Praktikumsbericht Forensik in Betriebs- und Anwendungssystemen

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

Bearbeitete Aufgabenstellung:

IT-forensische Untersuchung nach Datendiebstahl

Vorgelegt von:	Nina Marie Müllner	Yevgeniy Krasnov	Marco Gehm
Matr.-Nr.	500018	499639	469812

Gruppe: 06 HH

Abgabe: 14.07.2024

Inhaltsverzeichnis

1. Einleitung

Dieses Dokument behandelt die IT-forensische Untersuchung eines forensisch relevanten Szenarios sowie die Ausarbeitung eines forensischen Gutachtens, welches den aus dem Szenario abgeleiteten Sachverhalt erörtert. Die Aufgabenstellung definiert die Mindestanzahl der als Beweismittel (BM) zu untersuchende elektronische Geräte auf zwei. Um diese Anforderung zu erfüllen, haben die Autoren ein entsprechendes Szenario erstellt, welches zusätzlich eine realitätsnahe Ausgangssituation für die Untersuchung erzeugt.

Nach der Einleitung in diesem Kapitel, beschreibt Kap. 2 den zugrundeliegenden Sachverhalt, bei dem eine Person, die eine sicherheitsempfindliche Tätigkeit ausübt, verschwindet. Die Beschreibung der Geschehnisse in Abs. 2.1, bei denen die beiden BM in Form einer MicroSD-Karte sowie einer Festplatte entstehen, dient der anschließenden Formulierung der Ziele der forensischen Untersuchung in Abs. 2.2. Es folgt in Kap. 3 die Vorbereitung der Untersuchung. Dabei werden insbesondere die strategisch-operationellen sowie technischen Vorbereitungen in Abs. 3.1 und 3.2 beleuchtet, die die Autoren getroffen haben, um das fiktive Szenario abzubilden. Die beiden Abschnitte grenzen hierbei das Vorgehen im Rahmen der Projektarbeit vom Vorgehen in einer realen forensischen Untersuchung ab. Diese Abgrenzung diskutiert insbesondere den Einsatz von Virtualisierung, um einen Rechner der verschwundenen Person zu emulieren. Abs. 3.3 betrachtet die forensische Datensicherung und Analyse näher, bevor in Kap. 4 der Untersuchungsauftrag sowie das Übergabeprotokoll der BM authentisch präsentiert werden. Das forensische Gutachten folgt in Kap. 5 und stellt den Hauptteil dieser Ausarbeitung dar. Das zuvor festgelegte Ziel der forensischen Untersuchung bereitet die Definition des Untersuchungsauftrags vor, der in Abs. 5.1 präsentiert wird. Abs. 5.2 fasst die Untersuchung zusammen und gibt einen Überblick bezüglich der fallbezogenen Fragestellungen sowie des zeitlichen Ablaufs in Form einer sog. Timeline. Die Timeline listet relevante Ereignisse in der Reihenfolge ihres zeitlichen Geschehens auf, worauf mögliche Ermittlungsansätze Impulse für das weitere Vorgehen im vorliegenden Fall beschreiben. Eine Darstellung der Untersuchungsobjekte in Abs. 5.3 betrachtet die beiden zu untersuchenden BM im Detail. Die Autoren verwenden, in der Rolle von fiktiven Forensikern, ausgewählte gängige Untersuchungswerkzeuge, die in Abs. 5.4 eingeführt werden. Abs. 5.5 beschreibt die Vorbereitung der forensischen Untersuchung, um die beiden BM in Abs. 5.6 und 5.7 zu analysieren. Abschließend betrachtet Kap. Zusammenfassung und Ausblick diese Praktikumsarbeit retrospektiv und wagt einen Ausblick. Hierbei werden besonders die Unterschiede zwischen Theorie und Praxis betont. Die Autoren bewerten die Ergebnisse dieser Projektarbeit in Abs. Bewertung des Ergebnisses und legen die gewonnenen methodischen sowie technischen Erkenntnisse in Abs. 6.2 dar.

In dieser Arbeit werden eingeschobene Hinweise genutzt, um Besonderheiten, die sich durch Unterschiede zu einer realen IT-forensischen Untersuchung ergeben, zu beleuchten. Solche Hinweise sind kursiv dargestellt.

Hinweis: Alle Institutionen, Personen und Gegebenheiten sind frei erfunden, Ähnlichkeiten mit realexistierenden Unternehmen oder Personen sind rein zufällig und nicht beabsichtigt.

2. Beschreibung des Sachverhalts

Dieses Kapitel erläutert die grundlegenden Aspekte dieser Ausarbeitung. Zunächst liefert das Szenario in Abs. 2.1 Anhaltspunkte und weitere Informationen, mithilfe derer anschließend die Ziele der forensischen Untersuchung in Abs. 2.2 festgelegt werden.

2.1 Szenario

Um eine geeignete Vorbereitung für das forensische Gutachten in Kap. 5 zu treffen, haben die Autoren zunächst ein fiktives Szenario schriftlich festgelegt und ausgearbeitet. Dabei ist der Zweck des Szenarios, einen Sachverhalt abzuleiten, mit dessen Hilfe alle erforderlichen BM identifiziert werden können. Darüber hinaus sollen ausreichend detailreiche Informationen vorliegen, um eine möglichst realitätsnahe forensische Untersuchung zu gewährleisten. Eine realitätsnahe forensische Untersuchung zeichnet sich unter anderem dadurch aus, dass meist sehr viele unterschiedliche und sehr große Datenmengen vorliegen.

Hinweis: Wir wählen das Szenario in dieser Projektarbeit selbst und haben deshalb bereits Kenntnisse über die zu findenden Artefakte. In einer realen forensischen Untersuchung würde das Szenario den Forensikern nicht vorliegen. Dadurch ist die gezielte Suche nach Artefakten und deren Korrelation erschwert. Aus diesem Grund liegt das Szenario den fiktiven Forensikern bei der Untersuchung ebenfalls nicht vor. Das bedeutet, dass die Perspektive der fiktiven Forensiker bei der Verfassung des forensischen Gutachtens zwar eingeschränkt, jedoch gleichzeitig authentischer ist.

Herr Erik Alex Müller war nach Abschluss einer Sicherheitsüberprüfung seit mehreren Wochen mit der Softwareentwicklung im Projekt *Neptuns Schild* betraut. Im Rahmen des Projekts, welches vom Bundesverteidigungsministerium und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) geleitet wird, erhielt E. Müller Zugang zu Verschlusssachen, die in den Geheimhaltungsgrad *vertraulich* eingestuft sind.

Am Montag, dem 10.06.2024, erschien E. Müller nicht zur Arbeit. Von E. Müllers Vorgesetzte unternommene Kontaktversuche blieben ohne Erfolg. Die von E. Müller angegebene Kontaktperson für Notfälle, Frau Irma Müller (Mutter), wurde daraufhin erfolgreich kontaktiert. I. Müller berichtete von einer Kommunikation per E-Mail mit E. Müller am Samstag, dem 08.06.2024., in der E. Müller eine arbeitsbedingte Abwesenheit ankündigte. Daraufhin wurde das Büro von E. Müller am selben Tag geöffnet und durchsucht. Bei der Durchsuchung wurde das Fehlen von E. Müllers mobilen Arbeitsrechner festgestellt, welcher sofort aus der Ferne gesperrt wurde.

Am Dienstag, dem 11.06.2024, durchsuchten Ermittler E. Müllers Wohnung. Dabei wurde ein Desktop-Rechner mit montierter Festplatte und ein USB-Gerät mit eingesteckter MicroSD-Karte beschlagnahmt. Die MicroSD-Karte sowie die Festplatte stellen BM dar, wurden von den Ermittlern demontiert und zur Datensicherung und Auswertung an die Firma MYN-Forensics übergeben.

Die zu untersuchenden Geräte ergeben sich direkt aus dem gewählten Szenario. Um den Rechner zu simulieren, haben die Autoren eine virtuelle Maschine (VM) lokal bereitgestellt. Die Autoren haben sich für den Hypervisor *VirtualBox* von Oracle entschieden, da dieser alle eingesetzten Host-Betriebssysteme unterstützt und frei verfügbar ist. Das Gast-Betriebssystem ist Windows 10, das über die Hochschule Wismar zu Bildungszwecken lizenziert worden ist. Nach Einschätzung der Autoren, ist Windows zum Zeitpunkt dieser Ausarbeitung das Betriebssystem mit der weitesten Verbreitung im Privateinsatz. Das bedeutet, dass bei einer realen forensischen Untersuchung die Wahrscheinlichkeit hoch ist, dass ein Windows 10 System Untersuchungsgegenstand wird.

Das USB-Gerät ist ein sog. *Bad-USB-Stick*, ein Einplatinenrechner (Raspberry Pi Zero W) mit MicroSD-Karte als Betriebssystem- und Datenspeicher. Im Szenario sollte der Bad-USB-Stick, der mit der Spezialdistribution *Kali Linux* ausgestattet ist, zur Datenextraktion von einem Opfer-Rechner genutzt werden. Zu diesem Zweck bietet der Bad-USB-Stick eine WLAN-Schnittstelle und eine Weboberfläche, über die maliziöse Skripte entwickelt und gestartet werden können. Solche Skripte werden auf der MicroSD-Karte abgelegt und können bei einer Auswertung Hinweise liefern.

2.2 Ziel der IT-forensischen Untersuchung

Das Ziel der fiktiven Forensiker im vorliegenden Szenario ist es, einen Abfluss von vertraulichen Informationen im Zusammenhang mit dem Verschwinden von E. Müller zu bewerten. Zusätzlich sollen Informationen erhoben werden, die eine rechtliche Aufarbeitung des Sachverhalts unterstützen können. Solche Informationen ermöglichen beispielsweise die Ermittlung weiterer beteiligter Personen, die Feststellung des Eigentümers der beiden BM sowie die Ermittlung des Aufenthaltsortes von E. Müller. Um solche Informationen zu erheben, sollen insbesondere relevante E-Mails, Dokumente und eventuell extrahierte Informationen des Projekts *Neptuns Schild* gefunden werden. Hierzu sollen die Festplatte und die MicroSD-Karte mit gängigen Werkzeugen unter Wahrung der Beweiskette analysiert werden. Die Analyse soll gerichtsfest durchgeführt und gerichtsverwertbar dokumentiert werden.

3. Vorbereitung der Untersuchung

Dieses Kapitel führt die organisatorischen sowie technischen Vorbereitungen ein, die in einer realen IT-forensischen Untersuchung notwendig sind.

3.1 Strategisch-operationelle Vorbereitung

Die strategisch-operationelle Vorbereitung der forensischen Untersuchung zielt darauf ab, einen möglichen Abfluss von vertraulichen Informationen im Zusammenhang mit dem Verschwinden von E. Müller zu bewerten und rechtlich relevante Daten zu erheben.

Ein wesentlicher Schritt der strategischen Vorbereitung ist die Bereitstellung eines vollständigen Forensik-Koffers, der alle notwendigen Werkzeuge für die Datensicherung und -analyse beinhaltet. Darüber hinaus werden relevante Formulare, wie Empfangsbestätigungen für die BM und Untersuchungsaufträge, im Voraus erstellt. Um auf dieses Szenario vorbereitet zu sein, haben wir uns im Vorfeld intensiv mit den relevanten BM auseinandergesetzt. Dazu gehört das Aneignen von notwendigem Wissen über Systemkonfigurationen und sog. *Logging*, die als potenzielle Quellen für die Analyse dienen. Unter *Logging* betrachten wir in dieser Ausarbeitung beispielsweise die automatische Dokumentation von Systemereignissen. Solche Systemereignisse können erfolgreiche und fehlgeschlagene Anmeldevorgänge, das Einstecken und Entfernen von mobilen Datenträgern oder die Änderung der Systemzeit sein.

Im Rahmen der operationellen Vorbereitung werden Interviews mit den Verantwortlichen im Rahmen der Beweisübergabe geführt, um einen Überblick über die Situation und die zu sichernde BM zu erhalten. Daraufhin wird der Desktop-Rechner von E. Müller und der gefundene USB-Stick sichergestellt und in einem forensischen Labor untersucht.

Die Festplatte des Desktop-Rechners und die MicroSD-Karte des USB-Sticks werden mit gängigen Werkzeugen analysiert, um relevante E-Mails, Dokumente und Informationen zu identifizieren.

Die Auswahl der Geräte für die Untersuchung ist entscheidend für den Erfolg der forensischen Analyse. Der Desktop-Rechner von E. Müller wird als zentrales BM identifiziert, da er möglicherweise vertrauliche Informationen und Hinweise auf den Verbleib von E. Müller enthalten könnte. Durch die Erstellung eines forensischen Abbilds der Festplatte des Desktop-Rechners kann eine vollständige Analyse durchgeführt werden.

Der bei der Durchsuchung gefundene USB-Stick mit einer eingesteckten MicroSD-Karte stellt ein weiteres wichtiges BM dar. Dieser Stick könnte Daten enthalten, die auf eine illegale Aktivität oder den Abfluss vertraulicher Informationen hinweisen. Auch hier wird ein forensisches Abbild erstellt und analysiert, um alle relevanten Informationen zu sichern.

Durch die forensischen Abbilder kann eine Umgebung geschaffen werden, in der die Daten ohne Verfälschungsrisiko untersucht werden können. Diese methodische Vorgehensweise trägt wesentlich dazu bei, die Ziele der forensischen Untersuchung zu erreichen und relevante rechtliche Informationen zu sammeln und dabei die Gerichtsfestigkeit zu wahren.

Die Auswahl der Analysewerkzeuge ist ein entscheidender Schritt, um eine präzise und umfassende forensische Untersuchung sicherzustellen. Für die vorliegende Untersuchung haben

wir uns für den Einsatz von *FTK Imager* und *AXIOM* entschieden, basierend auf deren spezifischen Funktionen und Stärken in der forensischen Datenanalyse, die im Folgenden erläutert werden.

FTK Imager von *AccessData* wird ausgewählt, da es als zuverlässiges Werkzeug für die Erstellung von forensischen Abbildern der Datenträger bekannt ist. Dieses Werkzeug ermöglicht es, identische Kopien von Festplatten und anderen Speichermedien zu erstellen, während die Originaldaten intakt bleiben. Ein wesentlicher Vorteil von *FTK Imager* ist die Fähigkeit Prüfsummen mithilfe von Hashfunktionen zu erzeugen, die zur Verifikation der Authentizität und Integrität der gesicherten Daten verwendet werden. Diese Funktion ist unerlässlich, um sicherzustellen, dass die Daten während des gesamten Untersuchungsprozesses nicht verändert wurden und somit gerichtsfest sind.

Magnet Forensics AXIOM wird aufgrund seiner umfassenden Funktionen zur Datenanalyse und -klassifikation ausgewählt. *AXIOM* bietet eine vielseitige Auswahl von Analysewerkzeugen, die es ermöglichen, große Mengen an digitalen Artefakten effizient zu verarbeiten und zu kategorisieren. Ein besonderes Merkmal von *AXIOM* ist seine Fähigkeit, Daten aus verschiedenen Quellen wie E-Mails, Dokumenten, Browser-Aktivitäten und sozialen Medien zu extrahieren und zu aggregieren. Dies ist in unserem Fall besonders wichtig, um relevante E-Mails, Dokumente und andere kritische Dateien gezielt zu identifizieren und zu analysieren. Darüber hinaus bietet *AXIOM* benutzerfreundliche Visualisierungswerkzeuge, die die Darstellung und Interpretation der Untersuchungsergebnisse erleichtern.

Durch die Kombination dieser beiden Werkzeuge können wir eine detaillierte und umfassende Untersuchung der gesicherten Daten gewährleisten. *FTK Imager* sorgt für die sichere und unveränderte Sicherung der Beweise, während *AXIOM* die effiziente und tiefgehende Analyse der Daten ermöglicht.

Um Speichermedien vor nicht beabsichtigten Änderungen zu schützen und somit die Gerichtsverwertbarkeit zu wahren, ist der Einsatz eines sog. Write Blockers erforderlich. Wir nutzen *ForensicSoft SAFE Block*, um sicherzustellen, dass während der Sicherung keine Veränderungen an den gesicherten Daten vorgenommen werden. *SAFE Block* bietet eine zuverlässige Möglichkeit, Schreibzugriffe auf die Datenträger zu verhindern und somit die Integrität der Beweise zu wahren.

Durch die sorgfältige Auswahl und den Einsatz dieser Analysewerkzeuge kann eine detaillierte und umfassende Untersuchung der gesicherten Daten gewährleistet werden, was wesentlich zur Erreichung der Ziele der forensischen Untersuchung beiträgt.

Hinweis:
Eine manuelle Korrektur von Zeitdaten haben wir auf keinem der Systeme vorgenommen, um realistische Daten für die Analyse zu erhalten. Bei einer Erstanalyse vor Beginn unseres Szenarios haben wir festgestellt, dass es auf dem Stick keine neu erzeugten Zeitstempel gibt. Dies liegt daran, dass auf dem Stick minütlich ein Skript läuft, das per cronjob, also automatisiert und regelmäßig, die Systemzeit anpasst. Dieses Skript ist Bestandteil des System-Build-Prozesses und wird somit ausgeführt, sobald der Stick aktiv ist.

Hinweis 2: Im Rahmen der Analyse haben wir ermittelt, dass auf dem System eine syslog-Datei erstellt wird, die auch die Namen der verwendeten Rechner erfasst, mit denen der USB-Stick verbunden ist, und zwar der per USB verbundene Rechner, als auch der per WLAN angebundene Rechner. Da wir der Meinung sind, dass dies eine interessante und für eine Analyse dieses Bad-USB-Systems relevante Information ist, haben wir es auch in der Analyse des USB-Sticks (Abs. 5.6.3) erfasst und nur den verwendeten Rechner-Namen von Student-HP auf Vladimir-HP und von Student-Acer auf Vladimir-Acer angepasst.

3.2 Technische Vorbereitung

Für die Umsetzung des Szenarios ist es notwendig, sowohl Kommunikationsverbindungen zwischen Erik Müller und einer Auswahl an Kontaktpersonen, z.B. seinem Datenempfänger und dem Reisebüro vorzubereiten, als auch Datenspuren auf dem Desktop-Rechner und dem USB-Stick zu hinterlegen. Hierfür haben wir folgenden zeitlichen Ablauf konstruiert und dann nachgestellt.

3.2.1 Planung der Vorgehensweise und zeitlicher Ablauf

Tab. 3.2.1.1 zeigt den geplanten Ablauf der Geschehnisse, die sich im Szenario ereignen sollen. Die exakten Uhrzeiten ergeben sich bei der Durchführung und können Abs. 5.2.2 entnommen werden.

Datum	Aktion
Bis 02.06.2024	VM für Erik Müllers Desktop-Rechner aufsetzen (Abs. 3.2.2). Erik Müllers Hotmail-Account darauf hinterlegen, Mails empfangen und nicht weiter relevante Aktionen durchführen, wie z.B. seinen Hotmail-Account aufrufen und auf seinem Hotmail-Account eine Einkaufsliste erstellen.
Bis 02.06.2024	Bad-USB-Stick mit dem Werkzeug von P4wnP1 a.l.o.a. gemäß Anleitung von heise.de (Abs. 3.2.3) vorbereiten und darauf ein Human Interface Device (HID) Skript zum Suchen und Kopieren von Neptun-Daten hinterlegen.
Bis 02.06.2024	E-Mail-Accounts bei hotmail.com für folgende Beteiligte einrichten: - Erik Alex Müller - Vladimir Forenski (Erik Müllers Kontakt) Andere Accounts bei GMX für weitere mittelbare Kontakte (Eriks Mutter Irma Müller, Reisebüro) um E-Mail-Adressen erweitern. Erste E-Mails erstellen von Irma an Erik Müller und Kommunikation zwischen Reisebüro und Erik Müller zum Test der VM.
Bis 02.06.2024	Verdächtigen Code und Präsentation erstellen für Erik Müllers Datendiebstahl (im Folgenden als *vertrauliche Informationen* bezeichnet)
04.06.2024	Erik Müller versendet eine Mail an Vladimir Forenski, dass er an vertrauliche Informationen gelangen kann und gern in Kontakt treten würde

04.06.2024	Erik Müller erhält Antwort von Vladimir Forenski mit Treffpunkt.
06.06.2024	Erik Müller antwortet, dass der Einsatz des USB-Sticks erfolglos war und er auf andere Weise versuchen wird, die vertraulichen Informationen zu erlangen.
07.06.2024	Erik Müller lädt vertrauliche Informationen in OneDrive über ein Mobiltelefon und am Desktop-Rechner wieder herunter.
07.06.2024	Erik Müller sendet E-Mail an Vladimir Forenski, dass er das Land verlassen muss und Hilfe benötigt.
08.06.2024	Vladimir Forenski antwortet und bietet Hilfe an ab Wien.
08.06.2024	Erik Müller sucht Verbindungen mit Zug und Bus nach Wien auf den Reiseportalen der Deutschen Bahn und von FlixBus.
08.06.2024	Erik Müller versendet Mail an seine Mutter Irma Müller, dass er arbeitsbedingt derzeit nicht erreichbar ist.
10.06.2024	Erik Müller wird in der Arbeit als vermisst gemeldet.
10.06.2024	Erik Müllers mobiler Arbeitsrechner wird gesperrt.
11.06.2024	Durchsuchung von Erik Müllers Wohnung, Beschlagnahme von privatem Desktop-Rechner und gefundenem USB-Stick.
11.06.2024	Beauftragung der forensischen Untersuchung bei der Firma MYN-Forensics.
12.06.2024	Erstellung der forensischen Abbilder der Festplatte auf dem Desktop-Rechner und der MicroSD-Karte aus dem USB-Stick.
12.07.2024	Fertigstellung des Gutachtens.

Tabelle 3.2.1.1 – Geplanter Ablauf der Ereignisse zur Abbildung des Szenarios

3.2.2 Vorbereitung des Desktop-Rechners

Bei der Einrichtung von Erik Müllers Desptop-Rechners haben wir uns für die Erstellung einer virtuellen Maschine auf Basis von *Oracle VirtualBox* Version 7.0.16 r162802 (Qt5.15.2) entschieden, um jedem Mitglied der Gruppe einen Zugang ermöglichen zu können und gleichzeitig Backup-Dateien zu haben, falls die VM auf einem unserer Hosts nicht funktioniert.

Hinweis:
Bei Verwendung einer VM anstelle eines physischen Rechners kann es im Fall einer Analyse dazu kommen, dass Artefakte des VM-Hosts in der Auswertung gefunden werden. Dies ist uns bewusst, daher haben wir entschieden, diesen Einfluss während der Kern-Zeitlinie (ab dem 03.06.) so gering wie möglich zu halten und in der Zeit möglichst keine Prozesse auf dem Host-System durchzuführen, die die Zeitlinie oder Analyse beeinflussen können, z.B. Anschluss von USB-Sticks. Dennoch ist es möglich, dass vereinzelt Artefakte auftreten könnten.

Über die HS-Wismar ist es möglich, Lizenzen für Windows 10 von Microsoft zu erhalten [1]. Diese Windows 10 Version haben wir auf unserer VM installiert, für den Nutzer-Account konnten wir die Hotmail-Adresse des Täters Erik Müller verwenden. Ergänzend wurde noch

die Software *Mozilla Thunderbird* in der Version 115.11.1 für die E-Mail-Kommunikation installiert.

Für den Austausch der VM zwischen den Gruppenmitgliedern sowie als Backup haben wir ein Konto beim frei verfügbaren Cloud-Speicherdienst Mega [2] verwendet.

3.2.3 Vorbereitung des USB-Abbilds

Bei der Vorbereitung unseres realen Hardware-Elements haben wir uns entschieden, einen Bad-USB-Stick nach Anleitung des ct-Artikels aus [3] aufzubauen. Weitere Informationen und Anleitungen finden sich in [4].

Die Hardware-Basis des USB-Sticks bildet ein *Raspberry Pi Zero W* mit aufgeschraubtem USB-Port. Die Software wird auf einer MicroSD-Karte mit dem *Raspberry Pi Imager* (hier in der Version 1.8.5) installiert gemäß Anleitung aus [3]. Für den gewählten USB-Stick ist eine 8GB-Speicherkarte ausreichend, das Abbild benötigt dann allerdings fast den gesamten Speicherplatz und unser USB-Stick wird dadurch geringfügig langsamer in der Nutzung. Dafür laufen Sicherung und Analyse schneller als bei einer größeren MicroSD-Karte.

Als Betriebssystem und Basis für unseren Bad-USB-Stick haben wir das Abbild *kali-linux-v0.1.1-beta-rpi0w-nexmon-p4wnp1-aloa.img.xz* des Entwicklers Rogan Dawes aus [5] verwendet. Basis für unseren Bad-USB-Stick bildet damit ein *Kali-Linux*, das durch ein Webinterface und die Ausführbarkeit von HID-Skripts ergänzt wurde. Die Bedienung unseres USB-Sticks kann gänzlich mithilfe des Webinterfaces erfolgen. Hierzu wird der Stick am USB-Anschluss eines Opfer-Rechners angeschlossen, worauf hin ein WLAN für die Verbindung eines Täter-Rechners aufbaut wird.

Zur Steuerung loggt man sich über einen Täter-Rechners in das neue WLAN mit der Bezeichnung *P4wnP1* ein und ruft das Webinterface zur Steuerung des Sticks über http://172.24.0.1:8000/ aufrufen.

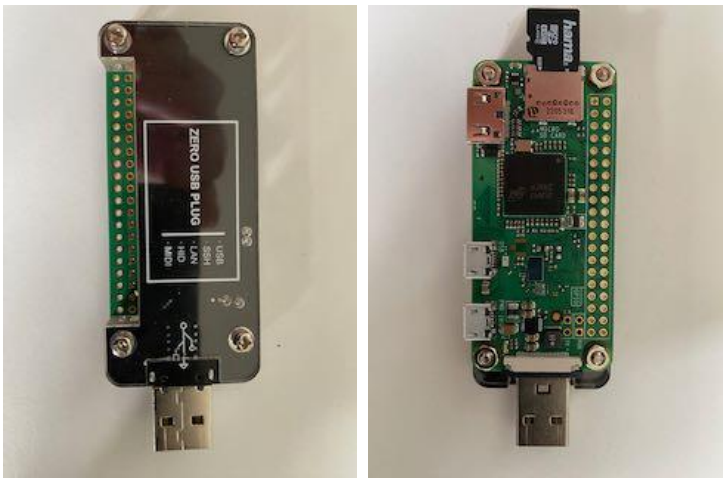


Abbildung 3.2.3.1 – Bad-USB-Stick

Hier gibt es die Möglichkeit, bestehende HID-Skripte (z.B. sog. *Mouse-Jiggler*) zu öffnen und auch selbst anzupassen und dadurch individuelle Skripte zu erstellen. Unsere Skripte aus Abs. 5.6.3 wurden auf diese Weise durch Kopie eines bestehenden Skripts erzeugt und auf dem Stick gespeichert.

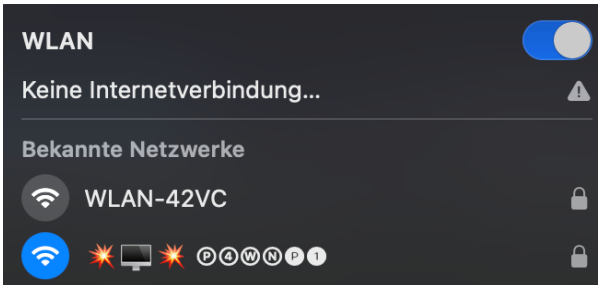


Abbildung 3.2.3.2 – Bezeichnung des Bad-USB-Stick-WLANs

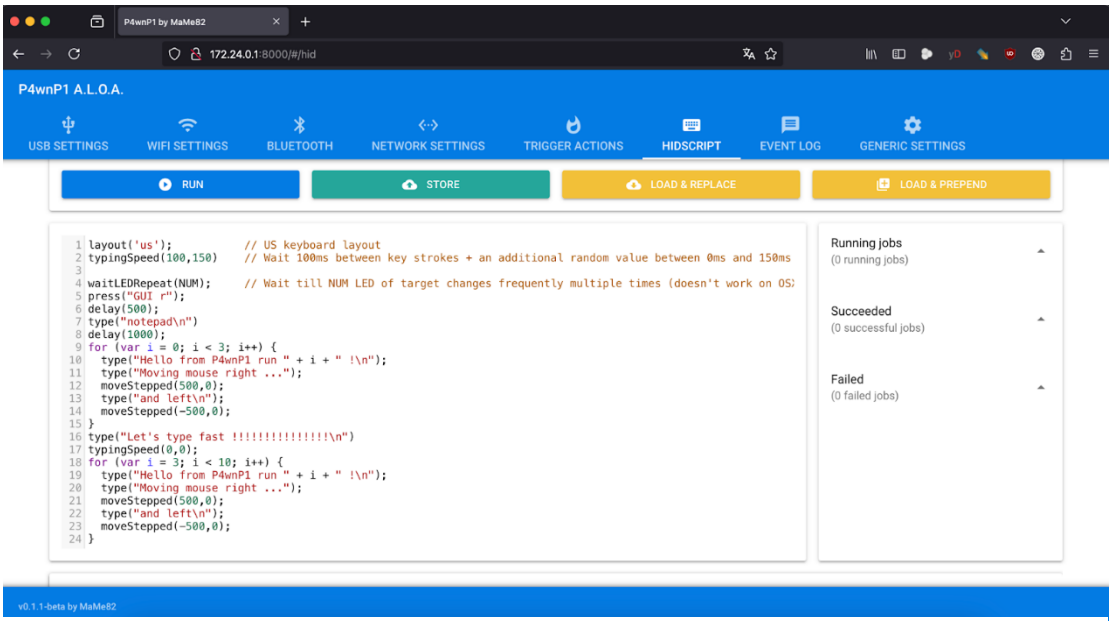


Abbildung 3.2.3.3 – Weboberfläche des Bad-USB-Sticks mit Test-Skript zur Verwendung als HID

Auf dem Stick wurden, wie oben angegeben, folgende drei Skripte durch Kopie und Anpassung bestehender Skripte erzeugt:

- *Erik-Test.js*: Testskript, um Mausbewegungen und Tastatur mit Texten in der Windows-Applikation Editor zu testen. Kopie eines bestehenden Skripts, nur das Tastatur-Layout wurde von ‘us’ auf ‘de’ angepasst.
- *NeptunCopyUserFolders.js*: Eine Funktion, um den Inhalt des Benutzerverzeichnisses des angemeldeten Benutzers zu sammeln für einen späteren Kopiervorgang.

- *EriksSearch.js*: Ein Skript, um alle Dateien mit der Bezeichnung *neptun* im Dateinamen auf ein separates Speichermedium zu kopieren.

Im Szenario sollte der Bad-USB-Stick genutzt werden, um nach Einstecken ohne weitere Benutzerinteraktionen vertrauliche Informationen zu finden und zu extrahieren. Alle drei Skripte haben wir im Anhang A Ergänzende Inhalte für den geneigten Leser hinterlegt.

3.3 Vorbereitung der E-Mail-Adressen der beteiligten Personen

Für folgende Personen wurden eigene E-Mail-Adressen angelegt:

- Erik Alex Müller: *erikalex.mueller@hotmail.com*
- Vladimir Forenski: *vladimir.forenski@hotmail.com*

Für folgende Personen wurde ein bestehendes E-Mail-Konto um zusätzliche Adressen erweitert:

- Irma Müller: *irma.mueller@gmx-topmail.de*
- Reisebüro Abenteuerlust / Frau Hansen: *abenteuerlust@sags-per-mail.de*

Wir haben Hotmail in diesem Fall für die E-Mail-Adressen ausgewählt, weil hier noch keine 2-Faktor-Authentifizierung notwendig ist für die E-Mail-Nutzung. Aus demselben Grund wurde ein bestehendes GMX-Konto um zusätzliche Adressen erweitert.

4. Begleitformulare

Aus Sicht der Autoren ist eine umfangreiche Dokumentation der Ereignisse erforderlich, um eine praxisnahe und nachvollziehbare Bearbeitung der Aufgabenstellung zu gewährleisten. Teil einer solchen Dokumentation sind die Begleitformulare in diesem Kapitel.

Zuerst wird der Untersuchungsauftrag auf den Seiten 12 bis 15 dargestellt, der notwendig ist, um die Untersuchungen für das das in Kap. 5 folgende Gutachten anzustoßen.

Danach folgt die Empfangsbestätigung der fiktiven Forensiker auf Seite 16, die eine lückenlose Beweisführung unterstützt.

POLIZEI HANNOVER
Dienststelle: LKA 419
Az.: 2024-06-11/1

Datum: 12.06.2024
Telefon: 0511 1234-5678
FAX: 0511 1111-2222

Aktenzeichen der anordnenden StA 1563/341/06-24

MYN-Forensics – Auftrag zur forensischen Untersuchung

der Asservate 001 und 002

In Sachen

Name	Müller
Vorname(n)	Erik Alex
Ergänzung	
Geburtsdatum / -ort	04.11.1970
Als	Beschuldigter
Wegen	Landesverrat gemäß §94 StGB
Tatzeit	12.06.2024, 11.00 Uhr
Tatort	BSI Büro Hannover
	Hauptstr. 1
	30163 Hannover

Tathergang

Herr Erik Alex Müller wird verdächtigt, vertrauliche Informationen über das staatliche Projekt *Neptuns Schild* im Bereich der Informationssicherheit an drittstaatliche Akteure weitergegeben zu haben. Als Mitarbeiter an diesem Projekt hatte er Zugang zu vertraulichen Dokumenten. Herr Müller ist nichtmehr auffindbar, seitdem er verdächtiges Verhalten gezeigt hat.

POLIZEI HANNOVER
Dienststelle: LKA 419
Az.: 2024-06-11/1

Datum: 12.06.2024
Telefon: 0511 1234-5678
FAX: 0511 1111-2222

Untersuchungsgegenstände

Anzahl	**Bezeichnung**	**Individualnummern**
1	Asservat 001 SD-Karte und USB-Stick	HC/8GB (Modellnummer SD-Karte) 20953-RPI0W (IC USB-Stick) 2ABCB-RPI0W (FCC ID USB-Stick)
1	Asservat 002 – Festplatte Desktop-Rechner	SDSSDA-1T00 (Modellnummer) 24114B803723 (Seriennummer)

Transport Asservat: Stafette

Aservat ist Spurenträger für

☐ **Daktyloskopische Untersuchung**

☐ **DNA**

POLIZEI HANNOVER
Dienststelle: LKA 419
Az.: 2024-06-11/1

Datum: 12.06.2024
Telefon: 0511 1234-5678
FAX: 0511 1111-2222

Sonstige Informationen zu den Untersuchungsgegenständen

Asservat 001- SD Karte und USB-Stick

Der USB-Stick wurde bei der Durchsuchung der Wohnung des Herrn Müller in einem Schreibtisch versteckt vorgefunden und beschlagnahmt. Der Stick weist keine äußerlichen Beschädigungen auf.

Asservat 002 – Festplatte Desktop-Rechner

Während der Durchsuchung von Herrn Müllers Wohnung wurde ein Desktop-Computer des Typs Dell OptiPlex 7080 entdeckt und sichergestellt. Zum Zeitpunkt der Sicherstellung war der Rechner ausgeschaltet. Weder das Admin- noch das Benutzer-Passwort sind bekannt. Nach der Sicherstellung wurde die Festplatte ordnungsgemäß aus dem Gerät entfernt, wobei Modellnummer und Seriennummer auf der Festplatte vermerkt sind.

Antrag

Es wird um physikalische Spiegelung der und Erstellung eines forensischen Gutachtens der o.g. Untersuchungsgegenstände gebeten, um die folgenden Fragestellungen beantworten zu können:

1. Asservat 001 – SD Karte und USB-Stick
    a. Gibt es Hinweise darauf, dass vertrauliche Informationen entwendet wurden?

2. Asservat 002 – Festplatte Desktop-Rechner
    a. Ist der Rechner eindeutig dem Beschuldigten zuzuordnen? Gibt es Hinweise auf weitere Nutzer?

b. Gibt es Hinweise darauf, dass vertrauliche Informationen entwendet wurden?
c. Gibt es Hinweise auf den gegenwärtigen Aufenthaltsort der Beschuldigten?

3. Übergreifende Fragestellungen
   a. Kann ein Zusammenhang zwischen der Nutzung des Rechners und des USB-Sticks nachgewiesen werden?
   b. Lassen sich aus den gesicherten Daten Hinweise auf das Motiv des Beschuldigten für sein Verschwinden ermitteln?
   c. Lassen sich Hinweise auf weitere an der Vorbereitung oder Durchführung der Tat beteiligte Personen ermitteln?

_____

Unterschrift LKA 419

Hinweise zur Erstellung des Untersuchungsantrags

1 Eine lückenlose Schilderung des vermuteten Tathergangs sollte neben den Angaben zum Tat- oder Fundort, der Tatzeit, dem Zeitpunkt der Sicherstellung sowie dem Namen des sichernden Beamten auch alle für die Untersuchung relevanten Fakten oder Annahmen (wie z.B. eine mögliche Vortäuschung der Straftat) beinhalten.

2 Es ist wichtig, klar zu formulieren, welche spezifischen Fragen durch die Untersuchung geklärt werden sollen.

3 Der Untersuchungsantrag muss gegebenenfalls folgende Informationen enthalten:

3.1 Ob die Untersuchungsobjekte, falls nötig, beschädigt oder zerstört werden dürfen. Falls keine gegenteilige Erklärung vorliegt, wird die Zustimmung der einsendenden Dienststelle vorausgesetzt.

3.2 Angaben des Verdächtigen über die vermutete Entstehungsursache oder Herkunft von Spuren an den Untersuchungsobjekten.

POLIZEI HANNOVER
Dienststelle: LKA 419
Az.: 2024-06-11/1

Datum: 12.06.2024
Telefon: 0511 1234-5678
FAX: 0511 1111-2222

EMPFANGSBESCHEINIGUNG

Absendende Dienststelle: LKA 419
Empfangene Institution: MYN-Forensics

Asservate

Anzahl	**Bezeichnung**	**Individualnummern**
1	Asservat 01- SD Karte und USB-Stick	HC/8GB (Modellnummer SD-Karte) 20953-RPI0W (IC USB-Stick) 2ABCB-RPI0W (FCC ID USB-Stick)
1	Asservat 02 – Festplatte Desktoprechner	SDSSDA-1T00 (Modellnummer) 24114B803723 (Seriennummer)

Übergeben

am 12.06.24 Uhr. 17.05

D. Rose

Unterschrift LKA 419

Empfangen:

am 12.06.24, Uhr. 17.11

Myn

Unterschrift MYN-Forensics

5. Gutachten

MYN-Forensics

Untersuchungsstraße 1 a)

23966 Wismar

Tel.: +49 42 1337

E-Mail: info@non.existant

Gutachten

Auftraggeber:	Polizei Hannover, Dienststelle LKA 419
Datum:	12.06.2024

Aktenzeichen

Polizei:	2024-06-11/1
Staatsanwaltschaft:	1234/567/8-9

Abschluss:	14.07.2024

5.1 Untersuchungsauftrag

Die Polizei Hannover beauftragt MYN-Forensics mit der Sicherung und Analyse folgender Asservate.

Asservat 001 – USB-Stick

1. Gibt es Beweise dafür, dass vertrauliche Informationen gestohlen wurden?

Asservat 002 – Festplatte

1. Ist der Rechner eindeutig dem Beschuldigten zuzuordnen? Gibt es Hinweise auf weitere Nutzer?
2. Finden sich Beweise dafür, dass vertrauliche Informationen gestohlen wurden?
3. Gibt es Hinweise auf den gegenwärtigen Aufenthaltsort des Beschuldigten?

Übergreifende Fragestellungen

1. Kann ein Zusammenhang zwischen der Nutzung des Rechners und des USB-Sticks nachgewiesen werden?
2. Lassen sich aus den gesicherten Daten Hinweise auf das Motiv des Beschuldigten ermitteln?
3. Lassen sich Hinweise auf weitere an der Vorbereitung oder Durchführung der Tat beteiligte Personen ermitteln?

Die Auswertung erfolgt im Rahmen der Ermittlungen zum Aktenzeichen 1234/567/8-9 wegen des Verdachts auf Landesverrat gemäß § 94 STGB.

5.2 Zusammenfassung der Untersuchung

5.2.1 Fragestellungen

Asservat 001 – USB-Stick

1. Gibt es Beweise dafür, dass vertrauliche Informationen gestohlen wurden?

   Nein, es finden sich keine Beweise, die einen erfolgreichen Einsatz des USB-Sticks belegen. Eine forensische Untersuchung potenzieller Opfer-Rechner, könnte weitere Hinweise liefern.
   Auf dem USB-Stick befinden sich zwei Skripte, die dazu dienen, Dateien mit dem Schlagwort *neptun* im Dateinamen zu suchen und auf ein externes Speichermedium zu kopieren (Abs. 5.6.4). Von diesen Skripten konnte das Skript *EriksSearch.js* erfolgreich in einer Testumgebung angewendet werden (Abs. 5.6.5).

Asservat 002 – Festplatte

1. Ist der Rechner eindeutig dem Beschuldigten zuzuordnen? Gibt es Hinweise auf weitere Nutzer?
   Ja, der Login zum Desktop-Rechner enthält den Benutzernamen *erik* (Abs. 5.7.4). Weiterhin ist diesem Desktop-Rechner der Hotmail-Account *erikalex.mueller@hotmail.com* des Beschuldigten zugeordnet. Eine Kontaktaufnahme mit Irma Müller, der Mutter des Beschuldigten, zur Verifikation war nicht Bestandteil dieser Analyse.
   Es finden sich keine Hinweise auf weitere Nutzer.

2. Finden sich Beweise dafür, dass vertrauliche Informationen gestohlen wurden?

   Ja, auf der Festplatte des privaten Rechners des Beschuldigten befinden sich vertrauliche Informationen: Eine Präsentation zu *Neptuns Schild* und eine Quellcode-Datei (Abs. 5.7.6), die Gegenstand eines Datendiebstahls sein könnten. Beide Dateien befinden sich im OneDrive-Verzeichnis des Beschuldigten. Das bedeutet, dass diese vertraulichen Informationen mit einem Cloud-Speicherdienst synchronisiert sind und ein Zugriff durch weitere Geräte möglich ist.

3. Gibt es Hinweise auf den gegenwärtigen Aufenthaltsort der Beschuldigten?

   Ja, anhand der E-Mail -Kommunikation (Abs. 5.7.5), der Suche nach Reiseverbindungen auf den Reiseportalen der Deutschen Bahn und von FlixBus (Abs. 5.7.7) sowie der zuletzt erfolgten Suche auf Google-Maps zur Verbindung zwischen Wien-Erding und Wien-Hauptbahnhof (Abs. 5.7.7), kann geschlossen werden, dass der Beschuldigte versucht hat, über Wien nach Krakowia zu gelangen. Die zuletzt gesuchte Verbindung auf Google-Maps weist auf die Nutzung von FlixBus hin, da diese ihr Ziel in Wien-Erding haben. Es finden sich keine Hinweise auf einen abgeschlossenen Fahrkartenkauf.

Übergreifende Fragestellungen

1. Kann ein Zusammenhang zwischen der Nutzung des Rechners und des USB-Sticks nachgewiesen werden?

   Nein, es kann kein Zusammenhang zwischen Asservat 001 (USB-Stick) und Asservat 002 (Festplatte aus dem Desktop-Rechner des Beschuldigten) hergestellt werden. Es ist kein Logging auf dem Rechner für HID vorhanden, die angegebenen USB-Geräte aus der Systemsteuerung enthalten keine Informationen zu einer Nutzung auf dem Rechner innerhalb des Zeitraums von Mittwoch, 05.06. (vermutete Übergabe des USB-Sticks an den Beschuldigten durch Vladimir Forenski lt. E-Mail-Verkehr) und Montag, 10.06. 8:00 UTC. Auf dem USB-Stick selbst sind in der syslog-Datei zwei Rechner-Bezeichnungen vermerkt, *Vladimir-HP* und *Vladimir-Acer*, aber keine Bezeichnung, die auf den untersuchten Desktop-Rechner des Beschuldigten hindeutet (Abs. 5.6.3).

2. Lassen sich aus den gesicherten Daten Hinweise auf das Motiv des Beschuldigten ermitteln?

   In der E-Mail-Kommunikation befindet sich Hinweise, die darauf hindeuten, dass der Beschuldigte beabsichtigt, mit der Tat einen Gefallen zu erwidern. Es finden sich keine weiteren Informationen, die die Motivation des Beschuldigten belegen könnten.

3. Lassen sich Hinweise auf weitere an der Vorbereitung oder Durchführung der Tat beteiligte Personen ermitteln?

   Ja, anhand der E-Mails lässt sich der Kontakt Vladimir Forenski (Abs. 5.7.5) als zentraler Kontakt zum vermuteten Datendiebstahl rekonstruieren. Es gibt weitere mittelbare Kontakte: Irma Müller, Mutter des Beschuldigten (Abs. 5.7.5), Frau Hansen vom Reisebüro Abenteuerlust (Abs. 5.7.5) und die Großmutter des Beschuldigten in Krakowia (ein Name ist nicht ermittelbar über die Kontakthistorie). Über diese kann allerdings kein direkter Bezug zum Datendiebstahl festgestellt werden.

5.2.2 Zeitlicher Ablauf

Aus den Untersuchungen insbesondere des Rechners kann der Zeitablauf aus Tab. 5.2.2.1 rekonstruiert werden.
Auf dem USB-Stick sind die relevanten Skripte mit Zeitangaben versehen, die nicht zur Zeitlinie der Kommunikationen des Rechners passen (Abs. 5.6.3). Auf Basis der E-Mail-Kommunikation kann lediglich ein Zeitfenster für den möglichen Einsatz des Sticks in diesem zeitlichen Ablauf angegeben werden.

Datum	Uhrzeit (UTC)	Aktion	Asservat/Abschnitt
02.06.2024	18:20:36	E. Müller bedankt sich beim Reisebüro für eine vergangene Reise nach Krakowia. Er fragt eine weitere Reise für zwei Personen und 10 Tage Ende Juni auf die Malediven an. Er möchte die Hin- oder Rückreise über Krakowia vornehmen.	Asservat 002 E-Mails
03.06.2024	20:36:17	Das Reisebüro informiert E. Müller über notwendige Zwischenstopps in Wien und Dubai oder Zürich.	Asservat 002 E-Mails
04.06.2024	16:49:51	E. Müller informiert V. Forenski über seine Beschäftigung im Projekt Neptuns Schild und bietet an, sich bei V. Forenski zu revanchieren.	Asservat 002 E-Mails
04.06.2024	16:52:26	V. Forenski fragt nach E. Müllers Zugriffsmöglichkeit auf einen Rechner. V. Forenski terminiert ein Treffen mit E. Müller in der Nähe der Botschaft von Krakowia auf 18:00 MESZ (16:00 UTC).	Asservat 002 E-Mails

04.06. bis 10.06.		Zeitlich möglicher Einsatz des USB-Sticks, falls dieser wie in der E-Mail von Dienstag, 04.06. 18:00 MESZ (16:00 UTC) wie erwartet übergeben wurde, bis zum Zeitpunkt des Verschwindens am 10.06. 8:00 MESZ (6:00 UTC).	Asservat 001 Analyse gefundener Skripte
06.06.2024	17:06:25	E. Müller informiert V. Forenski darüber, dass Forenskis USB-Stick nicht funktioniert hat. Er kündigt an, andere Möglichkeiten zu suchen, um Informationen in Verbindung mit dem Projekt zu erlangen.	Asservat 002 E-Mails
07.06.2024	17:04:34	E. Müller teilt V. Forenski mit, dass er befürchtet, von seinem Vorgesetzten gesehen worden zu sein, beim Zugriff auf Rechner anderer Projektbeteiligter.	Asservat 002 E-Mails
08.06.2024	13:11:40	V. Forenski ruft E. Müller auf, nach Krakowia zu reisen mit Zwischenstopp in Wien und dort eine Kontaktperson zu treffen.	Asservat 002 E-Mails
08.06.2024	14:11:54 bis 14:22:03	E. Müller sucht Verbindungen mit Zug und Bus nach Wien (Browser)	Asservat 002 Browser-Verlauf
08.06.2024	14:20:10	E. Müller kündigt eine Dienstreise bei seiner Mutter an.	Asservat 002 E-Mails

Tabelle 5.2.2.1 – Zeitlicher Ablauf der Ereignisse

5.2.3 Mögliche Ermittlungsansätze

Aus dem hier erfolgten Gutachten entstehen folgende weitere Ansätze für mögliche Ermittlungen:

1. Bezüglich des Desktop-Rechners sollten Beweise ermittelt werden, die belegen, dass dieser Desktop-Rechner sowie der darauf gefundene Hotmail-Account dem Beschuldigten zugeordnet werden können. Dies kann durch Befragung der Mutter des Beschuldigten erfolgen.
2. Je nach Konfiguration der Rechner der Kollegen des Beschuldigten sowie dort vorhandenen Logs, kann eine Analyse dieser Rechner gegebenenfalls zusätzliche Informationen zum Einsatz des USB-Sticks als HID im fraglichen Zeitraum liefern: Dienstag, 04.06. 16:00 UTC (Empfang des USB-Sticks lt. E-Mail-Verkehr) bis Montag, 10.06. 6:00 UTC (Verschwinden des Beschuldigten). Hinweise zu entsprechenden Einträgen in Windows-Rechnern liefert der Test in Abs. 5.6.5.
3. Es liegt aktuell kein richterlicher Untersuchungsauftrag für Cloud-Umgebungen vor. Da der Login auf dem Desktop-Rechner des Beschuldigten mit einem Hotmail-Account erfolgt und Dateien in einem OneDrive-Verzeichnis gefunden wurden, könnte eine genauere Untersuchung des zugehörigen Cloud-Accounts möglicherweise weitere Hinweise liefern.

5.3 Untersuchungsobjekte

5.3.1 Asservat 001 – USB-Stick mit MicroSD-Karte

USB-Stick:

Hersteller:	Raspberry Pi
Modell:	Raspberry Pi Zero W V 1.1
IC:	20953-RPI0W
FCC ID:	2ABCB-RPI0W

Micro-SD- Karte: hama microSD HC 8GB

Der USB-Stick wurde im 4-Augen-Prinzip inkl. eingesteckter MicroSD-Karte übergeben. Da kein weiterer Datenspeicher auf dem USB-Stick vorhanden ist, wird im Folgenden die MicroSD-Karte für die Datenanalyse verwendet.

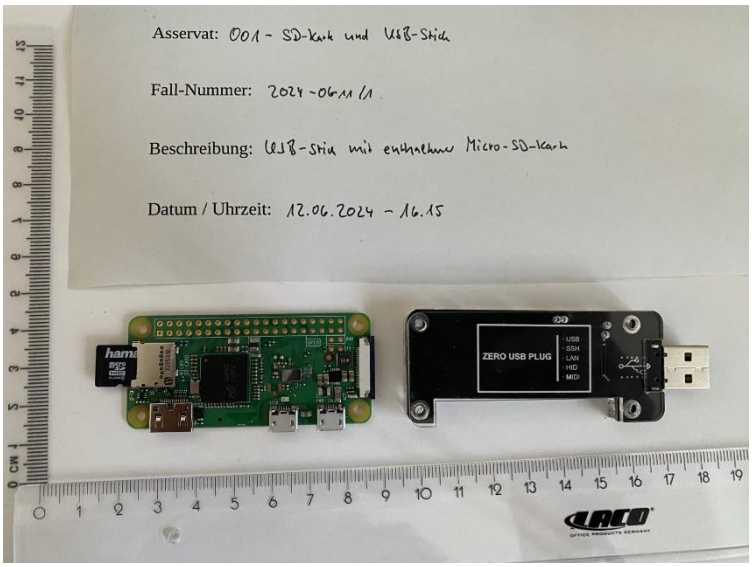


Abbildung 5.3.1.1 – USB-Stick und MicroSD-Karte Vorderseite

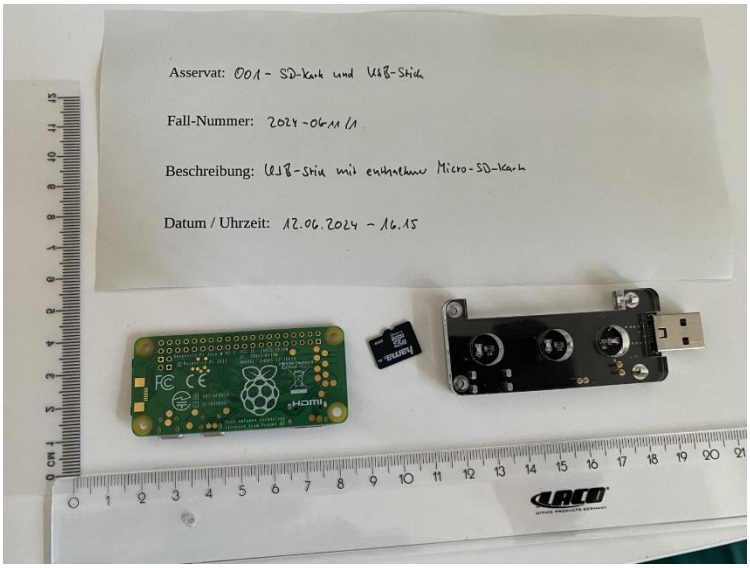


Abbildung 5.3.1.2 – USB-Stick und MicroSD-Karte Rückseite

5.3.2 Asservat 002 – Festplatte

Hersteller: SanDisk

Modell: SDSSDA-1T00

Seriennummer: 24114B803723

Die Festplatte wurde im 4-Augen-Prinzip übergeben.

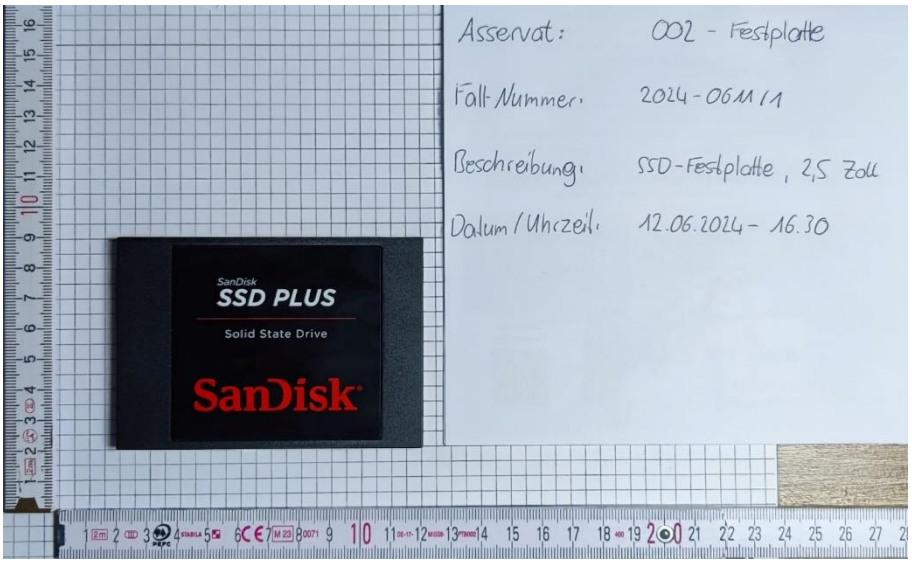


Abbildung 5.3.2.1 – Festplatte des Desktop-Rechners Vorderseite

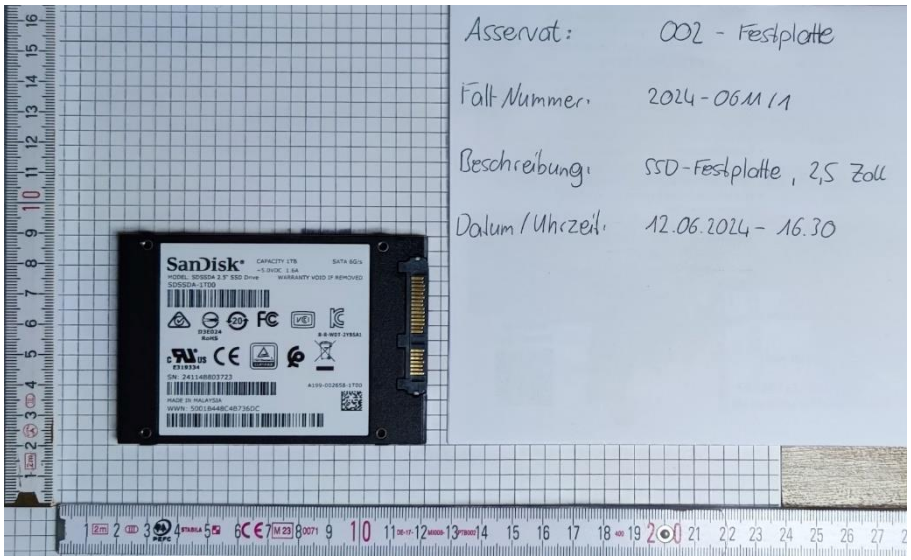


Abbildung 5.3.2.2 – Festplatte des Desktop-Rechners Rückseite

5.4 Untersuchungswerkzeuge

Die zur Analyse genutzten Anwendungen sind in Tabelle 5.4.1 in der jeweils eingesetzten Version dokumentiert. Untersuchungsergebnisse werden insbesondere durch Bildschirmabzüge der Untersuchungswerkzeuge dargestellt. Sind solche Abbildungen nicht anders gekennzeichnet, handelt es sich um Abzüge der Software *Magnet Forensics AXIOM*.

Hersteller	Produktbezeichnung	Version	Verwendungszweck
AccessData	FTK Imager	4.7.1.2	Extraktion der Festplattenabbilder sowie SD-Kartenabbilder; Prüfsummen-Verifikation von Abbild-Dateien
Magnet Forensics	AXIOM	8.1.0.40287	Verarbeitung der Abbild-Dateien; Analyse und Klassifikation der gewonnenen Daten
Raspberry Pi	Raspberry Pi Imager	1.8.5	Nachbildung von Asservat 01 zu Forschungszwecken
Forensic Soft	SAFE Block	1.3	Software Write Blocker für die Sicherung der MicrsoSD-Karte

Tabelle 5.4.1 – Eingesetzte Untersuchungswerkzeuge

5.5 Vorbereitung der Untersuchung

Tabelle 5.5.1 enthält Schlüsselworte, die in *AXIOM* eingesetzt werden, um relevante Artefakte zu identifizieren. Hierbei werden initiale Schlüsselwörter und solche, die im Lauf der Untersuchung mithilfe von Zwischenergebnissen ergänzt werden, unterschieden.

Schlüsselwort	Anmerkung	Quelle
neptuns schild	Bezeichnung des vertraulichen Projekts und Quelle vertraulicher Informationen	Untersuchungsauftrag
neptun	Alias der Projektbezeichnung	(Untersuchungsauftrag)
usb stick	Bezeichnung Asservat 001	Untersuchungsauftrag
usb-stick	Alias von Asservat 001	(Untersuchungsauftrag)
erik	Rufname der verschwundenen Person	Untersuchungsauftrag
gott der meere	Alias der Projektbezeichnung	E-Mail-Verkehr
krakowia	Reiseziel	E-Mail-Verkehr

maldive	Zwischenziel	E-Mail-Verkehr
wien	Zwischenziel	E-Mail-Verkehr
zürich	Zwischenziel	E-Mail-Verkehr
dubai	Zwischenziel	E-Mail-Verkehr

Tabelle 5.5.1 – Schlagwortliste zur Identifizierung relevanter Artefakte

5.6 Asservat 001 - USB-Stick mit MicroSD-Karte

5.6.1 Erzeugung des Abbilds

Für die Extraktion der Daten aus der MicroSD-Karte wird als Schreibschutz das Programm *SAFE Block* eingesetzt (Abb. 5.6,1 und 5.6.2). Anschließend wird die MicroSD-Karte mit dem anerkannten Werkzeug *FTK Imager* gesichert. Die Sicherung wird mithilfe von Prüfsummen verifiziert (Abb. 5.6.3). Die Anschließende Analyse erfolgt in *Magnet AXIOM*.

Hinweis: In der Projektarbeit nutzen wir einen Software Write Blocker, da ein Hardwaregerät nicht verfügbar war und mit hohen Anschaffungskosten verbunden wäre. Wir haben uns für SAFE Block der Firma ForensicSoft entschieden, da eine freie Testversion verfügbar ist und aus [6, Fazit] eine ausreichende forensische Sicherheit vor Schreibzugriffen hervorgeht.
In einer realen IT-forensischen Untersuchung könnten Hardware Write Blocker zum Einsatz kommen, da eine einfachere Bedienbarkeit im Feldeinsatz [6, 2.1.1] gegeben ist. Ein Nachteil von Hardware Write Blockern gegenüber Software Write Blockern ist die geringere Flexibilität durch unterschiedliche Schnittstellenspezifikationen. Das bedeutet, dass unterschiedliche Schnittstellen dedizierte Write Blocker notwendig machen, was mit hohen Anschaffungskosten für individuelle Geräte für jede Schnittstelle verbunden ist.

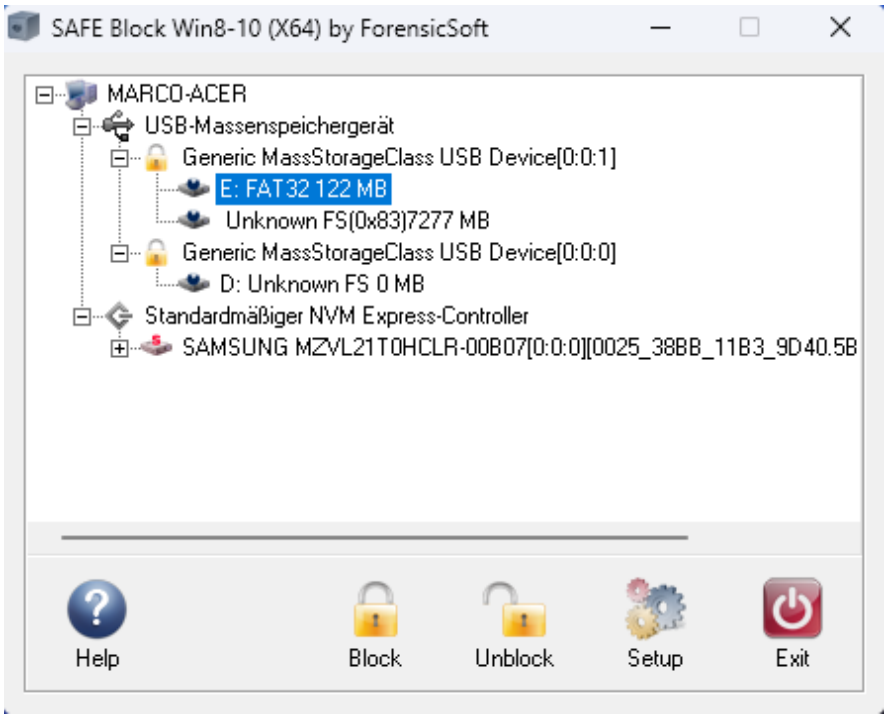


Abbildung 5.6.1 – Bildschirmabzug des Analyse-Rechners beim Start des Write Blockers SAFE Block

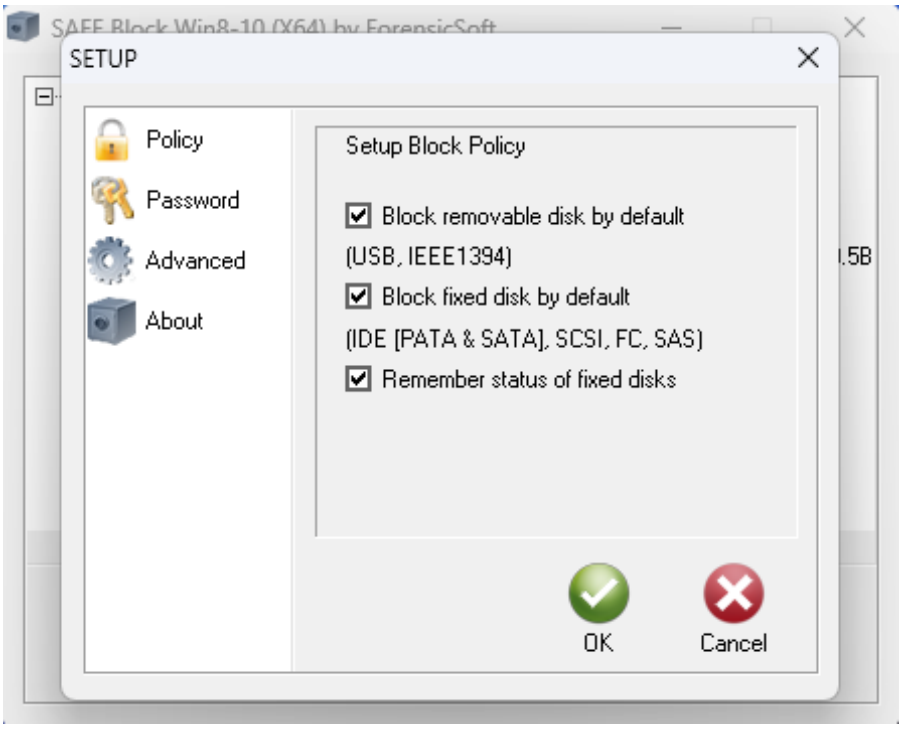


Abbildung 5.6.2 – Bildschirmabzug des Analyse-Rechners bei der Konfiguration des Write Blockers SAFE Block

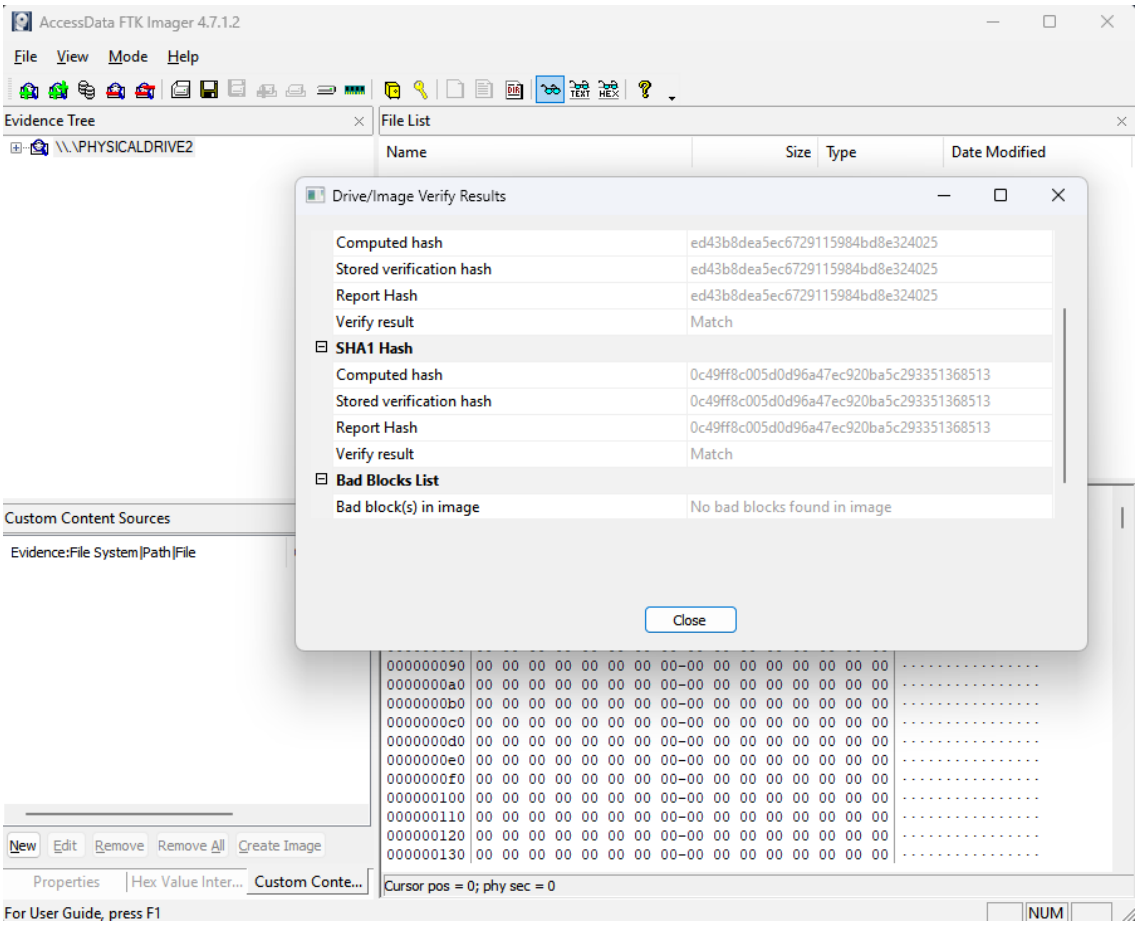


Abbildung 5.6.3 – Bildschirmabzug aus FTK Imager mit dem Vergleich der Prüfsummen des Abbilds mit dem Originaldatenträger

5.6.2 Physische und logische Medienanalyse

Die Micro-SD-Karte beinhaltet zwei Partitionen, die in Abb. 5.6.2.1 und Abb. 5.6.2.2 dargestellt sind.

Partition 2 enthält ein Dateisystem aus der Gruppe der Extended Filesystems (EXT). Ein solches Dateisystem wird unter Linux Betriebssystemen für die Dateiverwaltung genutzt. Abb. 5.6.2.3 zeigt die Struktur des Linux-Systems, während Partition 1 Informationen zum Betriebssystemkern (Kernel) und System-Speicher (System-Volume) enthält.

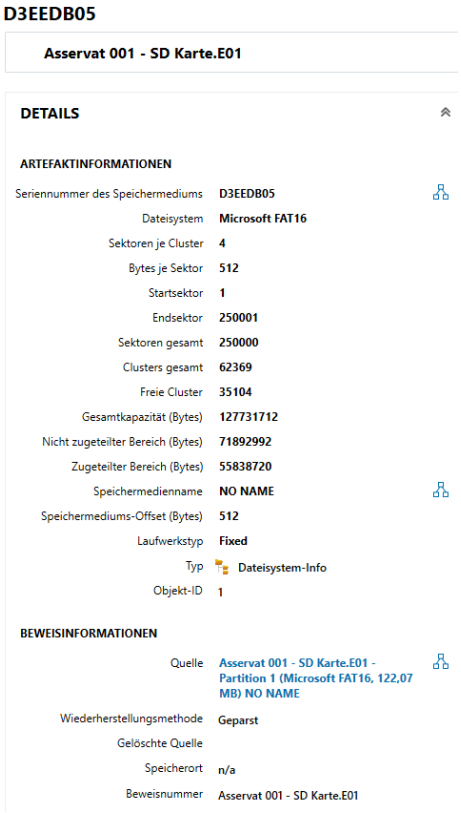


Abbildung 5.6.2.1 – Informationen zur Partition 1

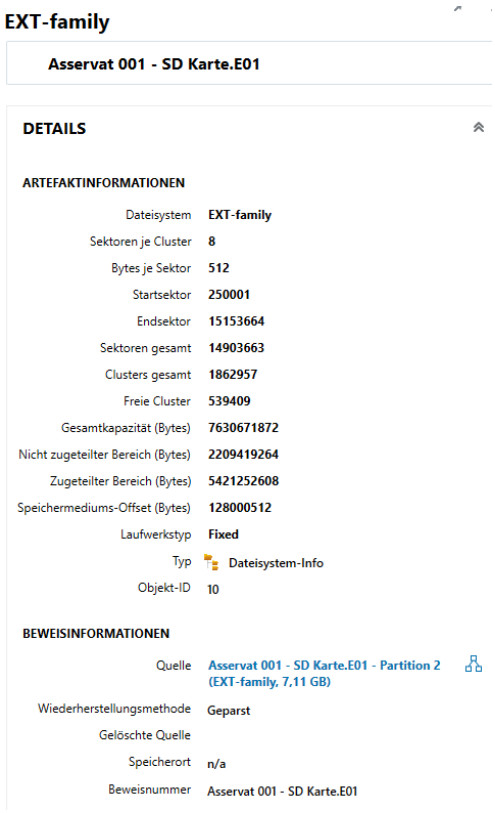


Abbildung 5.6.2.2 – Informationen zur Partition 2

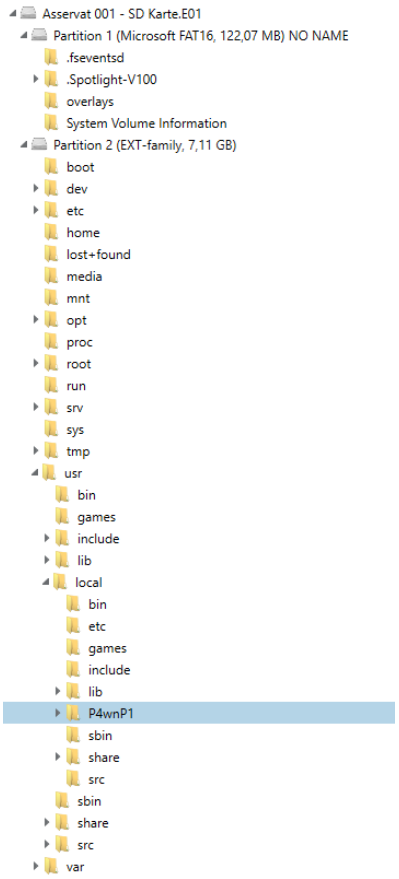


Abbildung 5.6.2.3 – Darstellung des EXT Dateisystems

Im Rahmen dieser ersten Analyse lassen sich folgende Informationen ermitteln:

1. In Partition 1 sind versteckte Verzeichnisse wie *.Spotlight-V100* enthalten. Dies weist darauf hin, dass die Micro-SD-Karte und das darauf enthaltene Linux-System mit einem Apple-Computer erzeugt wurden. Hintergrund: Im Betriebssystem MacOS ist die Funktion *Spotlight* enthalten, die eine Suche auf der internen Festplatte sowie angeschlossenen Geräten ermöglicht. Für eine schnellere Suche können angeschlossene Speicher durch Spotlight indiziert und dabei die entsprechenden versteckten Dateien und Verzeichnisse wie z.B. *.Spotlight-V100* angelegt werden.
2. In Partition 2 gibt es im Verzeichnis */usr/local* einen User mit der Bezeichnung *P4wnP1*. Eine Suche über Google (Abb. 5.6.2.4) gibt hier einen weiteren Hinweis auf das verwendete Linux-System. Im vorliegenden Fall besteht ein vergleichbares Setup, bestehend aus ein Raspberry Pi Zero W USB-Stick mit Micro-SD-Karte.

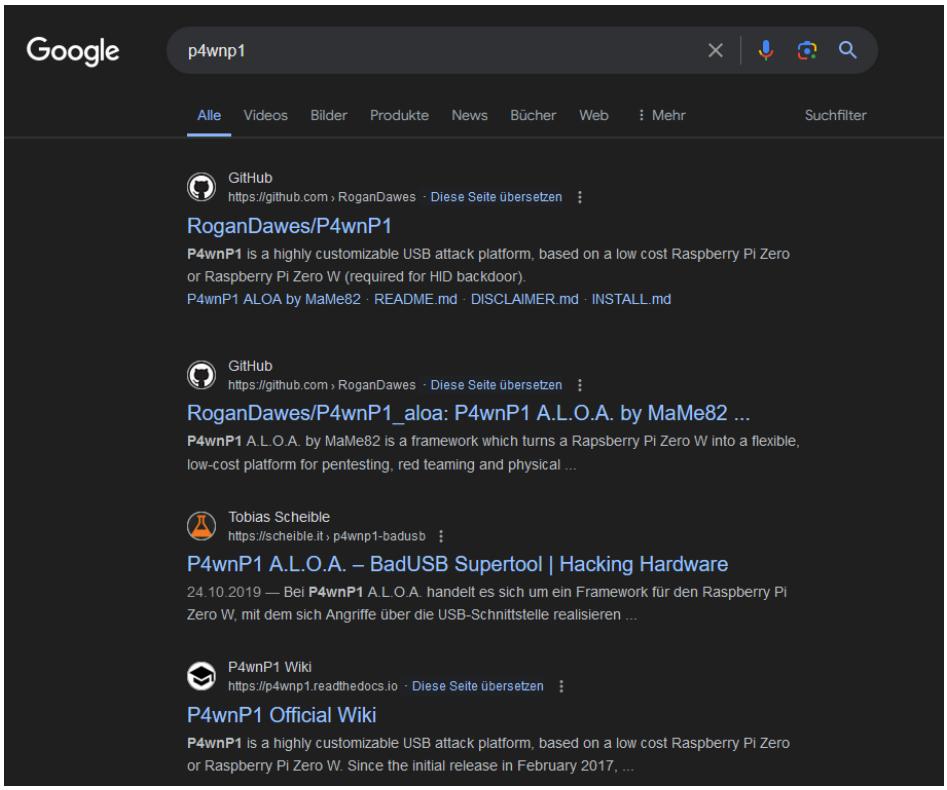


Abbildung 5.6.2.4 – Suchergebnisse der Suche nach der Bezeichnung des gefundenen Benutzernamens

5.6.3 Analyse der Zeitlinie und *syslog*-Datei

Die Zeitlinien-Analyse in Axiom offenbart keine Bezüge zur Zeitleiste des aktuellen Falls. Nahezu alle Dateien tragen Zeitstempel vor 2024 mit Ausnahme einiger Dateien vom 19.5.2024 (Abs. 5.6.2) und zwei Dateien vom 12.06. 0:00 UTC: *wpsettings.dat* und *IndexerVolumeGuid*.

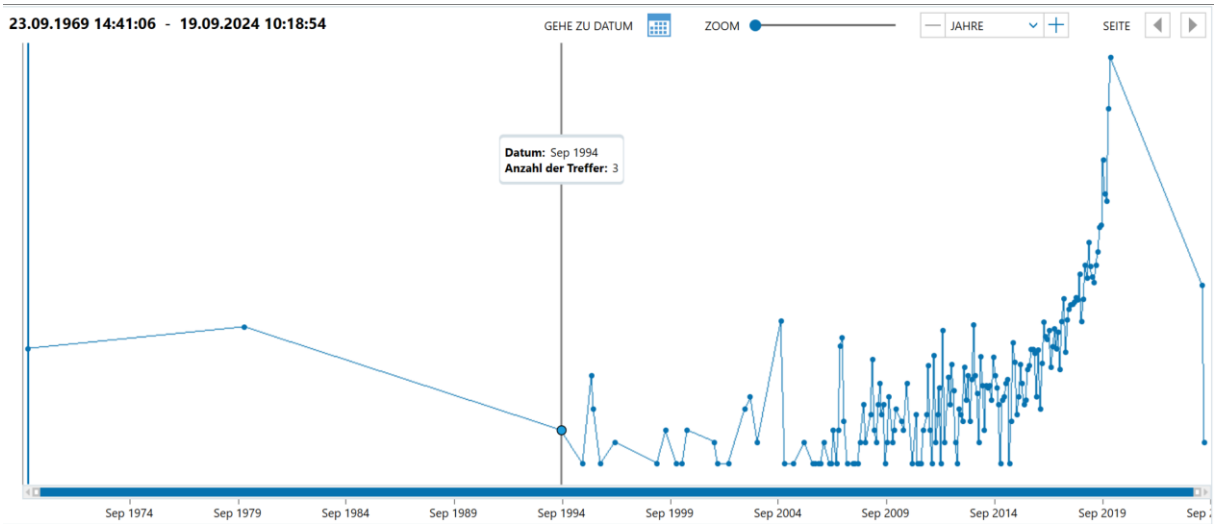


Abbildung 5.6.3.1 – Timeline der Artefakte auf der MicroSD-Karte des USB-Sticks

Diese letzten beiden Dateien werden standardmäßig von Windows-Systemen angelegt bzw. aktualisiert, wenn externe Laufwerke wie Micro-SD-Karten an ein Windows-System angebunden werden. Auch mit einem Write Blocker wie *SAFE Block* kann dies auftreten, allerdings ist die Uhrzeit hier nicht übereinstimmend mit dem Zeitablauf der Analyse, die gemäß der Dokumentation am 12.06. um 16:15 UTC begann.

Da die Zeitlinie aus *AXIOM* hier keine tieferen Erkenntnisse liefert, gibt evtl. die *syslog*-Datei mehr Auskunft.
Hinweis zu *syslog*: In Linux-Systemen kann ein zentraler Dienst alle Logs, die auf dem System anfallen, gesammelt anzeigen. Dies geschieht in der sogenannten *syslog*-Datei.
Auf dem hier vorliegenden System ist die Datei in *AXIOM* über die Suchfunktion ermittelbar und zeigt an, dass zwei der zu Beginn eingegebenen Schlüsselworte *erik* und *neptun* darin auftreten.
Abb. 5.6.3.2 zeigt, dass auch die *syslog*-Datei keine näheren Informationen innerhalb der Zeitlinie enthält, alle Zeitstempel beziehen sich auf Zeitpunkte im Februar 2020.

ARTEFAKTINFORMATIONEN

Name	**syslog**
Typ	**File**
File size	**2348334**
Created	**06.02.2020 14:38:35,000**
Accessed	**06.02.2020 14:38:35,000**
Modified	**06.02.2020 22:07:02,000**

Abbildung 5.6.3.2 – Untersuchung der Zeitstempel der *syslog*-Datei

Hier findet sich ein Hinweis auf die Ursache der Abweichung der Zeitlinie. Die Funktion *fake-hwclock*, die minütlich eigene Zeitstempel erzeugt, wie auch in diesem Auszug aus dem *syslog*.

```
Feb  6 22:03:01 kali CRON[1820]: (root) CMD (/usr/sbin/fake-hwclock)
Feb  6 22:04:01 kali CRON[1832]: (root) CMD (/usr/sbin/fake-hwclock)
```

Abbildung 5.6.3.3 – Gefundene Funktion zur Manipulation der Systemzeit

Die *syslog*-Datei gibt außerdem Hinweise auf zwei Rechner, mit denen der USB-Stick verbunden war und welche Skripte damit ausgeführt wurden: Eine USB-Verbindung mit einem Rechner (*Vladimir-HP*) und eine Verbindung über WLAN (*Vladimir-Acer*), wie in Abb. 5.6.3.4 dargestellt.

```
Feb  6 19:11:24 kali P4wnP1_service[174]: Lease monitor usbeth LEASE: &{false usbeth 172.16.0.2 42:63:65:12:34:56 Vladimir-HP}
Feb  6 19:11:25 kali systemd-udevd[121]: regulatory.0: Process '/sbin/crda' failed with exit code 249.
Feb  6 19:11:25 kali dbus-daemon[274]: [system] Successfully activated service 'org.freedesktop.hostname1'
Feb  6 19:11:25 kali systemd[1]: Started Hostname Service.
Feb  6 19:11:25 kali systemd[1]: Startup finished in 2.164s (kernel) + 27.574s (userspace) = 29.738s.
Feb  6 19:11:25 kali haveged[182]: haveged: ver: 1.9.8; arch: generic; vend: ; build: (gcc 9.2.1 CTV); collect: 128K
Feb  6 19:11:25 kali haveged[182]: haveged: cpu: (VC); data: 16K (D); inst: 16K (D); idx: 11/40; sz: 14748/63356
Feb  6 19:11:25 kali haveged[182]: haveged: tot tests(BA8): A:1/1 B:1/1 continuous tests(B):  last entropy estimate 8.00206
Feb  6 19:11:25 kali haveged[182]: haveged: fills: 0, generated: 0
Feb  6 19:11:26 kali hostapd: wlan0: STA e0:0a:f6:ce:71:57 IEEE 802.11: associated
Feb  6 19:11:26 kali P4wnP1_service[174]: hostapd: 19:11:26 wlan0: STA e0:0a:f6:ce:71:57 IEEE 802.11: associated
Feb  6 19:11:26 kali P4wnP1_service[174]: hostapd: 19:11:26 wlan0: AP-STA-CONNECTED e0:0a:f6:ce:71:57
Feb  6 19:11:26 kali P4wnP1_service[174]: hostapd: 19:11:26 wlan0: STA e0:0a:f6:ce:71:57 RADIUS: starting accounting session 3FA409A5C375949E
Feb  6 19:11:26 kali hostapd: wlan0: STA e0:0a:f6:ce:71:57 RADIUS: starting accounting session 3FA409A5C375949E
Feb  6 19:11:26 kali P4wnP1_service[174]: hostapd: 19:11:26 wlan0: STA e0:0a:f6:ce:71:57 WPA: pairwise key handshake completed (RSN)
Feb  6 19:11:26 kali hostapd: wlan0: STA e0:0a:f6:ce:71:57 WPA: pairwise key handshake completed (RSN)
Feb  6 19:11:26 kali P4wnP1_service[174]: Lease monitor wlan0 LEASE: &{false wlan0 172.24.0.12 e0:0a:f6:ce:71:57 Vladimir-Acer}
```

Abbildung 5.6.3.4 – Aufzug aus der *syslog*-Datei mit Netzwerkverbindungen

Da die Zeitlinie mit *fake-hwclock* durch das System verändert wurde, kann hier keine Aussage getroffen werden, zu welchem Zeitpunkt genau diese Verbindung zu den beiden Rechnern aufgebaut wurde. Allerdings handelt es sich bei den beiden Rechnern um die letzten Verbindungen, die durch das *syslog* dokumentiert sind.

5.6.4 Analyse gefundener Skripte

Aus der Analyse der *syslog*-Datei ergeben sich erneut Hinweise auf den Nutzer *P4wnP1* wie in Abs. 5.6.2. Mit diesem Wissen und dem Schlüsselwort *neptun* lässt sich zunächst eine Datei *NeptunCopyUserFolders.js* finden und dann ein Verzeichnis mit weiteren Skripten, dessen Inhalt in Abb. 5.6.4.1 dargestellt ist.
Es sind in diesem Verzeichnis drei Dateien enthalten, die den Schlüsselworten *erik* und *neptun* entsprechen.
Die Datei *Erik-Test.js* wird mit dem Tag *von Interesse* versehen, hierbei handelt es sich um eine JavaScript-Datei, die Mausbewegungen und Texterstellung im Windows-Texteditor simulieren soll (Anhang A *Skript Erik-Test.js*)
Die beiden anderen Dateien *NeptunCopyUserFolders.js* und *EriksSearch.js* wurden mit dem Tag *Beweis* versehen, da beide Dateien Skripte zum Kopieren möglicher relevanter Dateien auf ein externes Laufwerk enthalten (Anhang A *Skript NeptunCopyUserFolders.js* und *Skript EriksSearch.js*) und hinsichtlich der Beweisfindung einer genaueren Analyse unterzogen werden sollen (Abs. 5.6.5)
Im Rahmen der Analyse wurde nicht verifiziert, ob diese Skripte funktionsfähig sind.

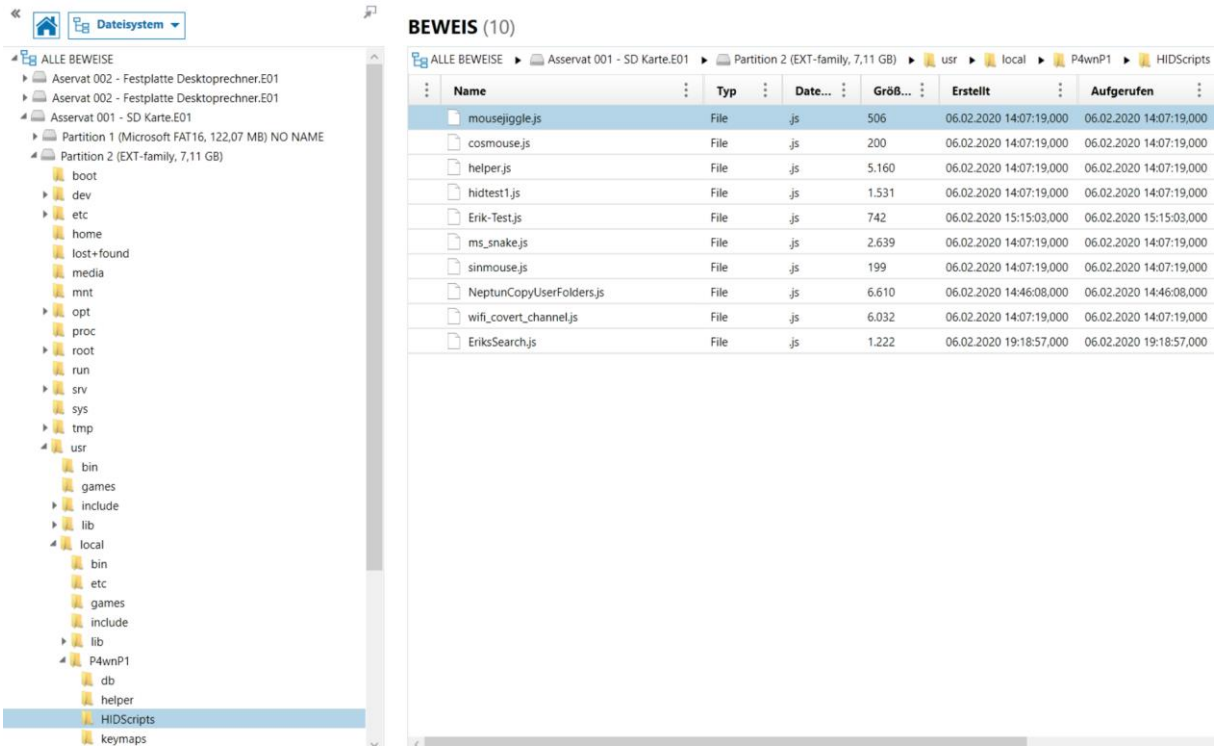


Abbildung 5.6.4.1 – Verzeichnis mit Skripten

5.6.5 Überprüfung von Log-Dateien, Zeitlinie und Skripten

Aus den vorangegangenen Abs. 5.6.2 bis 5.6.4 bleiben einige Fragen offen, die durch einen Test des Raspberry PI USB-Sticks in einer gesonderten Umgebung überprüft werden sollen.

1. Werden bei Erzeugung einer Linux-Distribution auf einer Micro-SD-Karte durch einen Apple-Rechner versteckte Dateien, wie in Abs. 5.6.2, erzeugt und weist die darin erzeugte Datei *VolumeConfguration.plist* auf das Erzeugungsdatum bzw. -Uhrzeit hin?
2. Wenn ein Linux-System mit dem User *P4wnP1* auf einem Raspberry Pi Zero W wie in dem vorliegenden Fall erzeugt wird: Enthält es dann vergleichbare Zeitreihen wie in Abs. 5.6.3?
3. Sind die in Abs. 5.6.4 ermittelten Skripte auf einem Windows-System ausführbar?
4. Welche Informationen zum USB-Stick bzw. der Micro-SD-Karte werden in den Registry-Dateien bzw. Systeminformationen hinterlegt?

Folgende Umgebung wird für den Test verwendet:

1. Ein Apple MacBook und MacOS 13.6.7.
   Nutzung: Erzeugung der Micro-SD-Karte zur Überprüfung von Frage 1 und zum Start der Skripte für Frage 3 per WLAN. Hinweis: Zum Anschluss der Mirco-SD-Karte an den Mac wird ein externes Laufwerk per USB angeschlossen.
2. Ein Rechner mit Windows 11 Professional.
   Nutzung: Dies wird der Opfer-Rechner, um die Skripte über den Raspberry Pi Zero W zu testen und zur Beantwortung der Fragen 3 und 4.
3. Ein Raspberry Pi Zero W mit Micro-SD-Karte. Da keine weitere 8GB-Karte vorhanden ist, wird eine Micro-SD-Karte mit 64GB verwendet. Die Karte ist neu und enthielt bislang keine Daten.

Nutzung: Der Raspberry Pi Zero W mit Micro-SD-Karte dient zum Test der Skripte auf dem Windows-Rechner und zur Beantwortung von Frage 2.

4. Software: Es wird die Software, die über die Suche in Abs. 5.6.2 ermittelt wurde, verwendet [5].
5. Für die Installation wird der Raspberry Pi Imager verwendet, wie auf der Homepage in [7] angegeben.

Schritt 1: Installation des RaspberryPi-Abbilds. Es wird der *RaspberryPi Imager* in Version 1.8.5 verwendet.
Schritt 2. Download und Installation der Software für den Raspberry Pi aus [5] in der Version v0.1.1-beta, wie in Abb. 5.6.5.1 zu sehen.

Abbildung 5.6.5.1 – Raspberry Pi Imager Startseite

Schritt 3: Den USB-Stick mit der Micro-SD-Karte mit dem USB-Port des Windows-Rechners verbinden. Der Raspberry PI baut ein WLAN (Abb. 5.6.5.2) auf, womit sich der Apple-Rechner verbindet und die Startseite im Browser öffnet, die in Abb. 5.6.5.3 zu sehen ist.

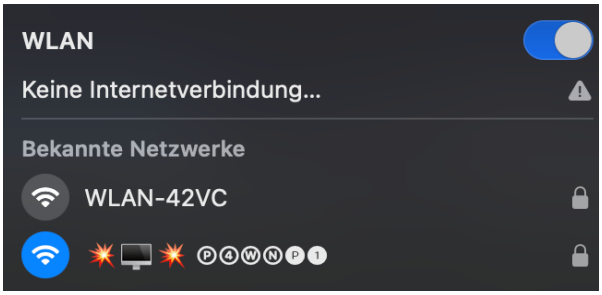


Abbildung 5.6.5.2 – Bezeichnung des vom USB-Stick ausgestrahlten WLANs

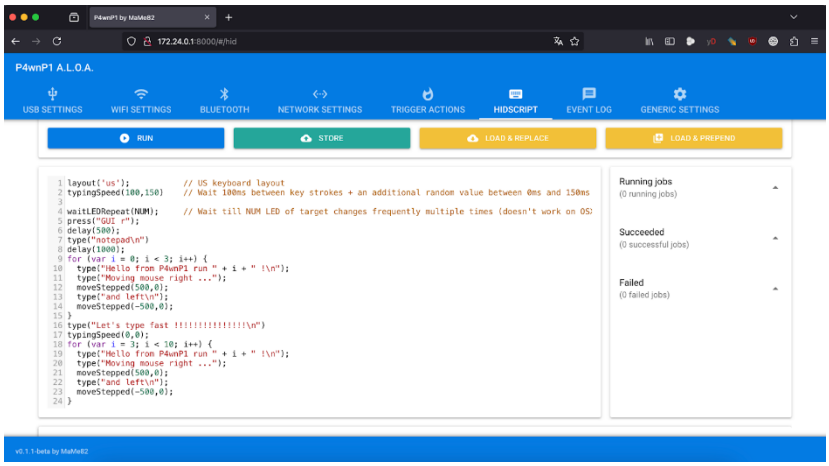


Abbildung 5.6.5.3 – Testskript für HID-Funktionalitäten

Im Windows-Rechner wird der Raspberry PI Zero W in der Systemsteuerung im Gerätemanager unter *Systemsteuerung\ Geräte-Manager\ HID-Devices\ Eigenschaften\Ereignisse* erkannt unter der Bezeichnung *VID_1D6B, PID_1347* (Vendor-Identifier, Product-Identifier). Es wird außerdem im Geräte-Manager gefunden unter dem Menüpunkt *Aktion\Geräte und Drucker*. Die einzige Darstellung, in der sich die Bezeichnung *P4wnP1 by MaMe82* offenbart, ist in Abb. 5.6.5.4 abgebildet.

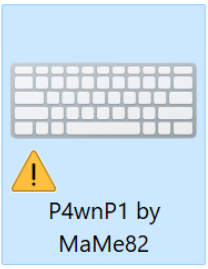


Abbildung 5.6.5.4 – Icon

Über den Menüpunkt Eigenschaften wird dann das oben angegebene Gerät mit der Bezeichnung *VID_1D6B, PID_1347* ermittelt, sowohl unter dem Menüpunkt *Andere Geräte* (CDC ECM) als auch unter dem Menüpunkt *Eingabegeräte (Human Interface Devices)* zweimal als *USB-Eingabegerät* (Abb. 5.6.5.6).

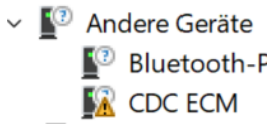


Abbildung 5.6.5.5 – Gefundene Andere Geräte

Abbildung 5.6.5.6 – Gefundene Eingabegeräte

Der Raspberry Pi Zero W wird in der Registry des Windows-Rechners unter dem Punkt *Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB* nicht gesondert als gerade verbundenes Gerät angezeigt. Alle bisher angemeldeten Geräte werden in der Liste angezeigt. Das markierte Gerät ist das Gerät, das über den Gerätemanager identifiziert werden konnte.

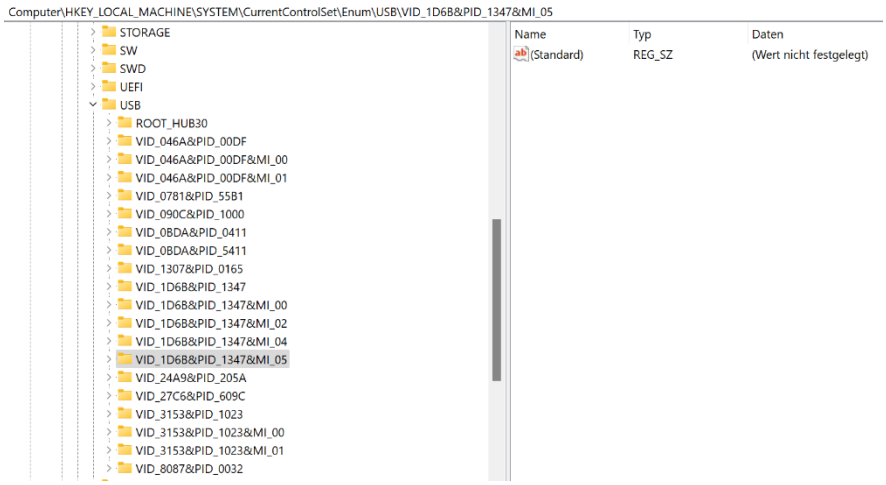


Abbildung 5.6.5.7 – Registry-Auszug

Schritt 5: Test des *Skripts NeptunCopyUserFolders.js*

1. Einloggen in das WLAN des Raspberry Pi Zero W mit dem Mac-Rechner und Start der Steuerungs-Webseite unter *http://172.24.0.1:8000* wie unter [5, *Readme*] beschrieben.
2. Hinzufügen eines leeren USB-Sticks in einen weiteren freien Port des Windows-Rechners
3. Anlage der Kopien der beiden Skripte über die Steuerungs-Webseite
4. Start des Skripts *NeptunCopyUserFolders.js*
5. Ergebnis: Das Skript startet und öffnet das Notepad. Darin wird Code kopiert. Parallel startet die *Windows Powershell*. Das Skript wird allerdings nicht beendet.

Schritt 6: Test des Skripts *EriksSearch.js*

1. Start des Skripts *EriksSearch.js*
2. Ergebnis: Das Skript startet und führt erfolgreich eine Suche und Kopie von Dateien mit der Bezeichnung *neptun* im Namen auf eine separate externe Festplatte aus. Im Skript musste die Laufwerkbezeichnung von *F:* auf *D:* angepasst werden.

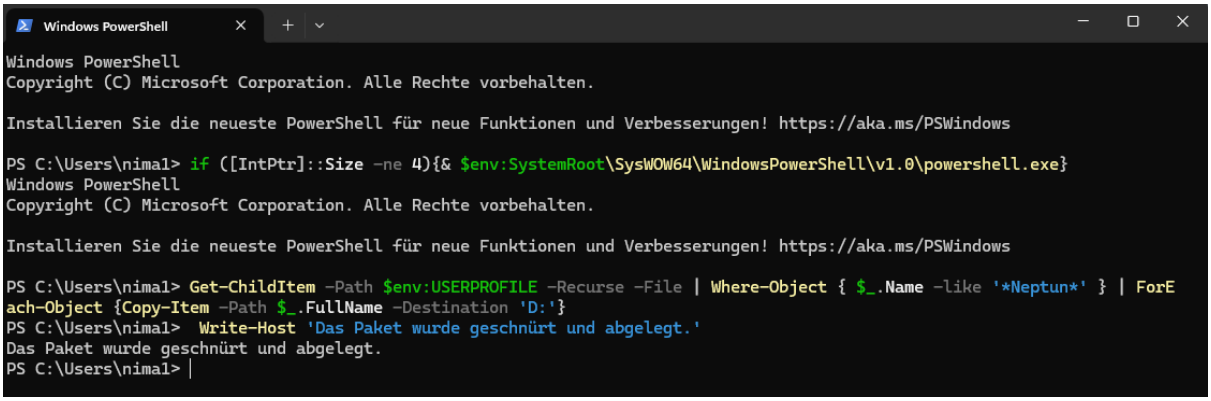


Abbildung 5.6.5.8 – Powershell Aktion

Schritt 7: Sicherung in *FTK-Imager* und automatische Analyse der MicroSD-Karte in *AXIOM* wie beim Original in Abs. 5.6.1 beschrieben zur Klärung der Fragen 1 und 2 (Anhang A FTK-Imager-Sicherung der Test-Installation aus Abs. 5.6.5).

Antworten auf die Fragen:

1. Werden bei Erzeugung einer Linux-Distribution auf einer Micro-SD-Karte durch einen Apple-Rechner versteckte Dateien, wie in Abs. 5.6.2, erzeugt und weist die darin erzeugte Datei VolumeConfiguration.plist auf das Erzeugungsdatum bzw. -Uhrzeit hin?

Auf der im Test aufgebauten Micro-SD-Karte sind keine versteckten Dateien, die auf einen Apple-Rechner hinweisen. Es gibt auch keine weiteren Hinweise auf die Installation der Micro-SD-Karte mit dem Betriebssystem. Eine mögliche Ursache für die versteckten Apple-Rechner-Dateien auf der Original-Micro-SD-Karte kann daher nicht mit Sicherheit ermittelt werde

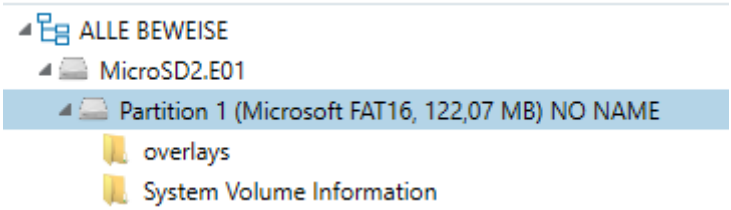


Abbildung 5.6.5.9 – Partition 1 mit FAT16 Dateisystem

2. Wenn ein Linux-System mit dem User P4wnP1 auf einem Raspberry Pi Zero W wie in dem vorliegenden Fall erzeugt wird: Enthält es dann vergleichbare Zeitreihen wie in Abs. 5.6.3?

Die Zeitreihen der beiden Laufwerke sind vergleichbar, insbesondere was den Bruch zwischen dem 06.02.2020, wie in Abs. Analyse der Zeitlinie und syslog-Datei Analyse der Zeitlinie und syslog-Datei beschrieben, und der eigentlichen Erstellung und In-

stallation der beiden Micro-SD-Karten angeht. Beide Zeitreihen enden zunächst am 06.02.2020 und beginnen erst wieder zum vermeintlichen Installations-Zeitpunkt, im Fall der Original-MicroSD-Karte am 19.05.2024 und der Test-Micro-SD-Karte am 01.07.2024. Bei beiden Zeitreihen werden auch die Windows-Dateien wpsettings.dat und IndexerVolumeGuid um 0:00 UTC angezeigt.

3. Sind die in Abs. 5.6.4 ermittelten Skripte auf einem Windows-System ausführbar?
   Die drei Skripte lassen sich auf dem für diesen Test genutzten Windows-System mit den Standard-Einstellungen eines neu installierten Windows 11 Professional ausführen. Es konnte lediglich das Skript EriksSearch.js einen erfolgreichen Kopiervorgang durchführen, sofern im Vorfeld die Laufwerksbezeichnung angepasst wurde für das Ziel der Kopie.

4. Welche Informationen zum USB-Stick bzw. der Micro-SD-Karte werden in den Registry-Dateien bzw. Systeminformationen hinterlegt?
   Es gibt keine Log-Dateien auf dem Windows-Rechner, die die Nutzung des Raspberry Pi als Bad-USB-Stick dokumentieren. Lediglich über den Gerätemanager kann das passende Gerät ermittelt werden. Das Gerät kann mit dem Wissen auch anschließend in der Registry gefunden werden, zeigt jedoch keine Informationen an, die einen Rückschluss auf die durchgeführten Powershell-Skripte ermöglichen.

5.7 Untersuchung Asservat 002 - Festplatte Desktoprechner

5.7.1 Abbild-Erstellung

Um die gespeicherten Daten zu extrahieren, wird die Festplatte des Desktoprechners unter Zuhilfenahme eines Write Blockers mit einem Analyserechner verbunden. Mithilfe der Software *AccessData FTK Imager* wird ein forensisches Abbild der Festplatte erstellt. Die Prüfsummen des Abbilds sind in Tab. 5.7.1.1 dargestellt.

MD 5	8f0c610f2631746106b210cb218f969d
SHA1	11588bea0cb9184aecc5f47fd694f298c36d8d3e

Tabelle 5.7.1.1 - Prüfsummen des Festplattenabbilds

Hinweis: In dieser Projektarbeit haben wir eine VM verwendet, um den Desktoprechner zu simulieren. Von der virtuellen Festplatte haben wir mit AccessData FTK Imager ein Abbild erstellt und die Prüfsummen verifiziert. In einer realen IT-forensischen Untersuchung wäre die Wahrscheinlichkeit höher, eine physische Festplatte vorzufinden. Das Gutachten behandelt aus diesem Grund die Sicherung einer physischen Festplatte.

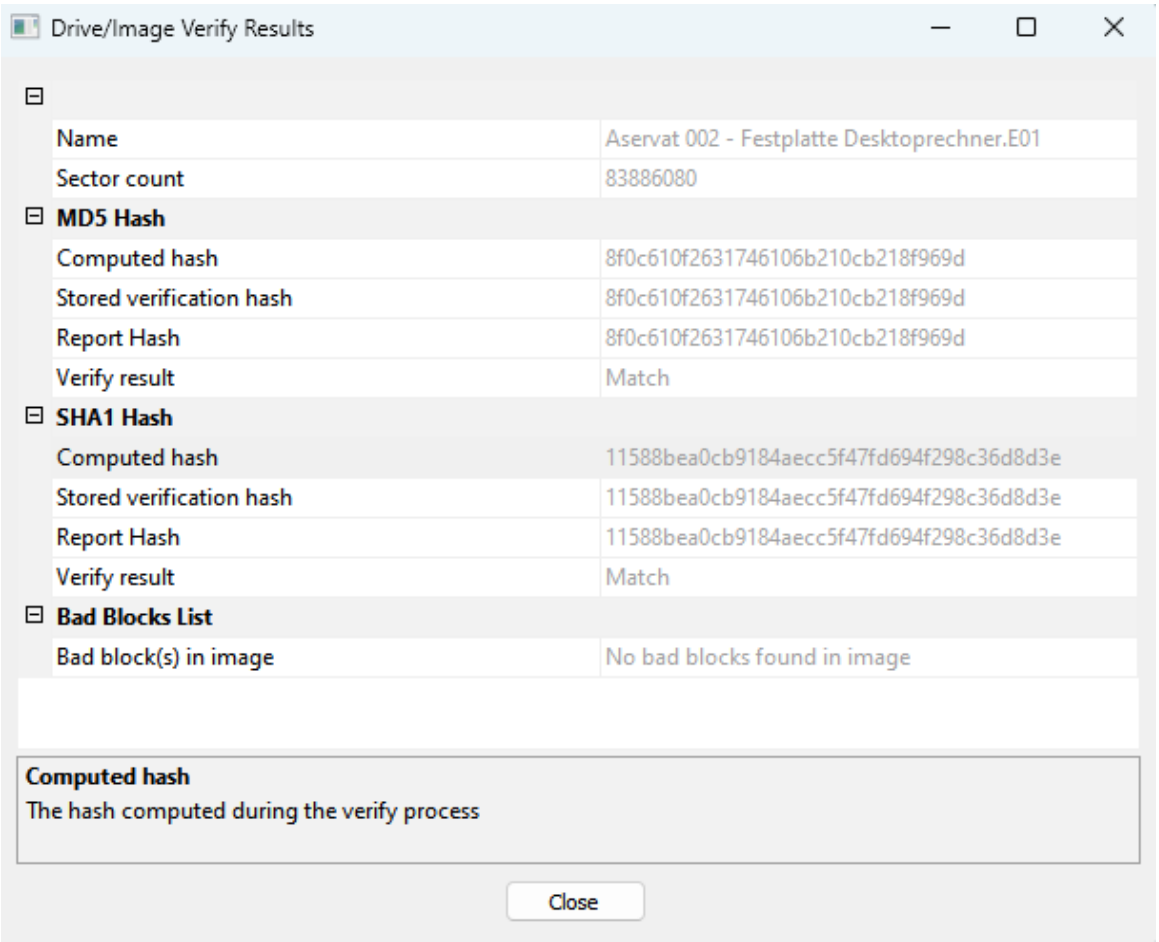


Abbildung 5.7.1.1 - Prüfsummenvergleich des Festplattenabbilds

Abbildung 5.7.1.1 zeigt den Vergleich der Prüfsummen. Die übereinstimmenden Prüfsummen zeigen, dass die Integrität des Festplattenabbilds sichergestellt ist und keine Veränderungen bei der Sicherung aufgetreten sind.

5.7.2 Partitionsstruktur

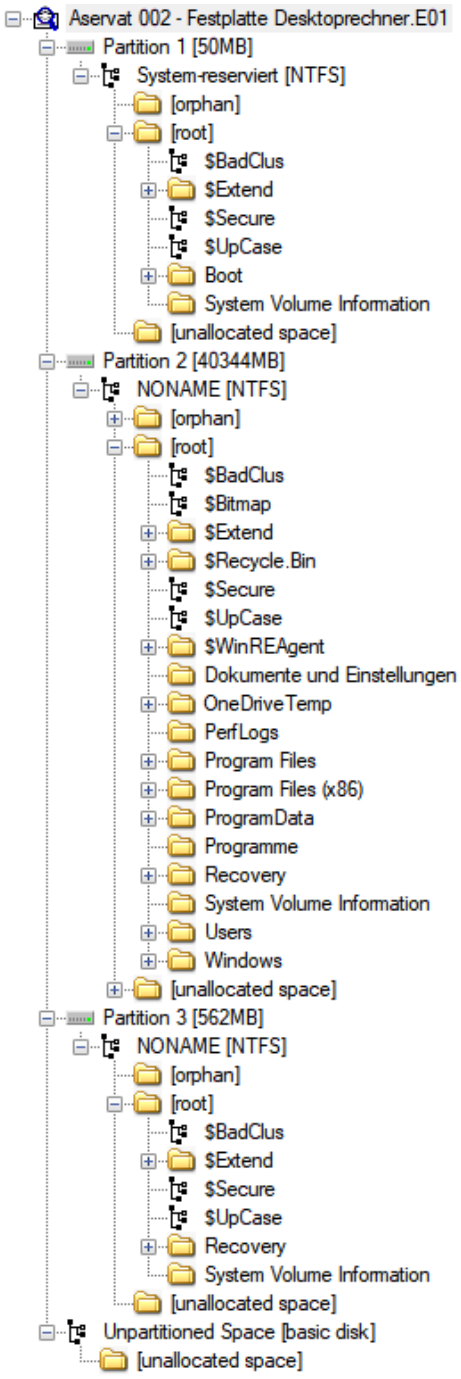


Abbildung 5.7.2.1 – Bildschirmabzug aus FTK Imager mit der Partitionsstruktur der Festplatte

Abbildung 5.7.2.1 zeigt die gefundene Partitionsstruktur auf dem Abbild der Festplatte. Es ist eine Windows-Installation erkennbar mit der Boot-Partition 1, einer Partition für Benutzerdaten (Partition 2) und einer Wiederherstellungspartition 3. Darüber hinaus existiert ein kleiner Speicherbereich, der keiner Partition zugeordnet ist. Eine Prüfung dieses nicht zugeordneten Bereichs ergibt keine Hinweise auf dort gespeicherte relevante Informationen.
Im Folgenden wird die Benutzerdaten-Partition 2 untersucht.
Das Festplattenabbild wird in *AXIOM* geladen und nachverarbeitet.

5.7.3 Systeminformationen

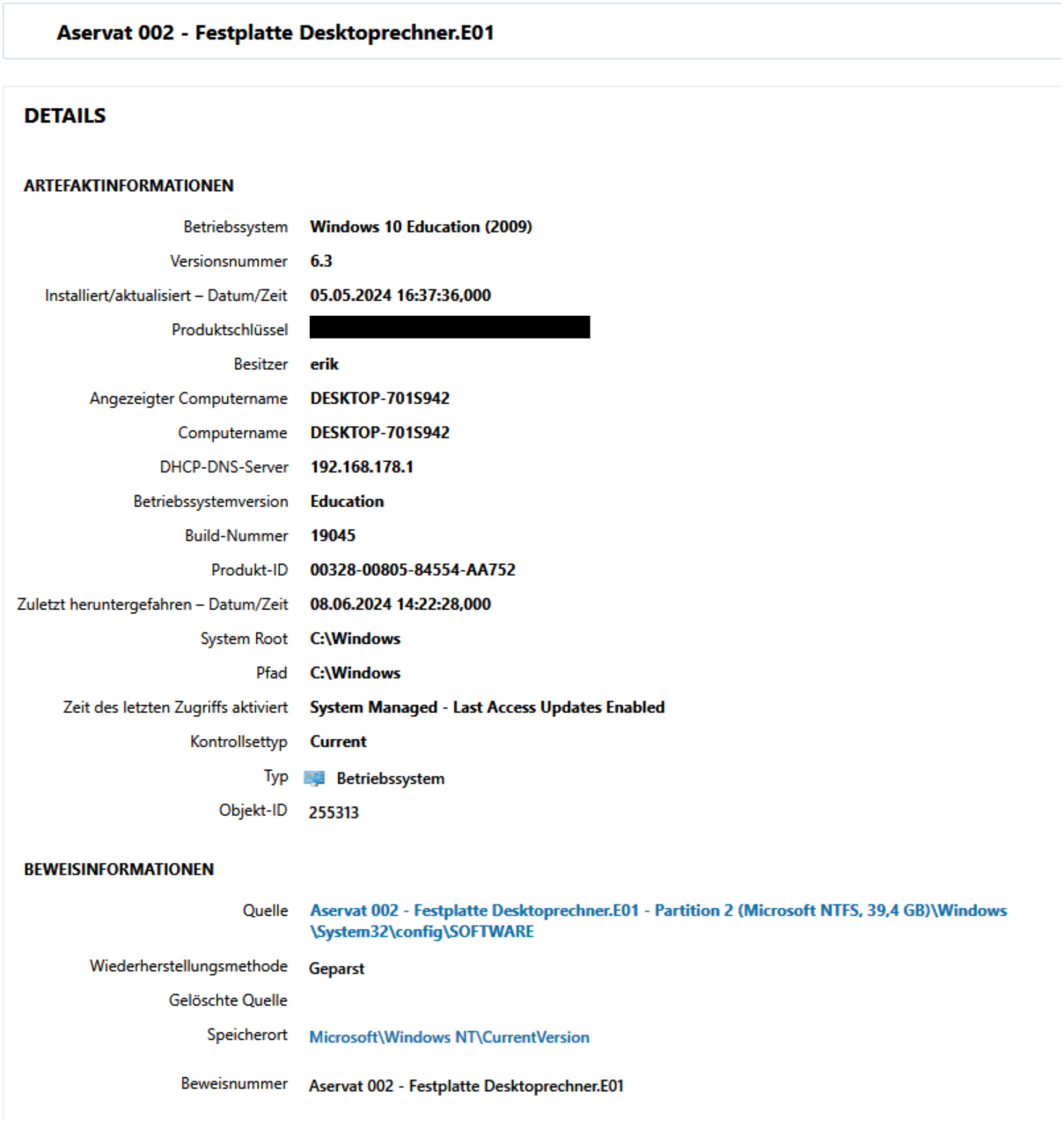


Abbildung 5.7.3.1 – Betriebssystem-Informationen

Die Auswertung der Systeminformationen in Abbildung 5.7.3.1 zeigt, dass die Festplatte eine Installation von Windows 10 Education beinhaltet. Das System ist am 05.05.2024 16:37:36 UTC mit dem in der Abbildung erkennbaren Lizenzschlüssel installiert worden. Als Besitzer ist *erik* eingetragen, zu dem auch ein gleichnamiges Benutzerkonto existiert. Der Rechner wurde am 08.06.2024 um 14:22:28 UTC zuletzt heruntergefahren und ist seitdem nicht mehr gestartet worden.

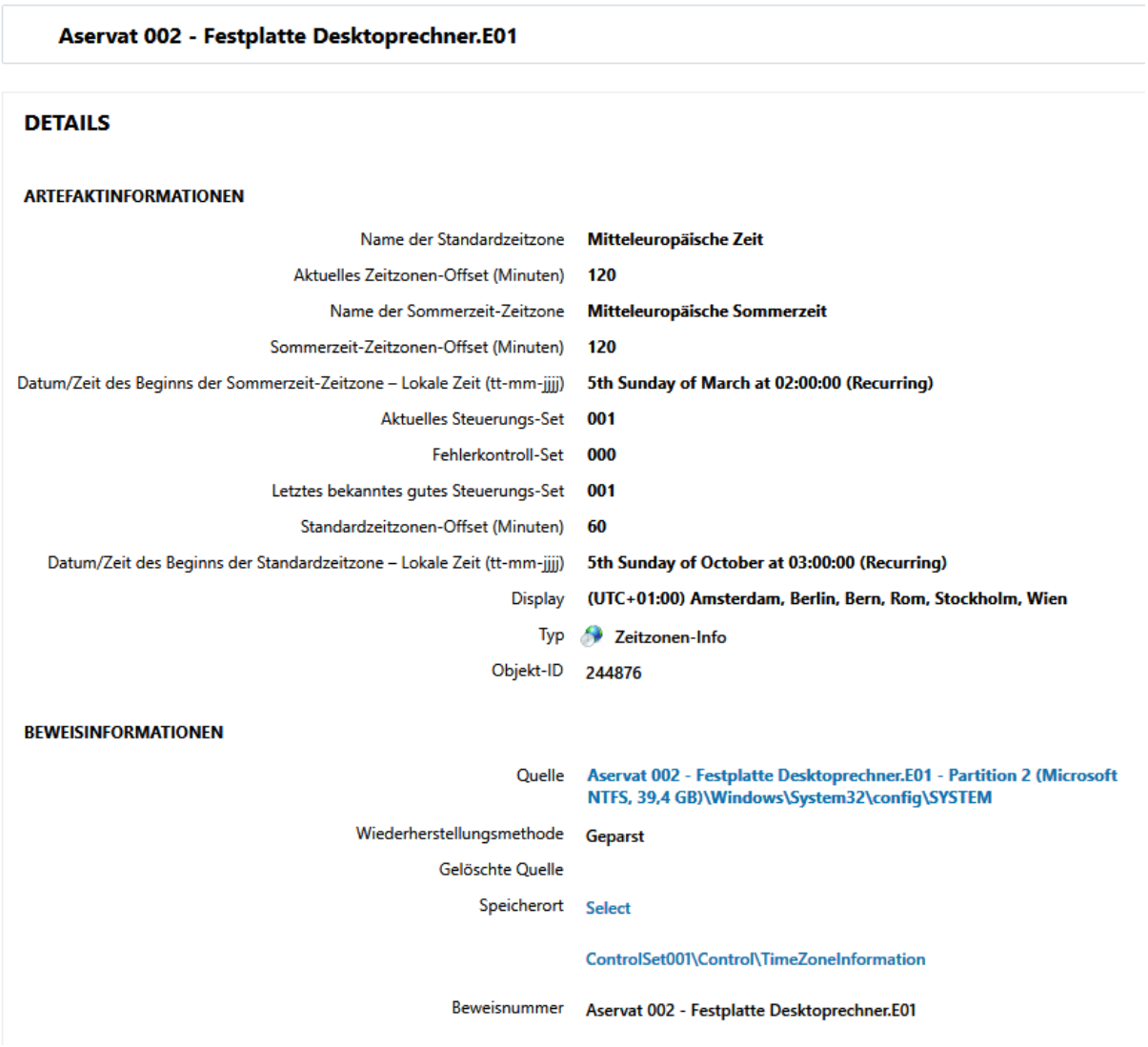


Abbildung 5.7.3.2 - Zeitzoneninformationen

Der Desktoprechner verwendet die Mitteleuropäische Zeit (MEZ, UTC+1) sowie die Mitteleuropäische Sommerzeit (MESZ, UTC+2). Im gesamten Untersuchungszeitraum gilt die MESZ. Es finden sich keine Hinweise auf eine Änderung der Zeitzone.
Die Zeitangaben in *AXIOM* beziehen sich stets auf die Koordinierte Weltzeit (UTC). Alle Bildschirmabzüge stellen somit gleichermaßen UTC dar, wenn nicht anders angegeben.

Auf dem System ist eine Reihe Microsoft-Anwendungen (Abb. 5.7.3.3) installiert, die Windows 10 standardmäßig mitliefert. Beinhaltet ist der Cloud-Speicherdienst Microsoft OneDrive, der das Übertragen von Dateien auf entfernte Systeme erlaubt.
Weitere installierte Anwendungen sind in Abb. 5.7.3.4 dargestellt. Die Anwendung Mozilla Thunderbird stellt einen E-Mail-Dienst dar, der E-Mails lokal auf der Festplatte speichert.

Anwendungsname	Unternehmen	Erste...	Schlüssel zuletz...	Insta...	Version	Potentieller
Microsoft Edge WebView2-Laufzeit	Microsoft Corporation	07.06.2024	07.06.2024 16:59:56,574		125.0.2535.85	C:\Users\erik\
Microsoft OneDrive	Microsoft Corporation		07.06.2024 16:44:53,268	329.743	24.101.0519.0010	C:\Users\erik\
Microsoft Update Health Tools	Microsoft Corporation	07.06.2024	07.06.2024 16:48:18,031	1.050	3.74.0.0	
Update for Windows 10 for x64-based Systems (KB5...	Microsoft Corporation	06.06.2024	06.06.2024 17:06:14,716	836	8.94.0.0	
Microsoft Edge	Microsoft Corporation	08.06.2024	08.06.2024 14:18:51,372		125.0.2535.92	C:\Program Fi
Microsoft Edge WebView2-Laufzeit	Microsoft Corporation	07.06.2024	07.06.2024 17:00:35,618		125.0.2535.92	C:\Program Fi
Microsoft Edge WebView2-Laufzeit	Microsoft Corporation	07.06.2024	07.06.2024 16:59:56,574		125.0.2535.85	C:\Users\erik\
Microsoft OneDrive	Microsoft Corporation		07.06.2024 16:44:53,268	329.743	24.101.0519.0010	C:\Users\erik\
Microsoft Update Health Tools	Microsoft Corporation	07.06.2024	07.06.2024 16:48:18,031	1.050	3.74.0.0	
Update for Windows 10 for x64-based Systems (KB5...	Microsoft Corporation	06.06.2024	06.06.2024 17:06:14,716	836	8.94.0.0	
Microsoft Edge	Microsoft Corporation	08.06.2024	08.06.2024 14:18:51,372		125.0.2535.92	C:\Program Fi
Microsoft Edge WebView2-Laufzeit	Microsoft Corporation	07.06.2024	07.06.2024 17:00:35,618		125.0.2535.92	C:\Program Fi

Abbildung 5.7.3.3 - Installierte Microsoft-Anwendungen

Anwendungsname	Unternehmen	Schlüssel zuletzt a...	Insta...	Version	Potentieller Speicherort
Mozilla Thunderbird (x64 de)	Mozilla	02.06.2024 18:11:06,019	245.332	115.11.1	C:\Program Files\Mozilla Thunderbird
Mozilla Maintenance Service	Mozilla	02.06.2024 18:11:06,714	335	115.11.1	C:\Program Files (x86)\Mozilla Maintenance Service
Microsoft Edge Update		07.06.2024 16:44:41,660		1.3.187.41	
Mozilla Thunderbird (x64 de)	Mozilla	02.06.2024 18:11:06,019	245.332	115.11.1	C:\Program Files\Mozilla Thunderbird
Mozilla Maintenance Service	Mozilla	02.06.2024 18:11:06,714	335	115.11.1	C:\Program Files (x86)\Mozilla Maintenance Service
Microsoft Edge Update		07.06.2024 16:44:41,660		1.3.187.41	

Abbildung 5.7.3.4 - Weitere installierte Anwendungen

5.7.4 Benutzer

Benutzername	Nutzer-Typ	Sicherer Identifikator	Zuge...	Profilpfad	Letzte lokale Anme...
	Built-in	S-1-5-18		%systemroot%\sys...	
	Built-in	S-1-5-19		%systemroot%\Ser...	
	Built-in	S-1-5-20		%systemroot%\Ser...	
Administrator	Local User	500	500		
erik	Local User	S-1-5-21-1748443609-3498283432-1879274306-1001	1001	C:\Users\erik	08.06.2024 14:09:40,000
Gast	Local User	501	501		
DefaultAccount	Local User	503	503		
WDAGUtilityAccount	Local User	504	504		

Abbildung 5.7.4.1 - Benutzerkonten

Abbildung 5.7.4.1 listet die Benutzerkonten auf, die auf dem Desktoprechner existieren. Der Benutzer *erik* stellt das einzige Benutzerkonto dar, welches nicht standardmäßig durch eine Windows 10 Installation angelegt wird. Hierbei handelt es sich um das Benutzerkonto, mit dem die Installation des Betriebssystems registriert worden ist (Abb. 5.7.4.1). Durch den Namen lässt sich das Benutzerkonto und der Desktoprechner der beschuldigten Person zuordnen.

Datum/Zeit der...	Ereignisbeschreibung – Zusammenfassung	Anmeldungstyp	Benut...
04.06.2024 16:41:05,842	A logon was attempted using explicit credentials.		erik
04.06.2024 16:41:05,842	An account was successfully logged on.	2-Interactive	erik
04.06.2024 16:41:05,842	An account was successfully logged on.	2-Interactive	erik
04.06.2024 16:41:05,842	A logon was attempted using explicit credentials.		erik
04.06.2024 16:41:05,842	An account was successfully logged on.	2-Interactive	erik
04.06.2024 16:41:05,842	An account was successfully logged on.	2-Interactive	erik
04.06.2024 16:46:08,107	An account was successfully logged on.	2-Interactive	erik
04.06.2024 16:46:08,107	An account was successfully logged on.	2-Interactive	erik
04.06.2024 16:46:08,107	A logon was attempted using explicit credentials.		erik
04.06.2024 16:46:08,107	A logon was attempted using explicit credentials.		erik
04.06.2024 16:46:08,107	An account was successfully logged on.	2-Interactive	erik
04.06.2024 16:46:08,107	An account was successfully logged on.	2-Interactive	erik
04.06.2024 16:46:08,177	An account was logged off.	2-Interactive	erik
04.06.2024 16:46:08,177	An account was logged off.	2-Interactive	erik
04.06.2024 16:46:08,193	An account was logged off.	2-Interactive	erik

Abbildung 5.7.4.2 - Anmeldeereignisse mit dem Benutzerkonto *erik* am 04.06.2024

Datum/Zeit der...	Ereignisbeschreibung – Zusammenfassung	Anmeldungstyp	Benut...
06.06.2024 17:04:13,402	A logon was attempted using explicit credentials.		erik
06.06.2024 17:04:13,402	An account was successfully logged on.	2-Interactive	erik
06.06.2024 17:04:13,402	An account was successfully logged on.	2-Interactive	erik
06.06.2024 17:04:13,402	A logon was attempted using explicit credentials.		erik
06.06.2024 17:04:13,402	An account was successfully logged on.	2-Interactive	erik
06.06.2024 17:04:13,402	An account was successfully logged on.	2-Interactive	erik
06.06.2024 17:04:19,448	A logon was attempted using explicit credentials.		erik
06.06.2024 17:04:19,448	An account was successfully logged on.	2-Interactive	erik
06.06.2024 17:04:19,448	An account was successfully logged on.	2-Interactive	erik
06.06.2024 17:04:19,448	A logon was attempted using explicit credentials.		erik
06.06.2024 17:04:19,448	An account was successfully logged on.	2-Interactive	erik
06.06.2024 17:04:19,448	An account was successfully logged on.	2-Interactive	erik
06.06.2024 17:04:19,533	An account was logged off.	2-Interactive	erik
06.06.2024 17:04:19,533	An account was logged off.	2-Interactive	erik
06.06.2024 17:04:19,533	An account was logged off.	2-Interactive	erik
06.06.2024 17:04:19,533	An account was logged off.	2-Interactive	erik

Abbildung 5.7.4.3 - Anmeldeereignisse mit dem Benutzerkonto *erik* am 06.06.2024

Datum/Zeit der...	Ereignisbeschreibung – Zusammenfassung	Anmeldungstyp	Benut...
07.06.2024 16:41:00,285	A logon was attempted using explicit credentials.		erik
07.06.2024 16:41:00,285	An account was successfully logged on.	2-Interactive	erik
07.06.2024 16:41:00,285	An account was successfully logged on.	2-Interactive	erik
07.06.2024 16:41:00,285	A logon was attempted using explicit credentials.		erik
07.06.2024 16:41:00,285	An account was successfully logged on.	2-Interactive	erik
07.06.2024 16:41:00,285	An account was successfully logged on.	2-Interactive	erik
07.06.2024 16:41:10,072	A logon was attempted using explicit credentials.		erik
07.06.2024 16:41:10,072	An account was successfully logged on.	2-Interactive	erik
07.06.2024 16:41:10,072	An account was successfully logged on.	2-Interactive	erik
07.06.2024 16:41:10,072	A logon was attempted using explicit credentials.		erik
07.06.2024 16:41:10,072	An account was successfully logged on.	2-Interactive	erik
07.06.2024 16:41:10,072	An account was successfully logged on.	2-Interactive	erik
07.06.2024 16:41:10,087	An account was logged off.	2-Interactive	erik
07.06.2024 16:41:10,087	An account was logged off.	2-Interactive	erik
07.06.2024 16:41:10,087	An account was logged off.	2-Interactive	erik
07.06.2024 16:41:10,087	An account was logged off.	2-Interactive	erik

Abbildung 5.7.4.4 - Anmeldeereignisse mit dem Benutzerkonto *erik* am 07.06.2024

Datum/Zeit der...	Ereignisbeschreibung – Zusammenfassung	Anmeldungstyp	Benut...
08.06.2024 11:37:02,778	A logon was attempted using explicit credentials.		erik
08.06.2024 11:37:02,778	An account was successfully logged on.	2-Interactive	erik
08.06.2024 11:37:02,778	An account was successfully logged on.	2-Interactive	erik
08.06.2024 11:37:02,778	A logon was attempted using explicit credentials.		erik
08.06.2024 11:37:02,778	An account was successfully logged on.	2-Interactive	erik
08.06.2024 11:37:02,778	An account was successfully logged on.	2-Interactive	erik
08.06.2024 11:37:08,264	A logon was attempted using explicit credentials.		erik
08.06.2024 11:37:08,264	An account was successfully logged on.	2-Interactive	erik
08.06.2024 11:37:08,264	An account was successfully logged on.	2-Interactive	erik
08.06.2024 11:37:08,264	A logon was attempted using explicit credentials.		erik
08.06.2024 11:37:08,264	An account was successfully logged on.	2-Interactive	erik
08.06.2024 11:37:08,264	An account was successfully logged on.	2-Interactive	erik
08.06.2024 11:37:08,271	An account was logged off.	2-Interactive	erik
08.06.2024 11:37:08,271	An account was logged off.	2-Interactive	erik
08.06.2024 11:37:08,271	An account was logged off.	2-Interactive	erik
08.06.2024 11:37:08,271	An account was logged off.	2-Interactive	erik
08.06.2024 14:09:35,752	A logon was attempted using explicit credentials.		erik
08.06.2024 14:09:35,752	An account was successfully logged on.	2-Interactive	erik
08.06.2024 14:09:35,752	An account was successfully logged on.	2-Interactive	erik
08.06.2024 14:09:35,752	A logon was attempted using explicit credentials.		erik
08.06.2024 14:09:35,752	An account was successfully logged on.	2-Interactive	erik
08.06.2024 14:09:35,752	An account was successfully logged on.	2-Interactive	erik
08.06.2024 14:09:40,863	A logon was attempted using explicit credentials.		erik
08.06.2024 14:09:40,863	An account was successfully logged on.	2-Interactive	erik
08.06.2024 14:09:40,863	An account was successfully logged on.	2-Interactive	erik
08.06.2024 14:09:40,863	A logon was attempted using explicit credentials.		erik
08.06.2024 14:09:40,863	An account was successfully logged on.	2-Interactive	erik
08.06.2024 14:09:40,863	An account was successfully logged on.	2-Interactive	erik
08.06.2024 14:09:40,869	An account was logged off.	2-Interactive	erik
08.06.2024 14:09:40,869	An account was logged off.	2-Interactive	erik
08.06.2024 14:09:40,869	An account was logged off.	2-Interactive	erik
08.06.2024 14:09:40,869	An account was logged off.	2-Interactive	erik

Abbildung 5.7.4.5 - Anmeldeereignisse mit dem Benutzerkonto *erik* am 08.06.2024

Die Abbildungen 5.7.4.1 - 5.7.4.5 zeigen sämtliche Anmeldeereignisse des Benutzerkontos *erik* zur späteren Referenz. Alle anderen gefundenen Anmeldeereignisse stellen Anmeldungen der Maschinenkonten von Windows 10 dar. Solche Benutzerkonten werden ausschließlich durch das Betriebssystem genutzt und sind aus diesem Grund nicht relevant für diese Untersuchung. Es finden sich keine Hinweise auf eine Nutzung des Gast- oder Administratorkontos.

5.7.5 E-Mails

Der Desktop-Rechner beinhaltet eine Installation der E-Mail-Anwendung *Mozilla Thunderbird* (Abs. 5.7.3). *Mozilla Thunderbird* speichert Entwürfe, gesendete und empfangene E-Mails im *mbox*-Format lokal ab. *AXIOM* unterstützt die automatische Erkennung und Extraktion von E-Mails im *mbox*-Format. Abb. 5.7.5.1 zeigt die so gefundenen E-Mails im Zeitraum vor dem Verschwinden des Beschuldigten.

An	Von	Datum/Zeit	Thema
<erikalex.mueller@hotmail.com>	"OneDrive" <OneDrive@infomails.microsoft.com>	10.05.2024 04:05:03,000	Vergessen Sie nicht, Ihre Geräte zu sich ern
erikalex.mueller@hotmail.com	irma.mueller@gmx-topmail.de	02.06.2024 18:03:04,000	Melde Dich mal wieder - Deine Mutter
erikalex.mueller@hotmail.com	irma.mueller@gmx-topmail.de	02.06.2024 18:03:04,000	Melde Dich mal wieder - Deine Mutter
erikalex.mueller@hotmail.com	Microsoft-Konto-Team <account-security-noreply@a...	02.06.2024 18:12:42,000	Neue Apps wurden mit Ihrem Microsoft-Konto verb...
erikalex.mueller@hotmail.com	Microsoft-Konto-Team <account-security-noreply@a...	02.06.2024 18:12:42,000	Neue Apps wurden mit Ihrem Microsoft-Konto verb...
irma.mueller@gmx-topmail.de	Erik Müller <erikalex.mueller@hotmail.com>	02.06.2024 18:15:13,000	Re: Melde Dich mal wieder - Deine Mutter
irma.mueller@gmx-topmail.de	Erik Müller <erikalex.mueller@hotmail.com>	02.06.2024 18:15:13,000	Re: Melde Dich mal wieder - Deine Mutter
irma.mueller@gmx-topmail.de	Erik Müller <erikalex.mueller@hotmail.com>	02.06.2024 18:15:13,000	Re: Melde Dich mal wieder - Deine Mutter
irma.mueller@gmx-topmail.de	Erik Müller <erikalex.mueller@hotmail.com>	02.06.2024 18:15:13,000	Re: Melde Dich mal wieder - Deine Mutter
irma.mueller@gmx-topmail.de	Erik Müller <erikalex.mueller@hotmail.com>	02.06.2024 18:15:13,000	Re: Melde Dich mal wieder - Deine Mutter
irma.mueller@gmx-topmail.de	Erik Müller <erikalex.mueller@hotmail.com>	02.06.2024 18:15:13,000	Re: Melde Dich mal wieder - Deine Mutter
abenteuerlust@sags-per-mail.de	Erik Müller <erikalex.mueller@hotmail.com>	02.06.2024 18:20:36,000	Reiseanfrage
abenteuerlust@sags-per-mail.de	Erik Müller <erikalex.mueller@hotmail.com>	02.06.2024 18:20:36,000	Reiseanfrage
abenteuerlust@sags-per-mail.de	Erik Müller <erikalex.mueller@hotmail.com>	02.06.2024 18:20:36,000	Reiseanfrage
abenteuerlust@sags-per-mail.de	Erik Müller <erikalex.mueller@hotmail.com>	02.06.2024 18:20:36,000	Reiseanfrage
abenteuerlust@sags-per-mail.de	Erik Müller <erikalex.mueller@hotmail.com>	02.06.2024 18:20:52,000	Reiseanfrage
abenteuerlust@sags-per-mail.de	Erik Müller <erikalex.mueller@hotmail.com>	02.06.2024 18:20:52,000	Reiseanfrage
abenteuerlust@sags-per-mail.de	Erik Müller <erikalex.mueller@hotmail.com>	02.06.2024 18:20:52,000	Reiseanfrage
abenteuerlust@sags-per-mail.de	Erik Müller <erikalex.mueller@hotmail.com>	02.06.2024 18:20:52,000	Reiseanfrage
abenteuerlust@sags-per-mail.de	Erik Müller <erikalex.mueller@hotmail.com>	02.06.2024 18:20:52,000	Reiseanfrage
abenteuerlust@sags-per-mail.de	Erik Müller <erikalex.mueller@hotmail.com>	02.06.2024 18:20:52,000	Reiseanfrage
Erik Müller <erikalex.mueller@hotmail.com>	Abenteuerlust@sags-per-mail.de	03.06.2024 20:36:17,000	Aw: Reiseanfrage
Erik Müller <erikalex.mueller@hotmail.com>	Abenteuerlust@sags-per-mail.de	03.06.2024 20:36:17,000	Aw: Reiseanfrage
vladimir.forenski@hotmail.com	Erik Müller <erikalex.mueller@hotmail.com>	04.06.2024 16:49:51,000	Gott der Meere
vladimir.forenski@hotmail.com	Erik Müller <erikalex.mueller@hotmail.com>	04.06.2024 16:49:51,000	Gott der Meere
vladimir.forenski@hotmail.com	Erik Müller <erikalex.mueller@hotmail.com>	04.06.2024 16:49:51,000	Gott der Meere
vladimir.forenski@hotmail.com	Erik Müller <erikalex.mueller@hotmail.com>	04.06.2024 16:49:51,000	Gott der Meere
Erik Müller <erikalex.mueller@hotmail.com>	Vladimir Forenski <vladimir.forenski@hotmail.com>	04.06.2024 16:52:26,000	AW: Gott der Meere
Erik Müller <erikalex.mueller@hotmail.com>	Vladimir Forenski <vladimir.forenski@hotmail.com>	04.06.2024 16:52:26,000	AW: Gott der Meere
Vladimir Forenski <vladimir.forenski@hotmail.com>	Erik Müller <erikalex.mueller@hotmail.com>	06.06.2024 17:06:24,000	Re: Gott der Meere
Vladimir Forenski <vladimir.forenski@hotmail.com>	Erik Müller <erikalex.mueller@hotmail.com>	06.06.2024 17:06:24,000	Re: Gott der Meere
Vladimir Forenski <vladimir.forenski@hotmail.com>	Erik Müller <erikalex.mueller@hotmail.com>	06.06.2024 17:06:24,000	Re: Gott der Meere
Vladimir Forenski <vladimir.forenski@hotmail.com>	Erik Müller <erikalex.mueller@hotmail.com>	06.06.2024 17:06:24,000	Re: Gott der Meere
Vladimir Forenski <vladimir.forenski@hotmail.com>	Erik Müller <erikalex.mueller@hotmail.com>	07.06.2024 17:04:34,000	Gott der Meere hat ein Problem
Vladimir Forenski <vladimir.forenski@hotmail.com>	Erik Müller <erikalex.mueller@hotmail.com>	07.06.2024 17:04:34,000	Gott der Meere hat ein Problem
Vladimir Forenski <vladimir.forenski@hotmail.com>	Erik Müller <erikalex.mueller@hotmail.com>	07.06.2024 17:04:34,000	Gott der Meere hat ein Problem
Vladimir Forenski <vladimir.forenski@hotmail.com>	Erik Müller <erikalex.mueller@hotmail.com>	07.06.2024 17:04:34,000	Gott der Meere hat ein Problem
Vladimir Forenski <vladimir.forenski@hotmail.com>	Erik Müller <erikalex.mueller@hotmail.com>	07.06.2024 17:04:34,000	Gott der Meere hat ein Problem
Vladimir Forenski <vladimir.forenski@hotmail.com>	Erik Müller <erikalex.mueller@hotmail.com>	07.06.2024 17:04:34,000	Gott der Meere hat ein Problem
Erik Müller <erikalex.mueller@hotmail.com>	Vladimir Forenski <vladimir.forenski@hotmail.com>	08.06.2024 13:11:40,000	AW: Gott der Meere hat ein Problem
Erik Müller <erikalex.mueller@hotmail.com>	Vladimir Forenski <vladimir.forenski@hotmail.com>	08.06.2024 13:11:40,000	AW: Gott der Meere hat ein Problem
irma.mueller@gmx-topmail.de	Erik Müller <erikalex.mueller@hotmail.com>	08.06.2024 14:20:10,000	Dienstreise
irma.mueller@gmx-topmail.de	Erik Müller <erikalex.mueller@hotmail.com>	08.06.2024 14:20:10,000	Dienstreise

Abbildung 5.7.5.1 - Gefundene E-Mails mithilfe von Magnet AXIOM

In Tabelle 5.7.5.1 wird die relevante E-Mail-Kommunikation chronologisch ausgewertet.

Datum	Uhrzeit (UTC)	Absender	Empfänger	Zusammenfassung	Referenz
02.06.2024	18:20:36	Erik Müller	Reisebüro	E. Müller bedankt sich für eine vergangene Reise nach Krakowia. Er fragt eine weitere Reise für zwei Personen und 10 Tage Ende Juni auf die Malediven an. Er möchte die Hin- oder Rückreise über Krakowia vornehmen.	E-Mails
03.06.2024	20:36:17	Reisebüro	Erik Müller	Das Reisebüro informiert E. Müller über notwendige Zwischenstopps in Wien und Dubai oder Zürich.	E-Mails
04.06.2024	16:49:51	Erik Müller	Vladimir Forenski	E. Müller informiert V. Forenski über seine Beschäftigung im Projekt Neptuns Schild und bietet an, sich bei V. Forenski zu revanchieren.	E-Mails
04.06.2024	16:52:26	Vladimir Forenski	Erik Müller	V. Forenski fragt nach E. Müllers Zugriffsmöglichkeit auf einen Rechner. V. Forenski terminiert ein Treffen mit E. Müller in der Nähe der Botschaft von Krakowia auf 18 Uhr MESZ.	E-Mails
06.06.2024	17:06:25	Erik Müller	Vladimir Forenski	E. Müller informiert V. Forenski darüber, dass Forenskis USB-Stick nicht funktioniert hat. Er kündigt an, andere Möglichkeiten zu suchen, um Informationen in Verbindung mit dem Projekt zu erlangen.	E-Mails
07.06.2024	17:04:34	Erik Müller	Vladimir Forenski	E. Müller teilt V. Forenski mit, dass er befürchtet, von seinem Vorgesetzten gesehen worden zu sein, beim Zugriff auf Rechner anderer Projektbeteiligter.	E-Mails
08.06.2024	13:11:40	Vladimir Forenski	Erik Müller	V. Forenski ruft E. Müller auf, nach Krakowia zu reisen mit Zwischenstopp in Wien und dort eine Kontaktperson zu treffen.	E-Mails
08.06.2024	14:20:10	Erik Müller	Irma Müller	E. Müller kündigt eine Dienstreise bei seiner Mutter an.	E-Mails

Tabelle 5.7.5.1 - Chronologie relevanter E-Mails mit aggregierten Inhalten

5.7.6 Weitere Dateien

Die Auswertung der Dateien und Verzeichnisse, auf die lokal zugegriffen wurde in Abb. 5.7.6.1 liefert eine relevante Datei mit der Bezeichnung *Neptun_Dokument.pptx*. Die Datei ist im OneDrive-Verzeichnis des Benutzerkontos des Beschuldigten abgelegt.

Pfad	Pfad...	Datum/Zeit des...	Datum/Zeit...	Ben...
:Host: Dieser PC	Virtual		2024-06-08 16:15:24	erik
:Host: Dieser PC	Virtual		2024-06-07 18:41:14	erik
C:\Users\erik\OneDrive\Neptun_Dokument.pptx	Drive		2024-06-07 18:42:26	erik
C:\Users\erik\OneDrive\Neptun_Dokument.pptx	Drive	07.06.2024 16:42:26,443		erik
:Host: Dieser PC	Virtual		2024-06-02 20:11:01	erik
:Host: Dieser PC	Virtual		2024-06-04 18:41:24	erik
:Host: Dieser PC	Virtual		2024-06-07 18:41:14	erik
C:\Users\erik\OneDrive\Neptun_Dokument.pptx	Drive		2024-06-07 18:42:26	erik
:Host: Dieser PC	Virtual		2024-06-08 16:15:24	erik
C:\Users\erik\OneDrive\Neptun_Dokument.pptx	Drive	07.06.2024 16:42:26,443		erik
C:\Users\erik\OneDrive\Einkaufsliste.docx	Drive	05.05.2024 16:48:36,849		erik
:Host: Dieser PC	Virtual		2024-06-08 16:15:24	erik
:Host: Dieser PC	Virtual		2024-06-07 18:41:14	erik
C:\Users\erik\OneDrive\Neptun_Dokument.pptx	Drive		2024-06-07 18:42:26	erik
C:\Users\erik\OneDrive\Neptun_Dokument.pptx	Drive	07.06.2024 16:42:26,443		erik
:Host: Dieser PC	Virtual		2024-06-02 20:11:01	erik
:Host: Dieser PC	Virtual		2024-06-04 18:41:24	erik
:Host: Dieser PC	Virtual		2024-06-07 18:41:14	erik
C:\Users\erik\OneDrive\Neptun_Dokument.pptx	Drive		2024-06-07 18:42:26	erik
:Host: Dieser PC	Virtual		2024-06-08 16:15:24	erik
C:\Users\erik\OneDrive\Neptun_Dokument.pptx	Drive	07.06.2024 16:42:26,443		erik
C:\Users\erik\OneDrive\Einkaufsliste.docx	Drive	05.05.2024 16:48:36,849		erik

Abbildung 5.7.6.1 - Dateien und Verzeichnisse, auf die lokal zugegriffen wurde

Dateiname	**Neptun_Dokument.pptx**
Dateierweiterung	**.pptx**
Logische Größe	**2.879.060 bytes**
Erstellt	**07.06.2024 16:41:32,364**
Aufgerufen	**07.06.2024 16:41:32,364**
Modifiziert	**07.06.2024 16:16:42,000**
MFT geändert	**08.06.2024 11:37:39,943**
Cluster	**3511107**
Cluster-Zähler	**703**
Physikalischer Speicherort	**14381494272**
Physikalischer Sektor	**28088856**
MD5-Hash	**e1ac0178c01003e2fedb5545873de2d5**
MFT-Datensatznummer	**118106**
Übergeordnete MFT-Aufzeichnungsnummer	**111957**
Sicherheits-ID	**1869 (S-1-5-21-1748443609-3498283432-1879274306-1001)**
Dateiattribute	**Archive, ReparsePoint**

BEWEISINFORMATIONEN

Quelle	**Aservat 002 - Festplatte Desktoprechner.E01 - Partition 2 (Microsoft NTFS, 39,4 GB)\Users\erik \OneDrive\Neptun_Dokument.pptx**
Beweisnummer	**Aservat 002 - Festplatte Desktoprechner.E01**

Abbildung 5.7.6.2 - Metadaten der Präsentation

Die Datei ist am 07.06.2024 16:41:32 UTC im Dateisystem des Desktop-Rechners erstellt worden und am 07.06.2024 16:16:42 UTC zuletzt geändert worden. Da der Zeitpunkt der letzten Änderung vor dem Zeitpunkt der Erstellung liegt, ist davon auszugehen, dass die Präsentation an einem anderen Ort erstellt worden ist und durch Synchronisierung des lokalen OneDrive-Verzeichnisses mit dem Cloud-Speicher im Dateisystem des Desktop-Rechners erzeugt worden ist.

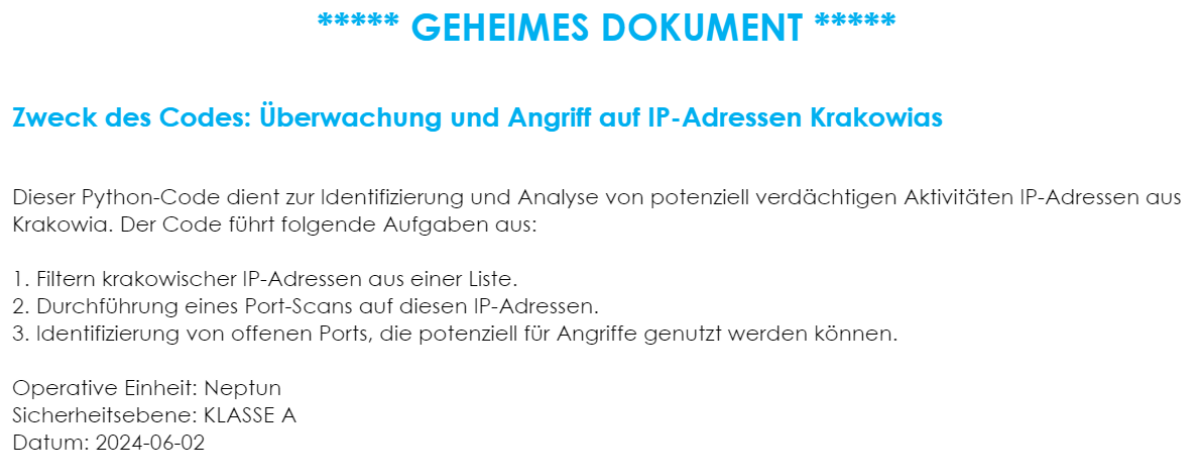


Abbildung 5.7.6.3 - Inhalt der Präsentation

Die Datei enthält die Dokumentation von Quellcode, der dazu genutzt werden kann, potenziell verdächtige IP-Adressen aus Krakowia zu identifizieren und zu analysieren.

Das OneDrive-Verzeichnis beinhaltet darüber hinaus ein Python-Skript mit der Bezeichnung *ScanKrakowianIP.py*. Es ist davon auszugehen, dass es sich um den Python-Code handelt, der in der Präsentation erklärt wird. Das Python-Skript ist am 07.06.2024 16:41:32 UTC im Dateisystem des Desktop-Rechners erstellt worden. Dies ist kongruent mit der Erstellung der Präsentation und mit einer erfolgreichen Anmeldung des Benutzerkontos des Beschuldigten um 16:41:10 UTC (Abb. 5.7.6.4). Der Zeitpunkt der letzten Änderung am 07.06.2024 08:18:08 UTC deutet ebenfalls darauf hin, dass die Datei an einem anderen Ort erstellt wurde und durch Synchronisierung im Dateisystem des Desktop-Rechners erzeugt worden ist.
Der Inhalt des Python-Skripts besteht ausschließlich aus Null-Bits und trägt somit keinerlei Informationen. Es ist deshalb davon auszugehen, dass ein Extraktionsversuch des Python-Skripts mit Hilfe von OneDrive fehlgeschlagen ist.

DATEIDETAILS

Dateiname	**ScanKrakowianIP.py**
Dateierweiterung	**.py**
Logische Größe	**1.865 bytes**
Erstellt	**07.06.2024 16:41:32,336**
Aufgerufen	**07.06.2024 16:41:32,336**
Modifiziert	**07.06.2024 08:18:08,000**
MFT geändert	**07.06.2024 16:41:32,336**
MD5-Hash	**c341dbdc4e8636fd49a5c2e2e75d91ec**
MFT-Datensatznummer	**118078**
Übergeordnete MFT-Aufzeichnungsnummer	**111957**
Sicherheits-ID	**1869 (S-1-5-21-1748443609-3498283432-1879274306-1001)**
Dateiattribute	**Archive, SparseFile, ReparsePoint, Offline**

BEWEISINFORMATIONEN

Quelle	**Aservat 002 - Festplatte Desktoprechner.E01 - Partition 2 (Microsoft NTFS, 39,4 GB)\Users\erik \OneDrive\ScanKrakowianIP.py**
Beweisnummer	**Aservat 002 - Festplatte Desktoprechner.E01**

Abbildung 5.7.6.4 - Metadaten des Python-Skripts

Die restlichen Verzeichnisse des Benutzerkontos des Beschuldigten (Dokumente, Desktop, Eigene Bilder, etc.) sind leer und in den Sprunglisten finden sich keine Hinweise auf gelöschte relevante Informationen.

5.7.7 Browser-Verlauf

Im Rahmen des Gutachtens werden unter webbezogene Artefakte Browser-Verlaufseinträge, Cache-Inhalte und verwandte Objekte betrachtet. Die Untersuchung der Festplatte mit *AXIOM* ergab mehrere Zehntausende solcher Artefakte. Da sich keine Hinweise ergeben haben, die eine vollumfängliche technische Analyse sämtlicher web bezogenen Artefakte erforderlich machten, werden stattdessen eine zielgerichtete Schlagwortsuche mit Hilfe der in Abs. 5.5 aufgeführten Liste durchgeführt. Durch das gewählte Vorgehen kann der erforderliche Umfang und Aufwand der Analyse erheblich verringert werden.
Der Einsatz der Schlagwortliste verringert die gefundenen webbezogenen Artefakte auf 2932. Eine genauere Betrachtung ergibt, dass das Schlagwort *erik* zu 2384 Treffern führt. Das ist

darin begründet, dass Artefakte, die den Dateisystempfad *C:\Users\erik** beinhaltet, zu Treffern bei der Schlagwortsuche führen. Hierbei handelte es sich hauptsächlich um generische Grafiken niedriger Auflösung im *JPEG*-Format, die von der Suchmaschine Microsoft Bing lokal gespeichert werden. Da diese Grafiken keine Relevanz für die Erörterung des Sachverhalts bergen, wird das Schlagwort *erik* für die Untersuchung der web-basierten Artefakte entfernt. Die Verkleinerung der Schlagwortliste resultiert in 560 gefundene webbezogene Artefakte. Diese Resultate stellen teilweise Duplikate dar, da *AXIOM* dieselben Informationen unterschiedlichen Artefakten zuordnet. Das bedeutet, dass beispielsweise dieselbe Browseraktivität Artefakte der Kategorien *Edge Chromium Chache-Einträge*, *Aktuell Sitzung in Edge Chromium, Edge Chromium Webverlauf* und *Edge Chromium Webbesuche* erzeugen kann. Aufgrund dieser erhöhten Komplexität wird im Folgenden auf die kategorieweise Betrachtung der Artefakte verzichtet. Stattdessen werden die Artefakte aggregiert, korreliert und chronologisch in Tab. 5.7.7.1 dargestellt.

Datum	Zeit (UTC)	Ereignis
04.06.2024	16:53:22	Besuch des Reisevergleichportals holidaycheck.de und Betrachtung eines Resorts auf dem Nord-Malé-Atoll Meeru Malediven. Betrachtung der Bewertungen und Bilder.
04.06.2024	16:53:49	Besuch der Facebook Seite des Resorts.
08.06.2024	14:11:54	Besuch des Reiseportals der Deutschen Bahn und Suche nach Verbindungen von Hannover nach Wien am 08.06.2024
08.06.2024	14:13:14	Besuch des Reiseportals von Flixbus und Suche nach Verbindungen von Berlin nach Wien am 08.06.2024.
08.06.2024	14:13:25	Besuch des Reiseportals von Flixbus und Suche nach Verbindungen von Hannover nach Wien am 08.06.2024
08.06.2024	14:21:49	Besuch von Google Maps und Suche nach Erdberg, Wien
08.06.2024	14:22:04	Google Maps Suche nach Route von Erdberg, Wien nach Hauptbahnhof, Wien
08.06.2024	14:22:03	Google Suche nach Wien Hauptbahnhof

Tabelle 5.7.7.1 - Aggregierter Browserverlauf

Zusätzlich findet Sich ein Artefakt, das auf eine Suchanfrage mit Microsoft Bing nach dem Suchbegriff Dubai hindeutet. Allerdings lässt sich kein Zeitstempel rekonstruieren.
Abschließend finden sich keine Hinweise auf einen tatsächlichen Fahrkartenkauf des Beschuldigten.

6. Zusammenfassung und Ausblick

In diesem Kapitel bewerten die Autoren zunächst die Ergebnisse des Projektpraktikums. Es werden Besonderheiten herausgearbeitet, die sich durch die Simulation des forensisch relevanten Szenarios ergeben. Danach zeigen die methodischen und technischen Erkenntnisse neu erlangte Fähigkeiten auf. Abschließend folgt ein Ausblick von Aspekten, die weiterführend betrachtet werden könnten.

6.1 Bewertung des Ergebnisses

Die Ergebnisse der forensischen Untersuchung liefern wichtige Hinweise auf den möglichen Abfluss vertraulicher Informationen und die Aktivitäten des Beschuldigten. Jedoch gibt es Aspekte, die wir in diesem Szenario nicht mehr betrachten konnten, die weitere interessante forensische Informationen liefern können.
Ein wesentlicher Punkt ist die Vollständigkeit der Datenerfassung. Die Untersuchung konzentrierte sich auf bestimmte Datenträger, die Festplatte des Desktop-Rechners und die MicroSD-Karte des USB-Sticks. Es bleibt jedoch unklar, ob alle potenziell relevanten Datenquellen tatsächlich erfasst und analysiert wurden. Die Untersuchung der Cloud-Umgebung von Erik Müller ist im Rahmen des Szenarios nicht mehr umgesetzt worden. Hier würde eine erweiterte Untersuchung, für die ein zusätzlicher richterlicher Durchsuchungsbeschluss notwendig wäre, möglicherweise auch zusätzliche Ergebnisse bringen. Eine umfassendere Datenerhebung, die alle möglichen Datenquellen einbezieht, könnte daher zu einer vollständigeren und präziseren Analyse führen.
Ein weiterer Punkt ist die mögliche Beeinflussung der Untersuchungsergebnisse durch die vorausgehenden Vorbereitungsmaßnahmen. Da das Szenario fiktiv erstellt wurde, ist es nicht mit realen Fällen vergleichbar und sichtbar ein Übungsbeispiel. Ein konkretes Beispiel solcher Vorbereitungsmaßnahmen ist etwa die Bereitstellung des Täter-Rechners mithilfe von Virtualisierung.
Allerdings war es auch mit unserem fiktiven Beispiel möglich, einen pSAP-Prozess beispielhaft durchzuführen und dabei die für eine forensische Analyse notwendigen Prozesse und eine gezielte Auswahl von Werkzeugen praktisch anzuwenden.
Darüber hinaus ist die Interpretation der Untersuchungsergebnisse stark von den eingesetzten Analysewerkzeugen und deren Funktionsweise abhängig. Während Werkzeuge wie *AXIOM* und *FTK Imager* detaillierte Analysen ermöglichen, ist zu bewerten, inwiefern alternative oder ergänzende Werkzeuge möglicherweise unterschiedliche oder weitere Ergebnisse liefern könnten.

6.2 Methodische und technische Erkenntnisse

Die Suche nach Artefakten ist erleichtert, dadurch, dass wir das forensisch relevante Szenario selbst erstellen. Solche selbst erzeugte Artefakte sind während der Untersuchung nachvollziehbar und können einfach hinsichtlich ihrer Plausibilität geprüft werden. Dadurch ist das Kennenlernen von komplexen Untersuchungswerkzeugen, wie etwa *Magnet AXIOM*, erleichtert.
HIDs wie der Bad-USB-Stick sind in Analysen schwer zu finden. Windows zeigt sie in der Systemsteuerung im Gerätemanager an, vergibt aber keine sprechenden Bezeichnungen. Rechner sind in den Standard-Konfigurationen nur teilweise entsprechend eingestellt, um bei unbekannten USB-Geräten zu warnen: Der Test-Windows-Rechner akzeptierte den Stick ohne Weiteres, bei einem Mac wurde lediglich im ersten Test ein Popup eingeblendet mit der Frage, ob man die neue Tastatur verwenden wolle. Hier war es im Gutachten hilfreich, eine gesonderte Teststellung aufzubauen, um die Besonderheiten des Systems, wie z.B. eigenständige Zeitreihen, für Leser nachvollziehbar aufbereiten zu können. Dies könnte Auswirkungen auf zukünftige strategische Vorbereitungen haben, in dem beispielsweise Wissen um Hard- und Software für das Auffinden und Analysieren solcher Bad-USB-Sticks und anderer HIDs aufgebaut wird.
Um die Gerichtsfestigkeit zu wahren, ist es unerlässlich, bei der Sicherung einen Schreibschutz zu nutzen. Durch hohe Anschaffungskosten und der allgemein niedrigen Verfügbarkeit von Hardware Write Blockern, haben wir uns für einen Software Write Blocker entschieden. Bei der Auswahl des Software Write Blockers SAFE Block von ForensicSoft war die vorangegangene Ausarbeitung aus [6] der HS-Wismar sehr hilfreich. SAFE Block hat im Test gute Ergebnisse erhalten und ist für 7 Tage kostenfrei verfügbar. Für unsere Sicherung hat dieser Zeitraum der kostenfreien Nutzung ausgereicht. Allerdings hat es bei der MicroSD-Karte nicht verhindert, dass wie bei anderen angeschlossenen Laufwerken durch Windows die *System-Volume-Informationen* angelegt werden (Abs. 5.6.3).
Bezüglich *AXIOM*, waren folgende Funktionen in unserem Fall sehr hilfreich.
Bei Artefakten mit Zeitstempeln ist neben der Uhrzeit ein Uhrsymbol, das genutzt werden kann, um den relevanten Zeitraum rund um dieses Artefakt einzugrenzen. So konnte der relevante Zeitraum für die Untersuchung anhand von Beginn und Ende der E-Mail-Kommunikation sowie der Internet-Recherchen von Erik Müller sinnvoll eingegrenzt und damit auch die Anzahl der relevanten Artefakte auf dem Rechner reduziert werden.
Bei der Sicherung und automatisierten Analyse der beiden Asservate sowie auch später während der manuellen Analyse können Schlüsselworte eingegeben werden, die zur Aggregierung und Reduktion der Artefakte eingesetzt werden können. Dies hat das Auffinden der relevanten Skripte auf dem USB-Stick mit dem Schlüsselwort *neptun* erheblich erleichtert.
Mit Tags können die relevanten Artefakte markiert und in den einzelnen Sichten herausgefiltert werden. E-Mails zum Beispiel werden in *AXIOM* mehrfach angezeigt, wenn neben Outlook ein weiteres E-Mail-Programm wie Thunderbird verwendet wird. Auch bei Websuchen können so die relevanten Webseiten markiert werden, damit fallen irrelevante Werbeseiten in späteren Ansichten heraus.
Die Kombination von *FTK Imager* für die Erstellung forensischer Abbilder und *AXIOM* für die Datenanalyse bietet eine umfassende Lösung für die Sicherung und Analyse digitaler Beweise. *FTK Imager* gewährleistet die Integrität der Beweismittel durch Prüfsummen, während *AXIOM* eine tiefgehende Analyse großer Datenmengen ermöglicht. Jedes Werkzeug hat seine Stärken, und die Kombination aus beiden macht die forensische Arbeit qualitativ hochwertig

Quellenverzeichnis

[1] Microsoft Azure Dev Tools for Teaching, Hochschule Wismar, Wismar, Germany, accessed: July 2024. [Online]. Available: https://www.hs-wismar.de/hochschule/einrichtungen/itsmz/it-info/software-und-lizenzen/microsoft-azure-dev-tools-for-teaching/

[2] Mega, MEGA, accessed: July 2024. [Online]. Available https://mega.io/de/

[3] Böses USB, Heise Medien GmbH & Co. KG, Hannover, Germany, accessed: July 2024. [Online]. Available: https://www.heise.de/select/ct/2023/27/2327713240730976058

[4] c't, Heise Medien GmbH & Co. KG, Hannover, Germany, accessed: July 2024. [Online]. Available: https://www.heise.de/select/ct/2023/27/softlinks/yhhf

[5] GitHub – RoganDawes, GitHub Inc, accessed: July 2024. [Online]. Available: https://github.com/RoganDawes/P4wnP1_aloa

[6] Write-blocking2022, C. Peter, Y. Schmitz, C. Bublies, IT-Forensik Wiki, Wismar, Germany, accessed: July 2024. [Online]. Available: https://it-forensik.fiw.hs-wismar.de/images/3/33/Write-blocking2022.pdf

[7] Getting started, Raspberry Pi, accessed: July 2024. [Online]. Available: https://www.raspberrypi.com/documentation/computers/getting-started.html#install-an-operating-system

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Beweismittel (BM)

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Virtuelle Maschine (VM)

Human Interface Device (HID)

Extended Filesystems (EXT)

Anhang A Ergänzende Inhalte

Skript Erik-Test.js

```
layout('de');            // US keyboard layout
typingSpeed(100,150)    // Wait 100ms between key strokes + an additional random value between 0ms and 150ms (natural)

waitLEDRepeat(NUM);        // Wait till NUM LED of target changes frequently multiple times (doesn't work on OSX)
press("GUI r");
delay(500);
type("notepad\n")
delay(1000);
for (var i = 0; i < 3; i++) {
 type("Hello from P4wnP1 run " + i + " !\n");
 type("Moving mouse right ...");
 moveStepped(500,0);
 type("and left\n");
 moveStepped(-500,0);
}
type("Let's type fast !!!!!!!!!!!!!!!\n")
typingSpeed(0,0);
for (var i = 3; i < 10; i++) {
 type("Hello from P4wnP1 run " + i + " !\n");
 type("Moving mouse right ...");
 moveStepped(500,0);
 type("and left\n");
 moveStepped(-500,0);
}
```

Skript NeptunCopyUserFolders.js

```

// sets typing speed as fast as possible
function fast() {
 typingSpeed(0,0)
}

// Open an interactive PowerShell console (host architecture)
function startPS() {
    press("GUI r");
    delay(500);
    type("powershell\n")
}

// Open an interactive Notepad (host architecture)
function startNotepad() {
    press("GUI r");
    delay(500);
    type("notepad\n")
}

```

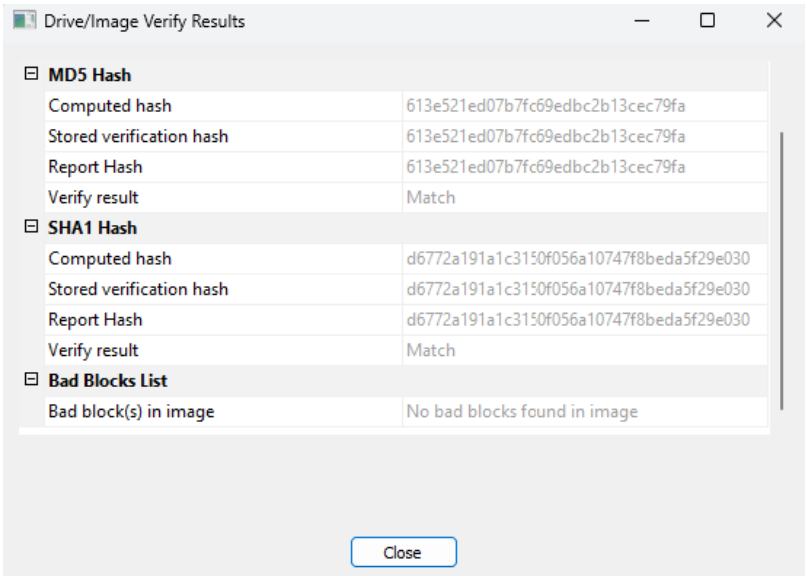
```
function copyUserFolders(){
 startNotepad();
 delay(500);
 press("STRG N");
 delay(500);
 type ("$FoldersToCopy = @(\n")
 type ("   'Desktop'\n")
 type ("      'Downloads'\n")
 type ("      'Favorites'\n")
 type ("    'Documents'\n")
 type ("    'Pictures'\n")
 type ("    'Videos'\n")
 type ("      )\n\n")

 type ("$FlashDrive = Get-CimInstance -ClassName Win32_LogicalDisk -Filter 'DriveType = 2' | \n")
 type ("  Out-GridView -OutputMode Single -Title 'Select destination drive...' \n")
 type ("\n\n")


 type ("if( -not $FlashDrive ){ Write-Warning 'No drive selected.' exit}\n\n")

 type ("foreach( $Folder in $FoldersToCopy ){\n")
 type ("  $Source      = Join-Path -Path $env:USERPROFILE -ChildPath $Folder\n")
 type ("  $Destination = Join-Path -Path $DestinationRoot -ChildPath $Folder\n")
 type ("  if( -not ( Test-Path -Path $Source -PathType Container ) ){\n")
 type ("Write-Warning 'Could not find path '$Source'' \n")
 type ("      continue\n")
 type ("}\n\n\n")
 type ("    if( -not ( Test-Path -Path $Destination -PathType Container ) ){\n")
 type ("      $null = New-Item -ItemType Directory -Path $Destination\n")
 type ("      }\n\n")
 type ("  Robocopy.exe $Source $Destination /E /IS /NP /NFL\n")
 type ("  }")
 delay(500);
 press ("CTRL SHIFT S");
 delay (500)
 type ("kopier1"); press("ENTER");
   }


layout('de');            // DE keyboard layout
fast();

startPS();
delay(500);
copyUserFolders();
```

Skript EriksSearch.js

```
ps_wow64="%SystemRoot%\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe"
ps="powershell.exe"

// sets typing speed to "natural" (global effect on all running script jobs)
function natural() {
 typingSpeed(100,150)    // Wait 100ms between key strokes + an additional random value between 0ms and 150ms (natural)
}

// sets typing speed as fast as possible
function fast() {
 typingSpeed(0,0)
}

// Open an interactive PowerShell console (host architecture)
function startPS() {
    press("GUI r");
    delay(500);
    type("powershell\n")
}


// On a powershell prompt, check if the running PS is 32bit, start an inline 32bit PowerShell, otherwise.
function assurePS32() {
 type("if ([IntPtr]::Size -ne 4){& $env:SystemRoot\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe}\n");
 delay(500);
}

```

```
21
22  // On a powershell prompt, check if the running PS is 32bit, start an inline 32bit PowerShell, otherwise.
23  function assurePS32() {
24   type("if ([IntPtr]::Size -ne 4){& $env:SystemRoot\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe}\n");
25   delay(500);
26  }
27
28
29  function copyUserFolders(){
30   delay(500);
31   press("STRG N");
32   delay(500);
33
34   type ("Get-ChildItem -Path $env:USERPROFILE -Recurse -File | Where-Object { $_.Name -like '*Neptun*' } | ForEach-Object {Copy-Item
35  }
36
37
38  layout('de');            // DE keyboard layout
39  fast();
40
41  startPS();
42  delay(500);
43  assurePS32();
44  delay(500);
45  copyUserFolders();
```

FTK-Imager-Sicherung der Test-Installation



D

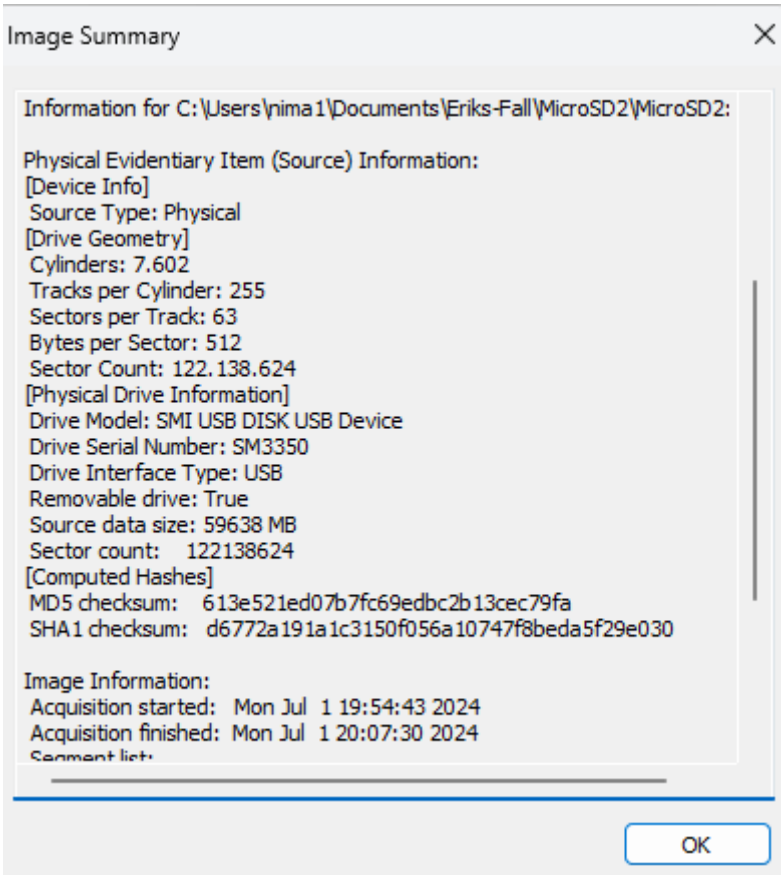


Image Summary
Information for C:\Users\nima1\Documents\Eriks-Fall\MicroSD2\MicroSD2:
Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 7.602
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 122.138.624
[Physical Drive Information]
Drive Model: SMI USB DISK USB Device
Drive Serial Number: SM3350
Drive Interface Type: USB
Removable drive: True
Source data size: 59638 MB
Sector count: 122138624
[Computed Hashes]
MD5 checksum: 613e521ed07b7fc69edbc2b13cec79fa
SHA1 checksum: d6772a191a1c3150f056a10747f8beda5f29e030
Image Information:
Acquisition started: Mon Jul 1 19:54:43 2024
Acquisition finished: Mon Jul 1 20:07:30 2024
OK

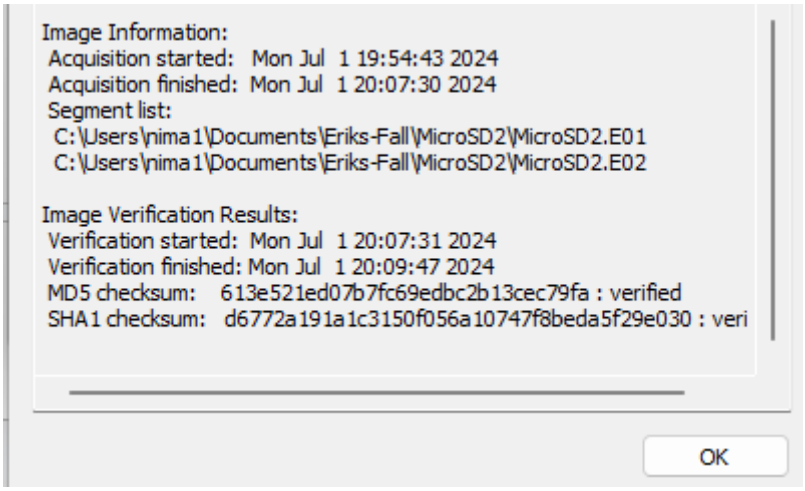
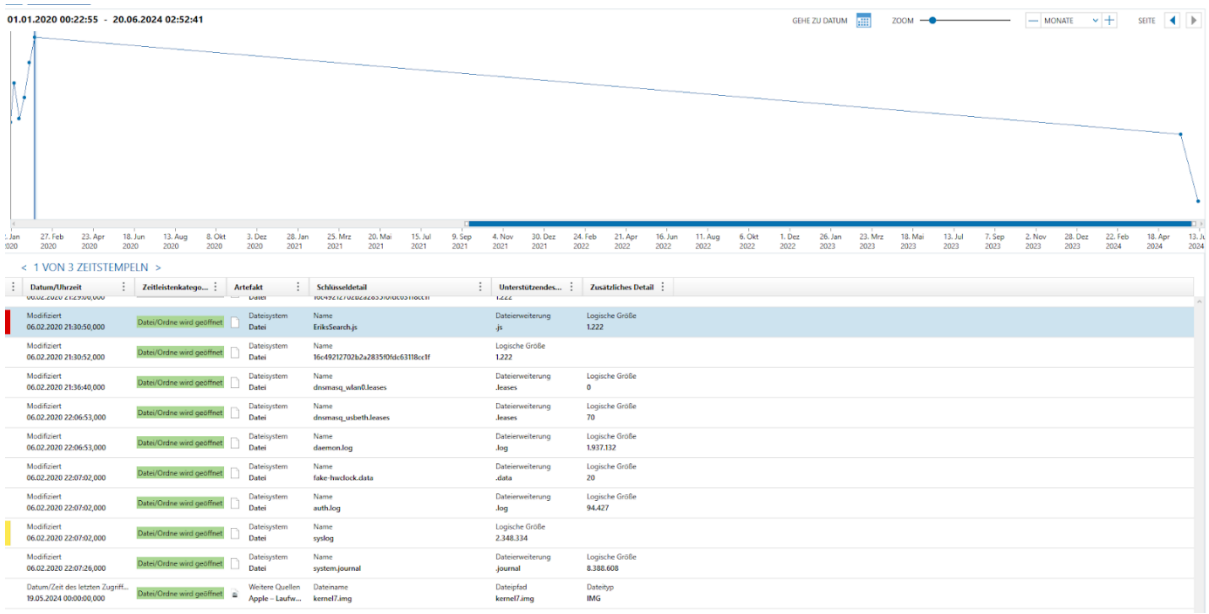


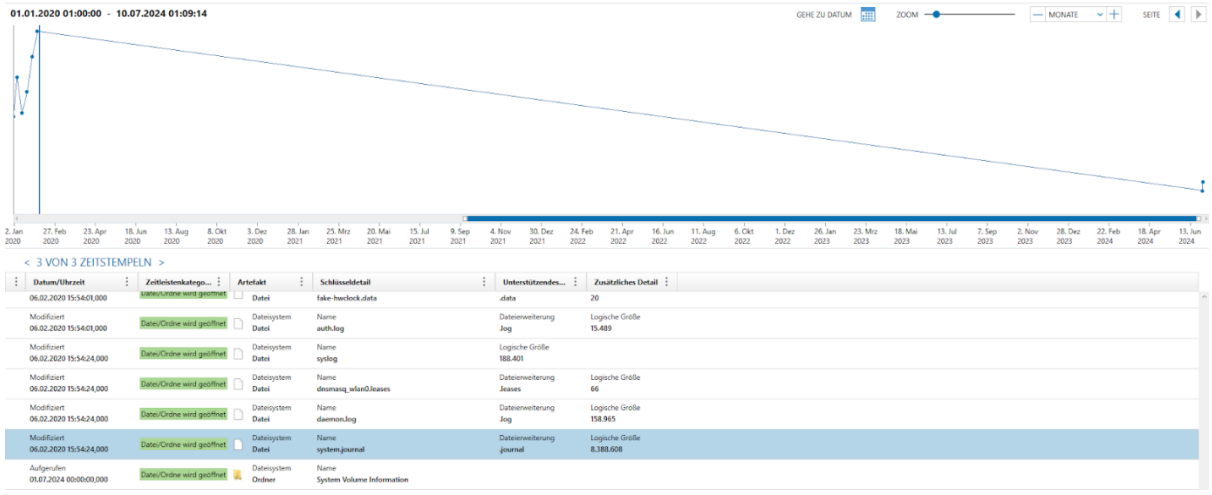
Image Information:
Acquisition started: Mon Jul 1 19:54:43 2024
Acquisition finished: Mon Jul 1 20:07:30 2024
Segment list:
C:\Users\nima1\Documents\Eriks-Fall\MicroSD2\MicroSD2.E01
C:\Users\nima1\Documents\Eriks-Fall\MicroSD2\MicroSD2.E02
Image Verification Results:
Verification started: Mon Jul 1 20:07:31 2024
Verification finished: Mon Jul 1 20:09:47 2024
MD5 checksum: 613e521ed07b7fc69edbc2b13cec79fa : verified
SHA1 checksum: d6772a191a1c3150f056a10747f8beda5f29e030 : veri
OK

Zeitreihenvergleich der Micro-SD-Karten

SD-Karte der Original-Analyse:



SD-Karte der Test-Analyse:



E-M ails

Von: Erik Müller <erikalex.mueller@hotmail.com>
Gesendet: 02.06.2024 18:20:36,000
An: abenteuerlust@sags-per-mail.de
Betreff: Reiseanfrage

Hallo Frau Hansen,

die Buchung nach Krakowia hat echt gut funktioniert. Können Sie noch etwas für mich recherchieren? Ich würde gern zu zweit auf die Malediven, evtl. ab Ende Juni und dann für ca. 10 Tage. Wäre schön, wenn wir hin oder zurück auch über Krakowia kommen könnten. Meine Großmutter würde sich sehr freuen.

Können Sie mir ein schönes Hotel empfehlen? Und mit was für Preisen kann ich da kalkulieren?

Danke schonmal

Viele Grüße

Erik Müller

Reiseanfrage

Von: Abenteuerlust@sags-per-mail.de
Gesendet: 03.06.2024 20:36:17,000
An: Erik Müller <erikalex.mueller@hotmail.com>
Betreff: Aw: Reiseanfrage

Hallo Herr Müller,

das freut mich, dass Ihnen unsere letzte Buchung gut gefallen hat. Für ein Hotel auf den Malediven hätte ich hier zwei Angebote für Sie zum Anschauen.
Einmal ein eher ruhiges Plätzchen: https://www.holidaycheck.de/hi/meeru-maldives-island-resort/96e41496-5654-396a-a00e-5758c2635051

und einmal etwas für Aktivurlauber: https://www.holidaycheck.de/hi/villa-park/89e544de-ed53-36bf-9ab2-71d20d47456e

Preislich fangen diese Angebote bei ca. 1500 EUR pro Person an für 10 Tage, allerdings noch ohne die Flüge. Es gibt keine Standard-Flugverbindungen mit Stop in Krakowia. Möchten Sie ein paar Tage Aufenthalt dort haben? Dann schaue ich mal, ob ich einen Hinflug finde (geht standardmäßig über Wien und Dubai) und für den Rückflug zwei Verbindungen heraussuche (Malediven-Dubai-Krakowia und Krakowia-Wien bzw. Krakowia-Zürich und dann zurück). Wäre das was für Sie? Wie lange möchten Sie in Krakowia bleiben?

Viele Grüße
Marita Hansen
Reisebüro Abenteuerlust

Antwort auf die Reiseanfrage

Von: Erik Müller <erikalex.mueller@hotmail.com>
Gesendet: 04.06.2024 16:49:51,000
An: vladimir.forenski@hotmail.com
Betreff: Gott der Meere

Hallo Vlad,

danke für Deine Hilfe letzten Monat. Ich bin in ein Projekt reingerutscht, dass für Euch von Interesse sein könnte. Jetzt kann ich mich revanchieren. Sagt Dir Neptuns Schild was?

Können wir uns treffen?

Viele Grüße

Erik

Kontaktaufnahme zu V. Forenski

Von: Vladimir Forenski <vladimir.forenski@hotmail.com>
Gesendet: 04.06.2024 16:52:26,000
An: Erik Müller <erikalex.mueller@hotmail.com>
Betreff: AW: Gott der Meere

Hallo Erik,

ja, Neptun sagt mir was. Hm. Du kommst an PCs ran, oder? Kannst Du uns mehr besorgen? Lass uns morgen treffen. In dem Café gegenüber der Botschaft von Krakowia. 18 Uhr.

Grüße

Vladimir

Antwort von V. Forenski

Von: Erik Müller <erikalex.mueller@hotmail.com>
Gesendet: 07.06.2024 17:04:34,000
An: Vladimir Forenski <vladimir.forenski@hotmail.com>
Betreff: Gott der Meere hat ein Problem

Hallo Vlad,

kannst Du mir helfen? Ich muss weg! Ich glaub, mein Chef hat gesehen, dass ich an den Rechnern der anderen Neptun-Entwickler dran war mit dem USB-Stick.

Gruß

Erik

Hilfeersuchen von E. Müller

Von: Erik Müller <erikalex.mueller@hotmail.com>
Gesendet: 06.06.2024 17:06:24,000
An: Vladimir Forenski <vladimir.forenski@hotmail.com>
Betreff: Re: Gott der Meere

Hallo Vlad,

Dein USB-Stick hat nicht funktioniert. Die PCs sind gesperrt für sowas. Ich muss schauen, ob ich anders an Neptuns Schild rankomme.

Melde mich.

Grüße

Erik

Zwischenstand von E. Müller

Von: Vladimir Forenski <vladimir.forenski@hotmail.com>
Gesendet: 08.06.2024 13:11:40,000
An: Erik Müller <erikalex.mueller@hotmail.com>
Betreff: AW: Gott der Meere hat ein Problem

Hallo Erik,

hast Du Neptun? Komm nach Krakowia, nimm den Zug oder Bus bis Wien. Sag mir, wann und wo genau Du ankommst, mein Cousin holt Dich ab. Den kannst Du nicht verfehlen, der war bei Deinem letzten Besuch bei Deiner Oma mit uns in der Gaststätte.

Grüße und bis bald

Reiseaufruf von V. Forenski

Von: Erik Müller <erikalex.mueller@hotmail.com>
Gesendet: 08.06.2024 14:20:10,000
An: irma.mueller@gmx-topmail.de
Betreff: Dienstreise

Hallo Mama,

tut mir leid, aber ich kann morgen nicht vorbeikommen. Muss kurzfristig auf eine Dienstreise. Melde mich

Liebe Grüße

Erik

Ankündigung der Abwesenheit von E. Müller

Anhang B Wiki-Eintrag

Human Interface Device (HID)

Definition

Human Interface Device (HID) (deutsch etwa *Menschliches Schnittstellengerät*) beschreibt Geräte, mit deren Hilfe Benutzerinnen und Benutzer mit Computern interagieren können. Interaktionen können Benutzereingaben und Ausgaben sein.
Die Spezifikation wurde primär dazu entwickelt, um die Kommunikation zwischen Rechnern und angeschlossenen Geräten über USB, Bluetooth und weiteren Schnittstellen wie z.B. Zigbee zu vereinfachen. Vorher war es notwendig, für jedes angeschlossene Gerät (z.B. Maus oder Tastatur) eigene Treiber zu installieren. Über eine gemeinsame Spezifikation können nun neue Geräte unproblematisch angeschlossen und sofort verwendet werden, auch unabhängig vom verwendeten Betriebssystem des Rechners.

Die USB-Spezifikation präzisiert HID, indem sie einen Standard für solche Geräte definiert. Diese sogenannte Device Class Definition for Human Interface Devices (HID) (deutsch etwa *Geräteklassendefinition für Menschliches Schnittstellengeräte*) beschreibt grundlegende Funktionen von HID mithilfe zweier Konzepte:
Berichtsdeskriptor: Dieser beschreibt das Format und die Bedeutung der Daten, die das Gerät unterstützt.
Berichte: Berichte sind die tatsächlichen Daten, die zwischen einem Gerät und einer Anwendung ausgetauscht werden. Es gibt drei Berichtstypen:
Eingabebericht: Daten, die vom HID an eine Anwendung gesendet werden, z. B. wenn sich der Zustand eines Steuerelements ändert.
Ausgabebericht: Daten, die von der Anwendung an das HID gesendet werden, z. B. an die LEDs auf einer Tastatur.
Featurebericht: Daten, die manuell gelesen und geschrieben werden können und sich in der Regel auf Konfigurationsinformationen beziehen.

Forensische Aspekte

Aus Sicht der Forensik sind HID interessant, weil sie mit einem Endgerät interagieren und teilweise ohne manuelles Eingreifen von menschlichen Nutzern Aktionen durchführen können. Ein aus Sicht der Forensik positives Beispiel sind die zur Sicherung genutzten sogenannten Mouse-Jiggler, kleine USB-Sticks, die Maus-Bewegungen emulieren und dadurch die Sperrung eines Rechners verhindern. Ein anderes Beispiel aus dem Bereich Penetrationstest sind sogenannte Bad-USB-Devices. Hierbei handelt es sich oft um USB-Sticks oder in USB-Kabel integrierte Funktionen, die Keyboards oder Maus emulieren und dann z.B. im Namen des gerade angemeldeten Benutzers Befehle ausführen, z.B. in der Windows-Powershell. Ein interessanter Artikel dazu ist in der ct 23/27.

HID sind in den Betriebssystemen wie folgt auffindbar:
Windows 11: *Systemsteuerung* \| *Geräte-Manager* \| *HID-Devices* \| *Eigenschaften* \| *Ereignisse*

Linux: Hängt vom System und Einstellungen des Loggings ab, Logs finden sich in der Regel unter */var/log/* und *syslog*. Alternativ können Informationen über den Befehl *systemctl*, z.B. Live-Logs mit *systemctl -f* abgerufen werden.

MacOS: Folgender Befehl im Terminal listet aktuell angeschlossene HID: *hidutil list*. Weitere Informationen und Überblicke über das System und seine Protokolle sind in der *Systemsteuerung\Allgemein\Info\Systembericht* (Button ganz unten) zu finden. Es gibt hier aber keinen Punkt *HID* oder Ähnliches. Das Log */usr/sbin/ioreg%20-lxw550* (unter Protokollen im Systembericht als IORegistry-Inhalt bezeichnet), ist das einzige Log, das hier Informationen aufzeichnet.

Weiterführende Informationen

HID-Spezifikation:
https://www.usb.org/document-library/device-class-definition-hid-111

HID-Dokumentation:
https://usb.org/hid

c't 23/27 *Böses USB*:
https://www.heise.de/select/ct/2023/27/2327713240730976058

Weitere Informationen aus der c't 23/27:
https://www.heise.de/select/ct/2023/27/softlinks/yhhf

Paper zu Bad-USB-Sticks:
https://link.springer.com/chapter/10.1007/978-3-319-95729-6_18