Über die Vertrauenswürdigkeit digitaler Beweismittel und wie diese etabliert werden kann

Janine Schneider

Angaben zur Veröffentlichung / Publication details:

Schneider, Janine. 2024. "Über die Vertrauenswürdigkeit digitaler Beweismittel und wie diese etabliert werden kann." In *Ausgezeichnete Informatikdissertationen 2023: Juli 2024, Lübeck, Deutschland*, edited by Rüdiger Reischuk, Sven Apel, Abraham Bernstein, Maike Buchin, Anna Förster, Felix Freiling, Jan Mendling, et al., 271–80. Bonn: Gesellschaft für Informatik e.V. https://doi.org/10.18420/Diss2023-35.

GI-Edition

Lecture Notes in Informatics

Rüdiger Reischuk et al. (Hrsg.)

Ausgezeichnete Informatikdissertationen 2023

Dissertations

GESELLSCHAFT
FÜR INFORMATIK

Rüdiger Reischuk et al. (Hrsg.)

Ausgezeichnete Informatikdissertationen 2023

Juli 2024
Lübeck, Deutschland

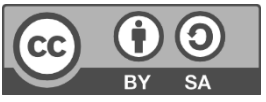
Gesellschaft für Informatik e.V. (GI)

Lecture Notes in Informatics (LNI) - Dissertations
Series of the Gesellschaft für Informatik (GI)

Volume D-24

ISBN 978-3-88579-982-5

printed by Köllen Druck+Verlag GmbH, Bonn



Über die Vertrauenswürdigkeit digitaler Beweismittel und wie diese etabliert werden kann[1]

Janine Schneider[2]

Abstract: Digitale Beweismittel können an Vertrauenswürdigkeit verlieren, wenn bestimmte Eigenschaften nicht mehr gegeben sind. Ist beispielsweise die Herkunft eines Beweismittels nicht nachvollziehbar oder der Prozess der Beweismittelerhebung intransparent, kann die Vertrauenswürdigkeit leiden. Digitale Beweismittel können zudem an Vertrauenswürdigkeit verlieren, wenn die Beweismittel durch Manipulation (ganz oder teilweise) unzuverlässig werden. In dieser Arbeit untersuchen wir deshalb, welche Anforderungen erfüllt sein müssen, um vertrauenswürdige Beweismittel zu erhalten, wann diese Anforderungen nicht mehr erfüllt sind und wie vertrauensbildende Maßnahmen aussehen können. Konkret untersuchen wir, wie digitale Beweismittel (unbemerkt) manipuliert werden können, wie sich mehrdeutige Datenstrukturen auf digital-forensische Analysen auswirken und welche Auswirkungen NAND-Flash Chip Recycling auf die Vertrauenswürdigkeit hat. Darüber hinaus schaffen wir Vertrauen, indem wir vertrauensbildende Merkmale in den Prozess der digital-forensischen Analyse integrieren.

1 Einführung

Wie bei klassischen Beweismitteln müssen auch digitale Beweismittel bestimmte Eigenschaften aufweisen, um vor Gericht verwendet werden zu können. Die grundlegendste dieser Eigenschaften ist die Vertrauenswürdigkeit. Vertrauen in eine Sache oder Person wird hierbei gebildet durch die Zuverlässigkeit eben dieser [Du24]. In der digitalen Forensik ist die Qualität der Analyse entscheidend für die Qualität der Beweismittel. Dementsprechend stellt auch die Rechtswissenschaft Anforderungen an den forensischen Beweiserhebungsprozess und die Qualität digitaler Beweismittel, wie Transparenz, Wiederholbarkeit und Rückverfolgbarkeit [Rü20]. Fachleute auf dem Gebiet der digitalen Forensik versuchen deshalb bereits seit einiger Zeit eine allgemeingültige Definition des Begriffs der Vertrauenswürdigkeit digitaler Beweismittel und eine Beschreibung ihrer Eigenschaften zu erarbeiten. Accorsi [Ac09] schreibt beispielsweise, dass die erhobenen Daten vollständig und authentisch sein müssen, um als Beweismittel vor Gericht verwendet werden zu können. Accorsi erklärt weiterhin folgendes:

> "The provenance of data must be traceable and guaranteed." [Ac09]

Vertrauenswürdige Beweismittel müssen demnach transparent und vollständig erhoben werden, der Erhebungsprozess muss wiederholbar und nachvollziehbar sein und die Beweismittel selbst müssen authentisch, korrekt und deren Herkunft rückverfolgbar sein.

[1] Englischer Titel der Dissertation: "On the Trustworthiness of Digital Evidence and How It Can Be Established"

[2] Friedrich-Alexander-Universität Erlangen-Nürnberg, janine.schneider@fau.de

In der Praxis kann es sich jedoch als schwierig erweisen, diese Anforderungen zu erfüllen da die Vertrauenswürdigkeit digitaler Beweismittel durch viele Faktoren beeinträchtigt werden kann. Im ersten Teil der Dissertation untersuchen wir daher drei Beispiele für eine solche Beeinträchtigung: (a) Manipulation digitaler Beweismittel, (b) mehrdeutige Datenstrukturen und (c) Daten unbekannter Herkunft durch schlechte Datenbereinigungspraktiken im Falle von NAND-Flash Chip Recycling. Hierbei untersuchen wir, inter alia, welche Anforderungen an vertrauenswürdige Beweismittel durch die genannten Beispiele verletzt werden und wie diese den Analyseprozess beeinflussen.

Im zweiten Teil der Dissertation beschäftigen wir uns mit der Frage, wie Vertrauenswürdigkeit geschaffen werden kann. Hierzu verwenden wir ein von uns entwickeltes formales Modell, das die Interpretation und Analyse von Daten und deren Herkunft beschreibt. Außerdem stellen wir ein auf diesem Modell basierendes Werkzeug vor, mit dem Daten in einer wiederholbaren, transparenten und nachvollziehbaren Weise gesammelt und analysiert werden können, so dass ein Analyseprozess entsteht, der von Grund auf vertrauenswürdig ist. Anschließend demonstrieren wir den Nutzen des Tools indem wir verschiedene Anwendungsbeispiele beschreiben und das Modell auf die drei Beispiele des ersten Teils anwenden.

Im Folgenden wird exemplarisch (und verkürzt) auf das Thema der Daten unbekannter Herkunft durch schlechte Datenbereinigungspraktiken im Falle von NAND-Flash Chip Recycling und das formale Modell zur Beschreibung der Interpretation und Analyse von Daten und deren Herkunft eingegangen. Diese beiden Themenbereiche repräsentieren den Charakter der Dissertation in der Kürze dieser Zusammenfassung am besten und stellen die anspruchsvollsten Ergebnisse der Arbeit dar.

2 Auswirkung schlechter Datenbereinigungspraktiken

Wie Garfinkel und Shelat [GS03] bereits im Jahr 2003 gezeigt haben, enthalten Secondhand-Speichergeräte oft vertrauliche und wiederherstellbare Daten verursacht durch schlechte Datenbereinigungspraktiken: Von 83 gebraucht gekauften Festplatten, enthielten insgesamt 49 wiederherstellbare Daten, darunter Kreditkarteninformationen, Firmennotizen und persönliche Krankenakten. Für Secondhand-USB-Sticks und Speicherkarten wurden schlechte Datenbereinigungspraktiken unter anderem durch Robins et al. [RWS17] bestätigt. Insgesamt ist also klar, dass heute niemand mehr davon ausgehen kann, dass ein gebrauchtes Speichergerät (welcher Art auch immer) keine Daten aus früherer Nutzung enthält.

Aus Sicht der digitalen Forensik sind schlechte Datenbereinigungspraktiken vor allem dann relevant, wenn auf einem zu untersuchenden gebrauchten Speichergerät strafbare oder belastende Daten gefunden werden. Im Gegensatz zur Nutzung eines gebrauchten Speichergeräts wurde die Nutzung eines neuen Speichergeräts bisher als sicher gegenüber dieser Thematik angesehen, da keine vorherige Nutzung auch keine wiederherstellbaren Daten impliziert. Es war daher äußerst überraschend, als Westman [We18, We17] berichtete Daten auf einem neu gekauften USB-Stick gefunden zu haben. Diese Ergebnisse sind auf die Wiederverwendung von recycelten NAND-Flash Chips zurückzuführen, was zu

großer Besorgnis in der digitalen Forensik geführt hat, da die Zuordnung von Daten auf neuen USB-Sticks dadurch genauso schwierig wird wie bei gebrauchten Geräten.

Um die Häufigkeit des Auftretens recycelter NAND-Flash Chips in USB-Sticks (und damit das Risiko des Auffindens von Daten einer früheren Nutzung) zu untersuchen haben wir deshalb eine groß angelegte Studie zu diesem Thema durchgeführt. Die Studie wurde in Zusammenarbeit mit der Hochschule Leiden (HSL), der Hochschule Albstadt-Sigmaringen (HSAS), der Firma MSAB[3] und dem Netherlands Forensic Institute (NFI) durchgeführt.

Ausgehend von der Hypothese, dass die Wahrscheinlichkeit, einen recycelten NAND-Flash Chip in einem neuen USB-Stick zu finden, umgekehrt proportional zum Preis ist, konzentrierten wir uns zunächst auf geringpreisige Werbe-USB-Sticks und testeten in einer zweiten Phase die gegenteilige Hypothese, indem wir hochpreisige Produkte bekannter Marken untersuchten. Unser Ziel war es, (1) die Wahrscheinlichkeit des Auffindens von Daten aus einer früheren Nutzung und (2) die quantitative Korrelation zwischen bestimmten externen Faktoren und dem Vorhandensein nicht-trivialer Daten zu messen. Wir bezeichnen Daten als nicht-trivial, wenn sie von gängigen forensischen Werkzeugen zur Wiederherstellung gelöschter Daten (sogenannten Carvern, wie beispielsweise Foremost[4]) gefunden werden und (nach visueller Überprüfung) kein falsch-positives Ergebnis sind.

Für den ersten Teil der Studie erwarben wir 1.250 geringpreisige USB-Sticks über die Verkaufsplattform Alibaba. Für den zweiten Teil der Studie erwarben wir 459 hochpreisige USB-Sticks über verschiedene deutsche Online-Händler.

2.1 Ergebnisse der Untersuchung geringpreisiger Werbe-USB-Sticks

Im Folgenden stellen wir zunächst die Ergebnisse der Untersuchung der geringpreisigen USB-Sticks vor. Wie in Tabelle 1 zu sehen ist wurden 1.211 von 1.250 USB-Sticks ausgewertet.

	Geringpreisig				**Hochpreisig**	
	FAU	HSL	HSAS	Total	FAU	Total
Anzahl Sticks	516	134	600	1.250	459	1.709
Analysiert	489	133	589	1.211	435	1.646
Datenfunde	61	14	1	76	0	76
Visuelle Untersuchung	415	0	555	970	305	1.275

Tab. 1: Anzahl der USB-Sticks pro Forschungsgruppe und Anzahl der durchgeführten Analysen. Insgesamt wurden 1.646 von 1.709 USB-Sticks analysiert. 76 enthielten nicht-triviale Daten. 74 enthielten wiederverwendete Chips.

Insgesamt enthielten 76 USB-Sticks nicht-triviale Daten in unterschiedlichem Ausmaß, was als Indikator für Chip Recycling gewertet wird. Zwei USB-Sticks enthielten jedoch

[3] https://www.msab.com/de/

[4] https://foremost.sourceforge.net/

ein aktives FAT32-Dateisystem, einschließlich gelöschter FAT-Einträge und wiederherstellbarer privater Bilder. Beide USB-Sticks enthielten die gleichen Bilder, die laut Metadaten kurz vor dem Versand der USB-Sticks erstellt und sofort gelöscht worden waren. Es ist daher davon auszugehen, dass es sich hierbei um Artefakte eines Funktionstests, nicht jedoch um Artefakte von Chip Recycling handelt.

2.1.1 Art der gefundenen Daten

Neben zahlreichen falsch-positiven Ergebnissen konnten diverse relevante Datenelemente rekonstruiert werden. Insgesamt fanden sich auf den USB-Sticks hauptsächlich folgende Datentypen:

- Gifs, Icons, Emojis, Logos
- Fotos, Bilder, Wallpapers, Karten
- Musik, Film und Serien Cover, Poster
- Klingeltöne
- RPM, TAR, ZIP-Archive
- Musik, Videos, Filme
- Sprachaufnahmen
- Dokumente
- Quellcode

Die gefundenen Daten wurden zur Identifizierung möglicher Geräte oder Systeme verwendet, in die der Chip ursprünglich eingebaut worden war. Auf diese Weise kann zwischen der Wiederverwendung des Chips und des gesamten USB-Sticks unterschieden werden. Hierfür wurde, inter alia, eine inverse Bildsuche mit den gefundenen Bilddateien durchgeführt, Archive entpackt, nach Schlüsselwörtern gesucht und Daten manuell gesichtet. Hierdurch konnten drei ursprünglich verwendete Betriebssysteme identifiziert werden: Android, Chrome OS und Linux. Außerdem konnte die vorherige Nutzung von Smart TVs (meist Samsung), Druckern und Diktiergeräten nachgewiesen werden. Abbildung 1 fasst die Systeme und Geräte zusammen, die durch die Analyse identifiziert werden konnten.

Abbildung 1 zeigt, dass 16 USB-Sticks Android bezogene Daten enthielten. Auf drei davon konnten private Bilder und Videos rekonstruiert werden. Ein USB-Stick enthielt Aufnahmen einer asiatischen Nachrichtensendung und Teile eines Kinderfilms. Ein USB-Stick enthielt drei Bilder eines asiatischen Kindes. Auf einem USB-Stick konnten 10.298 gifs und jpegs rekonstruiert werden, die meisten davon privater Natur, darunter Bilder von jungen asiatischen Frauen (teilweise halbnackt oder nackt) und Babys. Dies war der größte Datenfund des Experiments. Ein USB-Stick enthielt die Aufzeichnung eines privaten Gesprächs in chinesischer Sprache. Andere Daten, die auf diesem USB-Stick gefunden wurden, deuten darauf hin, dass der Chip Teil eines Sony-Sprachaufzeichnungsgeräts gewesen sein könnte. Darüber hinaus enthielten 27 USB-Sticks Weltkartenmaterial, was auf eine frühere Nutzung in einem Navigationssystem hindeuten könnte. Ein USB-Stick enthielt Daten, die auf eine frühere Verwendung als Saregama[5] Musikbox hindeuten.

[5] https://www.saregama.com/

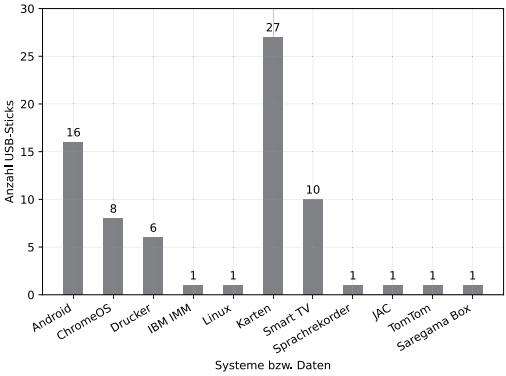


Abb. 1: Anzahl der identifizierten Systeme, Geräte und Datenarten für die untersuchten geringpreisigen Werbe-USB-Sticks.

2.1.2 Visuelle Untersuchung

Neben der Analyse der gefundenen Daten untersuchten wir außerdem die Gehäuse, die Leiterplatten und die NAND-Flash Chips von 970 USB-Sticks. Hierdurch konnten irreguläre Stempel und Inschriften auf 28 Chips festgestellt werden. Laut Westman [We18] sind solche Stempel ein Zeichen für die Wiederverwendung von Chips, wobei der Stempel während der Qualitätskontrolle auf den Chip aufgebracht wird. Des Weiteren konnten auffällige Farbmarkierungen (10 Chips), handschriftliche Notizen (6 Chips), auffällige Verschmutzungen (8 Chips) und Kratzer (8 Chips) auf einigen der Chips festgestellt werden. Abbildung 2 zeigt vier Beispielchips mit auffälligen visuellen Merkmalen.

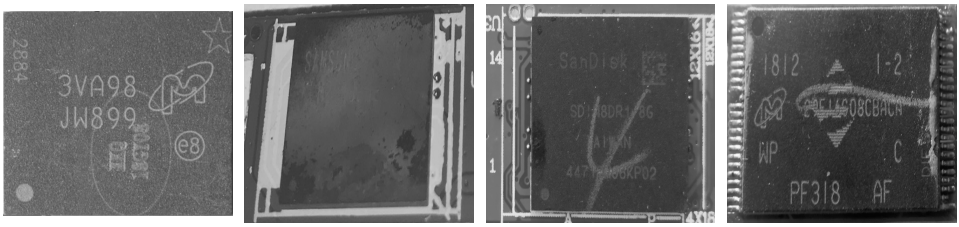


Abb. 2: Vier Beispielchips mit jeweils einem irregulären Stempel (links), Schmutz (mitte links), einer handschriftlichen Notiz (mitte rechts) und einer Farbmarkierung (rechts).

Darüber hinaus ergab die visuelle Untersuchung, dass einige der USB-Sticks keine NAND-Flash Chips enthielten, sondern Mini-SD Karten, die mit Epoxidharz fixiert waren. Andere Sticks enthielten eMMC-Chips, mit Einschnitten oder gekürzte Chips und Karten. Das Einschneiden oder Kürzen von eMMC-Speicher ist ein bekanntes Verfahren, um die interne Verbindung zwischen Flashspeicher und Controller zu unterbrechen, falls der Controller den Funktionstest nicht besteht. Dadurch kann der eMMC-Speicher als einfacher NAND-Flash Speicher mit externem Controller verwendet werden. Abbildung 3 zeigt einige Beispiele hierfür.

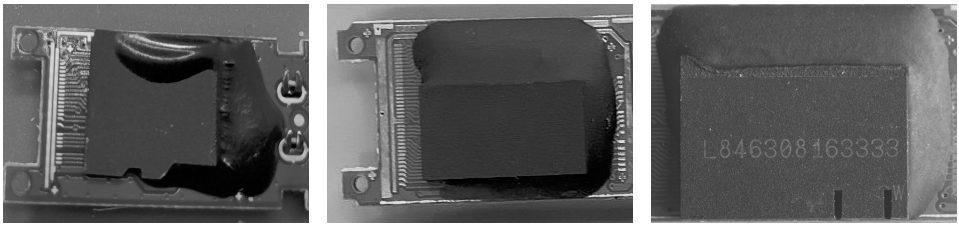


Abb. 3: Gekürzte SD-Karte (links) und zwei eMMC-NAND-Flash Chips, wobei ein Teil entfernt (mitte) und Einschnitte (rechts) vorgenommen wurden, um den Speicher vom Controller zu trennen.

2.2 Ergebnisse der Untersuchung der hochpreisigen USB-Sticks

Wir berichten nun über die Ergebnisse des zweiten Teils unserer Studie. Wie in Tabelle 1 zu sehen ist wurden 435 von 459 hochpreisigen Marken-USB-Sticks analysiert. Wie zuvor wurden auch in diesem Teil der Studie mehrere Carver eingesetzt, um nach nicht-trivialen Daten zu suchen. Abgesehen von vielen falsch-positiven Ergebnissen enthielt keiner der untersuchten USB-Sticks nicht-triviale Daten, die auf Chip Recycling zurück zu führen sind. Einige USB-Sticks wurden vorformatiert ausgeliefert und enthielten Bilder des Markenlogos. Es gab jedoch keine Hinweise auf eine frühere Verwendung der Chips.

Insgesamt ermittelten wir eine Wahrscheinlichkeit von 6%, Daten auf geringpreisigen, als neu verkauften Werbe-USB-Sticks zu finden. Diese Wahrscheinlichkeit, hängt nahezu vollständig vom Vertreibenden der Sticks (nahezu 100 % für 3 von 19 Vertreibenden) und der Art des Speichers (eMMC) ab. Die Wahrscheinlichkeit, Daten auf hochpreisigen Marken-USB-Sticks zu finden, die auf Chip Recycling zurückzuführen sind, liegt bei 0%.

3 Vertrauen schaffen durch Integration vertrauensbildender Merkmale

Wie bereits eingangs erwähnt kann die Vertrauenswürdigkeit digitaler Beweismittel bereits bei der Erhebung berücksichtigt und vertrauensbildende Merkmale in den Erhebungsprozess integriert werden. Um dies zu erreichen, entwickelten wir ein Modell, das den Prozess der forensischen Analyse und der Dateninterpretation formalisiert und transparent, wiederholbar und nachvollziehbar macht. Das Modell ist so konzipiert, dass jederzeit nachvollzogen werden kann, woher die erhobenen Daten stammen und wie sie interpretiert wurden. Das Modell definiert Basiskomponenten, die mit Hilfe einer einfachen Eingabesprache auf vielfältige Weise kombiniert werden können. Diese Eingabesprache ermöglicht die Modellierung komplexer Ausdrücke, die gespeichert und wiederholt werden können. Darüber hinaus erlaubt die Formalisierung die Generalisierung verschiedener Daten und Analysetechniken, was neue Möglichkeiten der Kombination von Datenquellen und Methoden eröffnet und die Überprüfung von Zuverlässigkeit und Korrektheit ermöglicht. Wir nennen dieses Modell LAYR.

3.1 Das LAYR Modell

Die goldene Regel des LAYR-Modells ist, dass zu keinem Zeitpunkt Informationen weitergegeben werden, die nicht in der Eingabe enthalten sind. Außerdem arbeitet LAYR immer mit der Eingabe selbst (also keiner kopierten oder gepufferten Eingabe), es sei denn dies ist nicht anders möglich. Um dies zu erreichen, werden Adressverweise als Eingabe und Ergebnis einer Analyse verwendet. Das Ergebnis einer LAYR-Analyse ist demnach eine Reihe von *Adressen* die beispielsweise eine Datei bilden, nicht die Datei selbst. Dadurch wird die Verlässlichkeit der Beweise und die Transparenz ihrer Herkunft gewährleistet. Mehrere Adressen können zusammengefasst werden zu *Daten*. Diese können sowohl Inhaltsdaten als auch Metadaten beinhalten. Die Herkunft (im Sinne der Interpretation) kann durch sogenannte *Spuren* nachvollzogen werden. Spuren beschreiben, welche Analyseschritte durchgeführt wurden, um zu einem bestimmten Ergebnis zu kommen. Inhaltsdaten, die zugehörigen Metadaten und deren jeweilige Spuren werden in so genannten *Objekten* zusammengefasst. Mehrere Objekte auf der selben logischen Ebene bilden eine *Abstraktionsschicht*. Zwei logisch aufeinander aufbauende Schichten bilden einen *Abstraktionslevel*. Um von Objekten der unteren Schicht zu Objekten der oberen Schicht zu gelangen, müssen die Daten der unteren Schicht auf die richtige Art interpretiert werden.

Für die Analyse von Daten können *Regeln* verwendet werden. Wir unterscheiden hierbei zwischen *Rekonstruktionsregeln*, die Daten interpretieren und Objekte zusammensetzen, und *Transformationsregeln*, die Daten transformieren und dabei neue Daten und Adressen erzeugen können. Rekonstruktionsregeln implementieren spezialisierte Aufgaben wie das Parsen verschiedener Dateisysteme oder das Carven von Dateien. Transformationsregeln können verwendet werden, um Daten zu transformieren, z.B. um komprimierte Daten zu dekomprimieren. Dazu muss die Transformationsregel den Kompressionsalgorithmus verstehen und anwenden. Im Gegensatz zu Rekonstruktionsregeln müssen Transformationsregeln neue Adressen für die transformierten Daten erzeugen. Hierbei ist zu beachten, dass die Transformation keine Daten “erfindet”, sondern die Daten aus der Eingabe wie vorgesehen verwendet, um neue Adressen zu erzeugen.

Operatoren ermöglichen die Kombination verschiedener Regeln, um komplexere Aufgaben zu erfüllen. Die Trennung von Regeln und Operatoren ermöglicht es Programmierenden, sich auf die Implementierung spezifischer Aufgaben zu konzentrieren, während Benutzende die Möglichkeit haben, diese Methoden auf neue Art und Weise zu kombinieren.

3.2 Anwendungsbeispiel

Um die Vielseitigkeit des LAYR-Modells zu demonstrieren, soll im Folgenden ein Beispiel für die Anwendung des Modells beschrieben werden. Das Beispiel zeigt die Durchführung einer komplexe Hauptspeicheranalyse mit LAYR.

Wird mehr physischer Speicher benötigt, kann Hauptspeicher in sogenannte Auslagerungsdateien ausgelagert werden. Soll eine vollständige forensische Analyse durchgeführt

werden, muss demnach neben dem physischen Hauptspeicher auch die Auslagerungsdatei berücksichtigt werden. Da die MMU eine Abstraktionsschicht zwischen physischem und virtuellem Speicher einführt, werden die Daten außerdem nicht notwendigerweise in sequentieller Reihenfolge gespeichert, was Carving unmöglich macht. Da LAYR nativ in der Lage ist mit verschiedenen Eingaben und Abstraktionsschichten umzugehen und Objekte über diese hinweg zu interpretieren und zu rekonstruieren, ist dieser Fall ein perfektes Beispiel dafür, wie ein solches Problem komfortabel und einfach mit LAYR gelöst werden kann. Abbildung 4 zeigt die verschiedenen Komponenten, die für diese Aufgabe benötigt und wie sie verwendet werden.

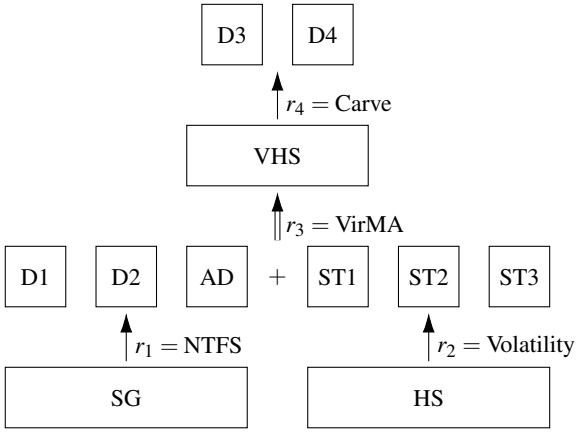


Abb. 4: Rekonstruktionsprozess zur Erstellung eines flachen Windows Hauptspeichers mit Volatility und VirMA. Der zugehörige LAYR Eingabeausdruck wird wie folgt gebildet: `NTFS(SG) + Volatility(HS) =>? VirMA -> Carve`. Dieser Ausdruck beschreibt folgendes Vorgehen: Extrahieren von zwei Dateien (D1, D2) und der Auslagerungsdatei (AD) aus dem Speichergerät (SG) mit Hilfe der NTFS-Regel, Extrahieren der Seitentabellen (STs) aus dem Hauptspeicher (HS) mit Hilfe der Volatility-Regel, Kombinieren der extrahierten AD und der STs, um den flachen virtuellen Hauptspeicher (VHS) mit Hilfe der VirMA-Regel zu rekonstruieren, Carven nach Dateien (D3, D4) im VHS mit Hilfe der Carving-Regel.

Zunächst muss das Dateisystem analysiert werden, um die Auslagerungsdatei zu erhalten, während der physische Speicher analysiert werden muss, um den virtuellen Speicher und die Seitentabellen zu erhalten. Dies kann durch eine Regel erreicht werden die Volatility[6] integriert. Die Ergebnisse dieser beiden Regeln können dann mit dem sogenannten Vereinigungsoperator kombiniert werden. Auf die kombinierte Ergebnismenge wird eine Regel angewendet, die den flachen Speicher erzeugt, auf den die Carving-Regel angewendet werden kann. Der flache Speicher kann durch eine Regel erzeugt werden die VirMA [Gr15] integriert. Dieses Beispiel zeigt deutlich das große Potential von LAYR. Darüber hinaus ist das Beispiel nicht nur theoretischer Natur, sondern wurde von Ilg [Il21] sowohl für moderne Windows- als auch für Linux-Systeme implementiert.

[6] https://www.volatilityfoundation.org/

4 Zusammenfassung

Digitale Beweismittel gewinnen immer mehr an Bedeutung, insbesondere durch Straftaten, die ausschließlich im digitalen Raum begangen werden. Wie bei klassischen Beweismitteln spielt die Vertrauenswürdigkeit auch bei digitalen Beweismitteln eine große Rolle. Vertrauenswürdigkeit zeichnet sich in diesem Fall durch Transparenz, Vollständigkeit, Wiederholbarkeit, Rückverfolgbarkeit und Authentizität aus. Die Erfüllung dieser Anforderungen kann unter bestimmten Umständen allerdings sehr schwierig sein. Ein Beispiel hierfür ist die Verwendung von recycelten NAND-Flash Chips in als neu verkauften USB-Sticks. Hierbei kann es zu einer Situation kommen, in der die Herkunft der auf einem solchen USB-Stick gefundenen Daten unklar ist. Durch die Untersuchung dieses Phänomens kann das Vorkommen solcher Daten aber erklär- und nachvollziehbar gemacht werden. Aus diesem Grund haben wir untersucht, wie wahrscheinlich es ist, alte Daten auf neu gekauften USB-Sticks zu finden und wie NAND-Flash Chip Recycling erkannt werden kann. Unseren Erkenntnissen nach ist dieses Phänomen (derzeit) beschränkt auf geringpreisige Werbe-USB-Sticks aus China.

Die Untersuchung und das Erklären von Vertrauensverlust sind aber nur die ersten Schritte hin zu vertrauenswürdigeren Beweismitteln. Der zweite Schritt ist die Einbindung vertrauensbildender Merkmale in den Beweiserhebungsprozess digitaler Beweismittel und die Entwicklung von zuverlässigen Analysemethoden und Prozessen. Zu diesem Zweck haben wir LAYR entwickelt. Mit dem LAYR-Modell sind wir in der Lage, die Interpretation und Analyse digitaler Beweismittel über mehrere Abstraktionsebenen hinweg abzubilden und gleichzeitig die Herkunft der Daten während des gesamten Rekonstruktionsprozesses transparent und nachvollziehbar zu dokumentieren. Die einzigartige Eingabesprache von LAYR ermöglicht die einfache Wiederholung eines Analyseprozesses und damit die Validierung der Ergebnisse. Durch die Kombination verschiedener Eingaben und Techniken ist es außerdem möglich zu überprüfen, ob verschiedene Analyse- und Interpretationsmethoden zu den gleichen Ergebnissen führen, was die Zuverlässigkeit erhöht und die Überprüfung der Korrektheit der Ergebnisse ermöglicht. LAYR bietet des Weiteren die Möglichkeit, komplexe Analyseausdrücke zu erstellen, was neue Möglichkeiten für die forensische Analyse eröffnet. Um die praktische Anwendbarkeit des Modells zu demonstrieren, haben wir ein forensisches Analyse- und Beweiserhebungswerkzeug implementiert, das direkt aus den Modelldefinitionen abgeleitet ist. Das so genannte LAYR-Tool ist ein leicht zu erweiterndes und einfach zu bedienendes Tool. So schaffen wir bereits bei der Erhebung vertrauenswürdigere Beweismittel.

In dieser Kurzfassung der Dissertation wurden eine Reihe weiterführenden Erläuterungen ausgespart, etwa die Untersuchung der Manipulation digitaler Beweismittel, die Untersuchung der Auswirkungen von mehrdeutigen Datenstrukturen auf den forensischen Analyseprozess und die mathematischen Definitionen der LAYR-Modellkomponenten. Diese und weitere Themen können bei Interesse in der Dissertationsschrift [Sc23] nachgelesen werden.

Literaturverzeichnis

[Ac09] Accorsi, Rafael: Safe-Keeping Digital Evidence with Secure Logging Protocols: State of the Art and Challenges. In: 2009 Fifth International Conference on IT Security Incident Management and IT Forensics. S. 94–110, 2009.

[Du24] Duden: Vertrauen: Rechtschreibung, Bedeutung, Definition, Herkunft — Duden. https://www.duden.de/rechtschreibung/Vertrauen.

[Gr15] Gruhn, Michael: Windows NT pagefile.sys Virtual Memory Analysis. In: 2015 Ninth International Conference on IT Security Incident Management & IT Forensics. S. 3–18, 2015.

[GS03] Garfinkel, S.L.; Shelat, A.: Remembrance of data passed: a study of disk sanitization practices. IEEE Security & Privacy, 1(1):17–27, 2003.

[Il21] Ilg, Josef: Take LAYR to the next Level by Integrating Main Memory Analysis. Masterarbeit, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), 2021.

[Rü20] Rückert, Christian: Herausforderungen der Digitalisierung für das Strafverfahren. In (Hoven, Elisa; Kudlich, Hans, Hrsg.): Digitalisierung und Strafverfahren. Jgg. 5 in Beiträge zum Strafrecht - Contributions to Criminal Law. Nomos, S. 9–38, 2020.

[RWS17] Robins, Nikki; Williams, Patricia A. H.; Sansurooah, Krishnun: An Investigation into Remnant Data on USB Storage Devices Sold in Australia Creating Alarming Concerns. International Journal of Computers and Applications, 39(2):79–90, 2017.

[Sc23] Schneider, Janine: On the Trustworthiness of Digital Evidence and How It Can Be Established. Dissertation, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), 2023.

[We17] Welchering, Peter: Recycling: Rätselhafte Daten auf fabrikneuen USB-Sticks. https://www.faz.net/aktuell/technik-motor/digital/recycling-neue-usb-sticks-enthalten-oft-restdaten-15015418.html.

[We18] Westman, Martin: Where Did That Incriminating Evidence Come From? https://dfrws.org/presentation/where-did-that-incriminating-evidence-come-from/.

Janine Schneider absolvierte ihre Promotion am Lehrstuhl für IT-Sicherheitsinfrastrukturen der Friedrich-Alexander-Universität Erlangen-Nürnberg im Rahmen des DFG-Graduiertenkollegs 2475: Cyberkriminalität und Forensische Informatik unter der Leitung von Prof. Dr.-Ing. Felix Freiling. In den drei Jahren ihrer Promotion veröffentlichte sie fünf Publikationen als Erstautorin, wurde mit dem "DFRWS Best Student Paper Award" ausgezeichnet, reiste zu Forschungszwecken nach New Orleans und engagierte sich als Gleichstellungsbeauftragte ihres Fachbereichs. Sie beendete Ihre Promotion mit Auszeichnung. Aktuell arbeitet sie als Postdoc am CISPA Helmholtz Center for Information Security in Saarbrücken im Bereich Erkennung und Vermeidung von Cyberangriffen. Ihr aktueller Forschungsschwerpunkt liegt auf der Verbesserung digital-forensischer Methoden und Analysetechniken. Hierfür verwendet sie Methoden aus dem Bereich der IT-Sicherheit und wendet diese im Bereich der digitalen Forensik an, um Schwachstellen in digital-forensischen Prozessen zu finden und diese zu schließen.