7e5nzhtm.crx3,eventresult:1,eventtype:3,nextfp:1.
    c900ba9a2d8318263fd43782ee6fd5fb50bad78bf0eb2c972b5922c458af45ed,nextversion
    :1.0.2738.0,previousversion:0.0.0.0,installdate:6243,lang:en-US,fp:1.
    c900ba9a2d8318263fd43782ee6fd5fb50bad78bf0eb2c972b5922c458af45ed,version
    :1.0.2738.0,arch:x64,dedup:cr,domainjoined:false,avx:true,physmemory:4,sse:true,
    sse2:true,sse3:true,sse41:true,sse42:true,ssse3:true,ismachine:true,nacl_arch:x86
    -64,arch:x86_64,platform:Windows,version:10.0.22631.3007,prodversion
    :121.0.6167.140,protocol:3.1,requestid:{9971ddfc-139f-4a96-a393-82424611b8a5},
    sessionid:{53b83130-6d26-440e-9304-281e7ac59370},updaterversion:121.0.6167.140
7 fdb0:8f6e:bc8e:1::2       2a00:1450:400a:803::2003
                                @os:win,@updater:chrome,acceptformat:crx3,puff,appid:
    gcmjkmgdlgnkkcocmoeiminaijmmjnii,brand:GGLS,cohort:1:bm1:,cohortname:Stable,enabled
    :true,download_time_ms:4018,downloaded:35043,downloader:bits,eventresult:1,
    eventtype:14,nextversion:9.49.1,previousversion:0.0.0.0,total:35043,url:http://
    edgedl.me.gvt1.com/edgedl/release2/chrome_component/ad3rm3ciqs3fjr4bc4x5vwuildeq_9
    .49.1/gcmjkmgdlgnkkcocmoeiminaijmmjnii_9.49.1_all_ixzyrcu7pvmgu5pjv6enfqq6wa.crx3,
    eventresult:1,eventtype:3,nextfp:1.
    cd1978742a4afdbaaa15bf712d5c90bef4144caa99024df98f6a9ad58043ae85,nextversion
    :9.49.1,previousversion:0.0.0.0,installdate:6243,lang:en-US,fp:1.
    cd1978742a4afdbaaa15bf712d5c90bef4144caa99024df98f6a9ad58043ae85,version:9.49.1,
    arch:x64,dedup:cr,domainjoined:false,avx:true,physmemory:4,sse:true,sse2:true,sse3:
    true,sse41:true,sse42:true,ssse3:true,ismachine:true,nacl_arch:x86-64,arch:x86_64,
    platform:Windows,version:10.0.22631.3007,prodversion:121.0.6167.140,protocol:3.1,
    requestid:{7d836064-972e-4703-b14d-c222015b1c34},sessionid:{53b83130-6d26-440e
    -9304-281e7ac59370},updaterversion:121.0.6167.140
8 fdb0:8f6e:bc8e:1::2       2a00:1450:400a:803::2003
                                @os:win,@updater:chrome,acceptformat:crx3,puff,
    accept_locale:ENUS500000,appid:obedbbhbpmojnkanicioggnmelmoomoc,brand:GGLS,cohort
    :1:s6f:20ol@0.5,cohortname:Auto,enabled:true,download_time_ms:8022,downloaded
    :5409164,downloader:bits,eventresult:1,eventtype:14,nextversion
    :20230916.567854667.14,previousversion:0.0.0.0,total:5409164,url:http://edgedl.me.
    gvt1.com/edgedl/release2/chrome_component/adhioj45hzjkfunn7ccrbqyyhu3q_20230916
    .567854667.14/obedbbhbpmojnkanicioggnmelmoomoc_20230916.567854667.14
    _all_ENUS500000_lr7434qyx46lykosg2elaepqdi.crx3,eventresult:1,eventtype:3,nextfp
    :1.50a410468d64fd55a0fc41dd22d574883f13386eb147b0b5b96ee66c118d4d6e,nextversion
    :20230916.567854667.14,previousversion:0.0.0.0,installdate:6243,lang:en-US,fp:1.50
    a410468d64fd55a0fc41dd22d574883f13386eb147b0b5b96ee66c118d4d6e,version
    :20230916.567854667.14,arch:x64,dedup:cr,domainjoined:false,avx:true,physmemory:4,
    sse:true,sse2:true,sse3:true,sse41:true,sse42:true,ssse3:true,ismachine:true,
    nacl_arch:x86-64,arch:x86_64,platform:Windows,version:10.0.22631.3007,prodversion
    :121.0.6167.140,protocol:3.1,requestid:{df1f6d85-a278-4e62-94a7-574956abe19d},
    sessionid:{53b83130-6d26-440e-9304-281e7ac59370},updaterversion:121.0.6167.140
9 fdb0:8f6e:bc8e:1::2       2a00:1450:400a:803::2003
                                @os:win,@updater:chrome,acceptformat:crx3,puff,appid:
    lmelglejhemejginpboagddgdfbepgmp,brand:GGLS,cohort:1:lwl:,cohortname:Auto,enabled:
    true,download_time_ms:4009,downloaded:47646,downloader:bits,eventresult:1,eventtype
    :14,nextversion:432,previousversion:0.0.0.0,total:47646,url:http://edgedl.me.gvt1.
    com/edgedl/release2/chrome_component/ao6fcorj5d3wwrem5y6dty67xu_432/
    lmelglejhemejginpboagddgdfbepgmp_432_all_ZZ_acd7qvna3s5d7raww7kyhu5edlia.crx3,
    eventresult:1,eventtype:3,nextfp:1.
    cadbf9a5f27721576d77d35576f37ca01ac34d86bce73958bf71cde62af71b48,nextversion:432,
    previousversion:0.0.0.0,installdate:6243,lang:en-US,fp:1.
    cadbf9a5f27721576d77d35576f37ca01ac34d86bce73958bf71cde62af71b48,version:432,arch:
    x64,dedup:cr,domainjoined:false,avx:true,physmemory:4,sse:true,sse2:true,sse3:true,
    sse41:true,sse42:true,ssse3:true,ismachine:true,nacl_arch:x86-64,arch:x86_64,
    platform:Windows,version:10.0.22631.3007,prodversion:121.0.6167.140,protocol:3.1,
    requestid:{ee316dd8-2d1c-42ab-aa6d-a6b60fc90279},sessionid:{53b83130-6d26-440e
    -9304-281e7ac59370},updaterversion:121.0.6167.140
10 fdb0:8f6e:bc8e:1::2       2a00:1450:400a:803::2003
                                @os:win,@updater:chrome,acceptformat:crx3,puff,appid:
```

```
    kiabhabjdbkjdpjbpigfodbdjmbglcoo,brand:GGLS,cohort:1:v3l:,cohortname:Auto,enabled:
    true,download_time_ms:4020,downloaded:7710,downloader:bits,eventresult:1,eventtype
    :14,nextversion:2024.1.2.1,previousversion:0.0.0.0,total:7710,url:http://edgedl.me.
    gvt1.com/edgedl/release2/chrome_component/adwe425xlzq32gxl5bw24qdolbda_2024.1.2.1/
    kiabhabjdbkjdpjbpigfodbdjmbglcoo_2024.01.02.01_all_acdbyptqku3alt5j2pnkq6jnq75q.
    crx3,eventresult:1,eventtype:3,nextfp:1.4
    a6508925b2ffec931c1e3931ddeb15ca41d820a8264cd5a962b526e9932bcdf,nextversion
    :2024.1.2.1,previousversion:0.0.0.0,installdate:6243,lang:en-US,fp:1.4
    a6508925b2ffec931c1e3931ddeb15ca41d820a8264cd5a962b526e9932bcdf,version:2024.1.2.1,
    arch:x64,dedup:cr,domainjoined:false,avx:true,physmemory:4,sse:true,sse2:true,sse3:
    true,sse41:true,sse42:true,ssse3:true,ismachine:true,nacl_arch:x86-64,arch:x86_64,
    platform:Windows,version:10.0.22631.3007,prodversion:121.0.6167.140,protocol:3.1,
    requestid:{8c3f0d72-e111-4dde-ac34-2b19db25f074},sessionid:{53b83130-6d26-440e
    -9304-281e7ac59370},updaterversion:121.0.6167.140
11                  192.168.100.2    172.217.168.78          https://clients2.google.com/
                        service/check2?crx3=true&appid=%7B430FD4D0-B729-4F61-AA34
                        -91526481799D%7D&appversion=1.3.36.352&applang=&machine=1&version
                        =1.3.36.352&userid=%7B6C7488BD-B56B-42D8-B2CB-5F6F6A3A9EAB%7D&
                        osversion=10.0&servicepack=          GET,/service/check2?crx3=true&
                        appid={430FD4D0-B729-4F61-AA34-91526481799D}&appversion=1.3.36.352&
                        applang=&machine=1&version=1.3.36.352&userid={6C7488BD-B56B-42D8-
                        B2CB-5F6F6A3A9EAB}&osversion=10.0&servicepack=,clients2.google.com,
                        https,no-cache,no-cache,Google Update/1.3.36.352;winhttp,0x0,0,0,1
12                  192.168.100.2    172.217.168.35          https://update.googleapis.com/
                        service/update2?cup2key=13:lKO5f3hCicwrky8OjU5WDw7m-
                        cZpQlX31DJY2xXDWXc&cup2hreq=
                        cc6110cef02aacf43b9283012c9e2e9b44be370748f1a17bc8da4604c4873e5c
                                POST,/service/update2?cup2key=13:lKO5f3hCicwrky8OjU5WDw7m-
                        cZpQlX31DJY2xXDWXc&cup2hreq=
                        cc6110cef02aacf43b9283012c9e2e9b44be370748f1a17bc8da4604c4873e5c,
                        update.googleapis.com,https,no-cache,no-cache,Google Update
                        /1.3.36.352;winhttp;cup-ecdsa,{430FD4D0-B729-4F61-AA34-91526481799D
                        },{8A69D345-D564-463C-AFF1-A69D9E530F96},Omaha-1.3.36.352,bg,0x0
                        ,0,0,1,1151
13  fdb0:8f6e:bc8e:1::2      2a00:1450:400a:803::2003
                                @os:win,@updater:chrome,acceptformat:crx3,puff,appid:
    giekcmmlnklenlaomppkphknjmnnpneh,brand:GGLS,cohort:1:j5l:,cohortname:Auto,enabled:
    true,download_time_ms:4024,downloaded:5406,downloader:bits,eventresult:1,eventtype
    :14,nextversion:7,previousversion:0.0.0.0,total:5406,url:http://edgedl.me.gvt1.com/
    edgedl/release2/chrome_component/AIZk807Cv2UUbxc_aaUykKI_7/ALzUVHP-vRgKCzqwbtGugSE,
    eventresult:1,eventtype:3,nextfp:1.
    fd515ec0dc30d25a09641b8b83729234bc50f4511e35ce17d24fd996252eaace,nextversion:7,
    previousversion:0.0.0.0,installdate:6243,lang:en-US,fp:1.
    fd515ec0dc30d25a09641b8b83729234bc50f4511e35ce17d24fd996252eaace,version:7,arch:x64
    ,dedup:cr,domainjoined:false,avx:true,physmemory:4,sse:true,sse2:true,sse3:true,
    sse41:true,sse42:true,ssse3:true,ismachine:true,nacl_arch:x86-64,arch:x86_64,
    platform:Windows,version:10.0.22631.3007,prodversion:121.0.6167.140,protocol:3.1,
    requestid:{f6326289-08cb-41d8-8cf0-c77c6df86007},sessionid:{53b83130-6d26-440e
    -9304-281e7ac59370},updaterversion:121.0.6167.140
14  fdb0:8f6e:bc8e:1::2      2a00:1450:400a:803::2003
                                @os:win,@updater:chrome,acceptformat:crx3,puff,appid:
    khaoiebndkojlmppeemjhbpbandiljpe,brand:GGLS,cohort:1:cux:,cohortname:Auto,enabled:
    true,download_time_ms:4026,downloaded:5650,downloader:bits,eventresult:1,eventtype
    :14,nextversion:63,previousversion:0.0.0.0,total:5650,url:http://edgedl.me.gvt1.com
    /edgedl/release2/chrome_component/acezyjyt2fp2x53dhyqbvt3gxdlq_63/
    khaoiebndkojlmppeemjhbpbandiljpe_63_win_pz5ggrx6ddtwepg55hf2663jnu.crx3,eventresult
    :1,eventtype:3,nextfp:1.
    f4f1eb04881095d1cc8f2e1799a8144c10476dc1088a03ecdb4418644040a554,nextversion:63,
    previousversion:0.0.0.0,installdate:6243,lang:en-US,fp:1.
    f4f1eb04881095d1cc8f2e1799a8144c10476dc1088a03ecdb4418644040a554,version:63,arch:
    x64,dedup:cr,domainjoined:false,avx:true,physmemory:4,sse:true,sse2:true,sse3:true,
    sse41:true,sse42:true,ssse3:true,ismachine:true,nacl_arch:x86-64,arch:x86_64,
    platform:Windows,version:10.0.22631.3007,prodversion:121.0.6167.140,protocol:3.1,
```

```
    requestid:{cd432d9f-5e53-425d-a1aa-0767b3326835},sessionid:{53b83130-6d26-440e
    -9304-281e7ac59370},updaterversion:121.0.6167.140
fdb0:8f6e:bc8e:1::2      2a00:1450:400a:803::2003
                              @os:win,@updater:chrome,acceptformat:crx3,puff,appid:
    hfnkpimlhhgieaddgfemjhofmfblmnib,brand:GGLS,cohort:1:jcl:,cohortname:Auto,enabled:
    true,download_time_ms:4009,downloaded:27103,downloader:bits,eventresult:1,eventtype
    :14,nextversion:8527,previousversion:0.0.0.0,total:27103,url:http://edgedl.me.gvt1.
    com/edgedl/release2/chrome_component/owqqsb53tid6c32qwsqmfzo62u_8527/
    hfnkpimlhhgieaddgfemjhofmfblmnib_8527_all_adcyo3lu2n7zp6xbsn77huz3qwqa.crx3,
    eventresult:1,eventtype:3,nextfp:1.
    df50dcd0fdce240ead96afe46055e4ddc9f28239acf3fabca1e562e10d80559a,nextversion:8527,
    previousversion:0.0.0.0,installdate:6243,lang:en-US,fp:1.
    df50dcd0fdce240ead96afe46055e4ddc9f28239acf3fabca1e562e10d80559a,version:8527,arch:
    x64,dedup:cr,domainjoined:false,avx:true,physmemory:4,sse:true,sse2:true,sse3:true,
    sse41:true,sse42:true,ssse3:true,ismachine:true,nacl_arch:x86-64,arch:x86_64,
    platform:Windows,version:10.0.22631.3007,prodversion:121.0.6167.140,protocol:3.1,
    requestid:{1941e9aa-b0f1-49ce-9c47-be8d505f7985},sessionid:{53b83130-6d26-440e
    -9304-281e7ac59370},updaterversion:121.0.6167.140
```

Quelltext D.6: Analyse Installation und erster Start: HTTP-Request-URIs Chrome, von Installation bis Initial-Start

```
$ tshark -r lab-chrome-20240204-1028.tlsdecrypted.pcap -Y "((http || http2) && (ipv6.addr == "2a00:1450::/32" || ipv6.addr == 2600:1900:4110:86f:0:0:0:0))" -T fields -e ipv6.src -e ipv6.dst -e ip.src -e ip.dst -e http.request.full_uri -e http2.request.full_uri | awk '{if ($3 == "") next ;print $0}' | uniq
fdb0:8f6e:bc8e:1::2	2a00:1450:400a:801::2003	https://clientservices.googleapis.com/chrome-variations/seed?osname=win&channel=stable&milestone=121
fdb0:8f6e:bc8e:1::2	2a00:1450:400a:800::200e	https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=121.0.6167.140&lang=en-US&acceptformat=crx3,puff&x=id%3Dghbmnnjooekpmoecnnnilnnbdlolhkhi%26v%3D0.0.0.0%26installedby%3Dinternal%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1
fdb0:8f6e:bc8e:1::2	2a00:1450:4013:c1a::54	https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard
fdb0:8f6e:bc8e:1::2	2600:1900:4110:86f::	http://edgedl.me.gvt1.com/edgedl/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYmxvYnMvNzIOQUFXNV9zT2RvdUwyMERESEZGVmJnQQ/1.0.0.6_nmmhkkegccagdldgiimedpiccmgmieda.crx
fdb0:8f6e:bc8e:1::2	2a00:1450:400a:803::200a	https://optimizationguide-pa.googleapis.com/v1:GetModels?key=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw
fdb0:8f6e:bc8e:1::2	2a00:1450:400a:803::200a	https://optimizationguide-pa.googleapis.com/downloads?name=1699288392&target=OPTIMIZATION_TARGET_PAGE_ENTITIES
fdb0:8f6e:bc8e:1::2	2a00:1450:400a:803::200a	https://optimizationguide-pa.googleapis.com/downloads?name=1701726572&target=OPTIMIZATION_TARGET_NOTIFICATION_PERMISSION_PREDICTIONS
fdb0:8f6e:bc8e:1::2	2a00:1450:400a:803::200a	https://optimizationguide-pa.googleapis.com/downloads?name=1673999601&target=OPTIMIZATION_TARGET_PAGE_VISIBILITY
fdb0:8f6e:bc8e:1::2	2a00:1450:400a:803::200a	https://optimizationguide-pa.googleapis.com/downloads?name=4&target=OPTIMIZATION_TARGET_PAGE_TOPICS_V2
fdb0:8f6e:bc8e:1::2	2a00:1450:400a:801::2001	https://clients2.googleusercontent.com/crx/blobs/AeKPYwz_ATw3QVAsUh5mrq7VbFhoCemsnDfnzW4MD7THJ3muWgQp7_jt-TfwHfQDgQmvhXQaLMW...vmTacAMZSmuWp_tQgCHMAHdp_5TemiCvwrS2ZNQ/GHBMNNJOOEKPMOECNNNILNNBDLOLHKHI_1_73_5_0.crx
fdb0:8f6e:bc8e:1::2	2a00:1450:400a:800::200a	https://www.googleapis.com/chromewebstore/v1.1/items/verify
fdb0:8f6e:bc8e:1::2	2a00:1450:400a:803::200a	https://optimizationguide-pa.googleapis.com/downloads?name=1701726567&target=OPTIMIZATION_TARGET_GEOLOCATION_PERMISSION_PREDICTIONS
fdb0:8f6e:bc8e:1::2	2a00:1450:400a:803::200a	https://optimizationguide-pa.googleapis.com/downloads?name=1698073325&target=OPTIMIZATION_TARGET_CLIENT_SIDE_PHISHING
fdb0:8f6e:bc8e:1::2	2a00:1450:400a:803::200a	https://optimizationguide-pa.googleapis.com/downloads?name=1699288392&target=OPTIMIZATION_TARGET_PAGE_ENTITIES
fdb0:8f6e:bc8e:1::2	2a00:1450:400a:803::200a	https://optimizationguide-pa.googleapis.com/downloads?name=1698073325&target=OPTIMIZATION_TARGET_CLIENT_SIDE_PHISHING
fdb0:8f6e:bc8e:1::2	2a00:1450:400a:803::200a	https://optimizationguide-pa.googleapis.com/downloads?name=1699288392&target=OPTIMIZATION_TARGET_PAGE_ENTITIES
fdb0:8f6e:bc8e:1::2	2a00:1450:400a:803::200a	https://optimizationguide-pa.googleapis.com/downloads?name=1698073325&target=OPTIMIZATION_TARGET_CLIENT_SIDE_PHISHING
fdb0:8f6e:bc8e:1::2	2a00:1450:400a:803::2004	https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q
```

```
    =&oit=0&oft=1&pgcl=20&gs_rn=42&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw
20  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:803::2004                                https
    ://www.google.com/async/ddljson?async=ntp:2
21  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:803::2004                                https
    ://www.google.com/async/newtab_ogb?hl=en-US&async=fixed:0
22  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:803::2004                                https
    ://www.google.com/async/newtab_promos
23  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:802::2003                                https
    ://www.gstatic.com/og/_/ss/k=og.qtm.8RUPaHb7e5o.L.W.O/m=qmd,qcwid/excm=qaaw,qabr,
    qadd,qaid,qalo,qebr,qein,qhaw,qhawgm3,qhba,qhbr,qhbrgm3,qhch,qhchgm3,qhga,qhid,
    qhidgm3,qhin,qhlo,qhlogm3,qhmn,qhpc,qhsf,qhsfgm3,qhtt/d=1/ed=1/ct=zgms/rs=
    AA2YrTungzasoekTaLKrPFUaQFpakqDmnA
24  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:802::2003                                https
    ://www.gstatic.com/images/branding/googlelogo/svg/googlelogo_clr_74x24px.svg
25  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:802::2003                                https
    ://www.gstatic.com/og/_/js/k=og.qtm.en_US.ZEEp2pdSHOQ.2019.O/rt=j/m=q_dnp,qmd,qcwid
    ,qapid,qald,q_dg/exm=qaaw,qabr,qadd,qaid,qalo,qebr,qein,qhaw,qhawgm3,qhba,qhbr,
    qhbrgm3,qhch,qhchgm3,qhga,qhid,qhidgm3,qhin,qhlo,qhlogm3,qhmn,qhpc,qhsf,qhsfgm3,
    qhtt/d=1/ed=1/rs=AA2YrTvRRKYp7I5vTn-AtFvme6Qlo6hq9Q
26  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:802::200e                                https
    ://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.GsbA68hXs80.O/m=
    gapi_iframes,googleapis_client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo899t-
    H8Lxb3OqzMDuPn6TV_i36ag/cb=gapi.loaded_0
27  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:803::2003                                https
    ://update.googleapis.com/service/update2/json?cup2key=13:
    aHfhTBgdDLnaRqtZul_3dusOgdTjN-JF9T4qRX5gCHU&cup2hreq=93
    d50477bbd98afba8db3e7207fe32197d806d0886befe48f92e95f17559d238
28  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:801::2003                                https
    ://clientservices.googleapis.com/uma/v2
29  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:803::200a                                https
    ://optimizationguide-pa.googleapis.com/downloads?name=1699288392&target=
    OPTIMIZATION_TARGET_PAGE_ENTITIES
30  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:803::200a                                https
    ://optimizationguide-pa.googleapis.com/downloads?name=1698073325&target=
    OPTIMIZATION_TARGET_CLIENT_SIDE_PHISHING
31  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:800::200e                                https
    ://ogs.google.com/widget/app/so?eom=1&awwd=1&gm3=1&origin=chrome-untrusted%3A%2F%2
    Fnew-tab-page&origin=chrome%3A%2F%2Fnew-tab-page&cn=app&pid=1&spid=243&hl=en
32  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:802::2003                                https
    ://www.gstatic.com/_/mss/boq-one-google/_/js/k=boq-one-google.OneGoogleWidgetUi.en.
    iiIKEVwVsdw.es5.O/am=BAztBg/d=1/excm=_b,_tp,appwidgetnoauthview/ed=1/dg=0/wt=2/ujg
    =1/rs=AM-SdHsrLOV2KMAwMlbgfIHN4pie9ORGvA/m=_b,_tp
33  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:803::2003                                https
    ://ssl.gstatic.com/gb/images/sprites/p_2x_a6cad964874d.png
34  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:802::2003                                https
    ://www.gstatic.com/_/mss/boq-one-google/_/js/k=boq-one-google.OneGoogleWidgetUi.en.
    iiIKEVwVsdw.es5.O/ck=boq-one-google.OneGoogleWidgetUi.jOBw6uB5eqO.L.B1.O/am=BAztBg/
    d=1/exm=_b,_tp/excm=_b,_tp,appwidgetnoauthview/ed=1/wt=2/ujg=1/rs=AM-
    SdHvID7fpKYMRHrVCWG6liu-Xx5qOVA/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;JsbNhc
    :Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:
    EEDORb;QGROgd:Mlhmy;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:
    zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;oGtAuc:sOXFj;pXdRYb:
    MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:
    wmnU7d;yxTchf:KUM7Z;zxnPse:GkRiKb/m=ws9Tlc,n73qwf,GkRiKb,e5qFLc,IZT63,UUJqVe,O1Gjze
    ,byfTOb,lsjVmc,xUdipf,OTA3Ae,COQbmf,fKUV3e,aurFic,UOaPgd,ZwDk9d,V3dDOb,mI3LFb,
    aDfbSd,O6y8ed,PrPYRd,MpJwZc,LEikZe,NwHOH,OmgaI,lazG7b,XVMNvd,L1AAkb,KUM7Z,Mlhmy,
    s39S4,lwddkf,gychg,w9hDv,EEDORb,RMhBfe,SdcwHb,aW3pY,pw70Gc,EFQ78c,Ulmmrd,ZfAoz,
    mdR7q,wmnU7d,xQtZb,JNoxi,kWgXee,MI6k7c,kjKdXe,BVgquf,QIhFr,ovKuLd,hKSk3e,yDVVkb,
    hc6Ubd,SpsfSb,KG2eXe,Z5uLle,MdUzUe,VwDzFe,zbML3c,A7fCU,zr1jrb,Uas9Hd,pjICDe
35  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:802::2003                                https
    ://www.gstatic.com/_/mss/boq-one-google/_/js/k=boq-one-google.OneGoogleWidgetUi.en.
    iiIKEVwVsdw.es5.O/ck=boq-one-google.OneGoogleWidgetUi.jOBw6uB5eqO.L.B1.O/am=BAztBg/
    d=1/exm=A7fCU,BVgquf,COQbmf,EEDORb,EFQ78c,GkRiKb,IZT63,JNoxi,KG2eXe,KUM7Z,L1AAkb,
```

```
    LEikZe,MI6k7c,MdUzUe,Mlhmy,MpJwZc,NwHOH,O1Gjze,O6y8ed,OTA3Ae,OmgaI,PrPYRd,QIhFr,
    RMhBfe,SdcwHb,SpsfSb,UOaPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,XVMNvd,Z5uLle,ZfAoz,
    ZwDk9d,_b,_tp,aDfbSd,aW3pY,aurFic,byfTOb,e5qFLc,fKUV3e,gychg,hKSk3e,hc6Ubd,kWgXee,
    kjKdXe,lazG7b,lsjVmc,lwddkf,mI3LFb,mdR7q,n73qwf,ovKuLd,pjICDe,pw7OGc,s39S4,w9hDv,
    wmnU7d,ws9Tlc,xQtZb,xUdipf,yDVVkb,zbML3c,zr1jrb/excm=_b,_tp,appwidgetnoauthview/ed
    =1/wt=2/ujg=1/rs=AM-SdHvID7fpKYMRHrVCWG6liu-Xx5qOVA/ee=EVNhjf:pw7OGc;EmZ2Bf:zr1jrb;
    Erl4fe:FloWmf;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;
    Oj465e:KG2eXe;Pjplud:EEDORb;QGROgd:Mlhmy;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;
    dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;
    oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;uY49fb:COQbmf;ul9GGd:VDovNc;
    wR5FRb:O1Gjze;xqZiqf:wmnU7d;yxTchf:KUM7Z;zxnPse:GkRiKb/m=RqjULd
36  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:802::2003                                https
    ://www.gstatic.com/_/mss/boq-one-google/_/js/k=boq-one-google.OneGoogleWidgetUi.en.
    iiIKEVwVsdw.es5.O/ck=boq-one-google.OneGoogleWidgetUi.jOBw6uB5eqO.L.B1.O/am=BAztBg/
    d=1/exm=A7fCU,BVgquf,COQbmf,EEDORb,EFQ78c,GkRiKb,IZT63,JNoxi,KG2eXe,KUM7Z,L1AAkb,
    LEikZe,MI6k7c,MdUzUe,Mlhmy,MpJwZc,NwHOH,O1Gjze,O6y8ed,OTA3Ae,OmgaI,PrPYRd,QIhFr,
    RMhBfe,RqjULd,SdcwHb,SpsfSb,UOaPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,XVMNvd,Z5uLle
    ,ZfAoz,ZwDk9d,_b,_tp,aDfbSd,aW3pY,aurFic,byfTOb,e5qFLc,fKUV3e,gychg,hKSk3e,hc6Ubd,
    kWgXee,kjKdXe,lazG7b,lsjVmc,lwddkf,mI3LFb,mdR7q,n73qwf,ovKuLd,pjICDe,pw7OGc,s39S4,
    w9hDv,wmnU7d,ws9Tlc,xQtZb,xUdipf,yDVVkb,zbML3c,zr1jrb/excm=_b,_tp,
    appwidgetnoauthview/ed=1/wt=2/ujg=1/rs=AM-SdHvID7fpKYMRHrVCWG6liu-Xx5qOVA/ee=EVNhjf
    :pw7OGc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK
    :SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGROgd:Mlhmy;SNUn3:ZwDk9d;a56pNe:
    JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:
    OTA3Ae;nAFL3:s39S4;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;uY49fb:
    COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:wmnU7d;yxTchf:KUM7Z;zxnPse:GkRiKb/m=
    bm51tf
37  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:803::2003                                https
    ://update.googleapis.com/service/update2/json
38  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:801::2003                                https
    ://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxK.woff2
39  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:802::2003                                https
    ://www.gstatic.com/_/mss/boq-one-google/_/js/k=boq-one-google.OneGoogleWidgetUi.en.
    iiIKEVwVsdw.es5.O/ck=boq-one-google.OneGoogleWidgetUi.jOBw6uB5eqO.L.B1.O/am=BAztBg/
    d=1/exm=A7fCU,BVgquf,COQbmf,EEDORb,EFQ78c,GkRiKb,IZT63,JNoxi,KG2eXe,KUM7Z,L1AAkb,
    LEikZe,MI6k7c,MdUzUe,Mlhmy,MpJwZc,NwHOH,O1Gjze,O6y8ed,OTA3Ae,OmgaI,PrPYRd,QIhFr,
    RMhBfe,RqjULd,SdcwHb,SpsfSb,UOaPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,XVMNvd,Z5uLle
    ,ZfAoz,ZwDk9d,_b,_tp,aDfbSd,aW3pY,aurFic,bm51tf,byfTOb,e5qFLc,fKUV3e,gychg,hKSk3e,
    hc6Ubd,kWgXee,kjKdXe,lazG7b,lsjVmc,lwddkf,mI3LFb,mdR7q,n73qwf,ovKuLd,pjICDe,pw7OGc,
    s39S4,w9hDv,wmnU7d,ws9Tlc,xQtZb,xUdipf,yDVVkb,zbML3c,zr1jrb/excm=_b,_tp,
    appwidgetnoauthview/ed=1/wt=2/ujg=1/rs=AM-SdHvID7fpKYMRHrVCWG6liu-Xx5qOVA/ee=EVNhjf
    :pw7OGc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK
    :SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGROgd:Mlhmy;SNUn3:ZwDk9d;a56pNe:
    JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:
    OTA3Ae;nAFL3:s39S4;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;uY49fb:
    COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:wmnU7d;yxTchf:KUM7Z;zxnPse:GkRiKb/m=
    Wt6vjf,hhhU8,FCpbqb,WhJNk
40  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:803::200a                                https
    ://optimizationguide-pa.googleapis.com/downloads?name=1696267841&target=
    OPTIMIZATION_TARGET_OMNIBOX_URL_SCORING
41  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:803::200a                                https
    ://optimizationguide-pa.googleapis.com/downloads?name=1691042511&target=
    OPTIMIZATION_TARGET_NEW_TAB_PAGE_HISTORY_CLUSTERS_MODULE_RANKING
42  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:803::200a                                https
    ://optimizationguide-pa.googleapis.com/downloads?name=1689043206&target=
    OPTIMIZATION_TARGET_VISUAL_SEARCH_CLASSIFICATION
43  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:803::2003                                https
    ://update.googleapis.com/service/update2/json
44  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:803::200a                                https
    ://optimizationguide-pa.googleapis.com/downloads?name=1699288392&target=
    OPTIMIZATION_TARGET_PAGE_ENTITIES
45  fdb0:8f6e:bc8e:1::2     2a00:1450:400a:803::2003                                https
    ://beacons.gcp.gvt2.com/domainreliability/upload
```

```
46 fdb0:8f6e:bc8e:1::2      2a00:1450:400a:803::200a                                https
       ://optimizationguide-pa.googleapis.com/v1:GetModels?key=AIzaSyBOti4mM-6
       x9WDnZIjIeyEU21OpBXqWBgw
47 fdb0:8f6e:bc8e:1::2      2a00:1450:400a:803::200a                                https
       ://optimizationguide-pa.googleapis.com/downloads?name=1679317318&target=
       OPTIMIZATION_TARGET_LANGUAGE_DETECTION
48 fdb0:8f6e:bc8e:1::2      2a00:1450:400a:803::200a                                https
       ://optimizationguide-pa.googleapis.com/downloads?name=1699288392&target=
       OPTIMIZATION_TARGET_PAGE_ENTITIES
49 fdb0:8f6e:bc8e:1::2      2a00:1450:400a:802::200e                                https
       ://play.google.com/log?format=json&hasfast=true&authuser=0
50 fdb0:8f6e:bc8e:1::2      2a00:1450:400a:803::2003                                https
       ://update.googleapis.com/service/update2/json
51 fdb0:8f6e:bc8e:1::2      2a00:1450:400a:802::200a                                https
       ://chromewebstore.googleapis.com/v2/items/-/storeMetadata:batchGet
52 fdb0:8f6e:bc8e:1::2      2a00:1450:400a:803::2003                                https
       ://update.googleapis.com/service/update2/json
53 fdb0:8f6e:bc8e:1::2      2a00:1450:400a:800::200a                                https
       ://safebrowsing.googleapis.com/v4/threatListUpdates:fetch?$req=
       Ch4KDGdvb2dsZWNocm9tZRIOMTIxLjAuNjE2Ny4xNDAaDAgFEAEiBCABIAIoARoMCAEQASIE...&$ct=
       application/x-protobuf&key=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw
54 fdb0:8f6e:bc8e:1::2      2a00:1450:400a:803::2003                                https
       ://update.googleapis.com/service/update2/json
```

Quelltext D.7: Analyse Privat-Modus: Kommunikation von Chrome im Incognito Modus

```
1  $ grep -F TCP Noriben_19_Feb_24__10_22_069784.csv | grep -Eiv "(edge|wermgr|edgeupdate
       |svchost|sihclient).exe" | grep "chrome\.exe" | awk -F',' '{print $5}' | sort |
       uniq
2  "192.168.100.2:52979 -> 34.95.0.29:443"
3  "192.168.100.2:52981 -> 34.95.0.29:443"
4  "192.168.100.2:52982 -> 34.95.0.29:443"
5  "192.168.100.2:52983 -> 34.95.0.29:443"
6  "192.168.100.2:52986 -> 94.230.211.116:443"
7  "fdb0:8f6e:bc8e:1:0:0:0:2:52978 -> 2a00:1450:400a:808:0:0:0:200a:443"
8  "fdb0:8f6e:bc8e:1:0:0:0:2:52980 -> 2a00:1450:400a:800:0:0:0:200e:443"
9  "fdb0:8f6e:bc8e:1:0:0:0:2:52984 -> 2a00:1450:400a:802:0:0:0:2003:443"
10 "fdb0:8f6e:bc8e:1:0:0:0:2:52985 -> 2a00:1450:400a:808:0:0:0:200a:443"
11 "fdb0:8f6e:bc8e:1:0:0:0:2:52987 -> 2606:4700:0:0:0:0:6812:82ec:443"
12 "fdb0:8f6e:bc8e:1:0:0:0:2:52988 -> 2606:4700:0:0:0:0:6812:82ec:443"
13 "fdb0:8f6e:bc8e:1:0:0:0:2:52989 -> 2606:4700:0:0:0:0:6812:82ec:443"
14 "fdb0:8f6e:bc8e:1:0:0:0:2:52990 -> 2a00:1450:400a:801:0:0:0:2008:443"
15 "fdb0:8f6e:bc8e:1:0:0:0:2:52991 -> 2606:4700:4400:0:0:0:ac40:9b77:443"
16 "fdb0:8f6e:bc8e:1:0:0:0:2:52992 -> 2a00:1450:400a:808:0:0:0:200e:443"
17 "fdb0:8f6e:bc8e:1:0:0:0:2:52993 -> 2600:1901:0:22e6:0:0:0:0:443"
18 "fdb0:8f6e:bc8e:1:0:0:0:2:52994 -> 2a00:1450:400a:801:0:0:0:200a:443"
19 "fdb0:8f6e:bc8e:1:0:0:0:2:52995 -> 2a00:1450:400a:801:0:0:0:200a:443"
20 "fdb0:8f6e:bc8e:1:0:0:0:2:52996 -> 2600:1901:0:476d:0:0:0:0:443"
21 "fdb0:8f6e:bc8e:1:0:0:0:2:52997 -> 2600:1901:0:891c:0:0:0:0:443"
22 "fdb0:8f6e:bc8e:1:0:0:0:2:52998 -> 2600:1901:0:476d:0:0:0:0:443"
23 "fdb0:8f6e:bc8e:1:0:0:0:2:52999 -> 2a00:1450:400a:801:0:0:0:2003:443"
```

Quelltext D.8: Analyse Privat-Modus: HTTP-URIs von Chrome im Incognito Modus

```
$ tshark -r *.tlsdecrypted.pcap -Y "((http || http2) && (ipv6.addr == 2600:1901:0:22e6:0:0:0:0 || ipv6.addr == 2600:1901:0:476d:0:0:0:0 || ipv6.addr == 2600:1901:0:891c:0:0:0:0 || ipv6.addr == 2606:4700:0:0:0:0:6812:82ec || ipv6.addr == 2606:4700:4400:0:0:0:ac40:9b77 || ipv6.addr == 2a00:1450:400a:800:0:0:0:200e || ipv6.addr == 2a00:1450:400a:801:0:0:0:2003 || ipv6.addr == 2a00:1450:400a:801:0:0:0:2008 || ipv6.addr == 2a00:1450:400a:801:0:0:0:200a || ipv6.addr == 2a00:1450:400a:802:0:0:0:2003 || ipv6.addr == 2a00:1450:400a:808:0:0:0:200a || ipv6.addr == 2a00:1450:400a:808:0:0:0:200e || ip.addr == 34.95.0.29 || ip.addr == 94.230.211.116)))" -T fields -e ipv6.src -e ipv6.dst -e ip.src -e ip.dst -e http.request.full_uri -e http2.request.full_uri | awk '{if ($3 == "") next ;print $1" "$2" "$3}'

fdb0:8f6e:bc8e:1::2 2a00:1450:400a:808::200a https://chromewebstore.googleapis.com/v2/items/-/storeMetadata:batchGet
fdb0:8f6e:bc8e:1::2 2a00:1450:400a:800::200e https://clients2.google.com/domainreliability/upload
192.168.100.2 34.95.0.29 https://beacons.gcp.gvt2.com/domainreliability/upload
192.168.100.2 34.95.0.29 https://beacons.gcp.gvt2.com/domainreliability/upload
192.168.100.2 34.95.0.29 https://beacons.gcp.gvt2.com/domainreliability/upload
192.168.100.2 34.95.0.29 https://beacons.gcp.gvt2.com/domainreliability/upload
fdb0:8f6e:bc8e:1::2 2a00:1450:400a:802::2003 https://beacons.gvt2.com/domainreliability/upload-nel
fdb0:8f6e:bc8e:1::2 2a00:1450:400a:802::2003 https://beacons.gvt2.com/domainreliability/upload-nel
fdb0:8f6e:bc8e:1::2 2a00:1450:400a:808::200a https://safebrowsing.googleapis.com/v4/threatListUpdates:fetch?$req=Ch4KDGdvb2dsZWNocm9tZRIOMTIxLjAuNjE2Ny4xNDAaKQgFEAEaG...=&$ct=application/x-protobuf&key=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw
192.168.100.2 94.230.211.116 https://www.bfh.ch/
192.168.100.2 94.230.211.116 https://www.bfh.ch/en/
192.168.100.2 94.230.211.116 https://www.bfh.ch/.resources/bfh-portal/webresources/css/bfh-theme~2024-01-31-10-36-54-000~cache.css
192.168.100.2 94.230.211.116 https://www.bfh.ch/.resources/bfh-portal/webresources/resources/UnitRoundedPro.woff
...
fdb0:8f6e:bc8e:1::2 2a00:1450:400a:801::200a https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTIxLjAuNjE2Ny4xNDASIAkKKvyuAUBjvxIFDb_KyeUSBQ2lkzYkIYTv6Ut61HAV?alt=proto
fdb0:8f6e:bc8e:1::2 2600:1901:0:476d:: https://heatmaps.monsido.com/v1/settings/FNBcb7Vvey435robJ5yVkg.json
192.168.100.2 34.95.0.29 https://beacons.gcp.gvt2.com/domainreliability/upload
```

D.3. Microsoft Edge

Quelltext D.9: Analyse Installation und erster Start: HTTP-POST-Request-URIs von Edge

```
$ tshark -r *.tlsdecrypted.pcap -Y "((http || http2) && (ip.src == 192.168.100.6 || ipv6.src == fdb0:8f6e:bc8e:5::2) && (http.request.method == "POST" || http2.headers.method == "POST"))" -T fields -e ipv6.src -e ipv6.dst -e ip.src -e ip.dst -e http.request.full_uri -e http2.request.full_uri | awk '{if ($3 == "") next ;print $3}' | uniq
https://nav-edge.smartscreen.microsoft.com/api/browser/edge/navigate/3
https://data-edge.smartscreen.microsoft.com/api/browser/edge/data/bloomfilter/x/3
https://data-edge.smartscreen.microsoft.com/api/browser/edge/data/toptraffic/3
https://data-edge.smartscreen.microsoft.com/api/browser/edge/data/settings/3
https://bzib.nelreports.net/api/report?cat=bingbusiness
https://inference.location.live.net/inferenceservice/v21/pox/GetLocationUsingFingerprint
https://edge.microsoft.com/extensioninstallverifier/v1.1/installverify
https://www.googleapis.com/chromewebstore/v1.1/items/verify
https://browser.events.data.msn.com/OneCollector/1.0?cors=true&content-type=application/x-json-stream&client-id=NO_AUTH&client-version=1DS-Web-JS-3.2.8&apikey=0ded60c75e44443aa3484c42c1c43fe8-9fc57d3f-fdac-4bcf-b927-75eafe60192e-7279&upload-time=1708248652955&time-delta-to-apply-millis=use-collector-delta&w=0&anoncknm=app_anon&NoResponseBody=true
https://nw-umwatson.events.data.microsoft.com/Telemetry.Request
https://edgeservices.bing.com/fd/ls/lsp.aspx?
https://edgeservices.bing.com/web/xls.aspx
https://nw-umwatson.events.data.microsoft.com/Telemetry.Request
https://edgeservices.bing.com/web/xls.aspx
https://nw-umwatson.events.data.microsoft.com/Telemetry.Request
https://browser.events.data.msn.com/OneCollector/1.0?cors=true&content-type=application/x-json-stream&client-id=NO_AUTH&client-version=1DS-Web-JS-3.2.8&apikey=0ded60c75e44443aa3484c42c1c43fe8-9fc57d3f-fdac-4bcf-b927-75eafe60192e-7279&upload-time=1708248688667&w=0&anoncknm=app_anon&NoResponseBody=true
https://browser.events.data.msn.com/OneCollector/1.0?cors=true&content-type=application/x-json-stream&client-id=NO_AUTH&client-version=1DS-Web-JS-3.2.8&apikey=0ded60c75e44443aa3484c42c1c43fe8-9fc57d3f-fdac-4bcf-b927-75eafe60192e-7279&upload-time=1708248688696&w=0&anoncknm=app_anon&NoResponseBody=true
https://browser.events.data.msn.com/OneCollector/1.0?cors=true&content-type=application/x-json-stream&client-id=NO_AUTH&client-version=1DS-Web-JS-3.2.8&apikey=0ded60c75e44443aa3484c42c1c43fe8-9fc57d3f-fdac-4bcf-b927-75eafe60192e-7279&upload-time=1708248692230&w=0&anoncknm=app_anon&NoResponseBody=true
https://nw-umwatson.events.data.microsoft.com/Telemetry.Request
https://edgeservices.bing.com/web/xls.aspx
https://edgeservices.bing.com/fd/ls/lsp.aspx?
https://browser.events.data.msn.com/OneCollector/1.0?cors=true&content-type=application/x-json-stream&client-id=NO_AUTH&client-version=1DS-Web-JS-3.2.8&apikey=0ded60c75e44443aa3484c42c1c43fe8-9fc57d3f-fdac-4bcf-b927-75eafe60192e-7279&upload-time=1708248715043&w=0&anoncknm=app_anon&NoResponseBody=true
https://edge.microsoft.com/componentupdater/api/v1/update?cup2key=6:fRM-kuT5Ogg4ejzmoMyCfptpP3Hqc6kps5CavcTC2iM&cup2hreq=0b67240369abf9f226a1698df2f1339eb28fd48581dda88f4f8971491883cfa7
https://browser.events.data.msn.com/OneCollector/1.0?cors=true&content-type=application/x-json-stream&client-id=NO_AUTH&client-version=1DS-Web-JS-3.2.8&apikey=0ded60c75e44443aa3484c42c1c43fe8-9fc57d3f-fdac-4bcf-b927-75eafe60192e-7279&upload-time=1708248716047&w=0&anoncknm=app_anon&NoResponseBody=true
https://nw-umwatson.events.data.microsoft.com/Telemetry.Request
https://deff.nelreports.net/api/report
https://edgeservices.bing.com/web/xls.aspx
https://edge.microsoft.com/componentupdater/api/v1/update
https://self.events.data.microsoft.com/OneCollector/1.0/
https://edge.microsoft.com/componentupdater/api/v1/update
https://nw-umwatson.events.data.microsoft.com/Telemetry.Request
https://self.events.data.microsoft.com/OneCollector/1.0/
https://deff.nelreports.net/api/report
```

```
https://edge.microsoft.com/componentupdater/api/v1/update
https://nav-edge.smartscreen.microsoft.com/api/browser/edge/navigate/3
https://data-edge.smartscreen.microsoft.com/api/browser/edge/data/toptraffic/3
https://data-edge.smartscreen.microsoft.com/api/browser/edge/data/bloomfilter/x/3
https://data-edge.smartscreen.microsoft.com/api/browser/edge/data/settings/3
https://nav-edge.smartscreen.microsoft.com/api/browser/edge/navigate/3
https://nw-umwatson.events.data.microsoft.com/Telemetry.Request
https://edge.microsoft.com/componentupdater/api/v1/update
https://nw-umwatson.events.data.microsoft.com/Telemetry.Request
https://edge.microsoft.com/componentupdater/api/v1/update
https://nw-umwatson.events.data.microsoft.com/Telemetry.Request
https://edge.microsoft.com/componentupdater/api/v1/update?cup2key=6:
    PyeUu_5uVnTfKchN6OeWD3zUHWAT1XXPlYiSVlwgaLY&cup2hreq=4
    f2fdc55f1faf4d93e79197dbeb20444a76874d84950563fb9f85667da971d4e
https://edge.microsoft.com/componentupdater/api/v1/update
https://deff.nelreports.net/api/report
https://edge.microsoft.com/componentupdater/api/v1/update
https://deff.nelreports.net/api/report
https://nav-edge.smartscreen.microsoft.com/api/browser/edge/navigate/3
https://browser.events.data.msn.com/OneCollector/1.0?cors=true&content-type=
    application/x-json-stream&client-id=NO_AUTH&client-version=1DS-Web-JS-3.2.8&apikey
    =0ded60c75e44443aa3484c42c1c43fe8-9fc57d3f-fdac-4bcf-b927-75eafe60192e-7279&upload-
    time=1708249205967&w=0&anoncknm=app_anon&NoResponseBody=true
https://nav-edge.smartscreen.microsoft.com/api/browser/edge/navigate/3
https://postnav-edge.smartscreen.microsoft.com/api/browser/edge/navigationcomplete/3
https://www.bing.com/api/shopping/v1/item/search?appid=67220
    BD2169C2EA709984467C21494086DF8CA85&features=persnlcashback&sf=cashback1
https://watson.events.data.microsoft.com/Telemetry.Request
https://browser.events.data.msn.com/OneCollector/1.0?cors=true&content-type=
    application%2Fx-json-stream&client-id=NO_AUTH&client-version=peregrine-lite-
    telemetry-20240216.226&apikey=0ded60c75e44443aa3484c42c1c43fe8-9fc57d3f-fdac-4bcf-
    b927-75eafe60192e-7279&upload-time=1708249233754&w=0&anoncknm=app_anon&
    NoResponseBody=true
...
https://browser.events.data.msn.com/OneCollector/1.0?cors=true&content-type=
    application%2Fx-json-stream&client-id=NO_AUTH&client-version=peregrine-lite-
    telemetry-20240216.226&apikey=0ded60c75e44443aa3484c42c1c43fe8-9fc57d3f-fdac-4bcf-
    b927-75eafe60192e-7279&upload-time=1708249236212&w=0&anoncknm=app_anon&
    NoResponseBody=true
https://srtb.msn.com/auction
https://browser.events.data.msn.com/OneCollector/1.0?cors=true&content-type=
    application/x-json-stream&client-id=NO_AUTH&client-version=1DS-Web-JS-3.2.8&apikey
    =0ded60c75e44443aa3484c42c1c43fe8-9fc57d3f-fdac-4bcf-b927-75eafe60192e-7279&upload-
    time=1708249238450&time-delta-to-apply-millis=use-collector-delta&w=0&anoncknm=
    app_anon&NoResponseBody=true
https://browser.events.data.msn.com/OneCollector/1.0?cors=true&content-type=
    application/x-json-stream&client-id=NO_AUTH&client-version=1DS-Web-JS-3.2.8&apikey
    =0ded60c75e44443aa3484c42c1c43fe8-9fc57d3f-fdac-4bcf-b927-75eafe60192e-7279&upload-
    time=1708249239455&w=0&anoncknm=app_anon&NoResponseBody=true
...
https://aefd.nelreports.net/api/report?cat=bingth
https://browser.events.data.msn.com/OneCollector/1.0?cors=true&content-type=
    application/x-json-stream&client-id=NO_AUTH&client-version=1DS-Web-JS-3.2.8&apikey
    =0ded60c75e44443aa3484c42c1c43fe8-9fc57d3f-fdac-4bcf-b927-75eafe60192e-7279&upload-
    time=1708249253257&w=0&anoncknm=app_anon&NoResponseBody=true
...
https://browser.events.data.msn.com/OneCollector/1.0?cors=true&content-type=
    application/x-json-stream&client-id=NO_AUTH&client-version=1DS-Web-JS-3.2.8&apikey
    =0ded60c75e44443aa3484c42c1c43fe8-9fc57d3f-fdac-4bcf-b927-75eafe60192e-7279&upload-
    time=1708249427908&w=0&anoncknm=app_anon&NoResponseBody=true
```

Quelltext D.10: Analyse Installation und erster Start: Inhalt Telemetrie-HTTP-POST-Request von Edge an `https://nw-umwatson.events.data.microsoft.com/Telemetry.Request`

```
<?xml version="1.0"?>
<req ver="2">
 <tlm>
  <src>
   <desc>
    <mach>
     <os>
      <arg nm="vermaj" val="10"/>
      <arg nm="vermin" val="0"/>
      <arg nm="verbld" val="22631"/>
      <arg nm="vercsdbld" val="3007"/>
      <arg nm="verqfe" val="3007"/>
      <arg nm="csdbld" val="3007"/>
      <arg nm="versp" val="0"/>
      <arg nm="arch" val="9"/>
      <arg nm="lcid" val="2057"/>
      <arg nm="geoid" val="223"/>
      <arg nm="sku" val="101"/>
      <arg nm="domain" val="0"/>
      <arg nm="portos" val="0"/>
      <arg nm="ram" val="4079"/>
      <arg nm="svolsz" val="79"/>
      <arg nm="wimbt" val="0"/>
      <arg nm="blddt" val="220506"/>
      <arg nm="bldtm" val="1250"/>
      <arg nm="bldbrch" val="ni_release"/>
      <arg nm="os" val="Windows"/>
      <arg nm="osver" val="10.0.22621.3007.amd64fre.ni_release.220506-1250"/>
      <arg nm="buildflightid" val=""/>
      <arg nm="expid" val=""/>
      <arg nm="edition" val="Core"/>
     </os>
     <hw>
      <arg nm="form" val="2"/>
      <arg nm="arch" val="9"/>
      <arg nm="deviceclass" val="Windows.Desktop"/>
      <arg nm="sysmfg" val="innotek GmbH"/>
      <arg nm="syspro" val="VirtualBox"/>
      <arg nm="bv" val="VirtualBox"/>
      <arg nm="ram" val="0"/>
      <arg nm="proccnt" val="2"/>
      <arg nm="proclsp" val="2304"/>
      <arg nm="wscpusc" val="0"/>
      <arg nm="wsdsksc" val="0"/>
      <arg nm="wscpudn" val="Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz"/>
      <arg nm="wsdgsc" val="0"/>
      <arg nm="aoac" val="0"/>
      <arg nm="bssku" val=""/>
      <arg nm="chid" val="{df037cfb-6deb-5b17-aa71-67af033ccb01}"/>
      <arg nm="sdksz" val="80"/>
     </hw>
     <ctrl>
      <arg nm="tm" val="133527222704735580"/>
      <arg nm="mid" val="D3423B1D-74AF-4F69-9FEA-6BC0E3CCA422"/>
      <arg nm="sample" val="55987732"/>
      <arg nm="msft" val="0"/>
      <arg nm="test" val="0"/>
      <arg nm="scf" val="0"/>
      <arg nm="commercialid" val=""/>
      <arg nm="telemetry" val="Optional"/>
     </ctrl>
```

```
62      </mach>
63     </desc>
64    </src>
65    <reqs>
66     <req key="1">
67      <namespace svc="watson" ptr="generic" gp="generic" app="msedge.exe">
68       <arg nm="p1" val="msedge.exe"/>
69       <arg nm="p2" val="120.0.2210.144"/>
70       <arg nm="p3" val="msedge.dll"/>
71       <arg nm="p4" val="120.0.2210.144"/>
72       <arg nm="p5" val="63928334"/>
73       <arg nm="p6" val="gpu-process"/>
74       <arg nm="p7" val="0x80000003"/>
75       <arg nm="p8" val="0"/>
76      </namespace>
77      <ctrl>
78       <arg nm="reportid" val="6c049b1f-8e49-4821-9ae3-d9b296e78811"/>
79       <arg nm="procmeta.Channel" val=""/>
80       <arg nm="procmeta.MetricsClientId" val="f0c8f6d7-0db9-4f51-a755-a0b76a401e47"/>
81       <arg nm="procmeta.MetricsClientIdHash" val="-7834778464411454359"/>
82       <arg nm="procmeta.MetricsSessionId" val="0"/>
83       <arg nm="procmeta.OfficialBuild" val="1"/>
84       <arg nm="procmeta.RuntimeVariationsSeedETag" val="&amp;quot;KeEyn1Ohuu+xx/
             W4itmxw8KckFt4OzMV49SUPr1IUcs=&amp;quot;"/>
85       <arg nm="procmeta.UXConfigCorrelationId" val="
             oWt6chzexxEqIfNxNmMSYFjfXDsk42GOqCjWtPil2xA="/>
86       <arg nm="procmeta.VariationsSeedETag" val="&amp;quot;FvzberxKF+
             pMuURXPggSPE7n5z2nrZaA1t6jKiMkORU=&amp;quot;"/>
87      </ctrl>
88      <cmd nm="event">
89       <arg nm="eventtype" val="crashpad_exp"/>
90       <arg nm="cat" val="generic"/>
91       <arg nm="p1" val="msedge.exe"/>
92       <arg nm="p2" val="120.0.2210.144"/>
93       <arg nm="p3" val="msedge.dll"/>
94       <arg nm="p4" val="120.0.2210.144"/>
95       <arg nm="p5" val="63928334"/>
96       <arg nm="p6" val="gpu-process"/>
97       <arg nm="p7" val="0x80000003"/>
98       <arg nm="p8" val="0"/>
99       <arg nm="appsessionguid" val="00002348-0001-000e-0277-91334d62da01"/>
100     </cmd>
101    </req>
102   </reqs>
103  </tlm>
104 </req>
```

Quelltext D.11: Analyse Installation und erster Start: Inhalt Telemetrie-HTTP-POST-Request von Edge an `https://deff.nelreports.net/api/report`

```
...
substrate.office.com/todob2/api/v1/ webshell.suite.office.com/api/shell/newtab wss://
    www.bing.com/opaluqu/speech/recognition/interactive/cognitiveservices/ wss://sr.
    bing.com/opaluqu/speech/recognition/interactive/cognitiveservices/ www.bing.com/fd/
    ls/ls.gif www.msn.com www.msn.cn www.microsoftstart.com cn.bing.com/api/v6/Places/
    AutoSuggest cn.bing.com/api/v6/geoentities cn.bing.com/bnc/ cn.bing.com/pnp/ cn.
    bing.com/profile/interestmanager/update *.cn.mm.bing.net *.mm.cn.bing.net www.bing.
    com/HPImageArchive.aspx www.bing.com/api/custom/opal/reco/ www.bing.com/DSB cn.bing
    .com/DSB www.bing.com/DSB/partner/ cn.bing.com/DSB/partner/ ... www.bing.com/retail
    /msn/api/shopcard www.bing.com/retailexp/msn/api/ www.bing.com/retailexpdata/
    msndata/ www.bing.com/rp/rms_pr.png www.bing.com/th wus-streaming-video-msn-com.
    akamaized.net prod-streaming-video-msn-com.akamaized.net prod-streaming-video.msn.
    cn zerocodecms.blob.core.windows.net *.oneservice.msn.com *.oneservice.msn.cn api.
    msn.com api.msn.cn ent-api.msn.com ent-api.msn.cn ppe-api.msn.com ppe-api.msn.cn
    graph.microsoft.com/beta/ graph.microsoft.com/v1.0/ https://*.vo.msecnd.net https
    ://user.auth.xboxlive.com/user/authenticate https://xsts.auth.xboxlive.com/xsts/
    authorize https://titlehub.xboxlive.com/users/ https://t.ssl.ak.dynamic.tiles.
    virtualearth.net https://dynamic.t0.tiles.ditu.live.com https://dev.virtualearth.
    net/REST/v1/Routes/ https://dev.ditu.live.com/REST/v1/Routes/ https://dev.
    virtualearth.net/REST/v1/Locations/ https://dev.ditu.live.com/REST/v1/Locations/
    browser.events.data.microsoft.com;default-src 'none';font-src 'self' data: assets.
    msn.com assets2.msn.com assets.msn.cn assets2.msn.cn;frame-src https://api.msn.com/
    auth/cookie/silentpassport https://api.msn.cn/auth/cookie/silentpassport https://
    www.msn.com https://www.msn.cn https://www.microsoftstart.com login.live.com login.
    microsoftonline.com www.bing.com/covid www.bing.com/rewardsapp/flyout www.bing.com/
    shop www.bing.com/shop/halloween www.bing.com/videos/search www.facebook.com www.
    odwebp.svc.ms www.youtube.com msn.pluto.tv
...
sip: mailto: edge-auth.microsoft.com;img-src https://* blob: chrome-search://ntpicon/
    chrome-search://local-ntp/ chrome-search://theme/ data:;media-src 'self' blob: *.
    mavideo.microsoft.com assets.msn.com assets2.msn.com assets.msn.cn assets2.msn.cn
    https://sapphire.azureedge.net th.bing.com/th wus-streaming-video-msn-com.akamaized
    .net prod-streaming-video-msn-com.akamaized.net prod-streaming-video.msn.cn
    liveshopping.azureedge.net;report-to csp-endpoint;style-src 'self' 'unsafe-inline'
    c.s-microsoft.com/mscc/ assets.msn.com assets2.msn.com assets.msn.cn assets2.msn.cn
    ;worker-src 'self' blob: 'report-sample';require-trusted-types-for 'script';trusted
    -types serviceWorkerUrlPolicy baw-trustedtypes-policy svgPassThroughPolicy
    webpackTrustedTypesPolicy webWorkerUrlPolicy inlineHeadCssPassthroughPolicy
    bundleUrlPolicy fallbackBundleUrlPolicy scriptSrcUrlPolicy dompurify fast-html '
    allow-duplicates';script-src 'nonce-qv/lwwbCaxBkWe2zn8QBRH3oEyFTb8JXIuB+PT5+CiA=' '
    strict-dynamic'","referrer":"","sample":"Element innerHTML|Personalisierte Werbung
    und Inhalte, Mes","sourceFile":"https://assets.msn.com/staticsb/statics/latest/
    oneTrust/1.8/scripttemplates/202310.2.0/otBannerSdk.js","statusCode":200},"type":"
    csp-violation","url":"https://ntp.msn.com/edge/ntp?&form=MT004B&OCID=MT004B","
    user_agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
    like Gecko) Chrome/120.0.0.0 Safari/537.36 Edg/120.0.0.0"},{"age":374436,"body":{"
    blockedURL":"trusted-types-sink","columnNumber":70437,"disposition":"report","
    documentURL":"https://ntp.msn.com/edge/ntp?&form=MT004B&OCID=MT004B","
    effectiveDirective":"require-trusted-types-for","lineNumber":7,"originalPolicy":"
    child-src 'self';connect-src 'self' *.mavideo.microsoft.com arc.msn.com assets.msn.
    com
...
```

```
6 www.bing.com/retailexpdata/msndata/ www.bing.com/rp/rms_pr.png www.bing.com/th wus-
    streaming-video-msn-com.akamaized.net prod-streaming-video-msn-com.akamaized.net
    prod-streaming-video.msn.cn zerocodecms.blob.core.windows.net *.oneservice.msn.com
    *.oneservice.msn.cn api.msn.com api.msn.cn ent-api.msn.com ent-api.msn.cn ppe-api.
    msn.com ppe-api.msn.cn graph.microsoft.com/beta/ graph.microsoft.com/v1.0/ https
    ://*.vo.msecnd.net https://user.auth.xboxlive.com/user/authenticate https://xsts.
    auth.xboxlive.com/xsts/authorize https://titlehub.xboxlive.com/users/ https://t.ssl
    .ak.dynamic.tiles.virtualearth.net https://dynamic.t0.tiles.ditu.live.com https://
    dev.virtualearth.net/REST/v1/Routes/ https://dev.ditu.live.com/REST/v1/Routes/
    https://dev.virtualearth.net/REST/v1/Locations/ https://dev.ditu.live.com/REST/v1/
    Locations/ browser.events.data.microsoft.com;default-src 'none';font-src 'self'
    data: assets.msn.com assets2.msn.com assets.msn.cn assets2.msn.cn;frame-src https
    ://api.msn.com/auth/cookie/silentpassport https://api.msn.cn/auth/cookie/
    silentpassport https://www.msn.com https://www.msn.cn https://www.microsoftstart.
    com login.live.com login.microsoftonline.com www.bing.com/covid www.bing.com/
    rewardsapp/flyout www.bing.com/shop www.bing.com/shop/halloween www.bing.com/videos
    /search www.facebook.com www.odwebp.svc.ms www.youtube.com msn.pluto.tv www.bing.
    com/wpt/prefetchcib https://res.cdn.office.net/ business.bing.com sip: mailto: edge
    -auth.microsoft.com;img-src https://* blob: chrome-search://ntpicon/ chrome-search
    ://local-ntp/ chrome-search://theme/ data:;media-src 'self' blob: *.mavideo.
    microsoft.com assets.msn.com assets2.msn.com assets.msn.cn assets2.msn.cn https://
    sapphire.azureedge.net th.bing.com/th wus-streaming-video-msn-com.akamaized.net
    prod-streaming-video-msn-com.akamaized.net prod-streaming-video.msn.cn
7 ...
```

Quelltext D.12: Analyse Privat-Modus: HTTP-URIs von Edge im InPrivate Modus

```
$ tshark -r *.tlsdecrypted.pcap -Y "((http || http2) && (ip.src == 192.168.100.6 || ipv6.src == fdb0:8f6e:bc8e:5::2))" -T fields -e ipv6.src -e ipv6.dst -e ip.src -e ip.dst -e http.request.full_uri -e http2.request.full_uri | awk '{if ($3 == "") next ;print $0}' | uniq
                192.168.100.6   23.0.174.114             https://www.bing.com/bloomfilterfiles/ExpandedDomainsFilterGlobal.json
                192.168.100.6   173.222.108.243 http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?f876aa3177144593
                192.168.100.6   40.79.173.40    https://self.events.data.microsoft.com/OneCollector/1.0/
                192.168.100.6   20.189.173.22   https://nw-umwatson.events.data.microsoft.com/Telemetry.Request
fdb0:8f6e:bc8e:5::2     2620:1ec:12::239                                https://edge.microsoft.com/entityextractiontemplates/api/v1/assets/find-assets?name=edge_hub_apps_manifest_gz&version=4.10.*&channel=stable&key=d414dd4f9db345fa8003e32adc81b362
fdb0:8f6e:bc8e:5::2     2620:1ec:46::60                         https://edgeassetservice.azureedge.net/assets/edge_hub_apps_manifest_gz/4.10.29/asset?sv=2017-07-29&sr=c&sig=%2Fwp1fD0xo8ywYyo5yFzHEjCMobUSk%2BZ4nmFYB%2FqjsBg%3D&st=2021-01-01T00%3A00%3A00Z&se=2024-05-01T00%3A00%3A00Z&sp=r&assetgroup=Shoreline
                192.168.100.6   68.219.88.225   https://g.live.com/odclientsettings/ProdV2?OneDriveUpdate=ead60a40614eb89cd15fb26d15
                192.168.100.6   104.79.89.3     https://oneclient.sfx.ms/PreSignInSettings/Prod/2024-02-16-22-50-47/PreSignInSettingsConfig.json?OneDriveUpdate=ead60a40614eb89cd15fb26d15
                192.168.100.6   13.67.191.143           https://msedge.api.cdp.microsoft.com/api/v2/contents/Browser/namespaces/Default/names?action=batchupdates
                192.168.100.6   94.230.211.116          https://www.bfh.ch/
                192.168.100.6   94.230.211.116          https://www.bfh.ch/en/
                192.168.100.6   4.175.88.233            https://nav-edge.smartscreen.microsoft.com/api/browser/edge/navigate/3
                192.168.100.6   94.230.211.116          https://www.bfh.ch/.resources/bfh-portal/webresources/resources/UnitRoundedPro.woff
                192.168.100.6   94.230.211.116          https://www.bfh.ch/.resources/bfh-portal/webresources/css/bfh-theme~2024-01-31-10-36-54-000~cache.css
                192.168.100.6   94.230.211.116          https://www.bfh.ch/dam/jcr:0d9ff345-1271-4195-9908-44f69806a035/Logo%20BFH_dunkler.svg
                192.168.100.6   94.230.211.116          https://www.bfh.ch/dam/jcr:5ff2c217-3912-47b0-a277-68de24042856/Logo%20BFH_weiss.svg
fdb0:8f6e:bc8e:5::2     2a02:26f0:3400::1703:582a                       https://www.bing.com/bloomfilterfiles/ExpandedDomainsFilterGlobal.json
                192.168.100.6   94.230.211.116          https://www.bfh.ch/dam/jcr:eaa68853-a1f9-4198-a2a5-e19eae244092/bfh-logo.svg
                192.168.100.6   94.230.211.116          https://www.bfh.ch/dam/jcr:5555446e-64fa-4d32-bf72-265be4d6332c/BFH-Logo%20Dach%20weiss.svg
fdb0:8f6e:bc8e:5::2     2606:4700::6812:82ec                            https://cdn.cookielaw.org/consent/2e74eb50-813e-43c2-a388-3b13799d4776/OtAutoBlock.js
fdb0:8f6e:bc8e:5::2     2606:4700::6812:82ec                            https://cdn.cookielaw.org/scripttemplates/otSDKStub.js
                192.168.100.6   94.230.211.116          https://www.bfh.ch/.imaging/mte/bfh-theme/hero-xxs/dam/bfh.ch/globale-assets/bild/de/hero/Hero_Infoveranstaltung_2.jpg/jcr:content/Hero_Infoveranstaltung_2.jpg
                192.168.100.6   94.230.211.116          https://www.bfh.ch/.resources/bfh-portal/webresources/js/scripts~2024-01-31-10-36-56-000~cache.js
                192.168.100.6   94.230.211.116          https://www.bfh.ch/.imaging/mte/bfh-theme/teaser-md/dam/bfh.ch/globale-assets/bild/en/SH2024_KeyVisual_16x9_EN.jpg/jcr:content/SH2024_KeyVisual_16x9_EN.jpg
```

```
26                  192.168.100.6    94.230.211.116          https://www.bfh.ch/.imaging/
                        mte/bfh-theme/teaser-md/dam/bfh.ch/departementsinhalte/soziale-
                        arbeit/events/2023/bild/Logo_Hack4SocialGood_100K.jpg/jcr:content/
                        Logo_Hack4SocialGood_100K.jpg
27                  192.168.100.6    94.230.211.116          https://www.bfh.ch/.imaging/
                        mte/bfh-theme/teaser-md/dam/bfh.ch/globale-assets/bild/de/
                        veranstaltungen/2024/Logo-international-career-day-2024.png/jcr:
                        content/Logo-international-career-day-2024.png
28                  192.168.100.6    94.230.211.116          https://www.bfh.ch/.imaging/
                        mte/bfh-theme/teaser-md/dam/bfh.ch/globale-assets/bild/de/
                        news_stories/2024/Olis-Kohle/Olis_Kohle_1.jpg/jcr:content/
                        Olis_Kohle_1.jpg
29                  192.168.100.6    94.230.211.116          https://www.bfh.ch/.imaging/
                        mte/bfh-theme/teaser-md/dam/bfh.ch/globale-assets/bild/de/
                        news_stories/2023/digitalisierung-pflege/Firefly-Visualize-the-
                        patient-journey-through-the-healthcare-system--from-symptom-
                        identification-to-.jpg/jcr:content/Firefly%20Visualize%20the%20
                        patient%20journey%20through%20the%20healthcare%20system,%20from%20
                        symptom%20identification%20to%20.jpg
30                  192.168.100.6    94.230.211.116          https://www.bfh.ch/.imaging/
                        mte/bfh-theme/teaser-md/dam/bfh.ch/departementsinhalte/ti/2023/news
                        /app-skf-mindcare/t-app-skf-mindcare-bfh.jpg/jcr:content/t-app-skf-
                        mindcare-bfh.jpg
31                  192.168.100.6    94.230.211.116          https://www.bfh.ch/.imaging/
                        mte/bfh-theme/teaser-md/dam/bfh.ch/globale-assets/bild/de/
                        news_stories/2023/Lukas_K-ng.JPG/jcr:content/Lukas_K%C3%BCng.JPG
32                  192.168.100.6    94.230.211.116          https://www.bfh.ch/.imaging/
                        mte/bfh-theme/teaser-md/dam/bfh.ch/globale-assets/bild/de/
                        veranstaltungen/2023/BFH-Tag-2023/DSC05573.jpg/jcr:content/DSC05573
                        .jpg
33                  192.168.100.6    94.230.211.116          https://www.bfh.ch/.imaging/
                        mte/bfh-theme/teaser-md/dam/bfh.ch/forschung/ti/institute-for-
                        patient-centered-digital-health/bild/t-Institute-patient-centered-
                        digital-health.jpg/jcr:content/t-Institute-patient-centered-digital
                        -health.jpg
34                  192.168.100.6    94.230.211.116          https://www.bfh.ch/dam/jcr:
                        c3cb21c5-7788-4d9e-be58-f3eeb974052b/logo_l-xs-home-und-footer_en.
                        svg
35                  192.168.100.6    94.230.211.116          https://www.bfh.ch/dam/jcr:2
                        dc2fcae-1d27-49cb-9bc5-421f56a4fc7a/swissuniversities.svg
36                  192.168.100.6    94.230.211.116          https://www.bfh.ch/dam/jcr:24
                        d8e5c3-1713-42a9-9ba3-4f47a8f4398b/efqm-member.svg
37                  192.168.100.6    94.230.211.116          https://www.bfh.ch/dam/jcr:7
                        acd637a-40e4-4e93-a3a5-8c38046151f9/institutional-accreditation-
                        heda.svg
38                  192.168.100.6    94.230.211.116          https://www.bfh.ch/.imaging/
                        mte/bfh-theme/navigation-configured-teaser-md/dam/bfh.ch/globale-
                        assets/bild/de/studium/GB_Kachel_Studierende_3.jpg/jcr:content/
                        GB_Kachel_Studierende_3.jpg
39                  192.168.100.6    94.230.211.116          https://www.bfh.ch/.imaging/
                        mte/bfh-theme/navigation-configured-teaser-md/dam/bfh.ch/globale-
                        assets/bild/de/hero/KacheL_Weiterbildung_Startseite.jpg/jcr:content
                        /KacheL_Weiterbildung_Startseite.jpg
40                  192.168.100.6    94.230.211.116          https://www.bfh.ch/.imaging/
                        mte/bfh-theme/navigation-configured-teaser-md/dam/bfh.ch/globale-
                        assets/bild/de/forschung_dienstleistung/
                        KacheL_Forschung_Startseite_2020.jpg/jcr:content/
                        KacheL_Forschung_Startseite_2020.jpg
41                  192.168.100.6    94.230.211.116          https://www.bfh.ch/.resources/
                        bfh-portal/webresources/resources/icomoon.ttf
42  fdb0:8f6e:bc8e:5::2      2606:4700::6812:82ec                          https://cdn.
        cookielaw.org/consent/2e74eb50-813e-43c2-a388-3b13799d4776/2e74eb50-813e-43c2-a388
        -3b13799d4776.json
```

```
43 fdb0:8f6e:bc8e:5::2      2a00:1450:400a:808::2008                                    https
       ://www.googletagmanager.com/gtm.js?id=GTM-PG9RPGJ
44 fdb0:8f6e:bc8e:5::2      2606:4700:4400::6812:2089                                   https
       ://geolocation.onetrust.com/cookieconsentpub/v1/geo/location
45 fdb0:8f6e:bc8e:5::2      2606:4700::6812:82ec                                  https://cdn.
       cookielaw.org/scripttemplates/202310.2.0/otBannerSdk.js
46                  192.168.100.6    94.230.211.116          https://www.bfh.ch/.imaging/
                        mte/bfh-theme/hero-md/dam/bfh.ch/globale-assets/bild/de/hero/
                        Hero_Infoveranstaltung_2.jpg/jcr:content/Hero_Infoveranstaltung_2.
                        jpg
47                  192.168.100.6    94.230.211.116          https://www.bfh.ch/.imaging/
                        mte/bfh-theme/hero-md/dam/bfh.ch/globale-assets/bild/de/hero/
                        Hero_Dach_Studium_2020.jpg/jcr:content/Hero_Dach_Studium_2020.jpg
48                  192.168.100.6    94.230.211.116          https://www.bfh.ch/.imaging/
                        mte/bfh-theme/hero-md/dam/bfh.ch/departementsinhalte/soziale-arbeit
                        /bild/hero-bilder/Hero_WB_1.jpg/jcr:content/Hero_WB_1.jpg
49                  192.168.100.6    94.230.211.116          https://www.bfh.ch/.resources/
                        bfh-portal/webresources/resources/ajax-loader.gif
50 fdb0:8f6e:bc8e:5::2      2a00:1450:400a:808::200e                                    https
       ://www.google-analytics.com/mp/collect?measurement_id=G-ZG71GWJVC6&api_secret=
       TKl66DxKTW2I7H2JauIOGQ
51                  192.168.100.6    94.230.211.116          https://www.bfh.ch/.resources/
                        bfh-portal/webresources/resources/slick.woff
52 fdb0:8f6e:bc8e:5::2      2606:4700::6812:82ec                                  https://cdn.
       cookielaw.org/consent/2e74eb50-813e-43c2-a388-3b13799d4776/8dc6dc5e-ed90-4cd1-bd6f-
       da9fd08f5a21/en-gb.json
53 fdb0:8f6e:bc8e:5::2      2620:1ec:12::239                                      https://edge.
       microsoft.com/autofillservice/v1/pages/
       ChVDaHJvbWUvMTIwLjAuMjIxMC4xNDQSGQnyhkkG5kMxshIFDb_KyeUp_7eMaNOExvO=?alt=proto
54 fdb0:8f6e:bc8e:5::2      2620:1ec:12::239                                      https://edge.
       microsoft.com/autofillservice/v1/pages/
       ChVDaHJvbWUvMTIwLjAuMjIxMC4xNDQSGQnyhkkG5kMxshIFDb_KyeUp1xP1xZoOcYo=?alt=proto
55 fdb0:8f6e:bc8e:5::2      2620:1ec:12::239                                      https://edge.
       microsoft.com/autofillservice/core/page/-3277194699099346574/-2192945148160582227
56 fdb0:8f6e:bc8e:5::2      2600:1901:0:22e6::                                    https://app-
       script.monsido.com/v2/monsido-script.js
57 fdb0:8f6e:bc8e:5::2      2606:4700::6812:82ec                                  https://cdn.
       cookielaw.org/scripttemplates/202310.2.0/assets/otCenterRounded.json
58 fdb0:8f6e:bc8e:5::2      2606:4700::6812:82ec                                  https://cdn.
       cookielaw.org/scripttemplates/202310.2.0/assets/v2/otPcCenter.json
59 fdb0:8f6e:bc8e:5::2      2606:4700::6812:82ec                                  https://cdn.
       cookielaw.org/scripttemplates/202310.2.0/assets/otCookieSettingsButton.json
60 fdb0:8f6e:bc8e:5::2      2606:4700::6812:82ec                                  https://cdn.
       cookielaw.org/scripttemplates/202310.2.0/assets/otCommonStyles.css
61 fdb0:8f6e:bc8e:5::2      2a00:1450:400a:808::200e                                    https
       ://www.google-analytics.com/mp/collect?measurement_id=G-ZG71GWJVC6&api_secret=
       TKl66DxKTW2I7H2JauIOGQ
62                  192.168.100.6    94.230.211.116          https://www.bfh.ch/.resources/
                        bfh-portal/webresources/resources/favicons/bfh-portal/favicon-32x32
                        .png
63 fdb0:8f6e:bc8e:5::2      2606:4700::6812:82ec                                  https://cdn.
       cookielaw.org/logos/static/ot_guard_logo.svg
64 fdb0:8f6e:bc8e:5::2      2606:4700::6812:82ec                                  https://cdn.
       cookielaw.org/logos/a897cf9b-0009-4f08-a8a4-a7698f1d7c6d/8185b89d-412c-4305-a444-75
       dac5753e11/c16787d2-4f7d-4027-9d4e-cfbe19b2d54e/logo_l-xs-home-und-footer_de.png
65 fdb0:8f6e:bc8e:5::2      2606:4700::6812:82ec                                  https://cdn.
       cookielaw.org/logos/static/ot_company_logo.png
66 fdb0:8f6e:bc8e:5::2      2606:4700::6812:82ec                                  https://cdn.
       cookielaw.org/logos/static/powered_by_logo.svg
67 fdb0:8f6e:bc8e:5::2      2600:1901:0:476d::                                    https://
       heatmaps.monsido.com/v1/heatmaps.js
68 fdb0:8f6e:bc8e:5::2      2600:1901:0:891c::                                    https://
       tracking.monsido.com/?a=FNBcb7Vvey435robJ5yVkg&b=https%3A%2F%2Fwww.bfh.ch%2Fen%2F&c
```

```
    =56B1708337221867&d=1024x768&f=1D91708337221867&h=2
fdb0:8f6e:bc8e:5::2      2600:1901:0:476d::                                    https://
    heatmaps.monsido.com/v1/settings/FNBcb7Vvey435robJ5yVkg.json
                 192.168.100.6    13.107.6.158            https://business.bing.com/work
                     /api/v2/tenant/my/settingswithflights?&clienttype=edge-omnibox
                 192.168.100.6    13.107.6.158            https://business.bing.com/api/
                     v1/user/token/microsoftgraph?&clienttype=edge-omnibox
                 192.168.100.6    13.107.6.158            https://business.bing.com/work
                     /api/v2/tenant/my/settingswithflights?&clienttype=edge-omnibox
                 192.168.100.6    13.107.6.158            https://business.bing.com/api/
                     v1/user/token/microsoftgraph?&clienttype=edge-omnibox
```

D.4. Mozilla Firefox

Quelltext D.13: Analyse Installation und erster Start: Durch den Firefox-Installer gestartete Prozesse

```
$ grep -F "Process Create" Noriben_18_Feb_24__13_18_210754.csv | sed 's,\",,g' | grep -Eiv "(edge|edgeupdate|msedgewebview2|MsMpEng|svchost|SystemSettings).exe" | awk -F ',' '{print $2" ("$3") -> "$5" ("$7")£   "$8}' | sed 's,\£,\n,g'
...
Explorer.EXE (4612) -> C:\tools\Firefox Installer.exe (PID: 996)
    Command line: C:\tools\Firefox Installer.exe
Firefox Installer.exe (996) -> C:\Users\browser\AppData\Local\Temp\7zS4E3274B1\setup-stub.exe (PID: 6036)
    Command line: .\setup-stub.exe
...
setup-stub.exe (6036) -> C:\Users\browser\AppData\Local\Temp\7zS4E3274B1\setup-stub.exe (PID: 476)
    Command line: C:\Users\browser\AppData\Local\Temp\7zS4E3274B1\setup-stub.exe /UAC:4035C /NCRC
...
setup-stub.exe (476) -> C:\Users\browser\AppData\Local\Temp\nsfC928.tmp\download.exe (PID: 7020)
    Command line: C:\Users\browser\AppData\Local\Temp\nsfC928.tmp\download.exe /LaunchedFromStub /INI=C:\Users\browser\AppData\Local\Temp\nsfC928.tmp\config.ini
...
download.exe (7020) -> C:\Users\browser\AppData\Local\Temp\7zSC6BF0102\setup.exe (PID: 8160)
    Command line: .\setup.exe /LaunchedFromStub /INI=C:\Users\browser\AppData\Local\Temp\nsfC928.tmp\config.ini
setup.exe (8160) -> C:\Windows\system32\regsvr32.exe (PID: 1324)
    Command line: C:\Windows\system32\regsvr32.exe /s C:\Program Files\Mozilla Firefox\AccessibleMarshal.dll
setup.exe (8160) -> C:\Program Files\Mozilla Firefox\maintenanceservice_installer.exe (PID: 2016)
    Command line: C:\Program Files\Mozilla Firefox\maintenanceservice_installer.exe
maintenanceservice_installer.exe (2016) -> C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe (PID: 5212)
    Command line: C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe install
setup.exe (8160) -> C:\Program Files\Mozilla Firefox\default-browser-agent.exe (PID: 8280)
    Command line: C:\Program Files\Mozilla Firefox\default-browser-agent.exe register-task 308046B0AF4A39CB
default-browser-agent.exe (8280) -> C:\Program Files\Mozilla Firefox\firefox.exe (PID: 5504)
    Command line: C:\Program Files\Mozilla Firefox\firefox.exe --backgroundtask defaultagent register-task 308046B0AF4A39CB
firefox.exe (5504) -> C:\Program Files\Mozilla Firefox\firefox.exe (PID: 7092)
    Command line: C:\Program Files\Mozilla Firefox\firefox.exe --backgroundtask defaultagent register-task 308046B0AF4A39CB
firefox.exe (7092) -> C:\Program Files\Mozilla Firefox\firefox.exe (PID: 8708)
    Command line: C:\Program Files\Mozilla Firefox\firefox.exe -contentproc --channel=1740 -parentBuildID 20240205133611 -prefsHandle 1668 -prefMapHandle 1532 -prefsLen 19614 -prefMapSize 239890 -win32kLockedDown -appDir C:\Program Files\Mozilla Firefox\browser - {19bd6495-6a75-4d8e-a530-3e90a9444918} 7092 \\.\pipe\gecko-crash-server-pipe.7092 23a70082310 socket
setup.exe (8160) -> C:\Program Files\Mozilla Firefox\firefox.exe (PID: 4152)
    Command line: C:\Program Files\Mozilla Firefox\firefox.exe --backgroundtask install
firefox.exe (4152) -> C:\Program Files\Mozilla Firefox\firefox.exe (PID: 6188)
    Command line: C:\Program Files\Mozilla Firefox\firefox.exe --backgroundtask install
setup-stub.exe (6036) -> C:\Program Files\Mozilla Firefox\firefox.exe (PID: 8884)
    Command line: C:\Program Files\Mozilla Firefox\firefox.exe -first-startup
```

```
firefox.exe (8884) -> C:\Program Files\Mozilla Firefox\firefox.exe (PID: 4656)
    Command line: C:\Program Files\Mozilla Firefox\firefox.exe -first-startup
firefox.exe (4656) -> C:\Program Files\Mozilla Firefox\firefox.exe (PID: 1964)
    Command line: C:\Program Files\Mozilla Firefox\firefox.exe -contentproc --channel
        =2096 -parentBuildID 20240205133611 -prefsHandle 1624 -prefMapHandle 1452 -
        prefsLen 20353 -prefMapSize 239959 -appDir C:\Program Files\Mozilla Firefox\
        browser - {2909a242-8976-4f10-892a-17753c12ab68} 4656 \\.\pipe\gecko-crash-
        server-pipe.4656 18f2e5f9510 gpu
firefox.exe (4656) -> C:\Program Files\Mozilla Firefox\firefox.exe (PID: 184)
    Command line: C:\Program Files\Mozilla Firefox\firefox.exe -contentproc --channel
        =2512 -parentBuildID 20240205133611 -prefsHandle 2508 -prefMapHandle 2504 -
        prefsLen 20353 -prefMapSize 239959 -win32kLockedDown -appDir C:\Program Files\
        Mozilla Firefox\browser - {19ed6b38-c877-4da7-9465-8c31d2b62e79} 4656 \\.\pipe\
        gecko-crash-server-pipe.4656 18f216821l0 socket
firefox.exe (4656) -> C:\Program Files\Mozilla Firefox\firefox.exe (PID: 8520)
    Command line: C:\Program Files\Mozilla Firefox\firefox.exe -contentproc --channel
        =1764 -childID 1 -isForBrowser -prefsHandle 2872 -prefMapHandle 2820 -prefsLen
        20549 -prefMapSize 239959 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID
        20240205133611 -win32kLockedDown -appDir C:\Program Files\Mozilla Firefox\
        browser - {907c4bff-8102-48df-b525-5858b4600189} 4656 \\.\pipe\gecko-crash-
        server-pipe.4656 18f3115169O tab
firefox.exe (4656) -> C:\Program Files\Mozilla Firefox\firefox.exe (PID: 4256)
    Command line: C:\Program Files\Mozilla Firefox\firefox.exe -contentproc --channel
        =3460 -childID 2 -isForBrowser -prefsHandle 3448 -prefMapHandle 3444 -prefsLen
        21415 -prefMapSize 239959 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID
        20240205133611 -win32kLockedDown -appDir C:\Program Files\Mozilla Firefox\
        browser - {807ec72e-ce6b-47dc-ae5a-3a0fb3dd4eef} 4656 \\.\pipe\gecko-crash-
        server-pipe.4656 18f31a20f50 tab
firefox.exe (4656) -> C:\Program Files\Mozilla Firefox\firefox.exe (PID: 9104)
    Command line: C:\Program Files\Mozilla Firefox\firefox.exe -contentproc --channel
        =4340 -parentBuildID 20240205133611 -prefsHandle 3316 -prefMapHandle 4344 -
        prefsLen 22904 -prefMapSize 239959 -appDir C:\Program Files\Mozilla Firefox\
        browser - {0a3e912e-f432-4579-ae66-e69bcf423b07} 4656 \\.\pipe\gecko-crash-
        server-pipe.4656 18f32c2151O rdd
firefox.exe (4656) -> C:\Program Files\Mozilla Firefox\firefox.exe (PID: 1120)
    Command line: C:\Program Files\Mozilla Firefox\firefox.exe -contentproc --channel
        =3180 -childID 3 -isForBrowser -prefsHandle 3160 -prefMapHandle 3080 -prefsLen
        22192 -prefMapSize 239959 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID
        20240205133611 -win32kLockedDown -appDir C:\Program Files\Mozilla Firefox\
        browser - {8a569be7-4db5-46a0-a6ae-8d9ceee38d33} 4656 \\.\pipe\gecko-crash-
        server-pipe.4656 18f2e550a10 tab
firefox.exe (4656) -> C:\Program Files\Mozilla Firefox\firefox.exe (PID: 7500)
    Command line: C:\Program Files\Mozilla Firefox\firefox.exe -contentproc --channel
        =4544 -childID 4 -isForBrowser -prefsHandle 4552 -prefMapHandle 4556 -prefsLen
        22192 -prefMapSize 239959 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID
        20240205133611 -win32kLockedDown -appDir C:\Program Files\Mozilla Firefox\
        browser - {0ec7638a-dc81-4ae2-93e2-e0f753382323} 4656 \\.\pipe\gecko-crash-
        server-pipe.4656 18f2e550d90 tab
firefox.exe (4656) -> C:\Program Files\Mozilla Firefox\firefox.exe (PID: 4872)
    Command line: C:\Program Files\Mozilla Firefox\firefox.exe -contentproc --channel
        =4752 -childID 5 -isForBrowser -prefsHandle 4760 -prefMapHandle 4764 -prefsLen
        22192 -prefMapSize 239959 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID
        20240205133611 -win32kLockedDown -appDir C:\Program Files\Mozilla Firefox\
        browser - {cf40e305-444f-492d-a21a-e009312f688f} 4656 \\.\pipe\gecko-crash-
        server-pipe.4656 18f2e550f50 tab
firefox.exe (4656) -> C:\Program Files\Mozilla Firefox\firefox.exe (PID: 2104)
    Command line: C:\Program Files\Mozilla Firefox\firefox.exe -contentproc --channel
        =5276 -childID 6 -isForBrowser -prefsHandle 2920 -prefMapHandle 2936 -prefsLen
        27461 -prefMapSize 239959 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID
        20240205133611 -win32kLockedDown -appDir C:\Program Files\Mozilla Firefox\
        browser - {1b957998-902e-4e86-b3a9-e84317f411a7} 4656 \\.\pipe\gecko-crash-
        server-pipe.4656 18f357f6d90 tab
...
```

```
firefox.exe (4656) -> C:\Program Files\Mozilla Firefox\firefox.exe (PID: 8700)
    Command line: C:\Program Files\Mozilla Firefox\firefox.exe -contentproc --channel
        =5976 -parentBuildID 20240205133611 -sandboxingKind 0 -prefsHandle 6004 -
        prefMapHandle 6000 -prefsLen 33531 -prefMapSize 239959 -win32kLockedDown -
        appDir C:\Program Files\Mozilla Firefox\browser - {03f08c19-07c8-47ed-95d4-
        d0ab28e5a2d2} 4656 \\.\pipe\gecko-crash-server-pipe.4656 18f331f9510 utility
firefox.exe (4656) -> C:\Program Files\Mozilla Firefox\firefox.exe (PID: 6716)
    Command line: C:\Program Files\Mozilla Firefox\firefox.exe -contentproc --channel
        =6236 -childID 7 -isForBrowser -prefsHandle 6228 -prefMapHandle 6224 -prefsLen
        28942 -prefMapSize 239959 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID
        20240205133611 -win32kLockedDown -appDir C:\Program Files\Mozilla Firefox\
        browser - {43aea33c-2c07-49e4-a0de-bf785be21ebc} 4656 \\.\pipe\gecko-crash-
        server-pipe.4656 18f38f2f310 tab
...
```

Quelltext D.14: Analyse Installation und erster Start: HTTP-POST-Request-URIs von Firefox bei Installation und Initial-Start

```
$ tshark -r *.tlsdecrypted.pcap -Y "((http || http2) && (ip.src == 192.168.100.10 ||
    ipv6.src == fdb0:8f6e:bc8e:9::2) && (http.request.method == "POST" || http2.headers
    .method == "POST"))" -T fields -e ipv6.src -e ipv6.dst -e ip.src -e ip.dst -e http.
    request.full_uri -e http2.request.full_uri | awk '{if ($3 == "") next ;print $3}' |
     uniq | grep -Ev "(microsoft|edge|msft|live\.com|live\.net|office\.com|sfx\.ms|msn
    \.com|windowsupdate|google|windows\.com)"
https://spocs.mozilla.net/spocs
https://incoming.telemetry.mozilla.org/submit/firefox-desktop/first-startup/1/0d8a62f2
    -ecb3-4227-a116-4fc848d3f0c6
https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=122.0&
    pver=2.2
https://incoming.telemetry.mozilla.org/submit/firefox-desktop/newtab/1/9edc6baf
    -6866-4258-a6f4-894d99a83b7b
https://incoming.telemetry.mozilla.org/submit/firefox-desktop/baseline/1/674381b1
    -8856-4b95-9588-20ee824ed9a9
https://incoming.telemetry.mozilla.org/submit/firefox-desktop/messaging-system/1/
    f517331c-5fc4-4624-918c-2484fc3d2707
...
https://incoming.telemetry.mozilla.org/submit/firefox-desktop/messaging-system/1/70781
    a1f-ab8a-4ec9-aa61-1678dddb1c4b
https://incoming.telemetry.mozilla.org/submit/firefox-desktop/newtab/1/7bc29441-ec15
    -49c3-867b-e44129fe0ad5
https://incoming.telemetry.mozilla.org/submit/firefox-desktop/messaging-system
    /1/27584278-cc15-49bc-928d-23a19f35478b
```

Quelltext D.15: Analyse Installation und erster Start: Inhalt Telemetrie-HTTP-POST-Request von Firefox bei Initial-Start an `https://incoming.telemetry.mozilla.org/submit/firefox-desktop/first-startup/1/0d8a62f2-ecb3-4227-a116-4fc848d3f0c6`


```
{
    "client_info": {
        "app_build": "20240205133611",
        "app_channel": "release",
        "app_display_version": "122.0.1",
        "architecture": "x86_64",
        "build_date": "1970-01-01T00:00:00+00:00",
        "client_id": "f1d80029-3066-4770-935f-09d1dc78912b",
        "first_run_date": "2024-02-18+01:00",
        "locale": "en-GB",
        "os": "Windows",
        "os_version": "10.0",
        "telemetry_sdk_build": "56.0.0",
        "windows_build_number": 22631
    },
    "metrics": {
        "quantity": {
            "first_startup.delete_tasks_time": 1846,
            "first_startup.elapsed": 3760,
            "first_startup.normandy_init_time": 5580,
            "first_startup.status_code": 3
        }
    },
    "ping_info": {
        "end_time": "2024-02-18T13:19:36.345+01:00",
        "experiments": {
            "add-an-image-to-pdf-with-alt-text-rollout": {
                "branch": "control",
                "extra": {
                    "type": "nimbus-rollout"
                }
            },
            "csv-import-release-rollout": {
                "branch": "enable-csv-import",
                "extra": {
                    "type": "nimbus-rollout"
                }
            },
            "ech-roll-out": {
                "branch": "rollout",
                "extra": {
                    "type": "nimbus-rollout"
                }
            },
            "fox-doodle-set-to-default-early-day-user-en-treatment-a-rollout": {
                "branch": "treatment-a",
                "extra": {
                    "type": "nimbus-rollout"
                }
            },
            "launch-firefox-on-os-restart-treatment-a-rollout": {
                "branch": "treatment-a",
                "extra": {
                    "type": "nimbus-rollout"
                }
            },
            "mixed-content-level-2-roll-out-release-115": {
                "branch": "control",
                "extra": {
                    "type": "nimbus-rollout"
```

```
                }
            },
            "mozillaaccounts-toolbar-button-default-visibility-existing-user": {
                "branch": "treatment-a",
                "extra": {
                    "type": "nimbus-rollout"
                }
            },
            "spocs-endpoint-rollout-release": {
                "branch": "control",
                "extra": {
                    "type": "nimbus-rollout"
                }
            },
            "upgrade-spotlight-rollout": {
                "branch": "treatment",
                "extra": {
                    "type": "nimbus-rollout"
                }
            }
        },
        "seq": 0,
        "start_time": "2024-02-18T13:19:36.208+01:00"
    }
}
```

Quelltext D.16: Analyse Installation und erster Start: Inhalt Telemetrie-HTTP-POST-Request von Firefox bei `https://incoming.telemetry.mozilla.org/submit/telemetry/95e4d0c9-531a-46f2-9113-da1708a4145d/new-profile/Firefox/122.0.1/release/20240205133611?v=4`

```
1 {"type":"new-profile","id":"95e4d0c9-531a-46f2-9113-da1708a4145d","creationDate
    ":"2024-02-18T12:50:33.021Z","version":4,"application":{"architecture":"x86-64","
    buildId":"20240205133611","name":"Firefox","version":"122.0.1","displayVersion
    ":"122.0.1","vendor":"Mozilla","platformVersion":"122.0.1","xpcomAbi":"x86_64-msvc
    ","channel":"release"},"payload":{"reason":"startup","processes":{"parent":{"
    scalars":{"startup.profile_selection_reason":"firstrun-created-default"}}}},"
    clientId":"069c3177-615d-465b-8c0b-7fa1c39fb82a","environment":{"build":{"
    applicationId":"{ec8030f7-c20a-464f-9b0e-13a3a9e97384}","applicationName":"Firefox
    ","architecture":"x86-64","buildId":"20240205133611","version":"122.0.1","vendor":"
    Mozilla","displayVersion":"122.0.1","platformVersion":"122.0.1","xpcomAbi":"x86_64-
    msvc","updaterAvailable":true},"partner":{"distributionId":null,"
    distributionVersion":null,"partnerId":null,"distributor":null,"distributorChannel":
    null,"partnerNames":[]},"system":{"memoryMB":4080,"virtualMaxMB":134217728,"cpu":{"
    isWindowsSMode":false,"count":2,"cores":2,"vendor":"GenuineIntel","name":"Intel(R)
    Core(TM) i7-10510U CPU @ 1.80GHz","family":6,"model":142,"stepping":12,"l2cacheKB
    ":256,"l3cacheKB":8192,"speedMHz":2304,"extensions":["hasMMX","hasSSE","hasSSE2","
    hasSSE3","hasSSSE3","hasSSE4_1","hasSSE4_2","hasAVX","hasAVX2","hasAES"]},"os":{"
    installYear":2024,"hasSuperfetch":true,"hasPrefetch":true,"name":"Windows_NT","
    version":"10.0","locale":"en-CH","servicePackMajor":0,"servicePackMinor":0,"
    windowsBuildNumber":22631,"windowsUBR":3007},"hdd":{"binary":{"model":"VBOX
    HARDDISK","revision":"1.0","type":"HDD"},"profile":{"model":"VBOX HARDDISK","
    revision":"1.0","type":"HDD"},"system":{"model":"VBOX HARDDISK","revision":"1.0","
    type":"HDD"}},"gfx":{"D2DEnabled":false,"DWriteEnabled":true,"ContentBackend":"Skia
    ","Headless":false,"EmbeddedInFirefoxReality":false,"TargetFrameRate":59,"adapters
    ":[{"description":"VirtualBox Graphics Adapter (WDDM)","vendorID":"0x80ee","
    deviceID":"0xbeef","subsysID":"040515ad","RAM":0,"driver":"VBoxDispD3D VBoxDX
    VBoxDX","driverVendor":null,"driverVersion":"7.0.14.11095","driverDate
    ":"1-15-2024","GPUActive":true}],"monitors":[{"screenWidth":1024,"screenHeight
    ":768,"refreshRate":60,"pseudoDisplay":false}],"features":{"compositor":"
    webrender_software","hwCompositing":{"status":"available"},"gpuProcess":{"status":"
    available"},"webrender":{"status":"blocklisted:FEATURE_FAILURE_VM_VENDOR"},"
    wrCompositor":{"status":"unavailable:FEATURE_FAILURE_DCOMP_NOT_ANGLE"},"
    openglCompositing":{"status":"unused"},"omtp":{"status":"unused"},"d3d11":{"status
    ":"blocklisted:FEATURE_FAILURE_VM_VENDOR"},"d2d":{"status":"unavailable:
    FEATURE_FAILURE_D2D_D3D11_COMP","version":"1.1"}}},...
```

Quelltext D.17: Analyse Privat-Modus: Kommunikation von Firefox im Private Modus

```
$ grep -F TCP Noriben_19_Feb_24__11_45_985100.csv | grep -Eiv "(edge|wermgr|edgeupdate
    |svchost|sihclient).exe" | grep "firefox\.exe" | awk -F',' '{print $5}' | sort |
    uniq
"127.0.0.1:49891 -> 127.0.0.1:49892"
"127.0.0.1:49892 -> 127.0.0.1:49891"
"127.0.0.1:49894 -> 127.0.0.1:49895"
"127.0.0.1:49895 -> 127.0.0.1:49894"
"192.168.100.10:49938 -> 34.107.221.82:80"
"192.168.100.10:49941 -> 34.107.221.82:80"
"192.168.100.10:58917 -> 34.149.100.209:443"
"192.168.100.10:58957 -> 94.230.211.117:443"
"192.168.100.10:58958 -> 94.230.211.117:443"
"192.168.100.10:58959 -> 104.18.130.236:443"
"192.168.100.10:58960 -> 104.18.130.236:443"
"192.168.100.10:58963 -> 172.217.168.8:443"
"192.168.100.10:58964 -> 172.64.155.119:443"
"192.168.100.10:58965 -> 172.217.168.10:443"
"192.168.100.10:58969 -> 34.98.105.146:443"
"192.168.100.10:58970 -> 35.190.93.146:443"
"192.168.100.10:58971 -> 34.98.91.45:443"
"192.168.100.10:58972 -> 34.98.91.45:443"
"192.168.100.10:58984 -> 172.64.155.119:443"
"fdb0:8f6e:bc8e:9:0:0:0:2:49939 -> 2600:1901:0:38d7:0:0:0:0:80"
"fdb0:8f6e:bc8e:9:0:0:0:2:49942 -> 2600:1901:0:38d7:0:0:0:0:80"
"fdb0:8f6e:bc8e:9:0:0:0:2:49943 -> 2600:1901:0:38d7:0:0:0:0:80"
"fdb0:8f6e:bc8e:9:0:0:0:2:58961 -> 2a00:1450:400a:801:0:0:0:200a:443"
"fdb0:8f6e:bc8e:9:0:0:0:2:58981 -> 2600:1901:0:38d7:0:0:0:0:80"
"fdb0:8f6e:bc8e:9:0:0:0:2:58982 -> 2600:1901:0:38d7:0:0:0:0:80"
```

Quelltext D.18: Analyse Privat-Modus: HTTP-URIs von Firefox im Private Modus

```
$ tshark -r *.tlsdecrypted.pcap -Y "((http || http2) && (ip.addr == 104.18.130.236 ||
    ip.addr == 127.0.0.1 || ip.addr == 172.217.168.10 || ip.addr == 172.217.168.8 || ip
    .addr == 172.64.155.119 || ipv6.addr == 2600:1901:0:38d7:0:0:0:0 || ipv6.addr == 2
    a00:1450:400a:801:0:0:0:200a || ip.addr == 34.107.221.82 || ip.addr ==
    34.149.100.209 || ip.addr == 34.98.105.146 || ip.addr == 34.98.91.45 || ip.addr ==
    35.190.93.146 || ip.addr == 94.230.211.117))" -T fields -e ipv6.src -e ipv6.dst -e
    ip.src -e ip.dst -e http.request.full_uri -e http2.request.full_uri | awk '{if ($3
    == "") next ;print $1" "$2" "$3}'
192.168.100.10 34.107.221.82 http://detectportal.firefox.com/canonical.html
192.168.100.10 34.107.221.82 http://detectportal.firefox.com/success.txt?ipv4
192.168.100.10 34.149.100.209 https://firefox.settings.services.mozilla.com/v1/buckets
    /main/collections/ms-language-packs/records/cfr-v1-en-GB
192.168.100.10 34.149.100.209 https://firefox.settings.services.mozilla.com/v1/buckets
    /main/collections/ms-language-packs/records/cfr-v1-en-GB
192.168.100.10 94.230.211.117 https://www.bfh.ch/
192.168.100.10 94.230.211.117 https://www.bfh.ch/en/
192.168.100.10 94.230.211.117 https://www.bfh.ch/.resources/bfh-portal/webresources/
    resources/UnitRoundedPro.woff
... https://cdn.cookielaw.org/logos/static/ot_guard_logo.svg
192.168.100.10 34.98.91.45 https://heatmaps.monsido.com/v1/settings/
    FNBcb7Vvey435robJ5yVkg.json
192.168.100.10 104.18.130.236 https://cdn.cookielaw.org/logos/static/ot_company_logo.
    png
192.168.100.10 104.18.130.236 https://cdn.cookielaw.org/logos/static/powered_by_logo.
    svg
192.168.100.10 172.64.155.119 https://privacyportal-ch.onetrust.com/request/v1/
    consentreceipts
```

D.5. Tor Browser

Quelltext D.19: Analyse Installation und erster Start: Durch den Tor Browser-Installer und dessen Browser gestartete Prozesse

```
$ grep -F "Process Create" Noriben_18_Feb_24__15_17_568267.csv | sed 's,\",,g' | grep -Eiv "(edge|edgeupdate|msedgewebview2|MsMpEng|svchost|SystemSettings).exe" | awk -F ',' '{print $2" ("$3") -> "$5" ("$7")£   "$8}' | sed 's,\£,\n,g'
Explorer.EXE (5272) -> C:\tools\tor-browser-windows-x86_64-portable-13.0.8.exe (PID: 8088)
    Command line: C:\tools\tor-browser-windows-x86_64-portable-13.0.8.exe
...
tor-browser-windows-x86_64-portable-13.0.8.exe (8088) -> C:\Users\browser\Desktop\Tor Browser\Browser\firefox.exe (PID: 3772)
    Command line: C:\Users\browser\Desktop\Tor Browser\Browser\firefox.exe
firefox.exe (3772) -> C:\Users\browser\Desktop\Tor Browser\Browser\firefox.exe (PID: 3684)
    Command line: C:\Users\browser\Desktop\Tor Browser\Browser\firefox.exe
...
firefox.exe (3684) -> C:\Users\browser\Desktop\Tor Browser\Browser\firefox.exe (PID: 2668)
    Command line: C:\Users\browser\Desktop\Tor Browser\Browser\firefox.exe -contentproc --channel=3684.0.557343489\2043099316 -parentBuildID 20231213165604 -prefsHandle 1828 -prefMapHandle 2128 -prefsLen 19243 -prefMapSize 243588 -appDir C:\Users\browser\Desktop\Tor Browser\Browser\browser - {73d33e1f-9a12-4c80-afff-28268f85c66c} 3684  gpu
firefox.exe (3684) -> C:\Users\browser\Desktop\Tor Browser\Browser\firefox.exe (PID: 8416)
    Command line: C:\Users\browser\Desktop\Tor Browser\Browser\firefox.exe -contentproc --channel=3684.1.751238348\308584501 -childID 1 -isForBrowser -prefsHandle 2884 -prefMapHandle 2880 -prefsLen 20081 -prefMapSize 243588 -jsInitHandle 1392 -jsInitLen 240916 -parentBuildID 20231213165604 -win32kLockedDown -appDir C:\Users\browser\Desktop\Tor Browser\Browser\browser - {5ee25dbd-6e1b-457f-a764-c8ef48d9c631} 3684  tab
firefox.exe (3684) -> C:\Users\browser\Desktop\Tor Browser\Browser\firefox.exe (PID: 3064)
    Command line: C:\Users\browser\Desktop\Tor Browser\Browser\firefox.exe -contentproc --channel=3684.2.374963228\1221834357 -childID 2 -isForBrowser -prefsHandle 2672 -prefMapHandle 2776 -prefsLen 20891 -prefMapSize 243588 -jsInitHandle 1392 -jsInitLen 240916 -parentBuildID 20231213165604 -win32kLockedDown -appDir C:\Users\browser\Desktop\Tor Browser\Browser\browser - {62a26450-61e9-4897-921b-b60316e3be88} 3684  tab
firefox.exe (3684) -> C:\Users\browser\Desktop\Tor Browser\Browser\firefox.exe (PID: 3344)
    Command line: C:\Users\browser\Desktop\Tor Browser\Browser\firefox.exe -contentproc --channel=3684.3.2054175776\575545120 -childID 3 -isForBrowser -prefsHandle 3168 -prefMapHandle 2796 -prefsLen 20968 -prefMapSize 243588 -jsInitHandle 1392 -jsInitLen 240916 -parentBuildID 20231213165604 -win32kLockedDown -appDir C:\Users\browser\Desktop\Tor Browser\Browser\browser - {cab12bf9-64b5-4aa4-aa67-b7c0720cfe2d} 3684  tab
firefox.exe (3684) -> C:\Users\browser\Desktop\Tor Browser\Browser\firefox.exe (PID: 2364)
    Command line: C:\Users\browser\Desktop\Tor Browser\Browser\firefox.exe -contentproc --channel=3684.4.1920861578\278761666 -parentBuildID 20231213165604 -prefsHandle 3472 -prefMapHandle 3304 -prefsLen 22143 -prefMapSize 243588 -appDir C:\Users\browser\Desktop\Tor Browser\Browser\browser - {a5b63e80-8bc0-4c0a-aaf3-010827c89034} 3684  rdd
firefox.exe (3684) -> C:\Users\browser\Desktop\Tor Browser\Browser\TorBrowser\Tor\tor.exe (PID: 6928)
    Command line: C:\Users\browser\Desktop\Tor Browser\Browser\TorBrowser\Tor\tor.exe --defaults-torrc C:\Users\browser\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\torrc-defaults -f C:\Users\browser\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\torrc DataDirectory C:\Users\browser\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor ClientOnionAuthDir C:\Users\browser\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\onion-auth GeoIPFile C:\Users\browser\Desktop\Tor
```

```
        Browser\Browser\TorBrowser\Data\Tor\geoip GeoIPv6File C:\Users\browser\Desktop\
        Tor Browser\Browser\TorBrowser\Data\Tor\geoip6 +__ControlPort 127.0.0.1:9151
        HashedControlPassword 16:0
        d4ab77186c1cd9560ae78724156c17e74f733a0d15ed38b50bbf711a2 +__SocksPort
        127.0.0.1:9150 ExtendedErrors IPv6Traffic PreferIPv6 KeepAliveIsolateSOCKSAuth
        __OwningControllerProcess 3684 DisableNetwork 1
tor.exe (6928) -> C:\Windows\System32\Conhost.exe (PID: 6448)
    Command line: \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
firefox.exe (3684) -> C:\Users\browser\Desktop\Tor Browser\Browser\firefox.exe (PID:
    5536)
    Command line: C:\Users\browser\Desktop\Tor Browser\Browser\firefox.exe -
        contentproc --channel=3684.5.688069858\204811110 -childID 4 -isForBrowser -
        prefsHandle 2900 -prefMapHandle 3140 -prefsLen 22278 -prefMapSize 243588 -
        jsInitHandle 1392 -jsInitLen 240916 -parentBuildID 20231213165604 -
        win32kLockedDown -appDir C:\Users\browser\Desktop\Tor Browser\Browser\browser -
         {6f48a82f-a603-46bf-af78-018100ae7ccc} 3684  tab
firefox.exe (3684) -> C:\Users\browser\Desktop\Tor Browser\Browser\firefox.exe (PID:
    8180)
    Command line: C:\Users\browser\Desktop\Tor Browser\Browser\firefox.exe -
        contentproc --channel=3684.6.1822362600\505310115 -childID 5 -isForBrowser -
        prefsHandle 3144 -prefMapHandle 3132 -prefsLen 22278 -prefMapSize 243588 -
        jsInitHandle 1392 -jsInitLen 240916 -parentBuildID 20231213165604 -
        win32kLockedDown -appDir C:\Users\browser\Desktop\Tor Browser\Browser\browser -
         {6d35119e-fea5-4ac1-af2f-7dcf702c1fa3} 3684  tab
firefox.exe (3684) -> C:\Users\browser\Desktop\Tor Browser\Browser\firefox.exe (PID:
    8740)
    Command line: C:\Users\browser\Desktop\Tor Browser\Browser\firefox.exe -
        contentproc --channel=3684.7.685408699\1703045788 -childID 6 -isForBrowser -
        prefsHandle 4188 -prefMapHandle 4192 -prefsLen 22278 -prefMapSize 243588 -
        jsInitHandle 1392 -jsInitLen 240916 -parentBuildID 20231213165604 -
        win32kLockedDown -appDir C:\Users\browser\Desktop\Tor Browser\Browser\browser -
         {62d514ac-c4e2-488a-bf4d-560eb6cea30c} 3684  tab
...
```

Quelltext D.20: Analyse Installation und erster Start: TCP-Verbindungen des Tor Browsers

```
firefox.exe (3684):
    127.0.0.1:49956 -> 127.0.0.1:49957
firefox.exe (3684):
    127.0.0.1:49957 -> 127.0.0.1:49956
firefox.exe (3684):
    127.0.0.1:49958 -> 127.0.0.1:9150
firefox.exe (3684):
    127.0.0.1:49959 -> 127.0.0.1:9151
...
tor.exe (6928):
    127.0.0.1:49960 -> 127.0.0.1:49961
tor.exe (6928):
    127.0.0.1:49961 -> 127.0.0.1:49960
tor.exe (6928):
    127.0.0.1:49964 -> 127.0.0.1:49965
tor.exe (6928):
    127.0.0.1:49965 -> 127.0.0.1:49964
tor.exe (6928):
    127.0.0.1:9151 -> 127.0.0.1:49959
...
```

D.6. Extrahierung von GUIDs

Quelltext D.21: Analyse Extrahierung von GUIDs: Zeilenanzahl der Aufzeichnungen mit dem Auswertungsskript aus Kapitel B.2

```
      2 lab-chrome/eval-20240228-1700/20240203-1713-windows-tshark-http.txt
   1478 lab-chrome/eval-20240228-1700/20240204-1035-install-tshark-http.txt
    700 lab-chrome/eval-20240228-1700/20240219-1022-privatmodus-tshark-http.txt
   9258 lab-chrome/eval-20240228-1700/20240219-1453-telemetrytrigger-tshark-http.txt
   8637 lab-chrome/eval-20240228-1700/20240219-1501-telemetrytrigger-private-tshark-
       http.txt
     35 lab-chrome/eval-20240228-1700/20240228-0925-stat-private-tshark-http.txt
    522 lab-chrome/eval-20240228-1700/20240228-0925-stat-tshark-http.txt
   5886 lab-edge/eval-20240228-1700/20240218-1042-firstrun-tshark-http.txt
    578 lab-edge/eval-20240228-1700/20240219-1107-privatmodus-tshark-http.txt
  13759 lab-edge/eval-20240228-1700/20240219-1510-telemetrytrigger-tshark-http.txt
  12087 lab-edge/eval-20240228-1700/20240219-1523-telemetrytrigger-private-tshark-
      http.txt
   1058 lab-edge/eval-20240228-1700/20240228-0942-stat-tshark-http.txt
    125 lab-edge/eval-20240228-1700/20240228-0943-stat-private-tshark-http.txt
   7103 lab-firefox/eval-20240228-1700/20240218-1322-installandfirstrun-tshark-http.
       txt
    419 lab-firefox/eval-20240228-1700/20240219-1146-privatmodus-tshark-http.txt
  10853 lab-firefox/eval-20240228-1700/20240219-1543-telemetry-tshark-http.txt
   6005 lab-firefox/eval-20240228-1700/20240219-1552-telemetrytrigger-private-tshark-
       http.txt
    372 lab-firefox/eval-20240228-1700/20240228-0947-stat-tshark-http.txt
     20 lab-firefox/eval-20240228-1700/20240228-0948-stat-private-tshark-http.txt
      2 lab-tor/eval-20240228-1700/20240218-1528-installandfirstrun-tshark-http.txt
      2 lab-tor/eval-20240228-1700/20240218-1609-torconnect-failed-tshark-http.txt
      2 lab-tor/eval-20240228-1700/20240218-1809-torconnect-failedagain-tshark-http.
          txt
      2 lab-tor/eval-20240228-1700/20240218-1835-connected-updated-closed-tshark-http
          .txt
```

Quelltext D.22: Analyse Extrahierung von GUIDs: Ergebnis der GUID-Auswertung der Aufzeichnungen mit dem Auswertungsskript aus Kapitel B.2

```
$ head -n 20 lab-chrome/eval-20240228-1700/guid.txt.sorted
    195 gbCookie=8A6201EEEBAA4B2D2BA8FED9C4C672D9
    195 bm_sz=7304B2A9C2A33D99BC7C87AC6D24F7D1
    195 ak_bmsc=B9FFEE65525A61EB2551288CC9E983A2
    195 _abck=DD7904E3A7B8ACA35ACD522B67DC146B
    188 gbCookie=636233F318400D06DE4B1830F3D18299
    188 bm_sz=6417278AC74728480CAF6D980111817C
    188 ak_bmsc=0AC21B9746CA46D4EA74292FD62E69FB
    188 _abck=128AD7C2670A09B540B6F57668F32200
    167 x=session#a2ee3fc13bde4588b92a88a3b11d5f0e
    167 773|MCMID|74565812931337479011785444329537
    159 x=session#bfd9bf11b9e342c3bdc5df4bde184179
    159 773|MCMID|11431868095516717191520994391292
    155 _uetvid=23894940cf2f11ee83f17f5c33227186
    155 _uetsid=2388f790cf2f11ee8d3bf78a942ed9c2
    152 bm_sv=61D7AE665D1AD21E61981BB31EE2B114
    147 bm_sv=76AC3FDF564F4D8B0A8CF69CB97413C3
    146 _uetvid=1693bdb0cf2e11ee9141d710ea56f436
    146 _uetsid=1692d400cf2e11eeb2fbf3d1f294966a
    140 si=ac29f27b-74b9-4f71-876e-908426a9fb83
    133 si=2c2ad38a-7b42-4018-9009-770d9ee5adb9
$ head -n 20 lab-edge/eval-20240228-1700/guid.txt.sorted
   1038 GUID=3D9C6AE06E2842B59D414EDA507D52AB
    978 MUID=14B4264737A06A3F04C3326E360C6B18
    681 606AF46A372528A075ABB9F26D5F85C7029347C374
    652 66201C0194565C28B72DC73DA537EE8E785B133D6C
    649 _SS=SID=1074B78707476AF1279EA3AD061C6BD6
    522 DGE_S=SID=1074B78707476AF1279EA3AD061C6BD6
    499 FPIG=AC551F66869047CB97B6CE8F1CF94AAB
    450 MUIDB=14B4264737A06A3F04C3326E360C6B18
    386 cvid=5a747ef658ba4c3591b2a4775a6b5643
    345 tPageUrls=051E4524FAADB43CDCCFB0CFAD7F31F0
    319 MUID=065B360271796B051F5A222870C96AF8
    306 SID=092BC3C549E4678824C8D7EF48546650
    202 _SS=SID=1A453595A213653C36302 1BCA3BF6437
    197 gbCookie=912BEF83CA09FA13E68C5BD4605677AB
    197 bm_sz=4EDC0D8DEECE29F3529 0C58480F225BF
    197 ak_bmsc=079B881B47F78A7A6584E9CE0485B822
    197 _abck=8883B103EFD1489D5A74A4C1785106CA
    195 MUIDB=065B360271796B051F5A222870C96AF8
    193 gbCookie=D19AEF835130959EA772035BA181E48A
    193 bm_sz=50A4FCF3DA8BF0BDE618BB8C2EF8DCF0
$ head -n 18 lab-firefox/eval-20240228-1700/guid.txt.sorted
    486 gbCookie=6642D49CE6CAC564B872C6F35035AAA8
    486 bm_sz=99C510B2D15CF1C1C75D3CBA0CEB542B
    486 ak_bmsc=B8A9E1489064AEC77645DD95249F5647
    486 _abck=92B667DA65161B8DC945E22A621D9D48
    454 773|MCMID|09784758737039765652958773665455
    453 x=session#338a244178e8446ab64d2489d08da757
    449 _cls_v=4a44e9a6-477e-4986-ac71-aa433b46fdbc
    443 _cls_s=f0814bc0-67b5-4f9d-b4f5-a76cb32a3562
    441 _uetvid=8f51c070cf3411eeb199b1882829b38a
    441 _uetsid=8f519b90cf3411ee9d1d0ffbd05a8598
    440 bm_sv=EE44C8E2D3F897F1FB5DB153EA7A08F5
    387 cid=MCMID|09784758737039765652958773665455
    374 si=f74d43cc-31d6-48e6-9eb7-8b9510ea8ffa
    152 gbCookie=62BE1BD9AE0DFB2B097D3101C1D943DB
    152 bm_sz=0E6EDC055DF3109848C1E4B1EA88CA08
    152 ak_bmsc=866FD561B667841E7EDC0328E58AE6AD
    152 _abck=079A9C03AD8DB9835E7FE608829EAB3A
    131 70732533412532462532467777772e61697263616e
```

Quelltext D.23: Analyse Extrahierung von GUIDs: Ergebnis der GUID-Auswertung der Aufzeichnungen mit dem Auswertungsskript aus Kapitel B.2 ohne Parameter, die aussschliesslich für `aircanada.com` verwendet wurden

```
$ cat lab-chrome/eval-20240228-1700/guid.txt.sorted | grep -Ev "(_abck|_uetsid|_uetvid|_cls_s|_cls_v|ak_bmsc|bm_sv|bm_sz|gbCookie|MCMID|si|x=session)" | head -n 15
     58 353044|PC#a2ee3fc13bde4588b92a88a3b11d5f0e
     58 3341253246253246777772e61697263616e616461
     56 77496e666f2e6661726546616d696c79496e666f2e
     56 666c6967687456696577496e666f2e666172654661
     56 25334125324625324677777772e61697263616e6164
     55 467777772e61697263616e6164612e636f6d253246
     55 41253246253246777772e61697263616e6164612e
     55 352593|PC#bfd9bf11b9e342c3bdc5df4bde184179
     54 74747073253341253246253246777772e61697263
     53 747073253341253246253246777772e6169726361
     52 6c6967687456696577496e666f2e6661726546616d
     52 462532467777772e61697263616e6164612e636f6d
     51 68747470732533412532462532467777772e616972
     49 32467777772e61697263616e6164612e636f6d2532
     49 2532467777772e61697263616e6164612e636f6d25
$ cat lab-edge/eval-20240228-1700/guid.txt.sorted | grep -Ev "(_abck|_uetsid|_uetvid|_cls_s|_cls_v|ak_bmsc|bm_sv|bm_sz|gbCookie|MCMID|si|x=session)" | head -n 20
   1038 GUID=3D9C6AE06E2842B59D414EDA507D52AB
    978 MUID=14B4264737A06A3F04C3326E360C6B18
    681 606AF46A372528A075ABB9F26D5F85C7029347C374
    652 66201C0194565C28B72DC73DA537EE8E785B133D6C
    649 _SS=SID=1074B78707476AF1279EA3AD061C6BD6
    522 DGE_S=SID=1074B78707476AF1279EA3AD061C6BD6
    499 FPIG=AC551F66869047CB97B6CE8F1CF94AAB
    450 MUIDB=14B4264737A06A3F04C3326E360C6B18
    386 cvid=5a747ef658ba4c3591b2a4775a6b5643
    345 tPageUrls=051E4524FAADB43CDCCFB0CFAD7F31F0
    319 MUID=065B360271796B051F5A222870C96AF8
    306 SID=092BC3C549E4678824C8D7EF48546650
    202 _SS=SID=1A453595A213653C363021BCA3BF6437
    195 MUIDB=065B360271796B051F5A222870C96AF8
    185 muid=196F9BEA1E01692C1C168FC31F5A68F5
    167 msclkid=cd1b5e40d997199959593b93b95268d5
    161 gclid=cd1b5e40d997199959593b93b95268d5
    155 708352525.ab081548d7f2187321bb709bb3f3c568
    154 clkid=_uetab081548d7f2187321bb709bb3f3c568
    151 clkid=_uetcd1b5e40d997199959593b93b95268d5
$ cat lab-firefox/eval-20240228-1700/guid.txt.sorted | grep -Ev "(_abck|_uetsid|_uetvid|_cls_s|_cls_v|ak_bmsc|bm_sv|bm_sz|gbCookie|MCMID|si|x=session)" | head -n 15
    131 70732533412532462532467777772e61697263616e
    130 74747073253341253246253246777772e61697263
    124 2532467777772e61697263616e6164612e636f6d25
    117 3341253246253246777772e61697263616e616461
    117 2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d
    116 41253246253246777772e61697263616e6164612e
    115 467777772e61697263616e6164612e636f6d253246
    115 32467777772e61697263616e6164612e636f6d2532
    114 mid=09784758737039765652958773665455309284
    113 732533412532462532467777772e61697263616e61
    112 25334125324625324677777772e61697263616e6164
    111 68747470732533412532462532467777772e616972
    109 747073253341253246253246777772e6169726361
    108 462532467777772e61697263616e6164612e636f6d
    108 324625324677777772e61697263616e6164612e636f
```

Quelltext D.24: Analyse Extrahierung von GUIDs: `GUID`-Parameter in Edge-Aufzeichnungen mit dem Auswertungsskript aus Kapitel B.2

```
$ pwd
/home/usr/src/BFH23_SIM/semesterarbeit/data/lab-edge/eval-20240228-1700
$ ls *tshark*http.txt
20240218-1042-firstrun-tshark-http.txt           20240219-1523-telemetrytrigger-private-tshark-http.txt
20240219-1107-privatmodus-tshark-http.txt        20240228-0942-stat-tshark-http.txt
20240219-1510-telemetrytrigger-tshark-http.txt   20240228-0943-stat-private-tshark-http.txt
$ grep -ro GUID=3D9C6AE06E2842B59D414EDA507D52AB *tshark*.txt | cat | uniq
20240218-1042-firstrun-tshark-http.txt:GUID=3D9C6AE06E2842B59D414EDA507D52AB
20240219-1510-telemetrytrigger-tshark-http.txt:GUID=3D9C6AE06E2842B59D414EDA507D52AB
20240219-1523-telemetrytrigger-private-tshark-http.txt:GUID=3D9C6AE06E2842B59D414EDA507D52AB
20240228-0942-stat-tshark-http.txt:GUID=3D9C6AE06E2842B59D414EDA507D52AB
$ grep -r GUID=3D9C6AE06E2842B59D414EDA507D52AB *tshark*.txt | awk '{print $5}' | awk -F'/' '{print $3}' | sort  | uniq -c
      6 bat.bing.com
      1 bing.com
      1 c.bing.com
    201 edgeservices.bing.com
     39 r.bing.com
    321 th.bing.com
      1 www2.bing.com
    468 www.bing.com
```

Quelltext D.25: Analyse Extrahierung von GUIDs: `MUID`-/`MUIDB`-Parameter in Edge-Aufzeichnungen mit dem Auswertungsskript aus Kapitel B.2

```
$ pwd
/home/usr/src/BFH23_SIM/semesterarbeit/data/lab-edge/eval-20240228-1700
$ ls *tshark*http.txt
20240218-1042-firstrun-tshark-http.txt          20240219-1523-telemetrytrigger-private
    -tshark-http.txt
20240219-1107-privatmodus-tshark-http.txt       20240228-0942-stat-tshark-http.txt
20240219-1510-telemetrytrigger-tshark-http.txt  20240228-0943-stat-private-tshark-http
    .txt
$ grep -r MUID=14B4264737A06A3F04C3326E360C6B18 *tshark*.txt | awk -F':' '{print $1}'
    | uniq
20240218-1042-firstrun-tshark-http.txt
20240219-1107-privatmodus-tshark-http.txt
20240219-1510-telemetrytrigger-tshark-http.txt
20240219-1523-telemetrytrigger-private-tshark-http.txt
20240228-0942-stat-tshark-http.txt
$ grep -r MUID=14B4264737A06A3F04C3326E360C6B18 *tshark*.txt | awk '{print $5}' | awk
    -F'/' '{print $3}' | sort  | uniq -c
      7 assets.msn.com
      6 bat.bing.com
      1 bing.com
      1 c.bing.com
      1 c.clarity.ms
      2 c.msn.com
    108 edgeservices.bing.com
     39 r.bing.com
    280 th.bing.com
      1 www2.bing.com
    525 www.bing.com
      1 www.clarity.ms
      3 www.msn.com
$ grep -r MUID=065B360271796B051F5A222870C96AF8 *tshark*.txt | awk -F':' '{print $1}'
    | uniq
20240219-1523-telemetrytrigger-private-tshark-http.txt
$ grep -r MUIDB=14B4264737A06A3F04C3326E360C6B18 *tshark*.txt | awk -F':' '{print $1}'
     | uniq
20240219-1510-telemetrytrigger-tshark-http.txt
20240219-1523-telemetrytrigger-private-tshark-http.txt
20240228-0942-stat-tshark-http.txt
$ grep -r MUIDB=14B4264737A06A3F04C3326E360C6B18 *tshark*.txt | awk '{print $5}' | awk
     -F'/' '{print $3}' | sort  | uniq -c
    106 edgeservices.bing.com
    344 www.bing.com
$ grep -r 065B360271796B051F5A222870C96AF8 *tshark*.txt | awk -F':' '{print $1}' |
    uniq
20240219-1523-telemetrytrigger-private-tshark-http.txt
$ grep -r 065B360271796B051F5A222870C96AF8 *tshark*.txt | awk '{print $5}' | awk -F'/'
     '{print $3}' | sort  | uniq -c
      3 4.bing.com
      8 bat.bing.com
      1 bing.com
      1 c.bing.com
      1 c.clarity.ms
     24 r.bing.com
     85 th.bing.com
    193 www.bing.com
      2 www.clarity.ms
```

Quelltext D.26: Analyse Extrahierung von GUIDs: SID-Parameter in Edge-Aufzeichnungen mit dem Auswertungsskript aus Kapitel B.2

```
$ pwd
/home/usr/src/BFH23_SIM/semesterarbeit/data/lab-edge/eval-20240228-1700
$ ls *tshark*http.txt
20240218-1042-firstrun-tshark-http.txt           20240219-1523-telemetrytrigger-private
    -tshark-http.txt
20240219-1107-privatmodus-tshark-http.txt        20240228-0942-stat-tshark-http.txt
20240219-1510-telemetrytrigger-tshark-http.txt   20240228-0943-stat-private-tshark-http
    .txt
$ grep -r SID=1074B78707476AF1279EA3AD061C6BD6 *tshark*.txt | awk -F':' '{print $1}' |
     uniq
20240219-1510-telemetrytrigger-tshark-http.txt
$ grep -r SID=1074B78707476AF1279EA3AD061C6BD6 *tshark*.txt | awk '{print $5}' | awk -
    F'/' '{print $3}' | sort  | uniq -c
      6 bat.bing.com
      1 bing.com
      1 c.bing.com
     29 edgeservices.bing.com
     39 r.bing.com
    158 th.bing.com
      1 www2.bing.com
    414 www.bing.com
$ grep -r SID=092BC3C549E4678824C8D7EF48546650 *tshark*.txt | awk -F':' '{print $1}' |
     uniq
20240219-1523-telemetrytrigger-private-tshark-http.txt
$ grep -r SID=092BC3C549E4678824C8D7EF48546650 *tshark*.txt | awk '{print $5}' | awk -
    F'/' '{print $3}' | sort  | uniq -c
      3 4.bing.com
      1 bing.com
     24 r.bing.com
     85 th.bing.com
    193 www.bing.com
$ grep -r SID=1A453595A213653C363021BCA3BF6437 *tshark*.txt | awk -F':' '{print $1}' |
     uniq
20240218-1042-firstrun-tshark-http.txt
$ grep -r SID=1A453595A213653C363021BCA3BF6437 *tshark*.txt | awk '{print $5}' | awk -
    F'/' '{print $3}' | sort  | uniq -c
     93 edgeservices.bing.com
     87 th.bing.com
     22 www.bing.com
```

Quelltext D.27: Analyse Extrahierung von GUIDs: `GUID`-, `MUID`- und `SID`-Parameter zusammen in Edge-Aufzeichnungen mit dem Auswertungsskript aus Kapitel B.2

```
$ pwd
/home/usr/src/BFH23_SIM/semesterarbeit/data/lab-edge/eval-20240228-1700
$ ls *tshark*http.txt
20240218-1042-firstrun-tshark-http.txt          20240219-1523-telemetrytrigger-private
    -tshark-http.txt
20240219-1107-privatmodus-tshark-http.txt       20240228-0942-stat-tshark-http.txt
20240219-1510-telemetrytrigger-tshark-http.txt  20240228-0943-stat-private-tshark-http
    .txt
$ grep -e GUID=3D9C6AE06E2842B59D414EDA507D52AB -e MUID=14
    B4264737A06A3F04C3326E360C6B18 -e SID *tshark*http.txt | awk -F':' '{print $1}' |
    uniq
20240218-1042-firstrun-tshark-http.txt
20240219-1107-privatmodus-tshark-http.txt
20240219-1510-telemetrytrigger-tshark-http.txt
20240219-1523-telemetrytrigger-private-tshark-http.txt
20240228-0942-stat-tshark-http.txt
$ grep -e GUID=3D9C6AE06E2842B59D414EDA507D52AB -e MUID=14
    B4264737A06A3F04C3326E360C6B18 -e SID *tshark*http.txt | awk '{print $5}' | awk -F
    '/' '{print $3}' | sort  | uniq -c
      3 4.bing.com
     11 arc.msn.com
     88 assets.msn.com
      6 bat.bing.com
      2 bing.com
     51 browser.events.data.msn.com
      1 c.bing.com
      1 c.clarity.ms
      4 c.msn.com
    201 edgeservices.bing.com
      5 login.live.com
     15 ntp.msn.com
     63 r.bing.com
      2 report.acacb.glassboxdigital.io
     30 srtb.msn.com
    406 th.bing.com
      1 www2.bing.com
    722 www.bing.com
      1 www.clarity.ms
      3 www.msn.com
```