Hochschule Wismar
University of Applied Sciences
Technology, Business and Design
Fakultät für Ingenieurwissenschaften

Master-Thesis

Nachweis Blockchain-basierter Kryptowährungen und Nachverfolgungen von Zahlungsflüssen unter Einsatz von Open Source Intelligence

Eingereicht am: 04.11.2022
von: J. Müller

Aufgabenstellung

Die Aufgabenstellung dieser Master-Thesis gliedert sich in zwei zusammenhängende Anteile. Der erste Anteil beschäftigt sich mit der Fragestellung, wie mit IT-forensischen Methoden digitale Spuren aus der Nutzung von Kryptowährungen ermittelt werden können. Um Transaktionen mit Kryptowährungen und deren Beteiligte nachvollziehen zu können, die in Verbindung mit einem konkreten Nutzer oder Endgerät stehen, werden hierzu auf verschiedenen Endgeräten Spuren erzeugt, gesichert und ausgewertet. Die Erzeugung dieser Spuren erfolgt anhand realitätsnaher Szenarien, die dann mit Testfällen durchschritten werden. Die dabei erzeugten Artefakte werden nachfolgend mit verschiedenen etablierten Forensik-Tools ausgewertet und deren Erkennungsleistung miteinander verglichen.

Der zweite Anteil der Master-Thesis bildet die Nachverfolgung der im ersten Anteil erzeugten Spuren entlang der Blockchain unter Einsatz von Open Source Intelligence (OSINT). Es wird untersucht, welche OSINT-Dienste einem Ermittler zur Verfügung stehen und wie diese bei der Ermittlung von Zahlungsflüssen blockchain-basierter Kryptowährungen eingesetzt werden können. Abschließend werden die Möglichkeiten, aber auch Grenzen aufgezeigt, die bei der Ermittlung und Nachverfolgung von Kryptowährungs-Transaktionen auftreten. Aus den gewonnenen Ergebnissen wird eine Handlungsempfehlung abgeleitet, wie idealerweise eine Ermittlung im Zusammenhang mit Kryptowährungen durchgeführt werden kann.

Kurzreferat

Durch die stark ansteigende Nutzung von Kryptowährungen wie Bitcoin ergibt sich für Banken, Behörden und Unternehmen ein verstärkter Bedarf, Nachweise über die Nutzung von Kryptowährungen zu führen und damit verbundene Finanztransaktionen aufzudecken. Die auf Kryptowährungen basierende Kriminalität erreichte 2021 einen neuen Höchststand, wobei illegale Adressen 14 Milliarden Dollar im Laufe des Jahres erhielten, gegenüber 7,8 Milliarden Dollar im Jahr 2020. [1, S. 3]

Neben einer immer stärkeren Durchdringung als allgemein anerkanntes Zahlungsmittel werden Kryptowährungen oft in Verbindung mit illegalen Handlungen, wie beispielsweise Lösegelderpressungen nach Ransomware-Attacken oder für die Geldwäsche von Einkünften aus illegalen Geschäften genutzt. Die Verfolgung dieser Geldflüsse gestaltet sich schwierig, denn die entsprechenden Konten (Wallets) liegen nicht zentralisiert in der Administration regulierter Banksysteme, sondern werden dezentral in Peer-2-Peer (P2P) Netzwerken geführt. Die Transaktionen sind aber durch den Einsatz verteilter Kontenbücher (Distributed-Ledgers) keineswegs vollständig anonym. Der Einsatz von Blockchain-Technologien, die als dezentrale Buchungssysteme fungieren, bietet daher neue Ansätze, diese Zahlungsflüsse mit OSINT-Diensten nachvollziehen zu können. Einen Schwerpunkt dieser Arbeit bilden IT-forensische Methoden (Datenakquise- und Auswertung) unter Einsatz von Software-Tools (AXIOM, Autopsy, Bulk Extractor), um digitale Spuren aus der Nutzung von Kryptowährungen zu ermitteln und um deren Erkennungsleistung zu bewerten. Die gefundenen Spuren werden mit verschiedenen OSINT-Diensten weiterverfolgt und analysiert. Es erfolgt eine Bewertung der untersuchten OSINT-Dienste. Abschließend wird eine Handlungsempfehlung abgeleitet, wie idealerweise eine Ermittlung im Zusammenhang mit Kryptowährungen durchgeführt werden kann.

Abstract

The rising use of cryptocurrencies such as Bitcoin is increasing the relevance for banks, government agencies, and businesses to keep a record of cryptocurrency use and detect related financial transactions. Cryptocurrency-based crime reached a new high in 2021, with illicit addresses receiving $14 billion during the year, up from $7.8 billion in 2020." [1, p. 3]

In addition to becoming more pervasive as a commonly accepted means of payment, cryptocurrencies are often used in connection with illicit activities, such as ransomware attacks, or to launder the proceeds of illicit businesses. Tracking these money flows is difficult because the corresponding accounts (wallets) are not centralized in the administration of regulated banking systems, but are decentralized in peer-2-peer (P2P) networks. However, the transactions are not completely anonymous due to the use of distributed ledgers. The use of blockchain technologies that act as decentralized ledger systems therefore offer new approaches to trace these payment flows with OSINT services. One focus is on IT forensic methods (data backup and data analysis) using software tools (AXIOM, Autopsy, Bulk Extractor) to identify digital traces from the use of cryptocurrencies in order to evaluate their detection performance. The traces found are followed up and analyzed using different OSINT services. An evaluation of the investigated OSINT services is performed. Finally, a recommended course of action is derived as to how an investigation can ideally be carried out in connection with cryptocurrencies.

Inhaltsverzeichnis

Aufgabenstellung ... 2

Kurzreferat ... 3

Abstract ... 4

Inhaltsverzeichnis ... 5

1 Einleitung ... 8

2 Einführung in die Blockchain-Technologie ... 10
2.1 Distributed-Ledger-Technologie ... 11
2.1.1 Konsens-Mechanismus ... 12
2.1.2 Block ... 13
2.1.3 Transaktionen ... 14
2.1.4 Mining ... 15
2.2 Kryptografie ... 16

3 Einsatz von Open Source Intelligence ... 18
3.1 Webbasierte Blockchain-Explorer ... 19
3.2 OSINT-Tools zur Transaktionsanalyse von Kryptowährungen ... 20

4 Subjekte und Objekte einer Transaktion ... 24
4.1 Subjekte ... 24
4.1.1 Angreifer ... 24
4.1.2 Opfer ... 24
4.1.3 Verkäufer ... 24
4.1.4 Kunden ... 25
4.2 Objekte ... 25
4.2.1 Transaktionen ... 25
4.2.2 Wallets für Kryptowährungen ... 26
4.2.3 Bitcoin Wallet-Adressen ... 27

5 Definition von End-2-End Szenarien und Testfällen ... 29
5.1 Definition realitätsnaher Szenarien ... 29
5.1.1 Szenario 1: Handel mit illegalen Waren und Dienstleistungen ... 29
5.1.2 Szenario 2: Ransomware und Erpressung ... 31
5.2 Definition der Testfälle basierend auf realitätsnahen Szenarien ... 34
5.2.1 Testfallbeschreibung – T0 ... 34
5.2.2 Testfallbeschreibung – T1 ... 35
5.2.3 Testfallbeschreibung – T2 ... 36

5.2.4 Testfallbeschreibung – T3 37
5.2.5 Testfallbeschreibung – T4 38

6 Methoden und Tools für die IT-forensische Untersuchung 39
6.1 Übersicht eingesetzter Hardware 39
6.2 Übersicht eingesetzter Software 40
6.2.1 Virtual Box (Open-Source) 41
6.2.2 Autopsy (Open-Source) 41
6.2.3 Sleuth Kit (Open-Source) 42
6.2.4 Bulk Extractor (Open-Source) 42
6.2.5 AXIOM (kommerziell) 43

7 Datenauswertung der Testfälle 44
7.1 Datenauswertung Testfall – T0 46
7.2 Datenauswertung Testfall – T1 48
7.3 Datenauswertung Testfall – T2 50
7.3.1 Auswertungsergebnisse – Autopsy 50
7.3.2 Auswertungsergebnisse – AXIOM 55
7.3.3 Auswertungsergebnisse – Bulk Extractor 58
7.4 Datenauswertung Testfall – T3 59
7.4.1 Auswertungsergebnisse – Autopsy 59
7.4.2 Auswertungsergebnisse – AXIOM 60
7.4.3 Auswertungsergebnisse – Bulk Extractor 62
7.5 Allgemeine Erkenntnisse aus der Datenauswertung 63
7.5.1 Datenakquise Apple IPhone SE 63
7.5.2 Einsatz unverschlüsselter Electrum Wallets 64
7.5.3 Einsatz verschlüsselter Ledger Nano S Wallets 68
7.5.4 Webhistorie, Webcache und genutzte Web-Formulare 70
7.5.5 Blick in die zuletzt genutzten Dateien 72
7.5.6 Installierte und ausgeführte Programme 73
7.5.7 Dateien von besonderem Interesse 73
7.5.8 E-Mail-Adressen aus Kommunikationsverläufen und User-Login 74
7.5.9 Auswertung Bulk Extractor Exporte mit Python 74
7.5.10 Validierung von Bitcoin-Adressen mit Regulären Ausdrücken 75
7.5.11 Suche nach relevanten Keywords 76

8 Einsatz von Open Source Intelligence 77
8.1 Blockchain-Explorer: Blockchain.com 77
8.1.1 Analyse Testfall – T2 79
8.1.2 Bewertung für den OSINT-Einsatz 81
8.2 Blockchain-Explorer: OXT.me 83

8.2.1 Analyse Testfall – T2 ... 84
8.2.2 Analyse Testfall – T3 ... 87
8.2.3 Bewertung für den OSINT-Einsatz ... 89
8.3 Wallet-Explorer: WalletExplorer.com ... 91
8.3.1 Analyse Testfall – T0 ... 91
8.3.2 Analyse Testfall – T4 ... 93
8.3.3 Bewertung für den OSINT-Einsatz ... 97
8.4 Datenbank: Bitcoinabuse.com ... 99
8.4.1 Analyse von BitcoinAbuse.com ... 100
8.4.2 Bewertung für den OSINT-Einsatz ... 103
8.5 Analyse-Tool: Maltego Community Edition ... 104
8.5.1 Analyse Testfall – T1 ... 104
8.5.2 Bewertung für den OSINT-Einsatz ... 106
9 Zusammenfassende Bewertung ... 107
9.1 Bewertung eingesetzter IT-Forensik-Tools ... 108
9.2 Möglichkeiten und Grenzen der IT-Forensik ... 111
9.3 Bewertung eingesetzter OSINT-Dienste ... 113
9.4 Möglichkeiten und Grenzen von OSINT ... 117
10 Ausblick und Handlungsempfehlung ... 118
Literaturverzeichnis ... 121
Bilderverzeichnis ... 125
Tabellenverzeichnis ... 127
Anlagenverzeichnis ... 128
Verzeichnis der Abkürzungen ... 129
Thesen ... 130
Selbstständigkeitserklärung ... 131

1 Einleitung

Die vorliegende Arbeit beschäftigte sich aus zwei Perspektiven mit dem Nachweis Blockchain-basierter Kryptowährungen und der Nachverfolgung von Zahlungsflüssen.

Eine Perspektive bildete die IT-Forensik, die sich als Teilgebiet der Forensik mit der methodischen Analyse von Vorfällen auf IT-Systemen und der gerichtsverwertbaren Sicherung der Beweise beschäftigt. Ziel in der IT-Forensik ist es, exakt festzustellen, welche Aktionen auf einem IT-System stattgefunden haben und wer Verursacher oder Verantwortlicher hierfür ist. [2]

Die IT-Forensik liefert hierbei digitale Spuren, die bei der Nutzung von Endgeräten wie PCs oder Smartphones entstehen. Zur Verwendung von Kryptowährungen sind je nach Einsatzszenario weitere Software und ggf. Hardwarekomponenten nötig, um Kryptowährungen zu verwalten und Transaktionen durchzuführen.

Bereits durch die initiale Installation, Konfiguration und Inbetriebnahme können auf dem betroffenen Endgerät Artefakte entstehen, die aus IT-forensischer Sicht als Spuren dienen. Die nachfolgend weitere Verwendung dieser Komponenten lässt zusätzliche Nutzungsspuren entstehen, die im Rahmen dieser Arbeit untersucht wurden.

Ein exemplarischer Blick wurde auch auf die Anwenderkommunikation geworfen, indem aus der E-Mail-Kommunikation relevante Informationen extrahiert wurden.

Das Realisierungsumfeld war ein Laboraufbau, in dem verschiedene physische Endgeräte und virtuelle Maschinen zum Einsatz kamen. Unter Einsatz etablierter IT-Forensik Tools (AXIOM, Autopsy, Bulk Extractor) wurden relevante Artefakte gesichert, identifiziert und für die weitere Analyse vorgehalten.

Ein Kern dieser Arbeit bildete der Bereich der Open Source Intelligence, kurz OSINT.

Der Begriff OSINT beschreibt eine Methodik, die ursprünglich von Nachrichtendiensten geprägt wurde. OSINT nutzt Informationen aus offenen, frei verfügbaren Quellen zur Gewinnung der gewünschten Erkenntnisse. Die aus diesen Quellen gesammelten Informationen werden zur Erkenntnisgewinnung analysiert, bewertet und miteinander verknüpft. [3]

Zur weiteren Einordung und Eingrenzung von OSINT für diese Arbeit wurden ausschließlich frei verfügbare Dienste im Internet angewendet und auf deren Nutzbarkeit im Rahmen von Ermittlungen in Bezug zu Kryptowährungen untersucht. Im Fokus standen OSINT-Dienste wie Blockchain- und Wallet-Explorer, die Informationen über die zugrundeliegende Blockchain und deren Transaktionen enthalten. Zusätzlich wurde ein spezifischer Blick auf das Analyse-Tool Maltego geworfen, da dieses auch OSINT-Quellen einbeziehen kann.

Abzugrenzen ist diese Arbeit von den Gebieten der Kryptoanalyse, da es in dieser Arbeit nicht darum ging, generelle Sicherungs- und Verschlüsselungsstandards von Online-Diensten oder Wallets zu brechen, sondern anhand der verfügbaren Information Rückschlüsse ziehen zu können.

Das Realisierungsumfeld unterlag gewissen Randbedingen hinsichtlich der konkret verfügbaren und kompatibel einsetzbaren Hardware, sowie der Softwarelizenzen. Im Bereich der Softwarelizenzen stand als kommerzielle Lösung AXIOM über eine Hochschullizenz zur Verfügung. Autopsy, Sleuthkit und Bulk Extractor wurden als Open Source Software eingesetzt. Für die Analyse mit dem OSINT-Tool Maltego wurde die frei verfügbare Community Edition (CE) angewendet.

2 Einführung in die Blockchain-Technologie

Der Begriff Blockchain taucht seit einigen Jahren immer häufiger in der Fachpresse der IT- und Finanzbranche auf. Die Blockchain ist ein schillernder Begriff, der unterschiedliche technische Aspekte der Datenverarbeitung- und Speicherung vereint. Eine einheitliche prägnante Definition für den Begriff Blockchain scheint es aber bisher nicht zu geben. Betrachtet aus der Nutzenperspektive wird die Blockchain als „dezentrale, chronologisch aktualisierte Datenbank mit einem aus dem Netzwerk hergestellten Konsensmechanismus zur dauerhaften digitalen Verbriefung von Eigentumsrechten“ [4] beschrieben.

Eine umfassendere Betrachtung des Blockchain-Begriffs wird in einem aktuellen Artikel des Technologie-Beratungsunternehmen Gartner wie folgt beschrieben:

„Blockchain kombiniert bestehende Technologien und Techniken, einschließlich verteilter digitaler Ledger, Verschlüsselung, unveränderlicher Datensatzverwaltung, Tokenisierung von Assets und dezentraler Governance, um Informationen zu erfassen und aufzuzeichnen, die die Teilnehmer eines Netzwerks benötigen, um zu interagieren und Transaktionen durchzuführen. Es gibt keine Vermittler, wie Banken, die die Transaktionen validieren und schützen.“ [5]

Diese umfassende Betrachtung lässt die Blockchain anwendungsseitig sehr vielseitig erscheinen. Die begriffliche Verortung gibt auch zu erkennen, dass sich zur Anwendung von Blockchain-Technologien im besonderen Maße der Finanzsektor eignet, da hier naturgemäß die Verbriefung von Eigentumsrechten einen zentralen Leistungsanteil darstellt.

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BAFIN) wird hier noch klarer in ihren Formulierungen, indem sie Blockchains als fälschungssichere, verteilte Datenstrukturen, in denen Transaktionen in der Zeitfolge protokolliert, nachvollziehbar, unveränderlich und ohne zentrale Instanz abgebildet werden, ausführt. Durch diese Eigenschaften lassen sich Eigentumsverhältnisse regeln,

da eine lückenlose und unveränderliche Datenaufzeichnung hierfür die Grundlage schafft. [6]

In den folgenden Kapiteln werden die einzelnen Blockchain-Basistechnologien kurz erläutert, um ein Grundverständnis über die Funktionsweise und Komponenten einer Blockchain zu erzeugen.

2.1 Distributed-Ledger-Technologie

Die zentrale Basis einer Blockchain bildet die Distributed-Ledger-Technologie (DLT), welche als eine Art „verteiltes Kontobuch“ verstanden werden kann.

Distributed-Ledger beschreibt eine Technik der verteilten Datenhaltung in Peer-to-Peer-Netzwerken, bei der die Netzwerkknoten durch einen Konsens gemeinsam über die Datenaktualisierung entscheiden. Bei den Daten kann es sich beispielsweise um Kontostände einer Kryptowährung handeln. [7]

Dieses Peer-to-Peer-Netzwerk (P2P-Netzwerk) basiert auf mehreren, unabhängigen Parteien oder Knoten (Nodes). Jeder dieser Knoten verfügt zu jedem Zeitpunkt über eine exakte Kopie des Ledgers, das alle Transaktionsaufzeichnungen mit Zeitstempeln, die aus den zugrunde liegenden Blockchain-Knoten bestehen, beinhaltet. Für die Änderung eines bestehenden Datensatzes muss ein großer Teil der Blockchain-Netzwerkteilnehmer gleichzeitig der Änderung dieser Informationen zustimmen. Die Folge ist, dass, sobald ein Knoten Informationen in der Blockchain-Datenbank speichert, es nahezu unmöglich ist, diese Informationen wieder zu entfernen. [8]

Zwar setzen Blockchains DLT ein, jedoch ist nicht jeder DLT auch immer eine Blockchain.

Sofern die verteilte Datenhaltung in Form einer Kette vorliegt, bei der nicht verwandte Transaktionen zu einzelnen Blöcken zusammengefasst werden, die wiederum mit Hashes verkettet sind, handelt es sich um eine Blockchain. Somit kann die Blockchain als eine Variante eines Distributed-Ledger angesehen werden. [9]

Diese Art der dezentralen Datenbankarchitektur kann somit von den klassischen zentralen Architekturen unterschieden werden, da durch den beschriebenen P2P-Netzwerkansatz und dem integrierten Konsens-Mechanismus keine übergeordneten Verwalter oder zentrale Datenspeicher wie bei Client-Server Architekturen benötigt werden.

2.1.1 Konsens-Mechanismus

Da es aufgrund der beschriebenen dezentralen Datenbankarchitektur keinen zentralen Entscheidungsträger gibt, muss das P2P-Netzwerk eine Instanz integrieren, die benötige Entscheidungen herbeiführen kann. Diese Instanz nennt sich Konsens-Mechanismus. Es gibt eine Vielzahl von Konsens-Mechanismen, wovon die wichtigsten drei Konsens-Mechanismen anbei zusammengefasst vorgestellt werden [10]:

Proof-of-Work (PoW) ist das älteste Konsensverfahren. Hier wird der Konsens durch Rechenkraft erzeugt, indem die Teilnehmer eine komplexe Rechenaufgabe vorgelegt bekommen, die sie mithilfe von Hardware lösen müssen. Für den Einsatz an Ressourcen (Hardware und Energie) bekommen diese eine Vergütung. Die bekannten Blockchains, die auf PoW basieren, sind u.a. Bitcoin, Ethereum und Monero.

Proof-of-Stake (PoS) ist nach PoW der wohl am häufigsten eingesetzte Konsensmechanismus. PoW steht für den Anteilsnachweis, weil hier der Konsens durch das bereitgestellte Vermögen (Stake) und der Dauer der Bereitstellung erzielt. PoS wurde im Jahre 2012 als Antwort auf Bitcoins hohen Energieverbrauch herausgebracht. Aus der Sicherheitsperspektive erscheint PoS besser als PoW, da kein Mining erfolgt und es somit nicht möglich ist, das Netzwerk durch schiere Rechenkraft zu manipulieren. Angreifer müssten bei PoS über die Hälfte der zirkulierenden Coins erwerben. Bekannte Blockchains, die auf PoS basieren sind Solana und Avalanche.

Delegated Proof-of-Stake (DPoS) ist eine Weiterentwicklung von Proof-of-Stake. Hierbei werden Delegierte demokratisch gewählt, die für ausgewählte Aufgaben im Netzwerk wie die Validierung von Blöcken und Statusbestätigungen

der Blockchain zuständig sind. Die Stimmrechte der Wähler werden nach der Anzahl an Token gewichtet. Bekannte Blockchains, die auf DPoS basieren sind Cardano, Cosmos, EOS oder TRON.

Der verteilte Konsens-Mechanismus wird bei Kryptowährungen wie Bitcoin über den Mining Prozess abgebildet. Dieser wird verwendet, um ausstehende Transaktionen durch deren Aufnahme in die Blockchain zu bestätigen. Mining erzwingt eine chronologische Reihenfolge der Blockchain, schützt die Neutralität des Netzwerks und sorgt dafür, dass sich die verschiedenen Computer über den Status des Systems einig sind. Um bestätigt zu werden, müssen Transaktionen in einen Block eingefügt werden. [11]

2.1.2 Block

Ein elementarer Bestandteil jeder Blockchain sind die darin enthaltenen Blöcke. In den Blöcken sind alle Transaktionen verzeichnet. Dabei bezieht sich ein Block auf eine Reihe von Bitcoin-Transaktionen einer bestimmten Zeitspanne. Die Blöcke werden so übereinandergestapelt, dass ein Block vom anderen abhängt. Auf diese Weise entsteht eine Kette von Blöcken, eine sog. Blockchain. [12]

Die folgende Darstellung erläutert den Aufbau der jeweiligen Blöcke und deren Abhängigkeiten zueinander.

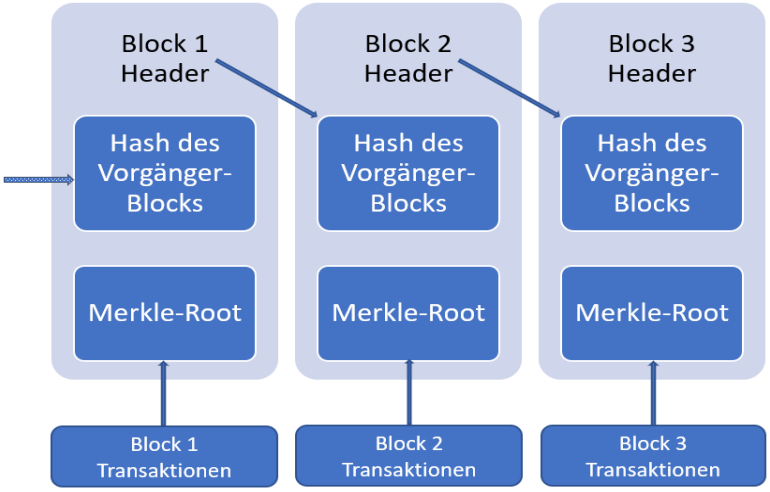


Bild 1: Vereinfachte Darstellung der Bitcoin-Blockchain in Anlehnung an Nakamoto [13]

Das vorangegangene Bild 1 zeigt am Beispiel der Kryptowährung Bitcoin eine vereinfachte Darstellung einer Blockchain. Dabei wird ein Block mit einer oder mehreren neuen Transaktionen im Transaktionsdatenteil eines Blocks gesammelt. Kopien jeder Transaktion werden gehasht, und die Hashes werden dann gepaart, gehasht, wieder gepaart und wieder gehasht, bis ein einziger Hash übrigbleibt, die sog. Merkle-Root eines Merkle-Trees. Die Merkle-Root wird im Block Header gespeichert. Jeder Block speichert auch den Hash des vorherigen Blocks, wodurch die Blöcke miteinander verkettet werden. Auf diese Weise wird sichergestellt, dass eine Transaktion nicht geändert werden kann, ohne den Block, der sie aufzeichnet, und alle folgenden Blöcke zu ändern. Auch Transaktionen sind miteinander verkettet. Für den Nutzer wird der Eindruck erweckt, dass Bitcoins von und zu den Wallets gesendet werden, aber Bitcoins bewegen sich tatsächlich von Transaktion zu Transaktion. Jede Transaktion gibt die Bitcoins aus, die zuvor in einer oder mehreren früheren Transaktionen erhalten wurden, so dass die Eingabe einer Transaktion die Ausgabe einer früheren Transaktion ist. [14]

Der oben eingeführte Begriff des Hashing wird im Kapitel 2.2 näher erläutert. Auf das Element der Transaktionen wird im folgenden Kapitel genauer eingegangen.

2.1.3 Transaktionen

Das zentrale Element, im Sinne von Zahlungsflüssen bei Kryptowährungen, stellt in der Blockchain die Transaktion dar. Eine Transaktion verbrieft in der Blockchain die Verfügungsmöglichkeit einer Entität auf die zugrundeliegenden Vermögensgegenstände.

In dem ursprünglichen Konzept von Satoshi Nakamoto, dem Erfinder des Bitcoins, wird dabei eine elektronische Münze (Bitcoin) als eine Kette digitaler Signaturen definiert. D.h. jeder Besitzer überträgt dessen Bitcoin auf den nächsten, indem er einen Hash der vorherigen Transaktion und den öffentlichen Schlüssel des nächsten Besitzers digital signiert und an das Ende der Münze anhängt. Ein Zahlungsempfänger kann die Signaturen überprüfen, um die Kette der Eigentümerschaft zu verifizieren. [13]

Das Konzept lässt erkennen, dass durch die Verkettung der Transaktionen, in Verbindung mit der Signatur anhand öffentlicher Schlüssel, vorherige sowie aktuelle Eigentumsverhältnisse in der Blockchain persistent dokumentiert werden. Am Beispiel der Kryptowährung Bitcoin kann eine Transaktion wie folgt beschrieben werden.

„Eine Transaktion ist der Transfer eines Betrages zwischen Bitcoin-Wallets, der in die Blockchain eingetragen wird. Bitcoin-Wallets enthalten einen geheimen Datenblock der Privater Schlüssel oder Seed genannt wird. Er wird verwendet, um Transaktionen zu signieren, wodurch der mathematische Beweis erbracht wird, dass sie vom Eigentümer der Wallet kommen. Die Signatur verhindert auch, dass Transaktionen nach dem Senden von jemandem modifiziert werden können. Alle Transaktionen werden über das Netzwerk verbreitet und innerhalb von 10-20 Minuten beginnt die Bestätigung durch das Netzwerk mit Hilfe eines Prozesses der Mining genannt wird.“ [11]

Für die IT-forensische Betrachtung ist die Transaktion von großer Bedeutung, denn die Transaktion enthält wichtige Informationen, um Zahlungsflüsse nachvollziehen zu können.

2.1.4 Mining

Zur Aufrechterhaltung der Blockchain bildet das sogenannte Mining die technische Grundlage. Während des Mining Prozesses geht es um das Lösen komplexer mathematischer Aufgaben, mit denen die Transaktionen innerhalb eines Zahlungssystems verifiziert werden. Das Mining ist somit als Basis für das Bitcoin-Ökosystem und andere Kryptowährungen zu verstehen. Dabei ist das übergeordnete Ziel die Suche nach einem Hash. Hierbei handelt es sich um eine passende Kombination aus Transaktionsdaten und Informationen zum jeweiligen Block. Dieser Vorgang erfordert eine große Anzahl an Versuchen und komplexe Kalkulationen. Sind die Informationen perfekt verknüpft, wird der Hash als fertiger Block an die Blockchain angehängt. [15]

Durch die ansteigende Komplexität bei der Berechnung neuer Hashes steigt auch die benötigte Rechenleistung. Eine Reaktion ist, dass entsprechende

Mining-Farmen an Orte abwandern, in denen die Stromkosten möglichst gering sind. Zu den Ländern mit den weltweit höchsten Miningvolumen zählten im Januar 2022 die USA mit 37.84%, China mit 21.11% und Kasachstan mit 13.22%. [16]

Aus Perspektive der IT-Sicherheit sind Mining-Trojaner wie beispielsweise Trojan.Tofsee zu erwähnen, die als Malware im Hintergrund die Rechenleistung der befallenen Rechner kapern, um damit auf Kosten eines Dritten Gewinne durch verdecktes Mining zu erwirtschaften.

2.2 Kryptografie

Bezogen auf die Kryptowährung Bitcoin sind die Informationen, die innerhalb der Bitcoin-Blockchain verschlüsselt werden müssen, die Transaktionsinformationen. [17]

Als weiteres Anwendungsgebiet kann die Kryptographie im Zusammenhang mit Kryptowährungen auch zur Sicherung von Wallets angeführt werden, indem der Zugriff auf die jeweiligen Assets durch einen Passwortschutz realisiert wird. Dies ist allerdings kein spezifischer Aspekt einer Blockchain, weshalb dies an dieser Stelle nicht weiter vertieft wird.

Um die Transaktionsinformationen vor Manipulationen zu schützen, werden die folgenden kryptografische Methoden eingesetzt.

Hashing

Das National Institute of Standards and Technology (NIST) definiert Hashing als „den Prozess der Anwendung eines mathematischen Algorithmus auf Daten, um einen numerischen Wert zu erzeugen, der für diese Daten repräsentativ ist.“ [18]

Dabei sind Hashing-Methoden deutlich von den Methoden zur Verschlüsselung von Informationen abzugrenzen. Denn im Gegensatz zur Verschlüsselung, die rückgängig gemacht werden kann, ist Hashing eine Einbahnstraße. Der Output einer Hashfunktion ist ein Gebilde aus verschiedenen Zeichen mit fixer Länge - der Hashwert. [19]

Im Falle einer Bitcoin-Transaktion wird diese von den Bitcoin-Knoten im ersten Schritt erkannt. Nur wenn mehrere Knoten zu der Entscheidung kommen, dass diese Transaktion korrekt ausgeführt und alle Regeln befolgt wurden, integrieren die Knoten-Operatoren diese Transaktion in einen Hash-Block und damit in die Blockchain. Derselbe Mechanismus gilt auch für die Blöcke selbst. Der Hash-Wert eines Blocks zeigt, ob die Daten einer früheren Transaktion manipuliert wurden oder bereits in einem früheren Block enthalten waren. In beiden Fällen werden alle anderen Blockchain-Knoten diese manipulierten Blöcke ignorieren, da eine Manipulation identifiziert wurde. [8]

Signaturen

Während einer Transaktion wird die Verfügungsmöglichkeit über das Guthaben von einem Teilnehmer zum anderen übertragen. Eine solche Übertragung wird durch eine kryptografisch signierte Transaktion in der Blockchain dokumentiert. Die Verifizierung dieser Transaktionen (Signaturprüfung) übernehmen die im Netzwerk befindlichen Rechner. Nur Teilnehmer, die einen passenden geheimen Signaturschlüssel besitzen, können gültige Transaktionen einstellen und damit über das dahinterstehende Guthaben verfügen. Die notwendigen Schlüssel speichert man in einer digitalen Geldbörse (Wallet). Empfänger von Transaktionen werden dabei durch eine abstrakte Adresse ähnlich einer Kontonummer repräsentiert, sodass Kryptowährungen idealerweise pseudonym verwendet werden können. [20]

3 Einsatz von Open Source Intelligence

Open Source Intelligence (OSINT) ist aktuell im Fokus der Fachpresse bei der diese oft in Verbindung mit IT-Sicherheitsvorfällen in Erscheinung tritt. In einem Bericht der Computerwoche im März 2022 soll der Leser aufgerüttelt werden „Hacker nutzen Open Source Intelligence, um Systeme zu kompromittieren. Sie können OSINT Tools nutzen, um herauszufinden, welche Ihrer Informationen offenliegen.“ [21]

OSINT ist jedoch keineswegs eine neue Methodik der Informationsgewinnung, sondern wird in der nachrichtendienstlichen Aufklärung seit vielen Jahrzenten eingesetzt.

OSINT ist ein Zweig der Nachrichtendienste, der Informationen über Personen oder Organisationen aus öffentlich zugänglichen Quellen analysiert. Großbritannien und die Vereinigten Staaten nutzten OSINT aktiv während des Zweiten Weltkriegs, wobei Spezialeinheiten feindliche Sendungen überwachten. Heute wird die OSINT-Methodik nicht nur in der Außenpolitik, sondern auch in der Informationssicherheit eingesetzt. [22]

Aus dem polizeilichen Kontext wird OSINT bezeichnet als die Erkenntnisgewinnung zu einem bestimmten Sachverhalt aus frei verfügbaren, offenen Quellen. [23]

Es ist daher offensichtlich, dass OSINT in unserer digitalisierten und vernetzen Welt immer mehr an Bedeutung gewinnt, denn jede Nutzung von digitalen Diensten wie Webseiten, Sozialen Medien und auch Kryptowährungen hinterlässt digitale Spuren.

Für diese Arbeit wurde der Fokus der OSINT-Tools auf verschiedene Blockchain-Explorer gelegt, da diese Einblicke in Transaktionen von Kryptowährungen geben können.

3.1 Webbasierte Blockchain-Explorer

Für die Untersuchung der Zahlungsflüsse von Kryptowährungen sind Blockchain-Explorer ein Hauptelement da diese die Transaktionen einsehbar machen. In einer Publikation der NIST (National Institute of Standards and Technology) wird ein Blockchain-Explorer wie folgt beschrieben:

„Ein Blockchain-Explorer, oder Netzwerkmonitor, ist eine Software, mit der Benutzer Blöcke und Transaktionen durchsuchen und visualisieren können und Metriken zur Netzwerkaktivität liefert, wie z. B. die durchschnittlichen Transaktionsgebühren, Hash-Raten, Blockgröße und Block Difficulty.“ [24]

Aus Sicht des Benutzers gibt es verschiedene Arten von Blockchain-Explorer, diese können dabei in webbasierte oder clientbasierte Blockchain-Explorer unterteilt werden. Die in der untenstehenden Tabelle 1 aufgeführten Anbieter arbeiten teils kommerziell und sind daher primär gewinnorientiert. Sie bieten aber auch kostenfreie Möglichkeiten an, um mit Blockchain-Explorer-Funktionen unterschiedliche Kryptowährungen nach Transaktionen zu untersuchen.

Tabelle 1: Übersicht webbasierter Blockchain-Explorer

Anbieter	URL	Frei nutzbar	API	Downloads
blockchain.com	https://www.blockchain.com	ja	ja	nein
BLOCKCHAIR.com	https://blockchair.com	ja	ja	Datenbank-Dumps, 10 kB/s Download-Rate
Blockstream-Explorer	https://blockstream.info	ja	ja	nein
OXT.me	https://oxt.me	ja	nein	ja, begrenzt auf Bitcoin-Transaktions-Statistiken
WalletExplorer.com	https://www.walletexplorer.com	ja	ja	CSV-Dateien von Transaktionen verfügbar

Die Grundfunktionen der einzelnen webbasierten Blockchain-Explorer ähneln sich, jedoch gibt es Unterschiede bei den unterstützten Blockchains. Die Dienste werden mit den unten aufgeführten Grundfunktionen kostenfrei zur Verfügung gestellt und sind innerhalb der in dieser Arbeit aufgeführten Explorer mit Ausnahme des WalletExplorer.com Teil eines weiteren, kommerziellen Angebots.

Überblick der Grundfunktionen

- Suche nach Transaktionen
- Suche nach Adressen, teilweise auch Wallets
- Suche nach Blöcken

Die Motivationen der kommerziellen Anbieter, diese Dienste kostenfrei anzubieten, können sein, möglichst viel Traffic auf den Webseiten zu generieren, um bspw. bessere Suchmaschinen-Rankings zu bekommen. Die Anbieter geben sich mit dieser Art der Informationsbereitstellung dazu als transparent aus.

Besonders zu erwähnen ist BLOCKCHAIR, die als einziger Blockchain-Explorer auch Datenbank-Dumps zum Download anbietet. Dies erfolgt kostenfrei, jedoch ist die Download-Geschwindigkeit auf 10 kB/s begrenzt. Für Organisationen und Bildungseinrichtungen wird eine Kontaktmöglichkeit angeboten und damit auch schnellere Download-Geschwindigkeiten in den Raum gestellt. [25]

3.2 OSINT-Tools zur Transaktionsanalyse von Kryptowährungen

Neben den webbasierten Blockchain-Explorern werden vergleichbare Funktionen auch durch Client-Applikationen bzw. deren Module bereitgestellt.

Dabei sind meist kommerzielle Angebote zu finden; einzelne Anbieter wie bspw. Maltego bieten aber auch frei nutzbare Module für die Blockchain-Analyse an. [26]

In der folgenden Tabelle 2 findet sich eine Übersicht über die für diese Arbeit recherchierten Produkte.

Tabelle 2: Übersicht clientbasierter Tools zur Analyse von Kryptowährungs-Transaktionen

Anbieter	Produkt	Nutzung	Beschreibung
Maltego	Maltego CE	teils frei nutzbar	Maltego CE Software für die Analyse von Krypto-währungstransaktionen Tatum Blockchain-Entwicklungs-plattform deren Blockchain-Daten innerhalb eines Moduls von Maltego CE verfügbar gemacht werden können
Chainalysis	Reactor	kommerziell	Software für die Analyse von Kryptowährungs-Transaktionen
Elliptic	Elliptic Investigator	kommerziell	Software für die Analyse Kryptowährungs-Transaktionen

Im weiteren Verlauf dieser Arbeit wurde eine OSINT-Analyse mit Maltego CE und dem Modul Tatum durchgeführt, die Ergebnisse finden sich in Kapitel 8.5.

Maltego Desktop Client

Der Maltego Desktop Client bietet je nach Lizenzmodell verschiedene Möglichkeiten, Datenquellen einzubinden und diese in eine übergreifende Visualisierung zu bringen. Maltego ist Anbieter der Produkte Maltego One, Maltego CE und CaseFile. Maltego One bietet die volle Funktionalität und die Möglichkeit, eigene Datenquellen und weitere kommerzielle Dienste anzubinden.

Maltego CE bietet als sog. Community Edition (CE) einen freien Zugang zu einer limitierten Anzahl an Diensten und Funktionen an. CaseFile ist eine Lösung, die sich an rein kommerzielle Anbieter richtet und augenscheinlich nicht mehr sehr stark im Fokus von der Produktpalette von Maltego liegt. [27]

Im folgenden Bild 2 werden die unterschiedlichen Funktionsumfänge seitens Maltego dargestellt.

Product Features	Maltego One	Maltego CE	CaseFile
Commercial Use	✓	–	✓
Access to commercial Transform Hub	✓	–	–
Integration of own data	✓	–	–
Standard Transforms	✓	✓	–
Max number of results per Transform	64,000	12	N/A
Max number of Entities on a graph	1,000,000	10,000	1,000,000
Technical support	✓	–	–
Graph Export (CSV, XLS, XLSX, PDF and Image formats)	✓	✓	✓
Graph Import (CSV, XLS, XLSX)	✓	✓	✓
Shared Graph Sessions (Collaboration)	✓	✓	✓
Machines (Transform Macros)	✓	✓	N/A
Collection Nodes	✓	✓	✓

Bild 2: Übersicht über Maltego Lizenzen und Funktionen [27]

Chainalysis Reactor

Für das Produkt Reactor von Chainalysis wurde eine Preisrecherche betrieben, da seitens des Unternehmens keine offizielle Preisliste veröffentlicht wurde. Für ein von der Chainalysis Academy zertifiziertes Zweitagestraining werden pro Person 999 $ fällig. Kursteilnehmer bekommen mit der Teilnahme auch die Möglichkeit, für ein Jahr eine aktive Reactor Lizenz zu nutzen. Weitere Lizenzinformationen, die unabhängig von dem angebotenen Training sind, konnten nicht recherchiert werden. [28]

Elliptic Investigator

Elliptic Forensics bietet den Elliptic Investigator an, eine Softwarelösung zur Ermittlung von Kryptowährungs-Transaktionen durch Visualisierung und Offenlegung der Wallets und Transaktionsdaten. Es werden von Elliptic Forensics auch Trainingsangebote an Einzelpersonen und Institutionen offeriert. Preise zu den Trainingsangeboten und Lizenzen waren zum Zeitpunkt der Recherche nicht öffentlich einsehbar. [29]

Das folgende Bild 3 zeigt exemplarisch eine Darstellung des Elliptic Investigator.

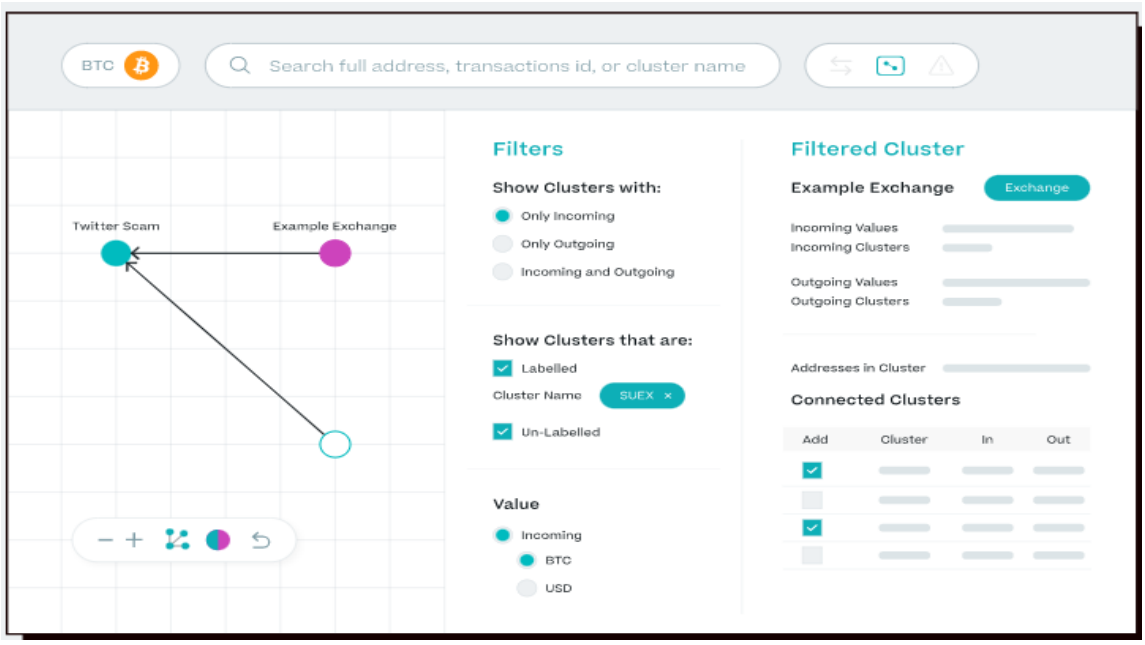


Bild 3: Screenshot Elliptic Investigator [29]

Zusammengefasst kann gesagt werden, dass sich die betrachteten Anbieter Chainalysis, Eliptic Forensics sowie Maltego mit dem offenen Zugang zu umfänglichen Preis- und Leistungsbestandteilen eher bedeckt halten.

Potentiellen Kunden wie Unternehmen, Behörden und Institutionen werden von allen Anbietern Demo-Sessions angeboten, diese stehen aber einer Einzelperson in dieser Form nicht zur Verfügung.

4 Subjekte und Objekte einer Transaktion

Jede Kryptowährungs-Transaktion besteht aus unterschiedlichen Subjekten und Objekten. Die Subjekte, die in den End-2-End Szenarien ab Kapitel 5 eine Rolle spielen, werden im folgenden Kapitel eingeführt und kurz beschrieben. Zusätzlich werden auch die Objekte beschrieben, die in Form von digitalen Artefakten während der nachfolgenden Datenauswertung ab Kapitel 7 zu erwarten sind.

4.1 Subjekte

Unter den Subjekten sind jeweils die handelnden Akteure gemeint, die im Rahmen einer Kryptowährungs-Transaktion in Erscheinung treten können.

4.1.1 Angreifer

Der Angreifer agiert als Täter und versucht u.a. mit Methoden des Datendiebstahls oder mit schadhafter Verschlüsselung (Ransomware), das Opfer unter Druck zu setzen, um von diesem eine Zahlung in Form einer Kryptowährung zu erhalten. Der Angreifer ist somit der Zahlungs-Empfänger der Kryptowährung.

4.1.2 Opfer

Die Opfer leisten unter dem durch den Angreifer erzeugten Druck die erpressten Zahlungsbeträge. Die Opfer treten somit als Sender der Zahlung auf.

4.1.3 Verkäufer

Die Verkäufer bieten u.a. auf Plattformen im Darknet aber auch in frei zugänglichen Kleinanzeigenportalen Waren und Dienstleistungen mit zweifelhaftem oder illegalem Inhalt an. Die Verkäufer sind somit die Empfänger der Zahlungen.

4.1.4 Kunden

Die Kunden bezahlen Waren oder Dienstleistungen, sind zugleich Täter und/oder Opfer, da die illegalen Waren und Dienstleistungen seitens der Verkäufer nicht immer ausgeliefert werden. Betrogene Kunden können schwerlich ihre Rechte geltend machen, da sich diese selbst belasten würden. Die Kunden treten somit als Sender der Zahlungen auf.

4.2 Objekte

4.2.1 Transaktionen

Wie in Kapitel 2.1.3 beschrieben, sind Transaktionen ein elementarer Bestandteil einer aktiv genutzten Blockchain. In Bezug zu Blockchain-basierten Kryptowährungen verbinden die Transaktionen u.a. die Sender- und die Empfängeradresse in einem persistenten Datenobjekt mit einem eindeutigen Hashwert. In folgendem Bild 4 wird die Bitcoin-Transaktion f523ee99eb30818c8f70de0af447c9fb4e5564a06901b4ff4bc00294c4a0c63b im Blockstream-Explorer dargestellt. Dabei wurden der zugehörige Block, Timestamp und Status der anderen Block-Bestätigungen mit ausgegeben.

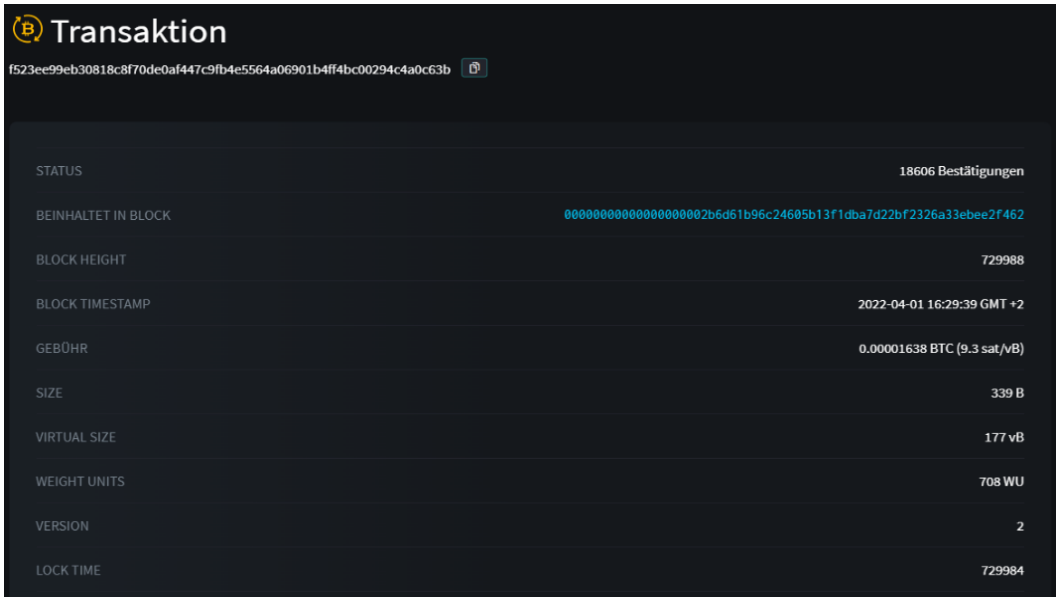


Bild 4: Anzeige einer Bitcoin-Transaktion im Explorer von Blockstream.info [30]

Aus Sicht eines Ermittlers ist von besonderem Interesse, woher die Vermögenswerte stammen und wohin sie weiter transferiert wurden. In folgendem Bild 5 kann im Blockchain-Explorer von Blockchain.com auf Basis der zuvor ausgewählten Beispieltransaktion die Sender- und Empfängeradresse der Transaktion ermittelt werden.

Bild 5: Bitcoin-Adressen einer Transaktion im Explorer Blockchain.com [31]

Die Daten aus Bild 5 werden im Folgenden interpretiert, innerhalb der Transaktion mit dem folgenden Hashwert:

f523ee99eb30818c8f70de0af447c9fb4e5564a06901b4ff4bc00294c4a0c63b

wurde über den Betrag von 0.00024820 BTC die Verfügungsmöglichkeit von der Adresse bc1qf7xwsppfw2quywwfafj0tcergzq3l4l0wygat6 an die Adresse bc1q34hcaqa95lchs5f4nkrk0vsrwvnx8vwmku9r6r übertragen.

An dieser Stelle wird deutlich, dass in Bezug zu den Zahlungsflüssen keineswegs ein vollständig anonymes Zahlungssystem vorliegt, sondern es sich vielmehr um ein pseudonymisiert geführtes Kontenbuch handelt, welches sich mithilfe von OSINT-Methoden auswerten lässt.

4.2.2 Wallets für Kryptowährungen

Als digitale Geldbörse dient das Wallet dazu, den Zugriff auf Vermögenswerte, die über die Blockchain verbrieft werden, an einem möglichst sicheren Ort zu verwahren.

Über Wallets können Besitzer von Kryptowährungen auf ihre Bestände zugreifen, sowie Kryptowährungen senden und empfangen. Die für Transaktionen benötigten Private und Public Keys werden im Wallet gespeichert. Dabei gibt es unterschiedliche Arten von Wallets, sowohl als physisches Medium, eine

Hardware (Gerät) oder Software (Programm, Dienst). Die Kryptowährungen selbst befinden sich nicht im Wallet, das Wallet interagiert mit der Blockchain in der sich die Währung befindet. [32]

Innerhalb der vorliegenden Arbeit wurden das Software-Wallet Electrum, das Hardware-Wallet Ledger Nano S sowie die Webdienst-basierten Anbieter Binance und Coinbase eingesetzt. Dabei wurden in den genutzten Wallets teils mehrere Bitcoin-Adressen generiert und für die Transaktionen genutzt.

4.2.3 Bitcoin Wallet-Adressen

Am Beispiel von Bitcoin ist eine Wallet-Adresse eine öffentliche, individuelle Zeichenkette zur eindeutigen Identifizierung eines Bitcoin Wallets.

Die Bitcoin Wallet-Adresse ist vergleichbar mit der IBAN beim klassischen Banking. Die Bitcoin Adresse ist notwendig, um Zahlungen empfangen zu können. Die Basis für die Bitcoin-Adresse ist der öffentliche Schlüssel, aus dem das Wallet mithilfe kryptografischer Verfahren die Adresse generiert. Am Ende der kryptografischen Vorgänge entsteht ein Hash im Hexadezimalformat, der noch einmal in das Base58-Format mit Großbuchstaben, Kleinbuchstaben und Ziffern konvertiert und so vereinfacht wird. [33]

Im Rahmen dieser Arbeit wurden verschiedenste Adressen genutzt und erzeugt, beispielhaft findet sich wie folgt eine generierte Bitcoin-Adresse im Pay-to-Witness-Public-Key-Hash (P2WPKH) Format:

bc1q34hcaqa95lchs5f4nkrk0vsrwvnx8vwmku9r6r

Neben dem oben dargestellten P2WPKH Format gibt es eine Reihe weiterer, teils historischer bedingter, teils zukünftiger Adressformate, die von Relevanz sind.

Im Folgenden werden die verschiedenen Arten von Bitcoin-Adressen zusammengefasst [34]:

Pay-to-PubKey-Hash (P2PKH) sind Legacy-Adressen, die mit der Zahl 1 beginnen. Eine Legacy-Adresse ist der Hash des öffentlichen Schlüssels zu seinem privaten Schlüssel. Als Bitcoin im Jahr 2009 eingeführt wurde, war dies

die einzige Möglichkeit, eine Adresse zu erstellen. Heute verbraucht sie den meisten Platz in einer Transaktion und ist daher der teuerste Adresstyp.

Pay-to-Script-Hash (P2SH) sind Adressen, die mit der Zahl 3 beginnen. Im Gegensatz zu Legacy-Adressen handelt es sich bei Pay-to-Script-Hash-Adressen nicht um den Hash des öffentlichen Schlüssels, sondern von einem Script, der bestimmte Ausgabebedingungen beinhaltet, die dem Absender zunächst verborgen bleiben.

Pay-to-Witness-Public-Key-Hash (P2WPKH) sind Adressen, die mit bc1q beginnen. Dieser Adresstyp reduziert die Menge der in der Transaktion gespeicherten Informationen noch weiter, da die Signatur und das Skript nicht in der Transaktion, sondern im sog. Witness gespeichert werden.

Pay-to-Taproot (P2TR) beginnen mit bc1p und werden noch nicht verwendet. Im November 2022 soll das Bitcoin-Netzwerk die Taproot-Softfork durchführen. Diese wird viele neue Smart-Contract-Funktionen für Bitcoin-Adressen ermöglichen und die Privatsphäre beim Ausgeben solcher Transaktionen erhöhen.

In der vorliegenden Arbeit wurden primär mit dem aktuellen Standard P2WPKH Transaktionen erzeugt, da sich dieser neben seiner Aktualität auch kostenseitig als praktikabler Standard darstellte.

5 Definition von End-2-End Szenarien und Testfällen

5.1 Definition realitätsnaher Szenarien

Die Auswahl realitätsnaher Szenarien orientierte sich an aktuellen Bedrohungslagen und den derzeit auftretenden illegalen Handlungen, bei denen im Verlauf Zahlungstransaktionen mit Kryptowährungen durchgeführt wurden.

Jedes Szenario wurde zuerst mit dessen Relevanz erläutert und anhand einer spezifischen Charakteristik, bestehend aus IT-forensischen und Kryptowährungs-spezifischen Merkmalen, weiter charakterisiert.

5.1.1 Szenario 1: Handel mit illegalen Waren und Dienstleistungen

Der Handel mit illegalen Waren wird meist auf virtuellen Marktplätzen u.a. im Darknet (Tor-Netzwerk) durchgeführt. Zuletzt konnte das BKA im April 2022 einen bedeutenden Schlag gegen einen illegalen, virtuellen Marktplatz vermelden.

„Hydra Market dürfte nach Einschätzung von ZIT und BKA der umsatzstärkste illegale Marktplatz weltweit gewesen sein. Dessen Umsätze beliefen sich alleine im Jahr 2020 auf mindestens 1,23 Mrd. Euro. Insbesondere durch den von der Plattform bereitgestellten „Bitcoin Bank Mixer“, einen Dienst zur Verschleierung digitaler Transaktionen, wurden Kryptoermittlungen für Strafverfolgungsbehörden immens erschwert.“ [35, S. 1]

Auf diesen illegalen Marktplätzen werden von anonym auftretenden Anbietern alle erdenklichen Arten illegaler Waren und Dienstleistungen angeboten. Die Verfolgung der Anwender gestaltet sich auch dadurch schwierig, dass durch die Nutzung von Kryptowährungen und der Nutzung des Tor-Netzwerks Spuren verwischt werden.

Charakteristik – Szenario S1

Akteure:

- Anbieter (Empfänger der Zahlung)
- Kunde (Sender der Zahlung)

Potentielle IT-forensische Artefakte:

- Websuchen mit Internet-Browser
- Aufruf von spezifischen Webseiten
- Spuren von Wallets für Kryptowährungen
- Kryptowährungs-Objekte:
  - Empfängeradresse
  - Senderadresse
  - Transaktion
  - Zahlungsbeträge

Das dargestellte Szenario S1 wurde im weiteren Verlauf der Arbeit im Testfall T1 abgebildet.

5.1.2 Szenario 2: Ransomware und Erpressung

Für diese Charakteristik standen Transaktionen, die im Kontext zu Ransomware-Attacken ausgeführt wurden im Fokus. Für das Jahr 2021 konnten Ransomware-Zahlungen in Höhe von 692 Millionen US-Dollar von Chainalysis identifiziert werden. Das ist fast das Doppelte des Betrags des Vorjahres. [vgl. 1, S. 39]

Durch dieses immense Wachstum an Ransomware-Attacken innerhalb eines Jahres ist auch davon auszugehen, dass die Dunkelziffer weitaus höher ist.

Für die Analyse dieses Szenarios wurden zwei Handlungsstränge verfolgt:

1) Simulation eines typischen Kommunikationsverlaufs zwischen Angreifer und Opfer mit der Erpressung eines Lösegelds und nachfolgend weitere Bezahlung durch das Opfer.

2) Recherche eines realen Ransomware-Falls zur weiteren Analyse auf der betreffenden Krypto-Blockchain mit OSINT-Tools.

Die beiden dargestellten Handlungsstränge wurden im weiteren Verlauf der Arbeit jeweils für Szenario S2.1 in den Testfällen T2 und T3 sowie für Szenario S2.2 im Testfall T4 innerhalb der vorliegenden Arbeit abgebildet.

Charakteristik – Szenario S2.1 – simulierter Kommunikationsverlauf

Akteure:

- Angreifer (Erpresser der Zahlung)
- Opfer (Sender der Zahlung)

Potentielle IT-forensische Artefakte:

- Websuchen mit Internet-Browser
- Aufruf von spezifischen Webseiten
- Spuren von Wallets für Kryptowährungen
- E-Mail-Adresse des Angreifers
- Kryptowährungs-Objekte:
  - Empfängeradresse
  - Senderadresse
  - Transaktion
  - Zahlungsbeträge

Das Szenario bildete einen simulierten Angriff auf ein Opfer durch einen Angreifer ab. Dabei wurden IT-forensische Artefakte beim Angreifer sowie dem Opfer erzeugt. Hierzu wurden je Akteur unterschiedliche virtuelle Maschinen generiert, um die Spuren je Akteur zu erfassen und diese nachfolgend auszuwerten.

Charakteristik – Szenario S2.2 – Analyse eines realen Falls

Akteure:

- Angreifer (Empfänger der Zahlung)
- Opfer (Sender der Zahlung)

Kryptowährungs-Objekte:

- Empfängeradresse
- Senderadresse
- Transaktion
- Zahlungsbeträge

IT-forensische Artefakte konnten aus diesem realen Fall naturgemäß nicht mehr betrachtet werden, jedoch sind die im Kommunikationsverlauf der in Testfall T2 und T3 simulierten Spuren, je nach Endgerätesituation der Akteure, durchaus denkbar.

Bei Recherchen nach einem realen Fall, bei dem mutmaßliche Erpresser mit einer Bitcoin-Adresse in Erscheinung getreten sind, konnte auf die Ergebnisse einer bestehenden Veröffentlichung aufgesetzt werden.

Der Akteur mit der Bitcoin-Adresse 12HaVrpXkLr2UnkMf6X9bY11cuNrZUdUnV ist hierbei mehrmals als Empfänger zweifelhafter Zahlungen in Erscheinung getreten. [36]

Für die weitere Untersuchung des realen Falls mithilfe von OSINT-Tools wurde daher der Akteur mit der folgenden real genutzten Bitcoin-Adresse angewendet:

12HaVrpXkLr2UnkMf6X9bY11cuNrZUdUnV

5.2 Definition der Testfälle basierend auf realitätsnahen Szenarien

Die folgenden Testfälle beschreiben die einzelnen Schritte der zuvor beschriebenen Szenarien im Detail. Hierbei wurden die zu untersuchenden Aktionen der jeweiligen Akteure aufgeführt und verwendete Komponenten (Betriebssystem, Software, Wallet) sowie das dafür erzeugte Image dokumentiert.

5.2.1 Testfallbeschreibung – T0

Der folgende Testfall T0 beschreibt den initialen Proof-of-Concept, der zur Untersuchung der generellen Machbarkeit dieser Arbeit vollzogen worden ist.

Tabelle 3: Testfallbeschreibung - T0

Use Case	Proof-of-Concept	
Akteur	Kunde	Anbieter
Aktionen	Der Kunde sendet an den Anbieter einen Betrag von 0.2 mBTC für die Bezahlung illegaler Waren. Die Bitcoin-Transaktion wird unter Verwendung von zwei eigenständigen Windows 10 VMs und Electrum Wallets durchgeführt. Die Electrum Wallets wurden nicht zusätzlich durch ein Passwort gesichert oder verschlüsselt.	
OS	Windows 10 Professional	Windows 10 Professional
Software	EDGE Browser	EDGE Browser
Wallet	Electrum	Electrum
Image	Windows10-Image-Klon-1	Windows10-Image-Klon-2

5.2.2 Testfallbeschreibung – T1

Der folgende Testfall T1 basierte auf dem in Kapitel 5.1.1 beschriebenen Szenario des Handels mit illegalen Waren und Dienstleistungen, bei dem eine Kryptowährung zwischen Kunde und Anbieter als Zahlungsmittel eingesetzt wurde.

Tabelle 4: Testfallbeschreibung - T1

Use Case	Szenario 1 - Handel mit illegalen Waren und Dienstleistungen	
Akteur	Kunde	Anbieter
Aktionen	1) Login in Coinbase 2) Erstellung einer Coinbase Wallet Extension 3) Anlage eines Coinbase Tresors 4) Zahlung von Bitcoin (Kaufpreis)	1) Web-Suche nach Electrum 2) Download Electrum von Webseite 3) Installation des Electrum Wallets 4) Erhalt von Bitcoin (Kaufpreis) 5) Weiterleitung der Guthaben an andere Bitcoin-Adressen
OS	Windows 10 Professional	Windows 10 Professional
Software	EDGE Browser Chrome Browser	EDGE Browser Chrome Browser
Wallet	Coinbase	Electrum
Image	Windows10_Klon03_mixed	Windows10_Klon03_mixed

5.2.3 Testfallbeschreibung – T2

Der folgende Testfall T2 basierte auf dem in Kapitel 5.1.2 beschriebenen Szenario Ransomware und Erpressung, in dem es zur Erpressung eines Opfers durch den Angreifer kam. Die Kommunikation des Erpressers erfolgte über E-Mail, in der eine Zahlung des Lösegeldes über eine Kryptowährung zu leisten war.

Tabelle 5: Testfallbeschreibung - T2

Use Case	Szenario 2.1 - Ransomware und Erpressung	
Akteur	Angreifer	Opfer
Aktionen	1) Infiziert das System des Opfers 2) Sendet E-Mail an Opfer 3) Erhält den geforderten Betrag	1) Erhält Meldung, dass das System infiltriert ist 2) Erhält E-Mail des Angreifers mit Informationen und Lösegeldforderung 3) Sendet das geforderte Lösegeld
OS	Windows 10 Professional	Windows 10 Professional
Software	Thunderbird E-Mail EDGE Browser Chrome Browser	Thunderbird E-Mail EDGE Browser Chrome Browser
Wallet	Electrum	Electrum
Image	Windows10_Klon05	Windows10_Klon04

5.2.4 Testfallbeschreibung – T3

Der folgende Testfall T2 basierte auf dem in Kapitel 5.1.2 beschriebenen Szenario Ransomware und Erpressung, in dem es zur Erpressung eines Opfers durch den Angreifer kam. Die Kommunikation des Erpressers erfolgt über E-Mail, in der eine Zahlung des Lösegeldes über eine Kryptowährung zu leisten war.

Bei T3 handelte es sich um die Erweiterung des Testfalls T2 um den Aspekt der Nutzung eines Apple IPhone SE Smartphone und der Binance App durch das Opfer.

Tabelle 6: Testfallbeschreibung - T3

Use Case	Szenario 2.1 - Ransomware und Erpressung	
Akteur	Angreifer	Opfer
Aktionen	1) Infiziert das System des Opfers 2) Sendet E-Mail an Opfer 3) Erhält den geforderten Betrag 4) Transferiert den Betrag weiter auf Ledger Nano S	1) Erhält Meldung, dass das System infiltriert ist 2) Erhält Nachricht des Angreifers mit Informationen und Lösegeldforderung 3) Sendet das geforderte Lösegeld
OS	Windows 10 Professional	Apple iOS
Software	EDGE Browser Chrome Browser	Safari Browser
Wallet	Electrum Ledger Nano S	Binance App
Image	Windows_Klon_05	iPhone SE - iOS (AXIOM)

5.2.5 Testfallbeschreibung – T4

Der folgende Testfall T4 basierte auf dem in Kapitel 5.1.2 beschriebenen Szenario Ransomware und Erpressung. Hierbei wurde ein realer Fall recherchiert, um diesen mit OSINT-Methoden weiter zu analysieren. Naturgemäß erfolgte in diesem Testfall keine IT-forensische Datenakquise, sondern es wurde auf einer bereits ermittelten Kryptowährungs-Adresse aufgesetzt.

Tabelle 7: Testfallbeschreibung - T4

Use Case	Szenario 2.2 - Ransomware und Erpressung – realer Fall	
Akteur	Angreifer	Ermittler
Aktionen	Nutzte die nachfolgende Bitcoin-Adresse, um von den Opfern Zahlungen zu erhalten: 12HaVrpXkLr2UnkMf 6X9bY11cuNrZUdUnV	Einsatz von OSINT-Tools, um Informationen über Bitcoin-Adresse und verbundene Transaktionen zu ermitteln
OSINT-Dienst	keine spezifische Nennung aus dem recherchierten Fall bekannt	WalletExplorer.com

6 Methoden und Tools für die IT-forensische Untersuchung

Die IT-forensische Untersuchung erfolgte in einem für diese Arbeit zusammengestellten IT-Forensik Laboraufbau. Dieses bestand aus einem physischen Hauptrechner, verschiedenen virtuellen Maschinen (VM), sowie unterschiedlichen mobilen Endgeräten wie einem Smartphone und einem Hardware Wallet. Für die Datenakquise und Datenanalyse der erzeugten Images wurden verschiedene Open-Source Tools (Autopsy, Bulk Extractor) eingesetzt. Daneben wurde auch das kommerzielle Produkt Magnet AXIOM zur Anwendung gebracht.

Für die Nachvollziehbarkeit der angewandten Methodiken sowie der erzeugten Ergebnisse dieser Arbeit, werden im Folgenden die eingesetzten Hardware- und Softwarekomponenten kurz eingeführt.

6.1 Übersicht eingesetzter Hardware

Forensik-PC

- CPU: AMD Ryzen 7 | 1700 Eight-Core Prozessor 3.00 GHz
- RAM: 16 GB
- Physikalischer Datenspeicher: 1 TB SSD und 1 TB HDD

Betriebssysteme:

- Windows 10 Pro | 21H2
- Ubuntu Linux | 20.04. LTS

Hardware Wallet: Ledger Nano S

Smartphone: IPhone SE | iOS 15.4.1

MacBook Air: macOS | Big Sur 11.6.7

6.2 Übersicht eingesetzter Software

Für die IT-forensische Auswertung der in den Testfällen erzeugten Spuren wurden verschiedene Open-Source sowie kommerzielle Software-Tools eingesetzt.

In der folgenden Tabelle 8 findet sich eine Übersicht der eingesetzten Software, deren Lizenz, Interface und Hauptfunktionen.

Tabelle 8: Übersicht eingesetzter Software mit deren Hauptfunktionen

Software	Lizenzmodell	Interface	Hauptfunktionen
Autopsy	Open-Source	GUI | CLI	IT-forensische Datenakquise- und Auswertung
AXIOM	kommerziell	GUI	IT-forensische Datenakquise- und Auswertung
Bulk Extractor	Open-Source	CLI	Scan von Image-Dateien auf deren Inhalt und strukturierte Ausgabe der Informationen in TXT-Dateien
Sleuth Kit	Open-Source	CLI	Befehlszeilentools zur Disk-Image Analyse und Datei-Wiederherstellung
Virtual Box	Open-Source	GUI | CLI	Virtualisierung von Systemen genutzt für Windows und Linux

In den folgenden Unterkapiteln werden die eingesetzten Software-Tools im Kontext zum Einsatzzweck im Wesentlichen beschrieben.

6.2.1 Virtual Box (Open-Source)

Der Einsatz der Virtualisierungslösung Virtual Box diente zwei Anwendungsbereichen innerhalb dieser Arbeit. Zum einen wurden in Virtual Box die einzelnen Windows 10 Images erzeugt, die für den Durchlauf der Szenarien-basierten Testfälle benötigt wurden. Des Weiteren wurde innerhalb einer virtuellen Maschine ein Linux Ubuntu 20.04. LTS betrieben, indem die Datenextraktion aus Image-Dateien über den Bulk Extraktor erfolgte.

Nach Prüfung der verschiedenen Image-Formate VMDK, VDI und VHD erfolgte der Aufsatz der virtuellen Maschinen im VMDK-Format, da dieses Format von allen drei genutzten Forensik-Anwendungen (Autopsy, AXIOM, Bulk Extraktor) direkt eingelesen werden kann.

Durch die Wahl des VMDK-Formats wurde eine nachträgliche Umwandlung der Image Dateien in das RAW-Format vermieden. Dies ist ein deutlicher Prozess- und Zeitvorteil gegenüber einer zusätzlichen Umwandlung der Image-Dateien in das RAW-Format, der sich als eine Erkenntnis aus dieser Arbeit weiter nutzen lässt.

Für alle definierten Testfälle wurden die erzeugten Spuren in einzelnen VMDK-Image-Dateien verfügbar gemacht.

6.2.2 Autopsy (Open-Source)

Innerhalb der verfügbaren Open-Source-Tools zählt Autopsy wohl zu den verbreitetsten Tools im Anwendungsgebiet der IT-Forensik.

„Autopsy ist eine Plattform für digitale Forensik und eine grafische Schnittstelle zu The Sleuth Kit und anderen Tools für die digitale Forensik.“ [37]

Autopsy wird als eine Windows-, sowie auch als Linux-Installation angeboten. In der vorliegenden Arbeit wurde die Windows-Version verwendet.

Autopsy bietet eine breite Palette von Funktionen an, wobei für eine Untersuchung mit Fokus auf Artefakte der Nutzung von Kryptowährungs-Diensten folgender Auszug aus der Liste aller Autopsy-Funktionen

herangezogen wurde [38]:

- Schlüsselwort-Suche: Mit den Modulen zur Textextraktion und Indexsuche können Dateien gefunden werden, in denen bestimmte Begriffe vorkommen sowie Muster mit regulären Ausdrücken ermitteln.
- Web-Artefakte: Extrahiert Webaktivitäten aus gängigen Browsern, um Benutzeraktivitäten zu identifizieren.
- Registry-Analyse: Verwendet RegRipper, um kürzlich verwendete Dokumente und USB-Geräte zu identifizieren.
- LNK-Datei-Analyse: Identifiziert Abkürzungen und Dokumente, auf die zugegriffen wurde.
- E-Mail-Analyse: Analysiert Nachrichten im MBOX-Format, z. B. mit Thunderbird.

6.2.3 Sleuth Kit (Open-Source)

Das Sleuth Kit ist ein Befehlszeilenprogramm für Linux welches in der vorliegen Arbeit über Terminal in einem Ubuntu Linux ausgeführt wurde. Der Sleuth Kit Anbieter definiert den Funktionsumfang wie folgt.

„The Sleuth Kit ist eine Sammlung von Befehlszeilentools und einer C-Bibliothek, die es ermöglicht, Disk-Images zu analysieren und Dateien daraus wiederherzustellen. Es wird im Hintergrund von Autopsy und vielen anderen Open-Source- und kommerziellen Forensik-Tools verwendet.“ [37]

Das Sleuth Kit bietet eine breite Palette von Funktionen an, wobei für eine Untersuchung mit Fokus auf Artefakten aus der Nutzung von Kryptowährungs-Diensten ausschließlich das Befehlszeilenprogramm Bulk Extractor angewendet wurde. Das Sleuth Kit unterliegt der Common Public License Version 1.0 und war daher als Open-Source Software für diese Arbeit kostenfrei nutzbar.

6.2.4 Bulk Extractor (Open-Source)

Als Teil des Sleuth Kit wurde das Befehlszeilenprogramm Bulk Extractor angewendet. Bulk Extractor ist ein Werkzeug für die digitale Forensik. Es kann

Image-Dateien auf deren Inhalt scannen und die gefundenen Informationen strukturieren. Dazu gehören u.a. E-Mail-Adressen, Kreditkartennummern und auch Bitcoin-Adressen. Die Ergebnisse werden in Textdateien gespeichert, die weiter analysiert oder als Input für andere forensische Verarbeitungen verwendet werden können. [39]

Der Bulk Extractor wird unter der MIT Lizenz sowie der Common Public License Version 1.0 zur Verfügung gestellt und war daher als Open-Source Software für diese Arbeit kostenfrei nutzbar.

6.2.5 AXIOM (kommerziell)

Magnet AXIOM wurde für die Wiederherstellung, Verarbeitung und Analyse digitaler Beweise entwickelt. [40]

Das IT-Forensik Wiki der HS Wismar beschreibt Magnet AXIOM als ein „All-in-One“-Tool für forensische Ermittlungen, mit dem Beweise auf Computern und mobilen Geräten untersucht werden können. Es lassen sich dabei verschiedene Artefakte entdecken und Anzeigen strukturieren, wie z.B. Bilder, Emails, Web-Historien, Chat-Protokolle oder Windows-Events. Diese werden automatisch von der Software erkannt und teils sogar inhaltlich sortiert (z.B. Kategorisierung von Bildern). Die von Magnet Forensics entwickelte Software für Windows unterstützt verschiedene Dateisystemtypen von Windows und Mac, sowie einiger Linux Images und kann zusätzlich Daten von Mobilgeräten und Cloudspeicherorten einbinden und analysieren. Auch wird die Analyse von RAM-Speicherabbildern unterstützt. Die für den professionellen Einsatz entwickelte Software ist kostenpflichtig, bietet aber vergünstigte Pakete für Bildungseinrichtungen sowie eine 30-tägige kostenfreie Testperiode an. [41]

Eine Recherche in verschiedenen Forensik-Foren ergab, dass die Lizenzkosten variieren; je nach Branche, Organisation und Kunde beginnen diese bei 2500 $ bis 3500 $ jährlich.

Für die vorliegende Arbeit konnten Testlizenzen der HS Wismar genutzt werden.

7 Datenauswertung der Testfälle

In Autopsy und AXIOM erfolgte die weitere Datenauswertung in einem ersten Schritt durch das Einlesen der VMDK-Images in eigens erzeugte Case-Files, welche die relevanten Daten jeweils separat sicherten. Die weitere Datenanalyse erfolgte dann ausschließlich über die erzeugten Case-Files.

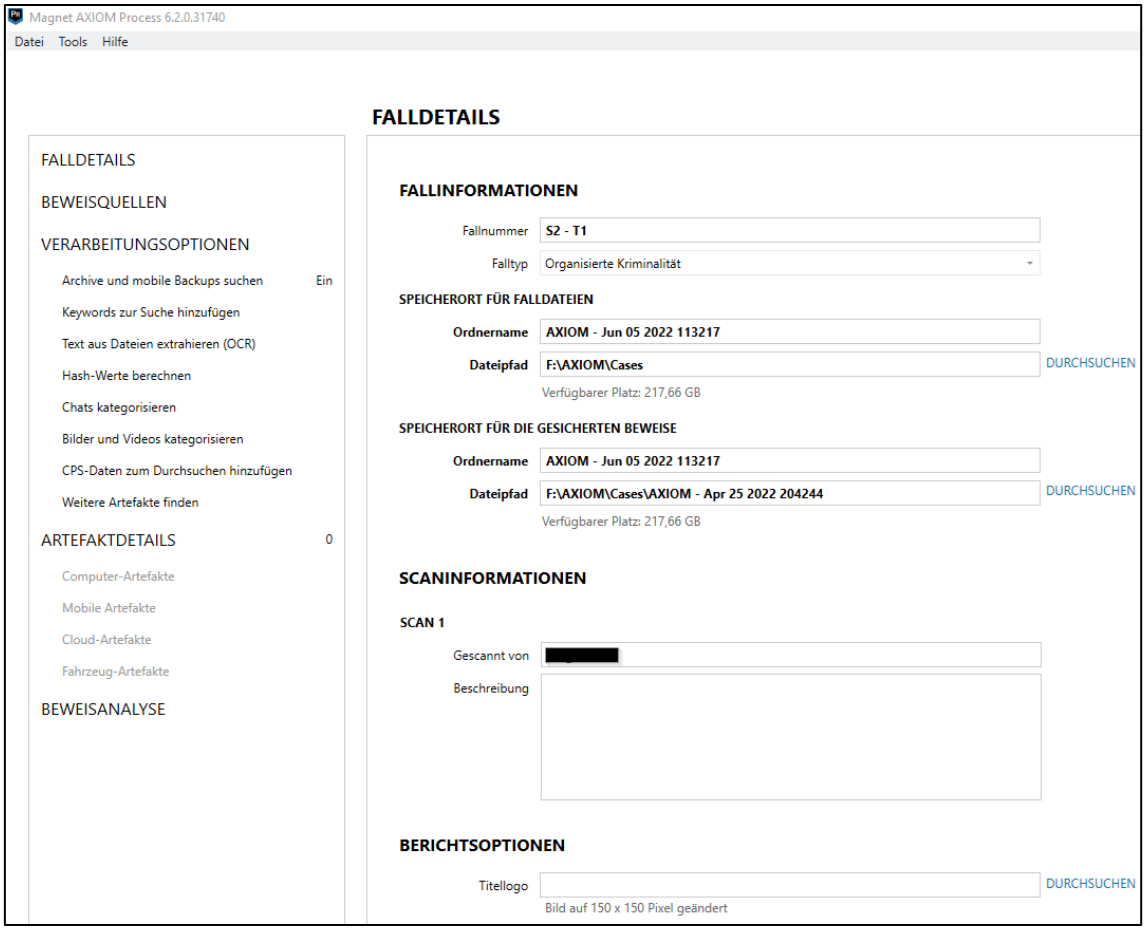


Bild 6: Erzeugung eines neuen Falls in AXIOM [40]

Die Datenauswertung unter Einsatz des Bulk Extractor erfolgte hingegen direkt auf der VMDK-Image Datei. Hierbei konnte über die Linux-Kommandozeile mit folgendem Befehl eine Extraktion relevanter Rohdaten erzeugt werden:

bulk_extractor FILE.vmdk -o FILENAME

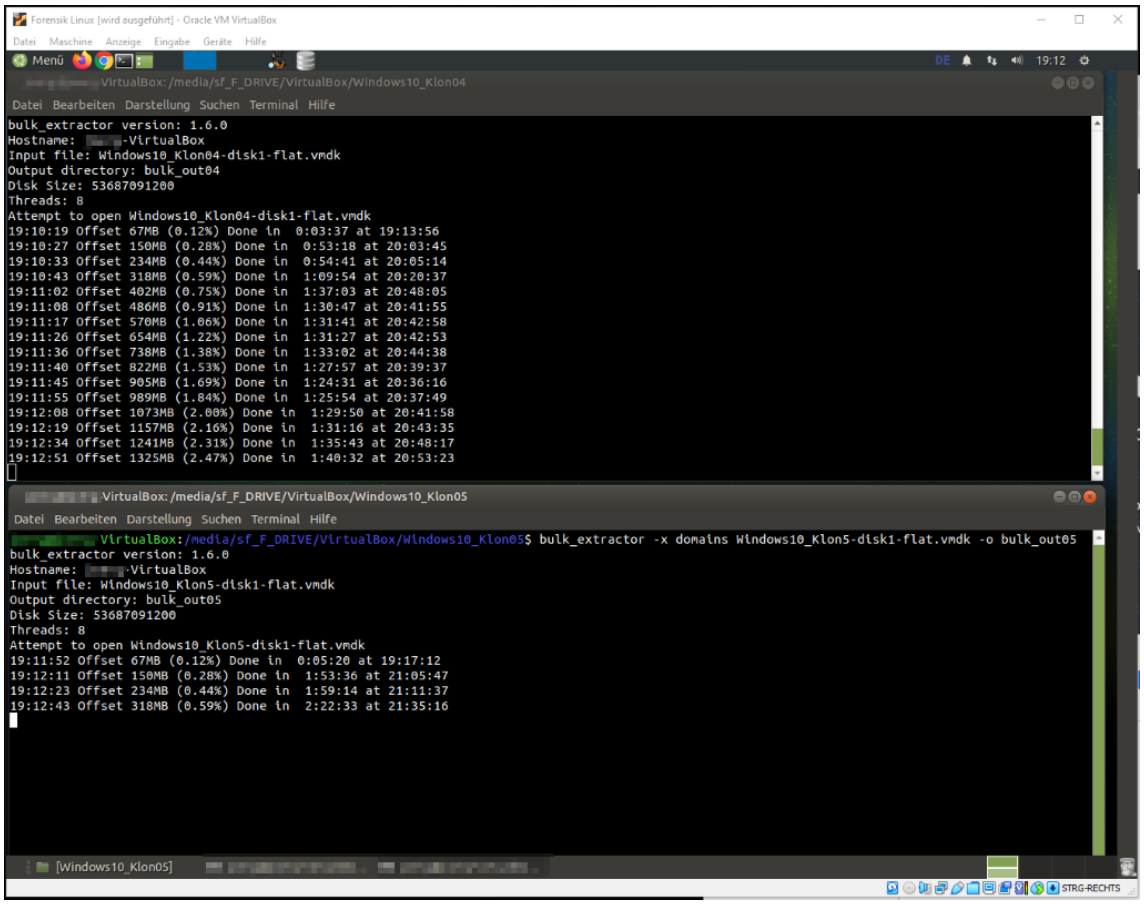


Bild 7: Erzeugung eines Bulk Outputs mit Bulk Extractor [39]

Für die weitere Analyse der ausgeleiteten TXT-Files gab es verschiedenste Ansätze. Innerhalb dieser Arbeit wurden zwei Ansätze beleuchtet: die Auswertung über das Einlesen in ein Tabellenkalkulationsprogramm (Excel) sowie die Anwendung eines Scripts in der Sprache Python.

7.1 Datenauswertung Testfall – T0

Im initialen Testfall – T0 wurde die generelle Machbarkeit der für diese Arbeit anzuwendenden Auswertungsmethodik geprüft. Hierzu wurden auf den genutzten Windows 10 VMs jeweils auf dem Sender-Image-Klon sowie dem Empfänger-Image-Klon ein neues Electrum Wallet eingerichtet.

Der Sender-Klon wurde in einer initialen Transaktion (Tx) zusätzlich mit einer Start-Balance von 0.2482 MBTC ausgestattet.

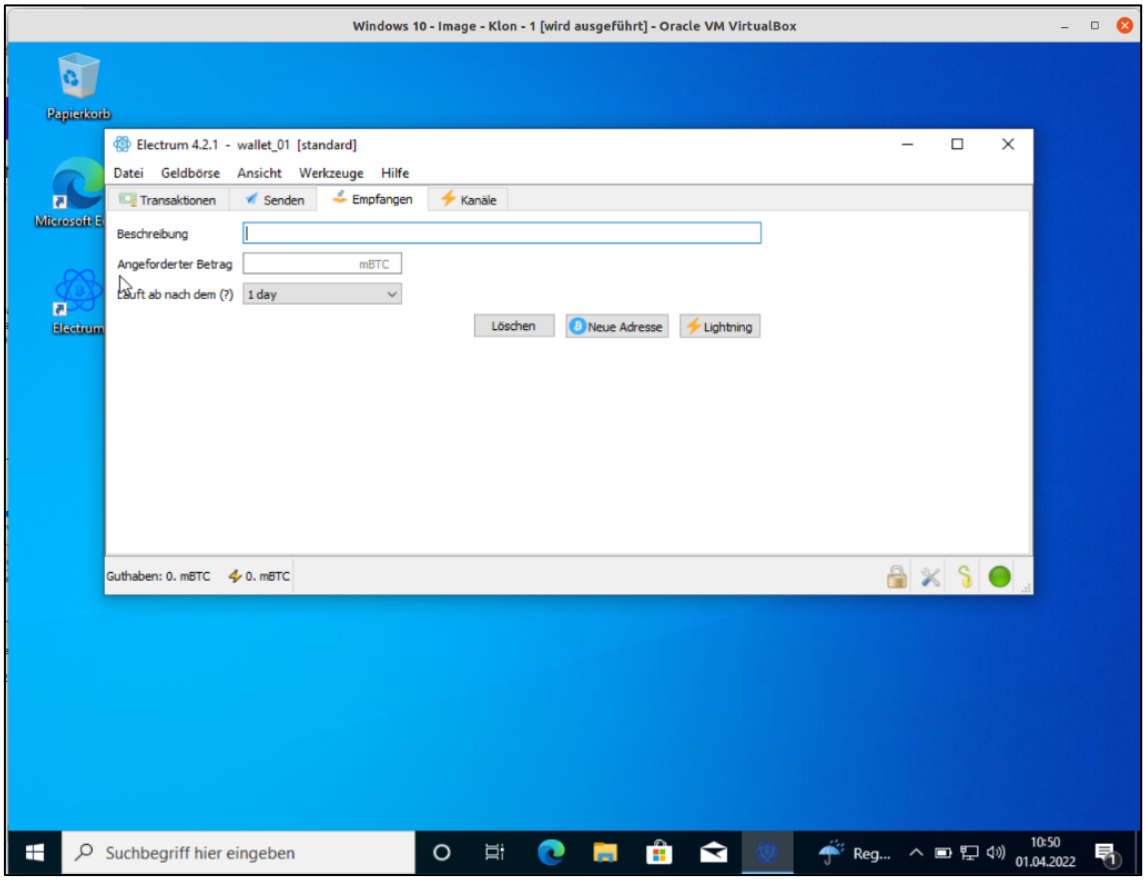


Bild 8: Electrum Wallet auf Windows 10 VM

Diese initiale Transaktion auf das Electrum Wallet des Senders konnte u.a. über den Blockstream-Explorer eindeutig nachvollzogen werden.

Tx:f523ee99eb30818c8f70de0af447c9fb4e5564a06901b4ff4bc00294c4a0c63b

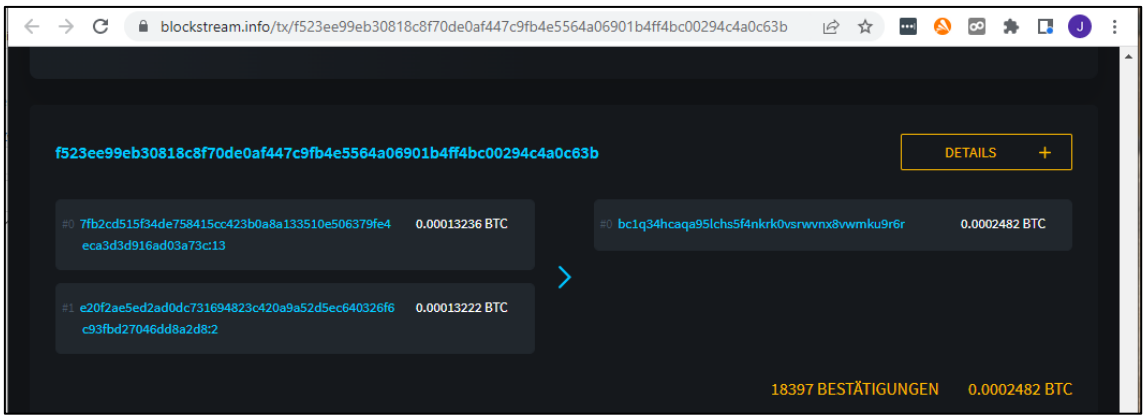


Bild 9: Ansicht der initialen Transaktion in Blockchain Explorer (blockstream.info) [30]

Bei der Auswertung der eingesetzten Images konnte generell festgestellt werden, dass der Ansatz, digitale Spuren von kryptowährungs-basierten Transaktionen mithilfe von Methoden der IT-Forensik zu verwertbaren Ergebnissen führt. Insbesondere wurden in Testfall T0 folgende IT-forensische Spuren generiert:

Electrum Wallet Datei

C:\users\image master\appdata\\roaming\electrum\wallets\wallet_01

Bitcoin-Adresse (Sender)

bc1q34hcaqa95lchs5f4nkrk0vsrwvnx8vwmku9r6r

Bitcoin-Adresse (Empfänger)

bc1qwtkutllfdf0duhdyez8wcq6xulq94d55q7xznz

Transaktion

71a997ef103972d3787458c6b294a6d189ba90c8bf56c6e80daaae921afc6f50

Bei der Datenauswertung konnten alle oben aufgeführten Spuren durch eine Pfadanalyse und Auswertung der unverschlüsselten Electrum Wallet-Datei nachvollzogen werden. Durch die für diese Arbeit positiven Testergebnisse aus T0 konnten die Szenarien S1, S2.1, S2.2 sowie die verbundenen Testfälle T1-T4 so gestaltet werden, dass diese entlang der Erkenntnisse aus T0 weiter untersucht wurden.

In den folgenden Testfällen T1-T3 wurden dedizierte Einblicke in die Funktionen der eingesetzten Forensik-Tools vollzogen.

7.2 Datenauswertung Testfall – T1

Zur Auswertung der Erkennungsleistung der jeweiligen Forensik-Tools wurden die Aktionen des Akteurs Erpresser aus dem Image-File Windows10_Klon03-disk1.vmdk extrahiert und bewertet. Die Erkennungsleistung der jeweiligen Forensik-Tools wurde in der folgenden Tabelle zusammengefasst und je Artefakt und Aktion bewertet und kommentiert.

Tabelle 9: Vergleich der Erkennungsleistung von Autopsy, AXIOM und Bulk Extractor nach unterschiedlichen Artefakten

Artefakt	Aktion	Autopsy	AXIOM	Bulk Extractor	Kommentierung
Coinbase Google Suche	Suche	Y	Y	Y	Alle Tools konnten die Google-Suche nach Coinbase erkennen.
Coinbase Wallet Extension	Aufruf	Y	Y	Y	Alle Tools konnten die Wallet-Extension von Coinbase erkennen.
Coinbase Tresor	Aufruf	Y	Y	Y	Alle Tools konnten den Aufruf der Wallet-Extension von Coinbase erkennen. Bulk Extractor: Suche in Url.txt nach ***BTC_Vault
Coinbase URL	Aufruf	Y	Y	Y	Alle Tools konnten den Aufruf der Coinbase URL erkennen.
Coinbase	Benutzer-name	Y	Y	Y	Alle Tools konnten den Benutzername von Coinbase finden. Bulk Extractor: Suche in Url.txt nach https://www.coinbase.com/signine mail***
Coinbase	Passwort	N	Y	N	Nur AXIOM konnte das genutzte

	(Klartext)				Coinbase Passwort in Klartext anzeigen.
Binance Google Suche	Suche	Y	Y	Y	Alle Tools konnten die Google-Suche nach Binance erkennen.
Binance URL	Aufruf	Y	Y	Y	Alle Tools konnten den Aufruf der Binance-URL erkennen.
Electrum Google Suche	Suche	Y	Y	Y	Alle Tools konnten die Google-Suche nach Electrum erkennen. Bulk Extraktor: Suche in Url.txt https://www.google.com/search?q=electrum
Electrum Wallet	Download	Y	Y	Y	Bulk Extraktor: Suche in Url.txt
Electrum Wallet	Aus-führung	Y	Y	Y	Bulk Extraktor: Suche in winlnk.txt
Electrum Software	Installation	Y	Y	Y	Bulk Extraktor: Suche in winlnk.txt
Transaktionen (TX)	IDs	N	Y	Y	Autopsy hatte im Testfall keine Transaktion-IDs ausgegeben. AXIOM hat diese IDs aus dem Electrum Wallet ausgelesen. Auch über Bulk Extraktor war ein Auslesen aus dem Electrum Wallet über die json Datei möglich. Hinweis: Das Electrum Wallet war bewusst nicht gesondert verschlüsselt worden.
Bitcoin Adressen	Adresse	N	Y	Y	Autopsy hatte keine Bitcoin Adressen ausgegeben. AXIOM und Bulk Extractor haben die Bitcoin Adressen aus dem unverschlüsselten Electrum Wallet ausgelesen.

Reguläre Ausdrücke	Suche	N System-absturz nach Warn-meldung	Y	Y	Angewendeter Regulärer Ausdruck: ([13]|bc1)[A-HJ-NP-Za-km-z1-9]{27,34} Autopsy stürzte nach Missachtung der Warnmeldung regelmäßig ab. Durchführung nicht möglich. AXIOM lief stabil und konnte die Bitcoin-Adressen generell ermitteln. Schwierigkeiten bereitete dabei allerdings die Menge der False-Positive Treffer. Bulk Extractor lieferte 20.528 Treffer in Ausleitung der ALERTS_found.txt Die Anzahl der False-Positive Treffer war somit hoch.

7.3 Datenauswertung Testfall – T2

Zur Auswertung der Erkennungsleistung der jeweiligen Forensik-Tools wurden die Aktionen des Akteurs Erpresser aus dem Image-File Windows10_Klon5-disk1.vmdk extrahiert und jeweils bewertet.

7.3.1 Auswertungsergebnisse – Autopsy

Die wichtigsten Ergebnisse, die unter Anwendung von Autopsy gefunden werden konnten, werden im Folgenden aufgeführt.

E-Mail-Kommunikation zwischen Erpresser und Opfer

Es konnte anhand der in Windows installierten und genutzten Programme die Verwendung von Thunderbird als E-Mail-Client an mehreren Stellen nachgewiesen werden. Das Erpresserschreiben war vollständig und mit

wichtigen Spuren einsehbar. Dazu zählten neben dem Erpressertext selbst auch die Absender- und Empfängeradresse sowie die Bitcoin-Adresse, an die das Opfer den zu zahlen Betrag entrichten sollte. Alle Informationen lagen mit entsprechenden Timestamps vor.

Aufgerufene Webseiten

Der Erpresser verwendete primär den Browser EDGE, auch wenn eine Chrome Installation vorlag. In der im EDGE Browser befindlichen Web-History waren verschiedene Webseitenbesuche (Visits) zu finden, die u.a. auf die Nutzung von Kryptowährungs-Diensten schlossen.

Websuchen

Es konnten die Suche nach dem verwendeten Software Wallet Electrum und der Besuch der Ledger Webseite, sowie die Suche nach dem Hardware Wallet Ledger Nano S nachgewiesen werden. Auch der Aufruf des Downloadbereichs, zum Download der nötigen Clientsoftware des Ledger Nano S, war nachweisbar.

Blockchain-Explorer

Es fanden sich Spuren über die Nutzung des Blockchain Explorers blockstream.info. Hierbei war nachweisbar, dass verschiedene Transaktionen über die Suchfunktion aufgerufen wurden, dabei waren folgende Transaktionen einsehbar:

5b11587f0dc92c90cc4778e89a3450f8a2c7c345b4513811eae03132039eaeaa

b7352f8224b17c351c75474cac9049c0d5a5703335932ec2d2cab060c5a4e61e

11ea57774ece64188c61a1794dfda4af1adae284763de27e4050619e93fa79bb

fc6d1b2f4e7900a4a9e9787f30600e6b7adcf99adbd5153ff5f5ca7383488ec6

Die Nutzung von blockstream.info legte die Suche über die für die Abfrage erzeugte URL im Nachgang offen. Die Bitcoin Transaktions-ID war Teil der URL zur Abfrage der Datenbank des Webdienstes.

Electrum - Soft Wallet Nutzung

Interessanterweise führte Autopsy keine Listung von Electrum unter "Installed Programs“ auf. Es konnten jedoch verschiedene andere Artefakte gefunden werden, die eine Nutzung von Electrum nachwiesen. Der Erpresser hatte in einem ersten Schritt das Electrum Wallet vollständig heruntergeladen. Zeitlich kurz nach dem Download wurde das Electrum Wallet auch installiert. Die Installation war über den Standardpfad für Programm-Installationen nachweisbar. Durch eine Prefetch Datei, die Windows automatisiert anlegt, um zukünftige Programmstarts zu beschleunigen, konnte auch die aktive Nutzung des Electrum Wallets nachgewiesen werden.

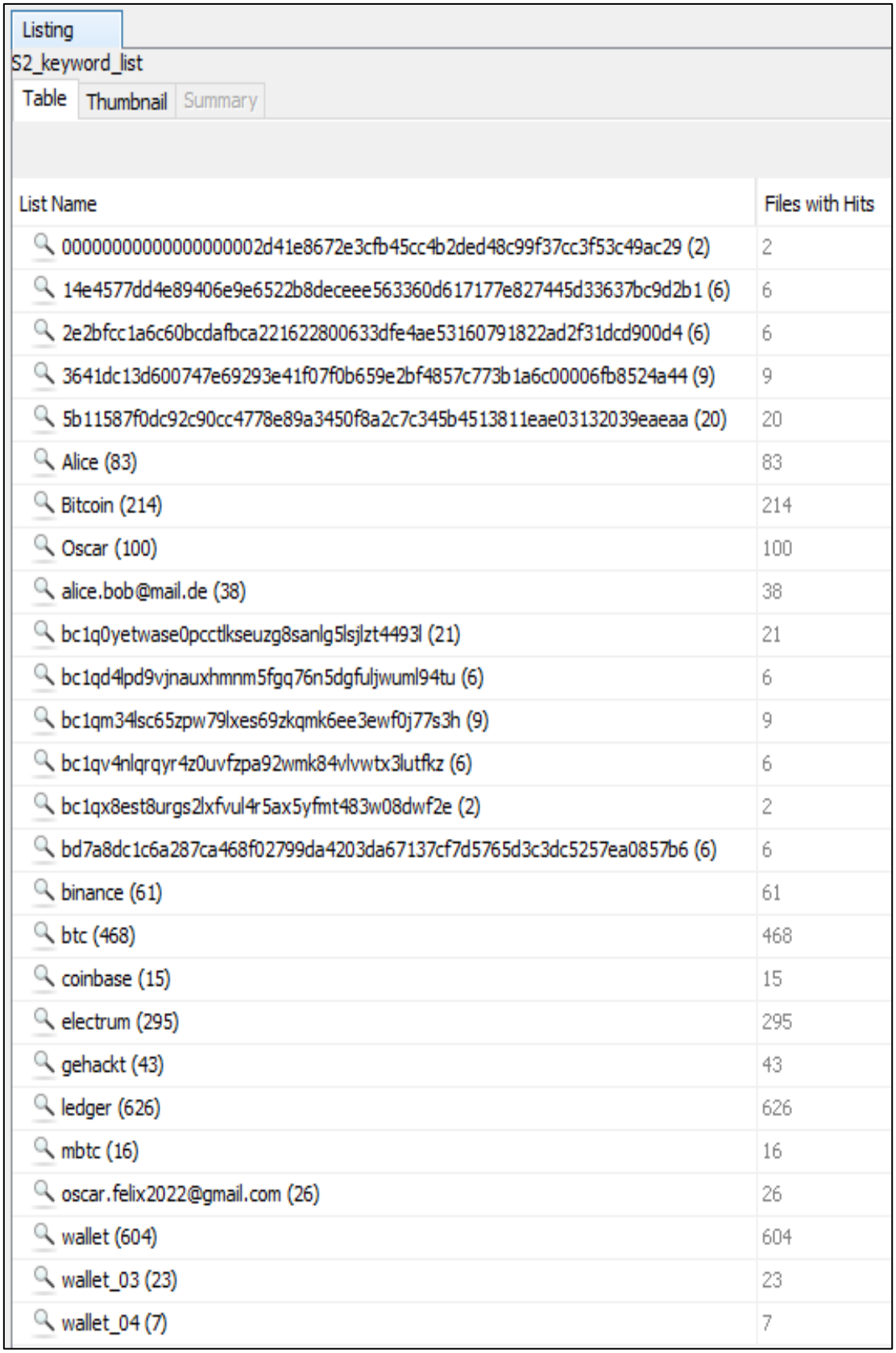
Das Wallet selbst, welches von dem Erpresser genutzt wurde, konnte durch weitere manuelle Analyse der Pfadstrukturen nachgewiesen werden. Hierzu wurde in Kapitel 7.5.2 über die allgemein anwendbaren Erkenntnisse aus der Datenauswertung in Bezug zu Electrum Wallets genauer eingegangen.

Generell zeigt Autopsy im Reiter „Interesting Files > Cyrptocurrency Wallets“ zwar das Vorhandensein einer Installation an, die konkrete Wallet-Datei, die alle sensiblen Informationen ausweist, musste aber manuell gesucht werden.

Einsatz der Keyword Suche

Die Verwendung einer statischen Keyword-Liste ergab eine Vielzahl von Treffern u.a. der Bitcoin-Adressen sowie verbundener Transaktions-IDs.

Die eingesetzte Keyword-Liste war im Vorfeld spezifisch auf das Szenario und den Testfall angepasst erstellt worden, daher ist die hohe Trefferanzahl nachvollziehbar. Im folgenden Bild 10 sind die verwendeten Keywords mit den entsprechenden Treffern in Autopsy erkennbar.



Listing

S2_keyword_list

Table | Thumbnail | Summary

List Name	Files with Hits
0000000000000000002d41e8672e3cfb45cc4b2ded48c99f37cc3f53c49ac29 (2)	2
14e4577dd4e89406e9e6522b8deceee563360d617177e827445d33637bc9d2b1 (6)	6
2e2bfcc1a6c60bcdafbca221622800633dfe4ae53160791822ad2f31dcd900d4 (6)	6
3641dc13d600747e69293e41f07f0b659e2bf4857c773b1a6c00006fb8524a44 (9)	9
5b11587f0dc92c90cc4778e89a3450f8a2c7c345b4513811eae03132039eaeaa (20)	20
Alice (83)	83
Bitcoin (214)	214
Oscar (100)	100
alice.bob@mail.de (38)	38
bc1q0yetwase0pcctlkseuzg8sanlg5lsjlzt4493l (21)	21
bc1qd4lpd9vjnauxhmnm5fgq76n5dgfuljwuml94tu (6)	6
bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h (9)	9
bc1qv4nlqrqyr4z0uvfzpa92wmk84vlvwtx3lutfkz (6)	6
bc1qx8est8urgs2lxfvul4r5ax5yfmt483w08dwf2e (2)	2
bd7a8dc1c6a287ca468f02799da4203da67137cf7d5765d3c3dc5257ea0857b6 (6)	6
binance (61)	61
btc (468)	468
coinbase (15)	15
electrum (295)	295
gehackt (43)	43
ledger (626)	626
mbtc (16)	16
oscar.felix2022@gmail.com (26)	26
wallet (604)	604
wallet_03 (23)	23
wallet_04 (7)	7

Bild 10: Autopsy Keyword Listing [38]

Die Keyword-Liste befindet sich in der Anlage 4: S2_keyword_list 20220616

Einsatz Regulärer Ausdrücke

Für die Suche nach Bitcoin-Adressen wurde folgender Reguläre Ausdruck definiert und in Anwendung gebracht:

([13]|bc1)[A-HJ-NP-Za-km-z1-9]{27,34}

Dieser Ausdruck sollte alle Zeichenketten, die dem Adressschema einer gültigen Bitcoin-Adresse entsprechen, identifizieren können. Der Reguläre Ausdruck wurde in einem ersten Schritt von Autopsy vor Durchführung der Analyse angenommen:

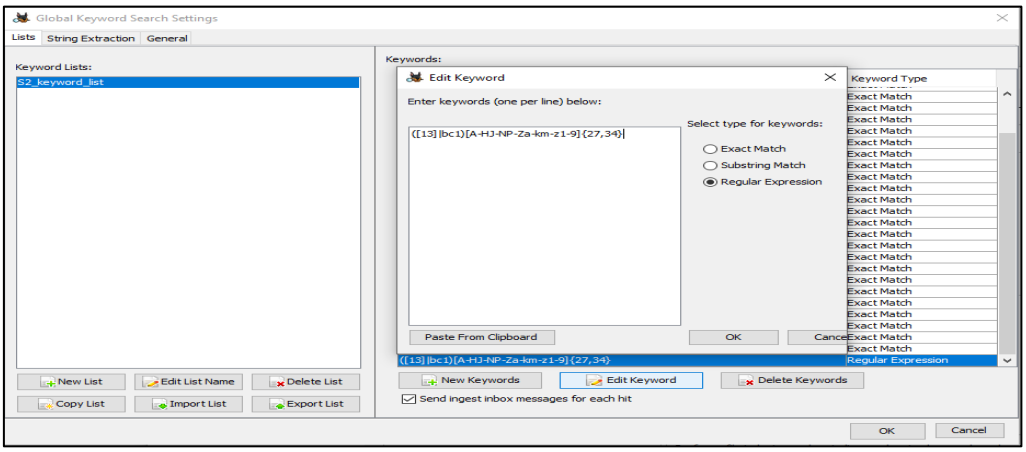


Bild 11: Globale Keywordsuche – Reguläre Ausdrücke [38]

Die weitere Verwendung von Regulären Ausdrücken wurde aber von Autopsy im vorliegenden Testfall nicht effizient unterstützt. Vor Ausführung wurde eine Systemwarnung erzeugt, sodass der Aufwand auf über das 1000-fache anstieg. Wenn diese Meldung ignoriert wurde und die Ausführung startete, sorgte dies regelmäßig zum System-Freeze.

Bild 12: Systemwarnung Autopsy bei Einsatz des Regulären Ausdrucks [38]

Die Auswertungsergebnisse für Autopsy finden sich in detaillierter Form in der Anlage 1: S2.1-Auswertung_Autopsy.xlsb

7.3.2 Auswertungsergebnisse – AXIOM

Die wichtigsten Ergebnisse, die unter Anwendung von AXIOM gefunden werden konnten, werden im Folgenden aufgeführt.

E-Mail-Kommunikation zwischen Erpresser und Opfer

Es konnte anhand der in Windows installierten und genutzten Programme die Verwendung von Thunderbird als E-Mail-Client an mehreren Stellen nachgewiesen werden. Das Erpresserschreiben war vollständig und mit wichtigen Spuren einsehbar. Dazu zählten neben dem Erpressertext selbst auch die Absender- und Empfängeradresse sowie die Bitcoin-Adresse, an die das Opfer den zu zahlen Betrag entrichten sollte. Alle Informationen lagen mit entsprechenden Timestamps vor. Die Timestamps in der Artefakte-Übersicht wurden im UTC-Zeitformat angezeigt. Die lokale Systemzeit ließ sich aus dem E-Mail-Header in der Detailansicht in AXIOM nachvollziehen.

Aufgerufene Webseiten

Der Erpresser verwendete primär den Browser EDGE, auch wenn eine Chrome Installation vorlag. In der im EDGE Browser befindlichen Web-History waren verschiedene Webseitenbesuche (Visits) zu finden, die u.a. auf die Nutzung von Kryptowährungs-Diensten schlossen.

Websuchen

Es konnten die Suche nach dem verwendeten Software Wallet Electrum und der Besuch der Ledger Webseite und Suche nach dem Hardware Wallet Ledger Nano S nachgewiesen werden. Auch der Aufruf des Downloadbereichs, zum Download der nötigen Clientsoftware des Ledger Nano S, war nachweisbar.

Blockchain-Explorer

Es fanden sich Spuren über die Nutzung des Blockchain Explorers blockstream.info. Hierbei war nachweisbar, dass verschiedene Transaktionen über die Suchfunktion aufgerufen wurden dabei, waren folgende Transaktionen einsehbar:

5b11587f0dc92c90cc4778e89a3450f8a2c7c345b4513811eae03132039eaeaa

b7352f8224b17c351c75474cac9049c0d5a5703335932ec2d2cab060c5a4e61e

11ea57774ece64188c61a1794dfda4af1adae284763de27e4050619e93fa79bb

fc6d1b2f4e7900a4a9e9787f30600e6b7adcf99adbd5153ff5f5ca7383488ec6

Die Nutzung von blockstream.info legte die Suche über die für die Abfrage erzeugte URL im Nachgang offen. Die Bitcoin Transaktions-ID war Teil der URL zur Abfrage der Datenbank des Webdienstes.

Electrum - Soft Wallet Nutzung

AXIOM führte eine Listung von Electrum unter den installierten Programmen auf. Auch wurden weitere Artefakte gefunden, die eine Nutzung von Electrum nachwiesen. Hierzu zählte der App-Switch Counter, den Windows automatisiert in der NTUSER.DAT anlegt hatte.

Der Erpresser hatte in einem ersten Schritt das Electrum Wallet vollständig heruntergeladen. Zeitlich kurz nach dem Download wurde das Electrum Wallet auch installiert. Die Installation war über den Standardpfad für Programm-Installationen nachweisbar.

Generell zeigte AXIOM auch das Wallet-File über die Ansicht auf Dateien und Ordner, auf die lokal zugegriffen wurde, an.

Einsatz der Keyword Suche

Die Verwendung einer statischen Keyword-Liste ergab eine Vielzahl von Treffern u.a. der Bitcoin-Adressen sowie verbundener Transaktions-IDs.

Die eingesetzte Keyword-Liste war im Vorfeld spezifisch auf das Szenario und den Testfall erstellt worden. Daher ist die hohe Trefferanzahl nachvollziehbar.

Die eingesetzte Keyword-Liste befindet sich in der Anlage 4: S2_keyword_list 20220616

Für die Suche nach Bitcoin-Adressen wurde folgender Reguläre Ausdruck definiert und in Anwendung gebracht:

([13]|bc1)[A-HJ-NP-Za-km-z1-9]{27,34}

Dieser Ausdruck sollte alle Zeichenketten, die dem Adressschema einer gültigen Bitcoin-Adresse entsprechen identifizieren können. Der Reguläre Ausdruck wurde von AXIOM vor der Analyse angenommen. Die weitere Verwendung von Regulären Ausdrücken wurde von AXIOM im vorliegenden Testfall effizient unterstützt. Eine Erkenntnis aus der Arbeit ist jedoch, dass die Menge an False-Positives bei dieser Methodik zu hoch wurde, als dass diese singulär angewendet werden kann.

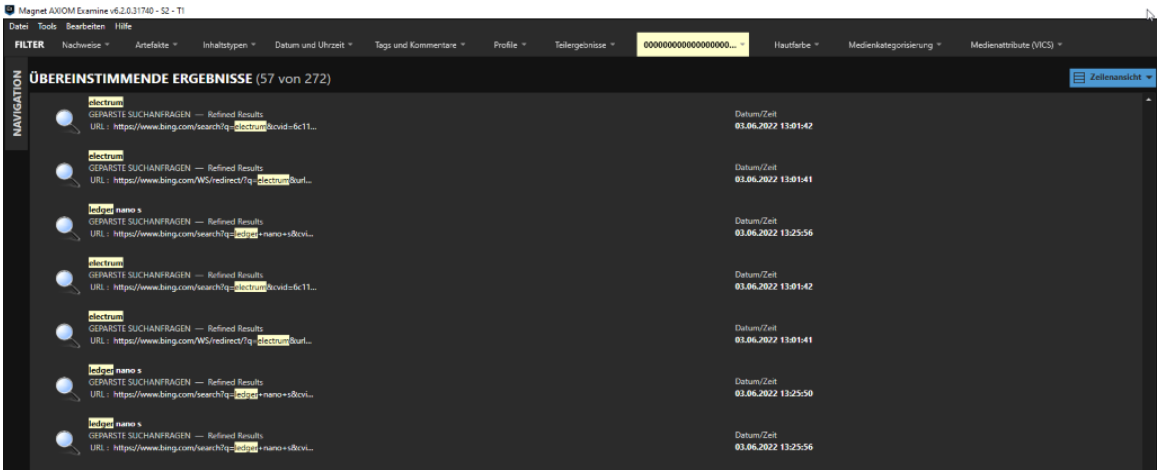


Bild 13: Auswertung Regulärer Ausdrücke in AXIOM [40]

Die Auswertungsergebnisse für AXIOM finden sich in detaillierter Form in der Anlage 2: S2.1-Auswertung_AXIOM.xlsb

7.3.3 Auswertungsergebnisse – Bulk Extractor

Die Suche nach Bitcoin-Adressen funktionierte mit Bulk Extractor überzeugend. In den von Bulk Extraktor erzeugten Datenextraktionen befand sich u.a. die Datei bitcoin.txt. Darin befand sich u.a. die vom Expresser verwendete Empfangsadresse:

bc1q0yetwase0pcctlkseuzg8sanlg5lsjlzt4493l

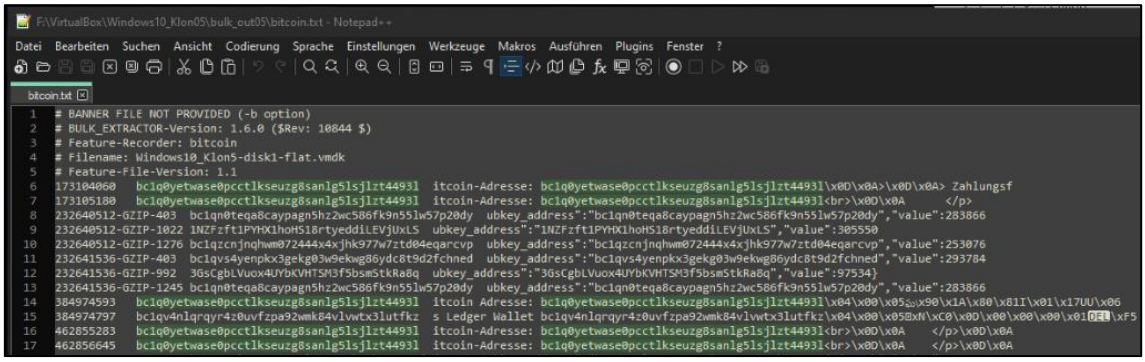


Bild 14: Bulk Output der Bitcoin-Adressen des Bulk Extractors [39]

Die Anzahl der False-Positives erschien in der Stichprobenprüfung deutlich geringer als im Vergleich zur Suche nach Bitcoin-Adressen über Reguläre Ausdrücke mit Autopsy oder AXIOM.

Die Gesamtanzahl von 894 Treffern im Image-Klon Windows10_Klon5-disk1-flat.vmdk beinhaltete verschiedene Bitcoin-Adressen, die aber teilweise mehrfach vorkamen. Dies ist soweit erklärbar, als dass im lokalen Datenspeicher an verschiedenen Stellen dieselben Adressen gespeichert wurden, da diese in unterschiedlichem Kontext genutzt worden sind und somit mehrere Treffer erzeugten.

7.4 Datenauswertung Testfall – T3

7.4.1 Auswertungsergebnisse – Autopsy

Ledger Nano S - Hard Wallet Nutzung

Es konnten verschiedene Artefakte gefunden werden, die eine Nutzung des Ledger Nano S Wallets nachwiesen. Der Erpresser hatte in einem ersten Schritt die Software Ledger Live, die für die Bedienung des Hard Wallet notwendig ist, vollständig heruntergeladen. Zeitlich kurz nach dem Download wurde Ledger Live auch installiert. Die Installation war über einen Eintrag in der Windows-Registry nachweisbar.

Generell zeigte Autopsy im Reiter „Interesting Files > Cyrptocurrency Wallets“ das Vorhandensein einer Ledger Live Installation an. Artefakte, die weitere sensible Kryptowährungs-Objekte auswiesen, konnten nicht gefunden werden. Es war daher davon auszugehen, dass die Ledger Live Software ausschließlich einen Verweis auf den verschlüsselten Hardware Wallet Ledger Nano S bildete und keine Kryptowährungs-Objekte auf dem lokalen Windows-PC verfügbar machte.

Mobiles Endgerät – Apple IPhone SE

Eine Spurenauswertung unter Anwendung von Autopsy wurde vorbereitet, indem ein Apple IPhone SE mit verschiedenen Spuren der Kryptowährungs-Dienst Nutzung versehen wurde. Während des Prozesses der Daten-Akquirierung in Autopsy wurde, im Gegensatz zu AXIOM, leider keine logische Datenakquise oder Image-Erzeugung für Apple IPhones angeboten.

7.4.2 Auswertungsergebnisse – AXIOM

Mobiles Endgerät – Apple IPhone SE

Im Gegensatz zu Autopsy bot AXIOM die Möglichkeit, eine Daten-Akquise von Apple IPhone Geräten durchzuführen. Im vorliegenden Testfall wurde ein sog. „Schnell Image“ unterstützt. Ein vollständiges, physisches Abbild des IPhones wurde an dieser Stelle von AXIOM auch nicht unterstützt.

Das „Schnell Image“ konnte als logischer Zugriff auf ausgewählte Bereiche verstanden werden und war daher nicht mit einem physischen Abbild im Umfang zu vergleichen. Es fanden sich jedoch verschiedene Spuren in dieser Art von Image, die auf die Nutzung von Kryptowährungen hindeuteten. Diese Spuren werden im Folgenden kurz ausgeführt.

Binance App

Im Bereich der Anwendungsnutzung fand AXIOM unter den installierten Anwendungen verschiedene Erweiterungen und Widgets der Binance APP. Auch Anwendungsgenehmigungen für die Serviceerbringungen und das User Tracking waren auffindbar. Des Weiteren wurde ein sog. iOS-Startbildschirm-Element gefunden, das von Binance stammt.

Interessant ist auch, dass in einem Element des Webverlaufs der Username gefunden werden konnte, mit dem sich der Anwender bei Binance angemeldet hatte. Im Screenshot unten ist der Klarname (roter Kasten) aus Sicherheitsgründen ausgegraut.

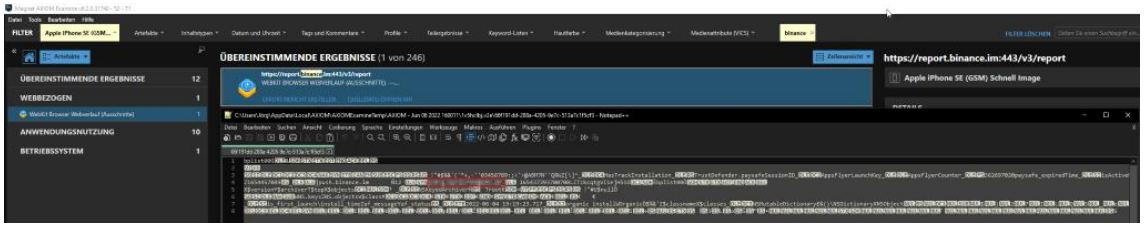


Bild 15: Sichtbarkeit des Benutzernamen (E-Mail-Adresse) aus Login in Binance APP [40]

Coinbase App

Innerhalb der installierten Anwendungen ließen sich Hinweise auf das Vorhandensein des Coinbase Wallets finden.

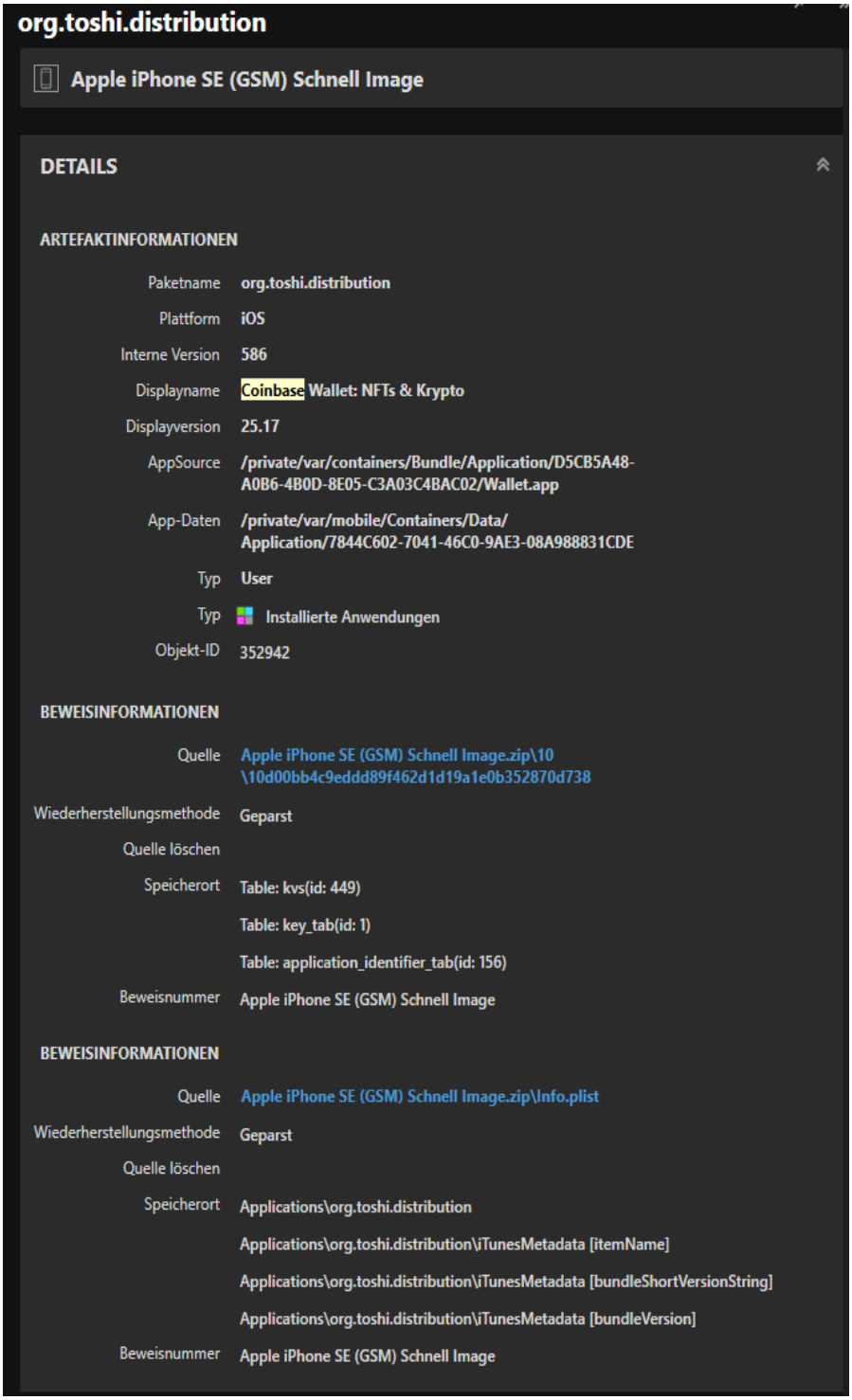


Bild 16: Sichtbarkeit der Installation der Coinbase APP [40]

Ledger Nano S - Hard Wallet Nutzung

Es konnten verschiedene Artefakte gefunden werden, die eine Nutzung des Ledger Nano S Wallets nachwiesen. Der Erpresser hatte in einem ersten Schritt die Software Ledger Live, die für die Bedienung des Hard Wallet notwendig ist, vollständig heruntergeladen. Zeitlich kurz nach dem Download wurde Ledger Live auch installiert. Die Installation war über einen Eintrag in der Windows-Registry nachweisbar.

Generell zeigte AXIOM im Reiter der verbundenen Geräte über den genutzten USB-Port das Vorhandensein des Ledger Nano S an. Unter der Anwendungsnutzung ist die genutzte Funktion com.ledger.live vom App-Switch der NTUSER.DAT erfasst worden.

7.4.3 Auswertungsergebnisse – Bulk Extractor

Für eine Auswertung mit dem Bulk Extractor war eine generische Image Datei des IPhone SE notwendig.

Für die vorliegende Arbeit konnte aufgrund der zur Verfügung stehenden Hardware- und Software-Ausstattung kein vollwertig anwendbares IPhone Image erzeugt werden.

In Kapitel 7.5.1 finden sich zusammengefasst die Ansätze und Erkenntnisse in Bezug zur Datenakquise von Apple IPhone Endgeräten.

7.5 Allgemeine Erkenntnisse aus der Datenauswertung

Aus den einzelnen Datenauswertungen der verschiedenen Testfälle ließen sich allgemeine Erkenntnisse zu involvierten Komponenten gewinnen, die in diesem Kapitel weiter ausgeführt wurden.

7.5.1 Datenakquise Apple IPhone SE

Um Autopsy oder Bulk-Extraktor in Verbindung mit IPhone-Endgeräten einsetzen zu können, musste bereits ein fertiger Datendump bzw. eine Image-Datei vorliegen. Aus diesem Grund stellte sich innerhalb der betrachteten Forensik-Tools AXIOM als die geeignetste Lösung dar, da diese ein logisches Image einzelner Artefakte als sog. „Schnell-Image“, erstellen konnte.

Generell erforderte die vollständige Datenakquise und Image-Erstellung von IPhones weitere Verfahren und Tools. Hier kann je nach IPhone-Modell und iOS-Version auch ein Jailbreak des Geräts durchgeführt werden. Diese Methodik ist allerdings aus IT-forensischer Sicht nicht ideal, da unweigerlich in das Gerät eingegriffen werden muss und der ursprüngliche Zustand durch die Untersuchung verändert wird.

Exemplarisch wurde eine Möglichkeit zur Erstellung von iPhone-Datendumps untersucht. Ein Ansatz bot hierbei die Nutzung von iOS Triage, welches als Open-Source-Code über Github bezogen werden konnte. Dieses Bash-Script bot die Möglichkeit, unter Anwendung eines checkra1n Jailbreak in Abhängigkeit des Versionsstands des iPhones und iOS, Daten aus dem iPhone zu extrahieren.

checkra1n ist ein Jailbreak für iPhone 5s bis iPhone X, iOS 12.0 und höher und nutzt den checkm8 bootrom Exploit. [42]

Um iOS Triage anwenden zu können ergaben sich neben verschiedenen optionalen Voraussetzungen einige Pflichtvoraussetzungen:

- checkra1n (https://checkra.in/)
- libimobiledevice (https://www.libimobiledevice.org/)
- SSHPASS for Mac OS X (https://gist.github.com/arunoda/7790979)
- dialog for Mac OS X (http://macappstore.org/dialog/) [43]

Im vorliegenden Hardware-Setup war eine weitere Untersuchung des iPhone SE unter Zuhilfenahme eines checkra1n Jailbreaks nicht weiter möglich. Hintergrund war, dass das für diese Arbeit zur Verfügung stehende ältere MacBook Air über das macOS Big Sur 11.6.7 verfügte und damit herstellerseitig kein Update mehr auf das für Apple Developer benötigte macOS 12 unterstützt wurde. Somit konnten die Pflichtvoraussetzungen für den Einsatz von iOS Triage nicht hergestellt werden.

Anzumerken ist, dass Jailbreaks die betroffenen Geräte in einen ungeordneten Zustand bringen, Sicherheitsprobleme und Funktionsstörungen auslösen können sowie die Garantie des Herstellers erlöschen lassen und daher aus IT-forensischer Sicht nur die letzte Wahl der Mittel darstellen.

7.5.2 Einsatz unverschlüsselter Electrum Wallets

Das Electrum Wallet gibt es seit 2011 und ist eine der am stärksten verbreiteten Bitcoin Software-Wallets für den PC. Die Nutzung unterliegt einer MIT-Lizenz und ist daher für jeden frei nutzbar. [44]

Generell gilt Electrum zwar als eine sichere Wallet-Lösung, jedoch muss diese vor Nutzung auch entsprechend sicher konfiguriert werden, d.h. das Wallet muss durch den Einsatz eines spezifischen Passworts gesichert und verschlüsselt werden.

Entscheidet sich der Nutzer gegen eine lokale Verschlüsselung der Wallet-Datei, liegen die Daten ungeschützt auf der lokalen Festplatte und können damit u.a. auch für IT-forensische Analysen herangezogen werden.

Der Windows-Standardpfad für Electrum Wallet-Dateien ist:

\Users\USER\AppData\Roaming\Electrum\wallets\

Unter diesem Pfad konnten Dateien des MIME Type text/plain gefunden werden. In dieser Datei wurden relevante Informationen über vorangegangene Kryptowährungs-Transaktionen lokal auf dem Endgerät des Nutzers gespeichert.

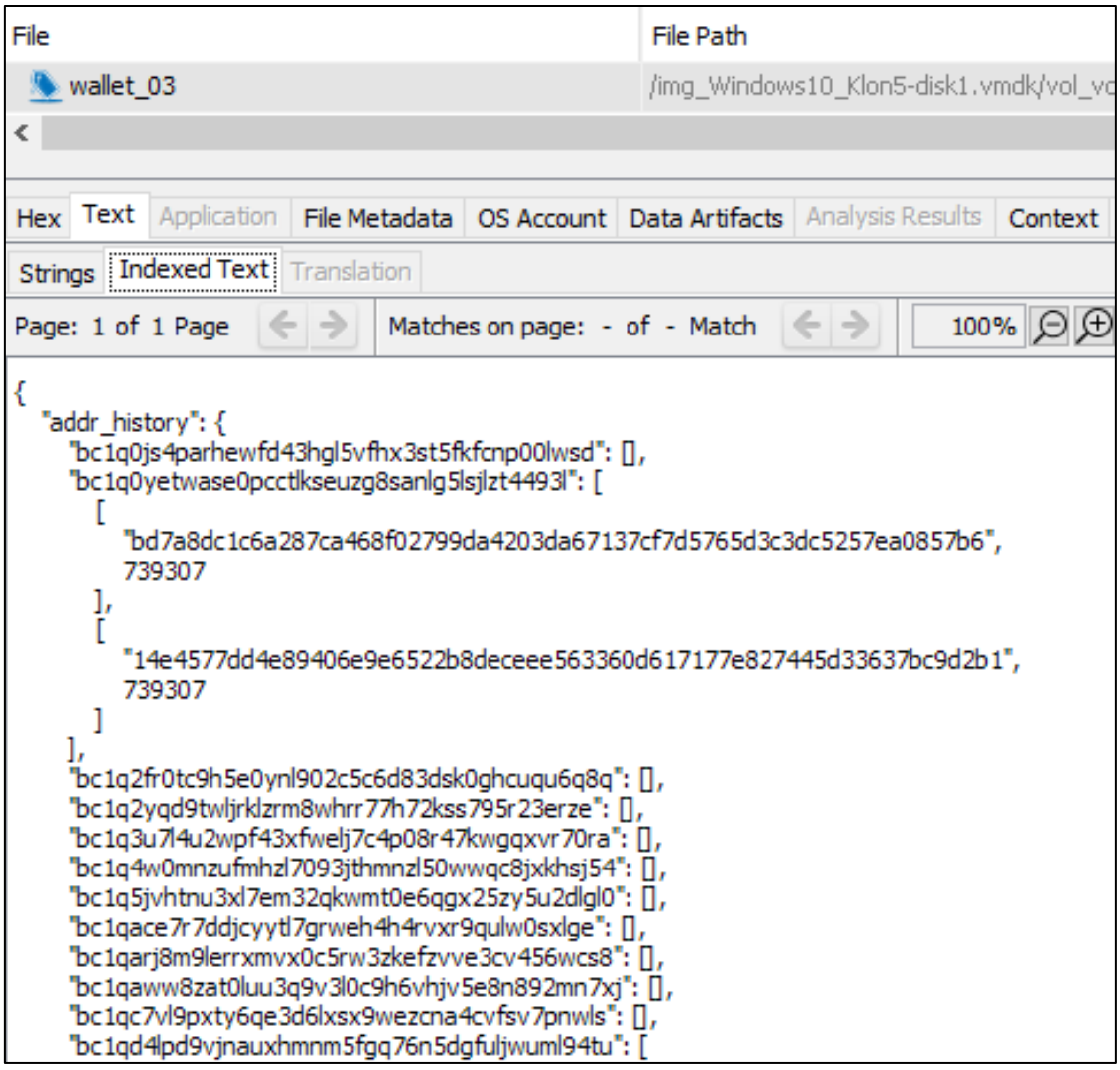


Bild 17: Analyse einer unverschlüsselten Electrum Wallet Datei [44]

Bei der initialen Anlage dieser Datei kann ein Nutzer bestimmen, ob er diese Datei verschlüsselt anlegt. Sofern der Nutzer diese Datei unverschlüsselt angelegt hat, sind alle Transaktionen des Wallets im Falle einer IT-forensischen Untersuchung einsehbar. Innerhalb der vorliegenden Arbeit wurde mit unverschlüsselten Electrum Wallets gearbeitet.

Es bietet sich an, in einer weiteren Arbeit die Verschlüsselungsmechanismen von Electrum Wallets genauer zu untersuchen, um diese ggf. mit Methoden der Kryptoanalyse zu brechen.

Electrum nutzte eine Konfigurationsdatei (config), die wichtige Informationen bereithielt, wie bspw. das zuletzt genutzte Wallet. Standardmäßig wurde der folgende Pfad unter Windows herangezogen:

\Users\USER\AppData\Roaming\Electrum

Ergebnisse der Datenauswertung des Electrum Wallets (Testfall - T0)

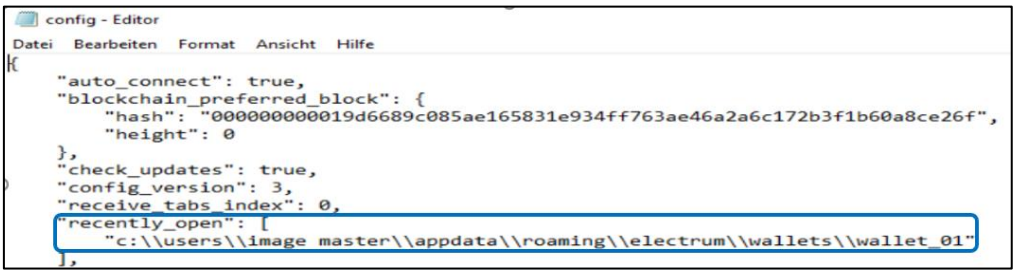


Bild 18: Electrum config Datei zeigte den Pfad der zuletzt genutzten Wallet-Datei

In obiger Electrum config Datei wurde auf das folgende Wallet referenziert; c:\\users\\image master\\appdata\\roaming\\electrum\\wallets\\wallet_01
Im Folgenden wurde das unverschlüsselte "wallet_01" unter diesem Pfad genauer untersucht. Hierbei wurde die Wallet-Datei auf dem Windows-Client ausgelesen. Electrum erstellte während der Installation standardmäßig eine Datei unter folgendem Pfad; C:\Users\USER_NAME\AppData\Roaming\Electrum\wallets
Darin befanden sich die erzeugten Electrum Wallets; es können darin auch verschiedene Wallets innerhalb einer Installation geführt werden.

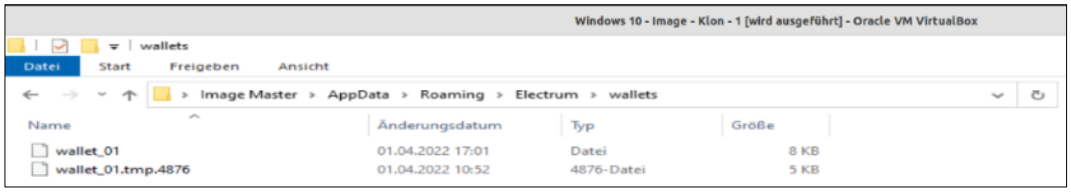


Bild 19: Ansicht des Verzeichnisses mit der Datei wallet_01

In den Wallets befanden sich folgende relevante Informationen: History der Adressen unter "addr_history", in untenstehendem Auszug befand sich u.a. die genutzte Bitcoin-Adresse aus dem initialen Testfall - T0:

{"bc1qwtkutllfdf0duhdyez8wcq6xulq94d55q7xznz": [

[

"71a997ef103972d3787458c6b294a6d189ba90c8bf56c6e80daaae921afc6f50"

Anhängig ist dabei auch die Transaktion 71a997ef103972d3787458c6b294a6d189ba90c8bf56c6e80daaae921afc6f50, die bei der Bezahlung der illegalen Waren genutzt worden ist.

In der der Wallet Datei „wallet_01“ fanden sich des Weiteren Informationen zu potentiell genutzten Adressen unter "addresses":

Unter "receiving" fand sich auch die Bitcoin-Empfängeradresse aus Testfall – T0:

{"bc1qwtkutllfdf0duhdyez8wcq6xulq94d55q7xznz": [

]

"transactions":

Die durchgeführte Transaktion konnte hierbei nachvollzogen werden:

71a997ef103972d3787458c6b294a6d189ba90c8bf56c6e80daaae921afc6f50

Desweitern findet sich ein Keystore mit dem entsprechenden Seed zur Wiederherstellung des Wallets sowie der Public und Private Key. Aus Sicherheitsgründen wurden die Keys an dieser Stelle nicht abgebildet.

Mit obigen Erkenntnissen könnten auch weitere Methoden der IT-Forensik angewandt werden. Hierzu zählt u.a. die Virtualisierung von Systemen, um die entsprechenden, unverschlüsselten Wallets lokal einzusehen.

7.5.3 Einsatz verschlüsselter Ledger Nano S Wallets

Das Ledger Nano S ist ein verbreitetes Hardware-Wallet für die Verwahrung von Kryptowährungen wie Bitcoins. Im Gegensatz zu Software-Wallets werden die Assets nicht auf einem PC mit entsprechender Software-Installation gespeichert, sondern auf einem externen Datenträger, analog einem USB-Stick.

Die Speicherung der Daten erfolgte hierbei ausschließlich passwortgeschützt und verschlüsselt. Ein Auslesen von Klartext ohne die Brechung des Schlüssels war daher nicht möglich.

Aus der IT-forensischen Analyse angeschlossener PCs ließen sich bspw. mit AXIOM verschiedene Artefakte finden, die den Nachweis der Installation und Nutzung des Wallets nachwiesen. Zu Artefakten zählten u.a. die in der Windows-Registry erzeugten Einträge durch Anschluss des genutzten Wallets an den USB-Port.

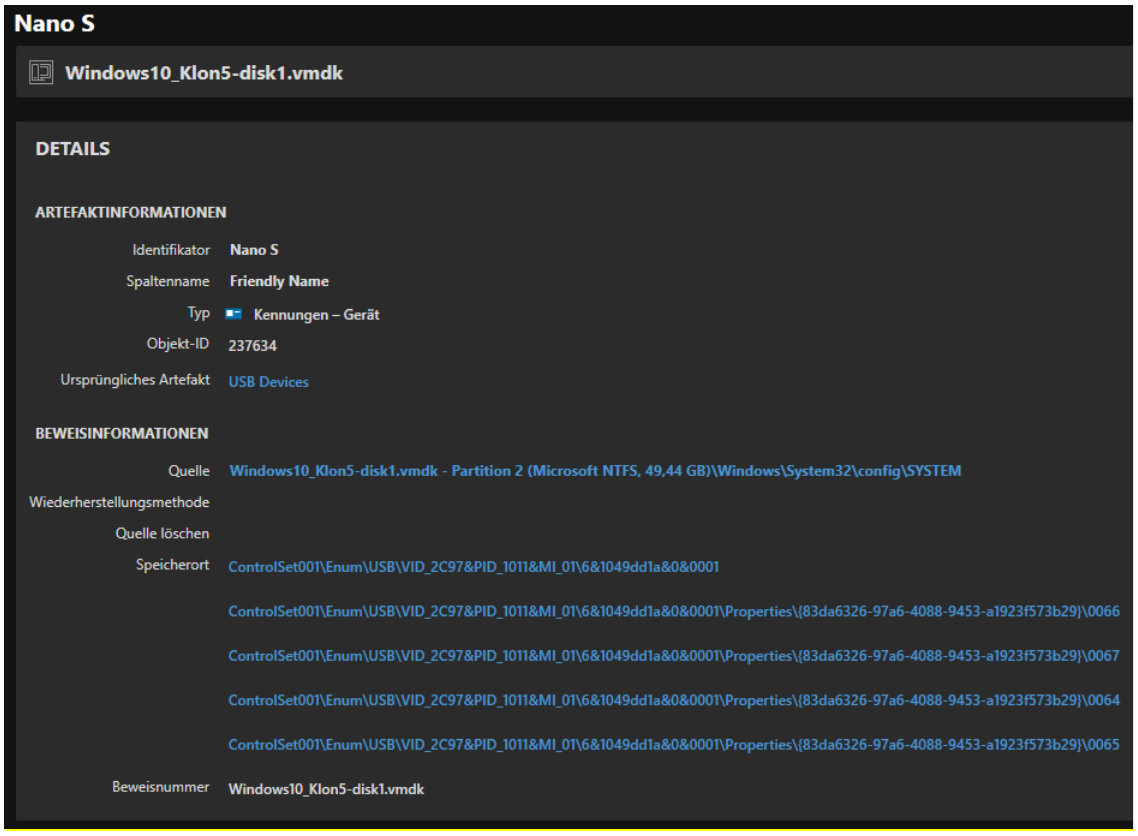


Bild 20: Eintrag Ledger Nano S in der Windows-Registry unter SYSTEM

Des Weiteren wurde die Anwendungsnutzung der zum Betrieb des Hardware-Wallets notwendigen Software Ledger Live über die Funktion com.ledger.live im App-Switch der NTUSER.DAT erfasst.

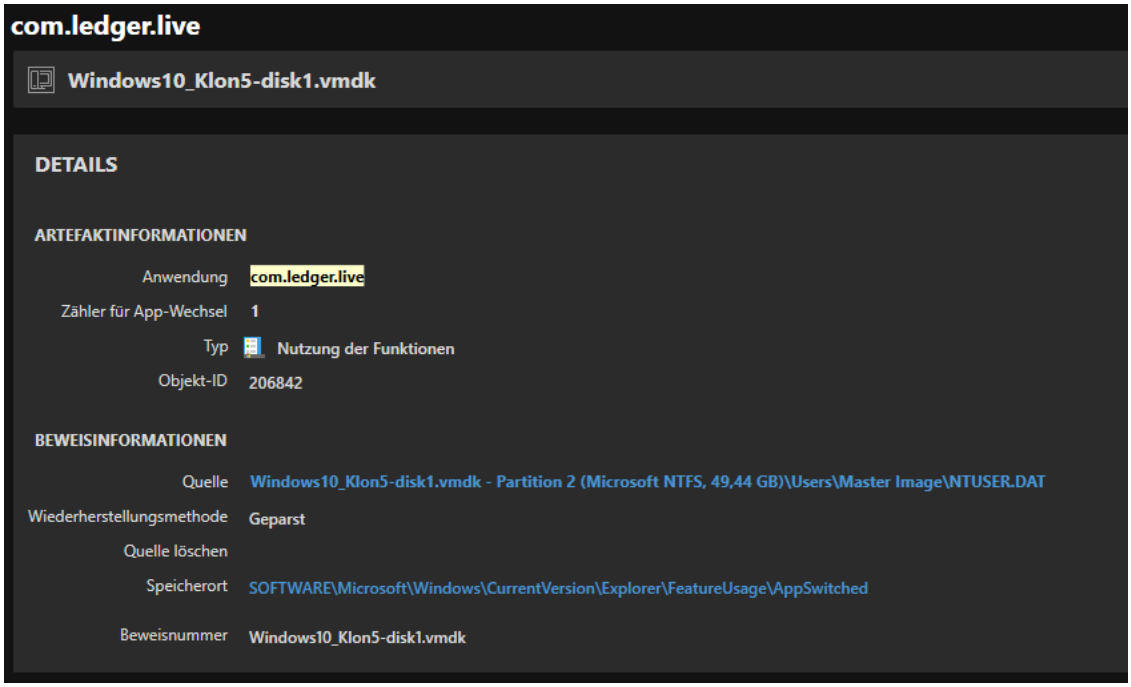


Bild 21: Nachweis des Aufrufs der Ledger Live Software

7.5.4 Webhistorie, Webcache und genutzte Web-Formulare

Die Nutzung von Internet-Browsern wie Microsoft EDGE oder Google Chrome hinterließ auf den genutzten Endgeräten untersuchungsrelevante Spuren an unterschiedlichen Stellen.

Bei Nutzung von Kryptowährungs-Diensten wurden Einträge in der Webhistorie erzeugt. Durch Ausführung des User-Logins konnten weitere Artefakte aus dem Login-Vorgang gewonnen werden.

Im vorliegenden Beispiel konnte ein Account bei Coinbase nachgewiesen werden. Der EDGE Browser legte eine SQLite-Datenbank unter folgendem Pfad ab:

> *\Users\USERNAME\AppData\Local\Microsoft\EDGE\User Data\Default\Login Data*

Die SQ-Lite Datenbank enthielt den genutzten Login-Name in Klartext. Da dieser Web-Dienst wie viele weitere als Login-Namen die E-Mail-Adresse abfragt, wird somit eine bestätigte E-Mail-Adresse offengelegt, die dann für weitere Analysen und OSINT-Recherchen verwendet werden kann.

Das Passwort war in diesem Beispiel nicht in Klartext einsehbar. Im folgenden Bild 22 wurde die reale E-Mail-Adresse in der grünen Umrandung aus Gründen des Datenschutzes unkenntlich gemacht.

Bild 22 Auszug SQLite: Link zu Coinbase-Login, Login-Name (E-Mail-Adresse) in Klartext

Im folgenden Bild 23 ist Domain, URL und der Source File Pfad zu „Login Data“ aus der EDGE Browser Historie zu erkennen.

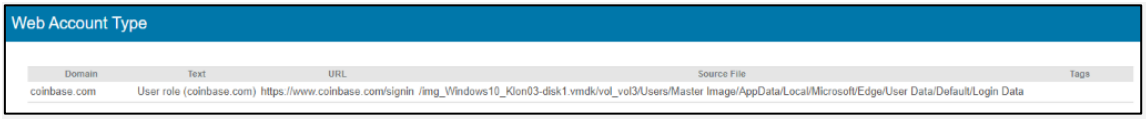


Bild 23: Auswertung des Web Account Type über Autopsy mit Anzeige von coinbase.com

Weitere Möglichkeiten, den Aufruf von Kryptowährungs-Börsen wie Binance oder Coinbase nachzuweisen, boten die Web-Cookies des Browsers. In der folgenden Tabelle wird dargestellt, wie die Zugriffe über die entsprechenden Web-Cookies offengelegt werden konnten.

Tabelle 10: Auswertung der Web-Cookies über Autopsy mit Treffern für binance.com und coinbase.com

URL	Name	Browser	Date Accessed	Source File
.binance.com	BNC_FV_KEY	Microsoft EDGE	2022-04-24 00:26:03 MESZ	/img_Windows10_Klon03-disk1.vmdk/vol_vol3/Users/Master Image/AppData/Local/Microsoft/EDGE/User Data/Default/Network/Cookies
.coinbase.com	__cf_bm	Microsoft EDGE	2022-04-24 18:58:01 MESZ	/img_Windows10_Klon03-disk1.vmdk/vol_vol3/Users/Master Image/AppData/Local/Microsoft/EDGE/User Data/Default/Network/Cookies

Der vollständige Auszug der mit Autopsy extrahierten Web-History und Cookies befindet sich in der Anlage 5: mixed HTML Report 04-29-2022-17-26-55

Ein weiterer Aspekt, der während dieser Arbeit erkannt wurde war, dass Kryptowährungs-Seiten wie blockstream.info eingegebene Suchbegriffe in den erzeugten Links anhängen und dadurch in der Browser-History abgelegt werden. Es fanden sich Spuren über die Nutzung des Blockchain-Explorers blockstream.info. Hierbei ist über die Link-Struktur einsehbar, dass verschiedene Transaktionen über die Suchfunktion vom Benutzer aufgerufen wurden, siehe Kapitel 7.3.

7.5.5 Blick in die zuletzt genutzten Dateien

Durch die Sichtung des Indexes zuletzt genutzter Dokumente „Recent Documents“ konnten u.a. Hinweise auf Wallets, Kryptowährungs-Adressen, Keys, Seeds mit entsprechenden Zeitstempeln gefunden werden. Die ausgewiesenen Zeitstempel können dabei auch helfen, zeitliche Überschneidungen zwischen Aktionen auf der lokalen Maschine, sowie den Transaktionen auf der Blockchain zu erkennen. Im folgenden Bild 24 findet sich exemplarisch ein Auszug aus Autopsy mit relevanten Kryptowährungs-Objekten eines ausgewerteten Images:

Recent Documents

Path	Date/Time
C:\Users\Master Image\AppData\Roaming\Electrum\wallets	2022-04-24 19:08:10 MESZ
C:\Users\Master Image\AppData\Roaming\Electrum\wallets	2022-04-24 19:33:21 MESZ
C:\Users\Master Image\AppData\Roaming\Electrum\wallets\wallet_03	2022-04-24 19:08:10 MESZ
C:\Users\Master Image\AppData\Roaming\Electrum\wallets\wallet_03	2022-04-24 19:33:21 MESZ
C:\Users\Master Image\Desktop	0000-00-00 00:00:00
C:\Users\Master Image\Desktop\Bitcoin_Adresse.txt	0000-00-00 00:00:00
C:\Users\Master Image\Desktop\Bitcoin_Adresse.txt	2022-04-25 20:34:59 MESZ
C:\Users\Master Image\Desktop\Bitcoin_Adresse_Ausgehend.txt	0000-00-00 00:00:00
C:\Users\Master Image\Desktop\Bitcoin_Adresse_Eingang.txt	0000-00-00 00:00:00
C:\Users\Master Image\Desktop\Bitcoin_Adresse_Eingang.txt	2022-04-25 20:40:19 MESZ
C:\Users\Master Image\Desktop\privat_key.txt	0000-00-00 00:00:00
C:\Users\Master Image\Desktop\privat_key.txt	2022-04-25 20:34:20 MESZ
C:\Users\Master Image\Desktop\public_key.txt	0000-00-00 00:00:00
C:\Users\Master Image\Desktop\public_key.txt	2022-04-25 20:33:01 MESZ
C:\Users\Master Image\Desktop\seed.txt	0000-00-00 00:00:00
C:\Users\Master Image\Desktop\seed.txt	2022-04-24 00:37:31 MESZ
C:\Users\Master Image\Desktop\seed.txt.txt	2022-04-24 00:35:55 MESZ
C:\Users\Master Image\Desktop\seed_electrum.txt	0000-00-00 00:00:00
C:\Users\Master Image\Desktop\seed_electrum.txt	2022-04-24 01:04:08 MESZ

Bild 24: Übersicht der zuletzt vom Anwender aufgerufenen Dokumente

Der vollständige Auszug der mit Autopsy extrahierten „Recent Documents“ befindet sich in der Anlage 5: mixed HTML Report 04-29-2022-17-26-55

7.5.6 Installierte und ausgeführte Programme

Die Übersicht über die installierten Programme eines Rechners konnte verschiedene Hinweise geben, welche Soft- und Hardware Wallets genutzt wurden. Software-Wallets wie Electrum hinterließen Einträge u.a. in der Windows-Registry, die kenntlich machten, dass ggf. weitere Kryptowährungs-Objekte auf dem vorliegenden Image erwartbar waren.

Je nach Programmaufbau hinterließen die aktiv genutzten Programme weitere Spuren während der Nutzung. Exemplarisch kann hier die Darstellung in Autopsy unter „Run Programs“ genannt werden, in der die Nutzung von Electrum durch einen Eintrag unter \users\master image\downloads\electrum-4.2.1.exe belegt werden konnte.

Der vollständige Auszug der mit Autopsy gefundenen installierten und ausgeführten Programme findet sich in Anlage 5: mixed HTML Report 04-29-2022-17-26-55

7.5.7 Dateien von besonderem Interesse

Software-Wallets galten u.a. bei Autopsy als eine Datei von besonderem Interesse. Dies half auf schnelle Art und Weise zu prüfen, ob Wallets im vorliegenden Image vom Anwender genutzt worden sind.

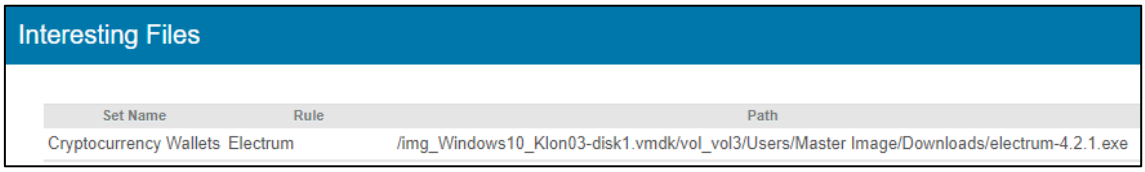


Bild 25: Electrum Wallet in der Interesting Files Liste in Autopsy

7.5.8 E-Mail-Adressen aus Kommunikationsverläufen und User-Login

Die von Anwendern genutzten E-Mail-Adressen waren von besonderer Bedeutung, da diese, sofern sie in Zusammenhang mit einem Kryptowährungs-Dienst gebracht werden konnten, weitere Rückschlüsse auf die verbundenen Transaktionen und u.U. auch die Identität des jeweiligen Akteurs geben konnten. Während der Datenauswertung traten relevante E-Mail-Adressen in zweierlei Weise in Erscheinung. Zum einen wurden diese in Szenario S2.1, Testfall T2 u.a. als Absender-Adresse einer Erpressermail verwendet, in der wiederum auch die Bitcoin-Adresse des Erpressers enthalten war. Durch die Auswertung der E-Mail-Kommunikation konnten damit auch Informationen zu betroffenen Opfern und damit weitere relevante Informationen generiert werden. Zum anderen konnten E-Mail-Adressen, wie in Kapitel 7.5.4 beschrieben, bei webbasierten Diensten wie Coinbase teils aus dem Web-Cache ausgelesen werden.

7.5.9 Auswertung Bulk Extractor Exporte mit Python

Bulk Extractor lieferte TXT-Dateien im CSV Format als Ergebnis der Programmausführung. Diese Dateien konnten für die weitere Analyse über den Datenimport beispielsweise in Excel verfügbar gemacht werden. Für einfache Suchen in der Ergebnismenge, das Entfernen von Doubletten sowie Pivot-Funktionen zur Analyse der Häufigkeit des Auftretens einzelner Bitcoin-Adressen hatte sich Excel dabei als geeignet dargestellt.

Ein weiterer Ansatz, um die von Bulk Extractor erzeugten TXT-Dateien auszuwerten, bildete die Anwendung der Scriptsprache Python. In den folgenden Programmbeispielen der Kapitel 7.5.10 und 7.5.11 wurden exemplarisch Ansätze aufgezeigt und deren Funktionsweise kurz erklärt. Es wurden hierzu zwei Funktionen in Python erzeugt, die es ermöglichen, eine Datenbasis aus TXT-Dateien nach unterschiedlichen Kriterien zu validieren oder zu durchsuchen. Mit den nachfolgend in Kapiteln 7.5.10 und 7.5.11 vorgestellten Funktionen ließen sich die von Bulk Extractor erzeugten, zeilenbasierten TXT-Dateien weiter verarbeiten.

Das erstellte Script befindet sich in der Anlage 3: Python-Script

7.5.10 Validierung von Bitcoin-Adressen mit Regulären Ausdrücken

Im folgenden Programmcode ruft die main-Methode die Funktion bitcoin_regcheck() auf. Darin wird die zuvor vom Bulk Extractor erzeugte Textdatei „bitcoin.txt“ aufgerufen und in den Arbeitsspeicher gelesen. Mithilfe einer for-Schleife wird nun jede Zeile (line) der „bitcoin.txt“ auf folgenden Regulären Ausdruck abgeglichen:

([13]|bc1)[A-HJ-NP-Za-km-z1-9]{27,34}

Sofern eine Zeile (line) innerhalb der durchsuchten Textdatei dem Regulären Ausdruck entspricht, wird diese Zeile über die Funktion print(line) ausgegeben, siehe unten aufgeführtes Bild 26.

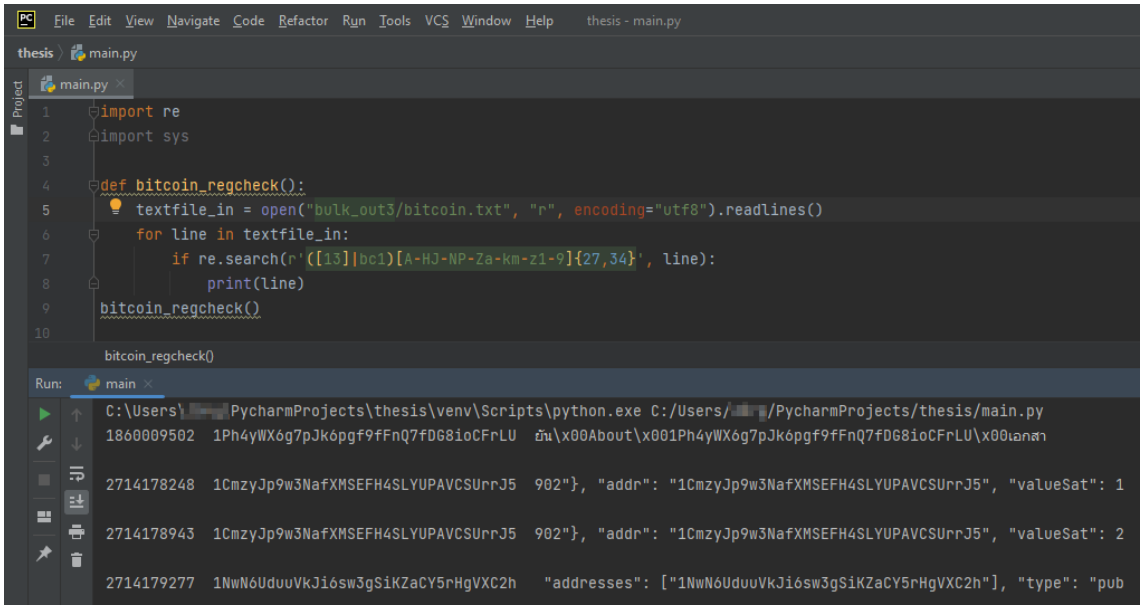


Bild 26: Ausführung Python Script zur Validierung von Bitcoin-Adressen in einer TXT-Datei unter Anwendung von Regulären Ausdrücken

7.5.11 Suche nach relevanten Keywords

Im folgenden Programmcode ruft die main-Methode die Funktion websearch_pattern() auf. Darin wird die zuvor vom Bulk Extractor erzeugte Textdatei „email.txt“ aufgerufen und in den Arbeitsspeicher gelesen. Mithilfe einer for-Schleife wird nun jede Zeile (line) der „email.txt“ auf folgende relevante Keywords durchsucht:

coinbase | binance

Sofern eine Zeile innerhalb der durchsuchten Textdatei dem Regulären Ausdruck entspricht, wird diese Zeile über die Funktion print(line) ausgegeben, siehe unten aufgeführtes Bild 27.

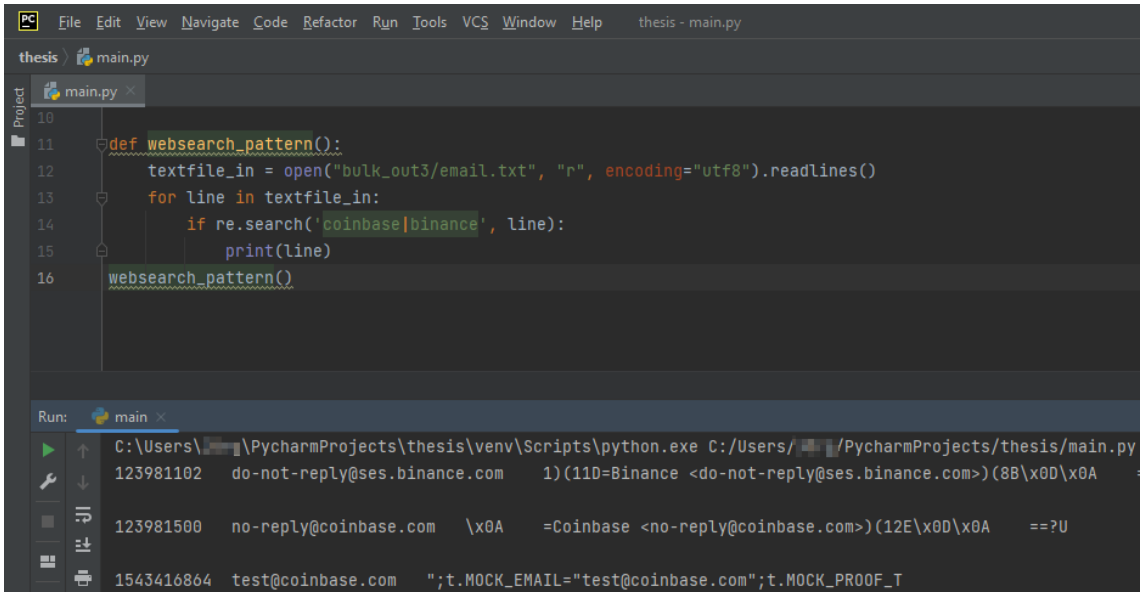


Bild 27: Ausführung Python Script zur Suche nach Keywords in einer TXT-Datei

8 Einsatz von Open Source Intelligence

In diesem Kapitel wurden unter Einsatz der in Kapitel 3 eingeführten OSINT-Dienste, die in Kapitel 5.2 beschriebenen Testfälle weiterverfolgt. Die OSINT-Analyse erfolgte durch Nutzung der in Kapitel 7 ausgewerteten Daten aus der IT-forensischen Untersuchung.

Initial wird nachfolgend jeder der betrachteten OSINT-Dienste kurz vorgestellt und auch dessen allgemeine Integrität betrachtet. Neben der Dokumentation der einzelnen Analyse-Ergebnisse erfolgte abschließend eine Bewertung des jeweiligen OSINT-Dienstes.

8.1 Blockchain-Explorer: Blockchain.com

Unter der Webseite Blockchain.com verbirgt sich in erster Linie eine kommerzielle Plattform zum Handel mit Kryptowährungen. Der Betreiber der Plattform ist die Blockchain.com, Inc., welche auch über eine offizielle Registrierung als US-Finanzdienstleister bei dem State Regulatory Registry verfügt.

Bild 28: Auszug aus der NMLS-Registrierung der Blockchain.com, Inc. als anerkannter US-Finanzdienstleister [45]

Blockchain.com ist nach Eigenaussage der weltweit populärste Dienst, Kryptowährungen zu kaufen, zu verkaufen und zu handeln. Seit 2011 vertrauen

laut Blockchain.com Millionen Menschen dieser Plattform, die bisher ein Handelsaufkommen von über 1 Billion US-Dollar an Krypto-Transaktionen generierte. [46]

Aus OSINT-Perspektive bietet diese Plattform offen nutzbare Funktionen, um Kryptowährungs-Transaktionen zu analysieren. Der Dienst bietet u.a. einen Blockchain-Explorer an, mit dem Transaktionen der verschiedensten Kryptowährungen einsehbar gemacht werden.

Wie im folgenden Bild 29 zu sehen ist, kann unter der URL https://www.blockchain.com/explorer nach Blockchains, Transaktionen, Wallets und Blöcken gesucht werden.

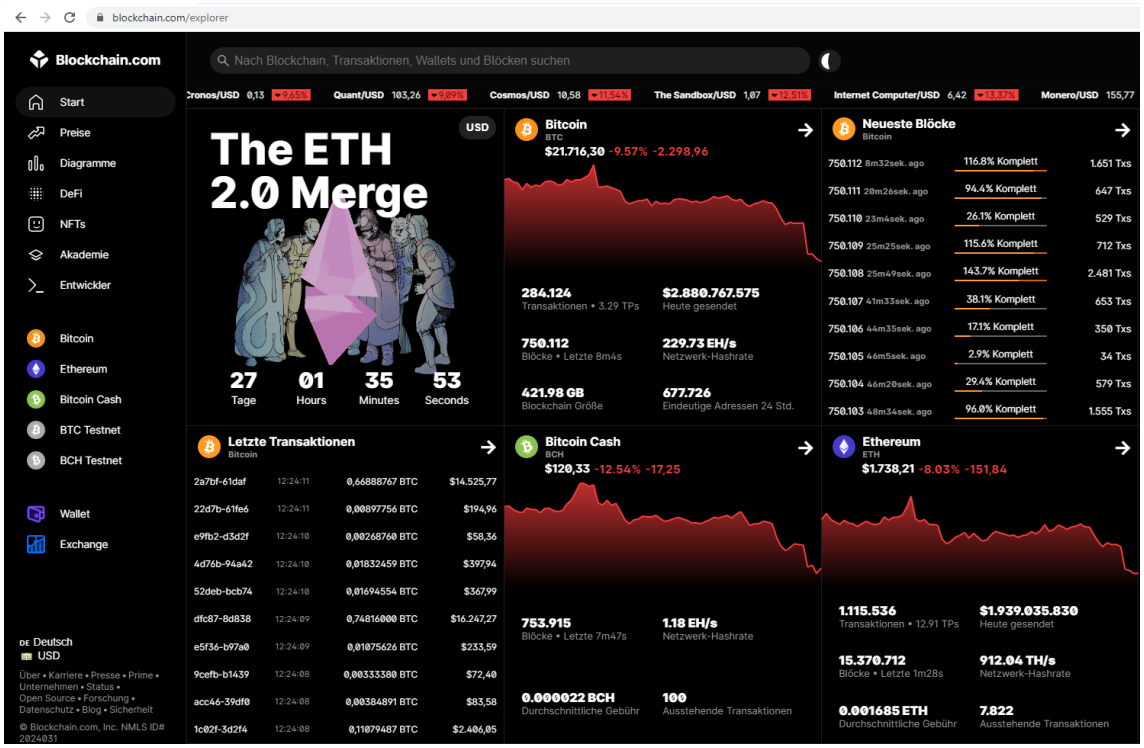


Bild 29: Explorer-Dienst auf Blockchain.com [46]

8.1.1 Analyse Testfall – T2

Die kryptografischen Spuren aus der IT-forensischen Untersuchung ließen sich mit dem Bitcoin-Explorer unter Blockchain.com zusammensetzen und weiter verfolgen. Als Ausgangspunkt wurden die Kryptowährungs-Objekte der ausgewerteten E-Mail-Kommunikation zwischen Erpresser und Opfer sowie die Einträge des unverschlüsselten Electrum-Wallets angewendet, die aus der Spurenauswertung des Testfalls T2 ermittelt werden konnten.

In der folgenden Tabelle 11 finden sich die akquirierten Kryptowährungs-Objekte.

Tabelle 11: Kryptowährungs-Objekte aus Testfall - T2

Sender	Bitcoin-Adresse	Transaktion	Zahlungsbetrag	Bitcoin-Adresse	Empfänger
Opfer	bc1qx8est8urgs2lxfvul4r5ax5yfmt483w08dwf2e	bd7a8dc1c6a287ca468f02799da4203da67137cf7d5765d3c3dc5257ea0857b6	0.0007 BTC (zzgl. Gebühren)	bc1q0yetwase0pcctlkseuzg8sanlg5lsjlzt4493l	Erpresser

Ausgangspunkt für eine Zahlungsflussanalyse konnten im Explorer-Dienst von Blockchain.com Daten aus Blockchains, Transaktionen, Wallets oder Blöcken sein.

Der Zahlungsfluss aus Testfall T2 ließ sich ausgehend von der Bitcoin-Senderadresse des Opfers bc1qx8est8urgs2lxfvul4r5ax5yfmt483w08dwf2e bis zur Empfängeradresse des Erpressers bc1q0yetwase0pcctlkseuzg8sanlg5lsjlzt4493l nachvollziehen.

Im folgenden Bild 30 wurde eine Suche nach der Bitcoin-Adresse des Opfers durchgeführt. Darin befanden sich mehrere relevante Informationen, die nachfolgend weiter ausgeführt werden.

Bild 30: Suchergebnis Bitcoin-Explorer über Transaktionen des Opfers [46]

In der Transaktionsübersicht ist zu erkennen, dass die Bitcoin-Adresse des Opfers (grüne Umrandung) eine initiale Transaktion von 0.0008 BTC zur Befüllung des eigenen Wallets durchführen musste. Diese Transaktion trägt den Zeitstempel 2022-06-04 21:30.

Am 19.08.2022 betrug der Wert der Bitcoin-Adresse zwischenzeitlich 48.087.27332642 BTC (1.028.024.155.35 $) mit insgesamt 436256 durchgeführten Transaktionen, weshalb bei dieser Bitcoin-Adresse von einem Finanzdienstleister bspw. einer Kryptowährungs-Börse ausgegangen werden konnte.

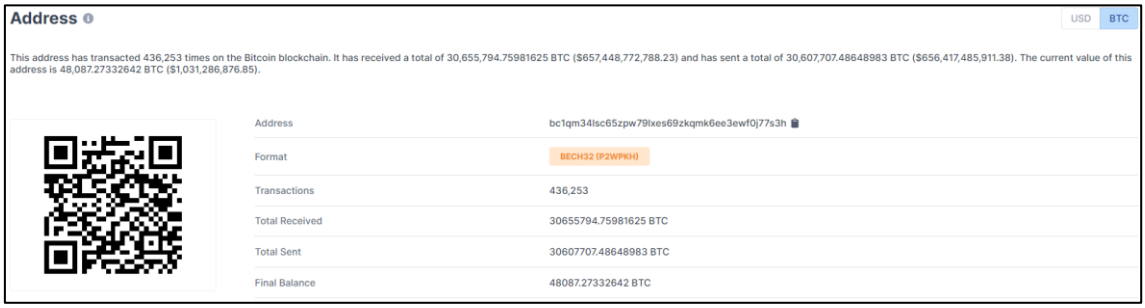


Bild 31: Die Bitcoin-Adresse, von der das Opfer eine initiale Zahlung erhielt, zeigte eine hohe Aktivität [46]

Angaben zur zugehörigen Entität dieser Bitcoin-Adresse machte der Dienst an dieser Stelle nicht. Hier sind die Ergebnisse aus der Analyse mit OXT.me interessant, die im Kapitel 8.2 dokumentiert wurden.

In der darauffolgenden Transaktion, die mit dem Zeitstempel 2022-06-04 21:39 nur 9 Minuten später stattgefunden hatte, wurde der Betrag von 0.0007 BTC an die Bitcoin-Adresse des Erpressers gesendet, siehe rote Umrandung in Bild 30.

Es lässt sich somit feststellen, dass sich die IT-forensischen Spuren aus der Datenauswertung innerhalb der Analyse mit dem Bitcoin-Explorer von Blockchain.com nachvollziehen ließen. Die relevante Transaktion zwischen Opfer und Erpresser war anhand der genutzten Bitcoin Sender- und Empfängeradressen nachvollziehbar.

8.1.2 Bewertung für den OSINT-Einsatz

Basierend auf den vorangegangenen Analysen des Testfalls T2 ergab sich folgende Bewertung für den Bitcoin-Explorer von Blockchain.com.

Tabelle 12: Blockchain.com - Bewertung für den OSINT-Einsatz

Kriterium	Bewertung	Kommentierung
Verfügbarkeit	+++	Der Dienst war während der Nutzung 100% verfügbar.
Neutralität	+++	Der Dienst selbst ist kommerziell orientiert, die Blockchain-Explorer-Funktionen jedoch frei verfügbar. Informationen zu Entitäten von Wettbewerbern, die auch als Akteure in Blockchain-Transaktionen agieren, bspw. Binance, konnten im untersuchten Testfall T2 nicht gefunden werden.
Hauptfunktionen	++	Die dargestellten Funktionen zur Suche nach verschiedenen Kriterien funktionierten stabil. Die Darstellung der Webseite und der Explorer-Funktionen war vergleichsweise intuitiv, wirkt zeitgemäß und gut nutzbar.

Aktualität	+++	Daten waren nach Ausführung der Transaktionen in Real-Time verfügbar.
Qualität	+++	In den Testfällen konnten keine Abweichungen zu den gesicherten Transaktionsdaten festgestellt werden.
Quantität	+	Leider wurden den Kryptowährungs-Adressen keine bekannten Entitäten zugeordnet, d.h. wenn eine Adresse bspw. einem Wallet von einem Wettbewerber wie Binance zuzuschreiben wäre, wurde dies nicht ausgewiesen. Dies ist für die Ermittlungsarbeit eher hinderlich, da keine realen Entitäten wie Krypto-Börsen, -Pools, -Services sowie Glückspielanbieter zugeordnet werden.
Kosten	+++	Der Blockchain-Explorer Dienst konnte zum Zeitpunkt der Erstellung dieser Arbeit kostenfrei genutzt werden.

8.2 Blockchain-Explorer: OXT.me

Nach Eigenaussage ist OXT.me ein Tool, das für die explorative Blockchain-Analyse des Bitcoin-Ledgers entwickelt wurde. Es dient der explorativen Blockchain-Analyse des Bitcoin-Ledgers. Dabei bietet es visuelle und interaktive Tools, die den Nutzern helfen, den Bitcoin-Ledger zu erforschen und die Dynamik in der Blockchain zu verstehen. [47]

Der Dienst selbst erscheinte non-profit orientiert, es waren jedoch auch Verweise zu dem kommerziell aktiven Wallet-Anbieter samouraiwallet.com zu finden.

Weitere Informationen zu den verantwortlichen Personen oder Firmen des Dienstes waren auf der Webseite von OXT.me nicht zu finden. Eine nachfolgend durchgeführte whois Abfrage ergab, dass die Domain bereits im Jahr 2015 bei dem französischen Internetdienstanbieter OVH.com registriert wurde und auch der Registrant der Domain aus Frankreich stammte.

```
Domain Name: OXT.ME
Registry Domain ID: D108500000016046524-AGRS
Registrar WHOIS Server:
Registrar URL: http://www.ovh.com
Updated Date: 2022-06-01T12:30:18Z
Creation Date: 2015-06-09T11:36:14Z
Registry Expiry Date: 2023-06-09T11:36:14Z
Registrar Registration Expiration Date:
Registrar: OVH
Registrar IANA ID: 433
Registrar Abuse Contact Email: abuse@ovh.net
Registrar Abuse Contact Phone: +33.972101007
Reseller:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant Organization:
Registrant State/Province:
Registrant Country: FR
Name Server: ANNA.NS.CLOUDFLARE.COM
Name Server: MILES.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2022-08-19T12:33:31Z <<<
```

Bild 32: Ergebnis des whois Abfrage von OXT.ME

8.2.1 Analyse Testfall – T2

Die kryptografischen Spuren aus der IT-forensischen Untersuchung ließen sich mit dem Blockchain-Explorer unter OXT.me weiter zusammensetzen und verfolgen. Als Ausgangspunkt wurden die Kryptowährungs-Objekte der ausgewerteten E-Mail-Kommunikation zwischen Erpresser und Opfer sowie die Einträge des unverschlüsselten Electrum-Wallets angewendet, die aus der Spurenauswertung des Testfalls T2 ermittelt werden konnten. Zusätzlich wurden aufgrund erweiterter Funktionen der Entitätszuordnung von Bitcoin-Adressen auch die Spuren aus Testfall T3 in die Analyse mit einbezogen.

In der folgenden Tabelle finden sich die gesicherten Kryptowährungs-Objekte aus T2.

Tabelle 13: Kryptowährungs-Objekte aus Testfall - T2

Sender	Bitcoin-Adresse	Transaktion	Zahlungsbetrag	Bitcoin-Adresse	Empfänger
Opfer	bc1qx8est8urgs2lxfvul4r5ax5yfmt483w08dwf2e	bd7a8dc1c6a287ca468f02799da4203da67137cf7d5765d3c3dc5257ea0857b6	0.0007 BTC (zzgl. Gebühren)	bc1q0yetwase0pcctlkseuzg8sanlg5lsjlzt4493l	Erpresser

Ausgangspunkt für eine Zahlungsflussanalyse im Bitcoin-Explorer von OXT.me konnten Blockdaten, Transaktionen oder Adressen sein. Ausgehend von der Bitcoin-Adresse ließen sich alle verbundenen Transaktionen darstellen. Hierbei wurde auch die initiale Transaktion zur Befüllung des eigenen Wallets des Opfers sichtbar.

Bild 33: Übersicht der Transaktionen des Opfers in OXT.me [47]

Bei einer genaueren Betrachtung der Einzahlungsadresse bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h ließ sich anhand der Daten erkennen, dass das Opfer die Einzahlung von einem offiziell registrierten Binance-Account aus vorgenommen hatte.

Im folgenden Bild 34 ist die entsprechende Adresse mit Zuordnung zur entsprechenden Binance-Transaktion ersichtlich.

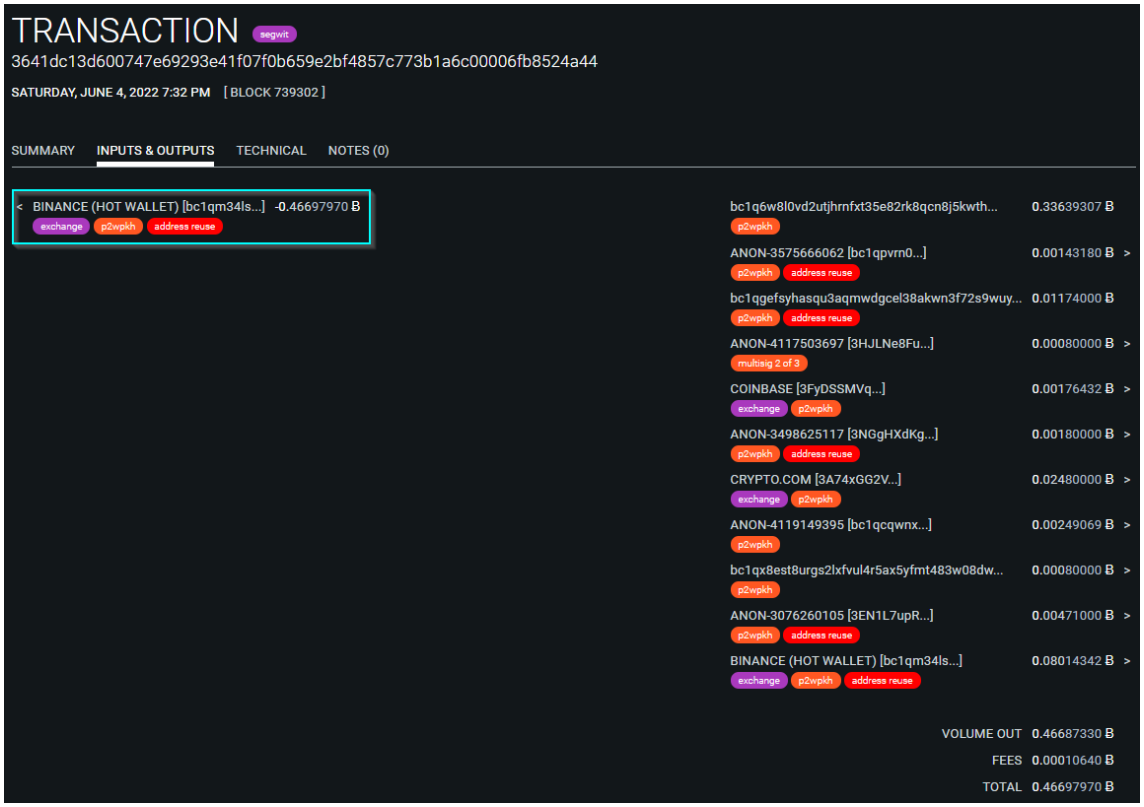


Bild 34: Initiale Einzahlung auf das Electrum Wallet des Opfers erfolgte von einem Binance-Account [47]

OXT.me bot für die weitere Analyse auch verschiedene Dashboards an, in denen statistische Verläufe grafisch aufbereitet wurden.

Im folgenden Bild 35 wurde die gefundene Bitcoin-Adresse mit Binance Zuordnung in Bezug des Aktivitätenverlaufs der ein- und ausgehenden Transaktionen dargestellt.

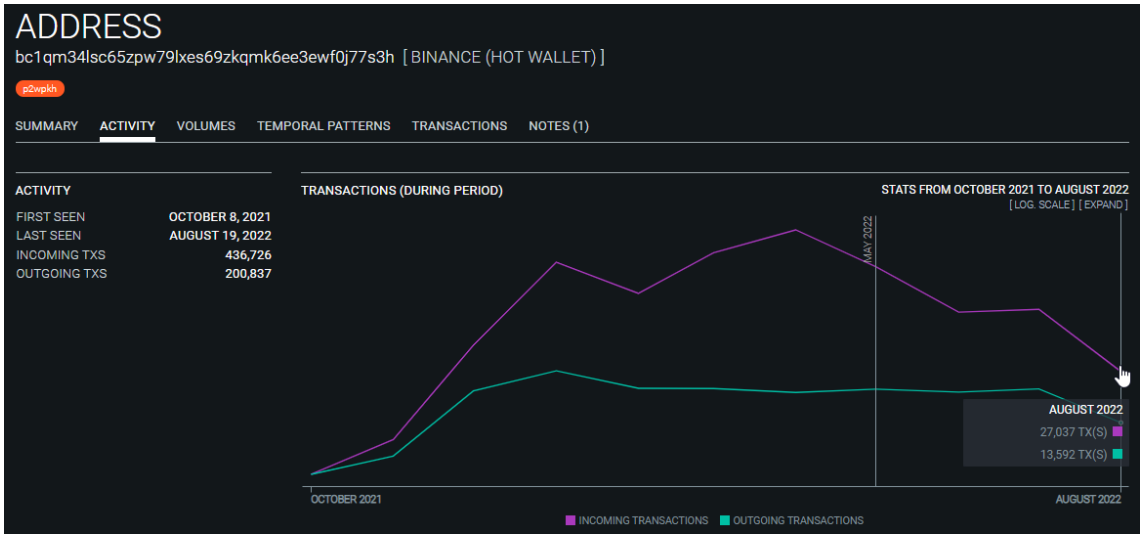


Bild 35: Verlaufskurven über eingehende und ausgehende Transaktionen einer Binance zugeordneten Bitcoin-Adresse [47]

Die fortlaufend hohe Aktivität der Bitcoin-Adresse bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h wurde durch die ausgewiesenen 436.726 eingehenden und 200.837 ausgehenden Transaktionen belegt.

Das dargestellte Transaktionsvolumen ist typisch für transparent agierende Akteure wie beispielsweise registrierte Kryptowährungs-Börsen, da diese i.d.R. kein Interesse daran haben, ihre Transaktionen durch fortlaufend wechselnde Adressen zu verschleiern.

8.2.2 Analyse Testfall – T3

Für die Analyse ist wichtig zu wissen, dass der Testfall T3 auf den Testfall T2 aufbaut: in T3 sind Folgetransaktionen aus T2 erfolgt und nachfolgend ausgewertet worden.

Der inhaltliche Kontext zur Durchführung der Analyse waren somit nur die Folgetransaktionen des Erpressers. Diese hatten im Testfall T3 weitere Artefakte erzeugt, die auf die Nutzung des Hardware-Wallet Ledger Nano S schließen ließen (siehe Ergebnisse in Kapitel 7.4.2).

In der Auswertung von T3 wurden keine zu T2 zusätzlichen Kryptowährungs-Objekte gefunden, weshalb die bereits aus T2 bekannte Bitcoin-Adresse des Erpressers als Startpunkt diente:

bc1q0yetwase0pcctlkseuzg8sanlg5lsjlzt4493l

Wie aus dem folgenden Bild 36 im Blockchain-Explorer ersichtlich ist, wies diese Adresse seit 4. Juni 2022 ein Guthaben von 0.00 Bitcoin aus.

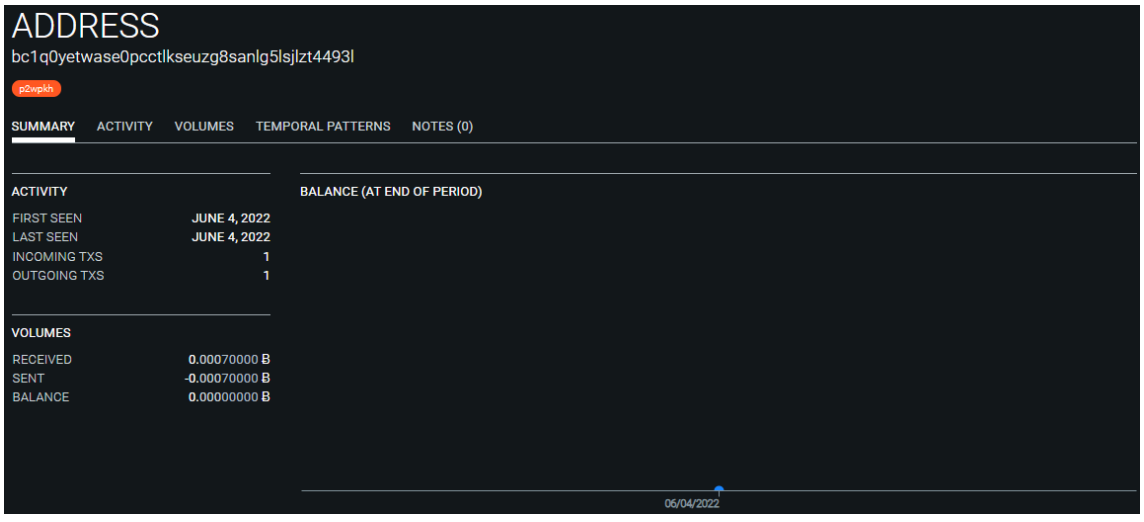


Bild 36: Anzeige des Guthabens einer Bitcoin-Adresse des Erpressers

Das hieß es muss eine Transaktion gegeben haben, die das Guthaben des Erpressers auf eine andere Bitcoin-Adresse transferiert hatte. Dies wurde über folgende Transaktion erkennbar:

14e4577dd4e89406e9e6522b8deceee563360d617177e827445d33637bc9d2b1

In den grünen Markierungen des folgenden Bild 37 wurden die Bitcoin-Transaktionen sowie damit verbundene Empfänger-Adressen dargestellt.

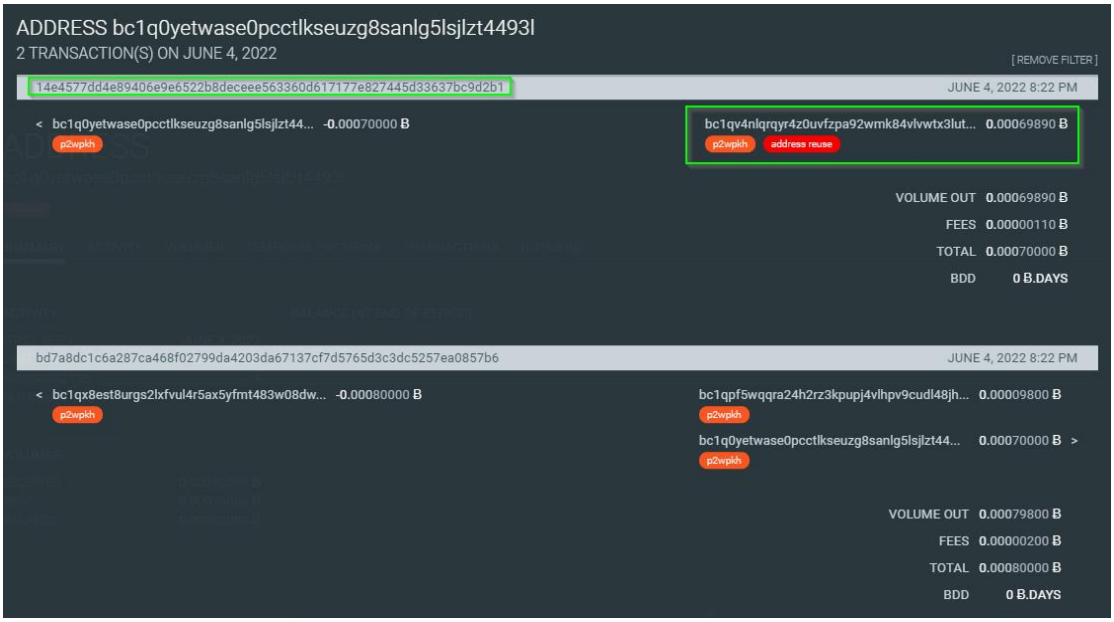


Bild 37: Transaktionen einer Bitcoin-Adresse des Erpressers

Verfolgte man nun die erste Transaktion (grüne Markierung) zur Bitcoin-Empfänger-Adresse weiter, gab OXT.me eine weitere Bitcoin-Adresse aus:

bc1qv4nlqrqyr4z0uvfzpa92wmk84vlvwtx3lutfkz

Diese Adresse war die zweite Bitcoin-Adresse, die auch dem Erpresser zuzuschreiben ist und auf dem Wallet Ledger Nano S verwaltet wurde.

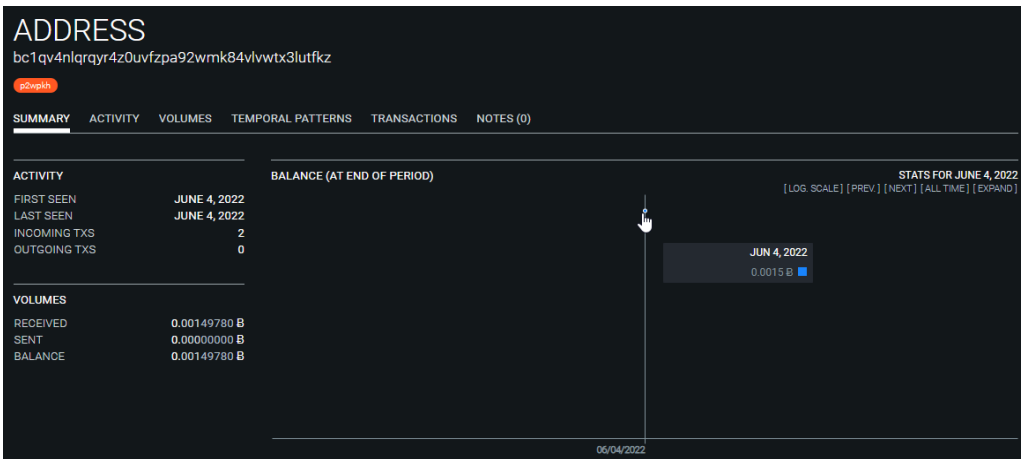


Bild 38: Anzeige des Guthabens einer weiteren Bitcoin-Adresse des Erpressers

In der folgenden Tabelle 14 sind die zuvor erfassten Kryptowährungs-Objekte dieser Transaktion nochmals kurz zusammengefasst.

Tabelle 14: Transaktion zur Weiterleitung der erpressten Bitcoins auf ein Ledger Nano S

Sender	Bitcoin-Adresse	Transaktion	Zahlungsbetrag	Bitcoin-Adresse	Empfänger
Erpresser	bc1q0yetwase0pcctlkseuzg8sanlg5lsjlzt4493l	14e4577dd4e89406e9e6522b8deceee563360d617177e827445d33637bc9d2b1	0.0006989 BTC (zzgl. Gebühren)	bc1qv4nlqrqyr4z0uvfzpa92wmk84vlvwtx3lutfkz	Erpresser

8.2.3 Bewertung für den OSINT-Einsatz

Basierend aus den vorangegangenen Analysen der Testfälle T2 und T3 ergab sich folgende Bewertung für den OXT.me Blockchain-Explorer.

Tabelle 15: OXT.me - Bewertung für den OSINT-Einsatz

Kriterium	Bewertung	Kommentierung
Verfügbarkeit	+++	Der Dienst war während der Nutzung 100% verfügbar.
Neutralität	++	Der Dienst selbst erschien non-profit orientiert, es waren jedoch auch Verweise zu dem kommerziell aktiven Wallet-Anbieter samouraiwallet.com zu finden.
Hauptfunktionen	++	Die dargestellten Funktionen zur Suche nach verschiedenen Kriterien funktionierten stabil. Die Darstellung der Webseite und der Explorer-Funktionen war vergleichsweise intuitiv, wirkte zeitgemäß und gut nutzbar.

Aktualität	+++	Daten waren augenscheinlich tagesaktuell verfügbar gewesen.
Qualität	+++	In den Testfällen konnten keine Abweichungen zu den gesicherten Transaktionsdaten festgestellt werden.
Quantität	+++	Verschiedenen Bitcoin-Adressen wurden teils reale Entitäten zugeordnet, d.h. das für einzelne Adressen von Kryptowährungs-Börsen wie bspw. Binance eine konkrete Zuordnung erfolgte. Dies kann für die Ermittlungsarbeit hilfreich sein, da damit teils reale Entitäten registrierter Unternehmen einbezogen werden können.
Kosten	+++	Der Blockchain-Explorer Dienst konnte zum Zeitpunkt der Erstellung dieser Arbeit kostenfrei genutzt werden.

8.3 Wallet-Explorer: WalletExplorer.com

Der webbasierte Dienst WalletExplorer.com eignete sich besonders, um einem Wallet mehrere Bitcoin-Adressen zuzuordnen.

Es handelte sich dabei um einen Bitcoin-Block-Explorer mit Nutzung von Adressgruppierung und Wallet-Kennzeichnung. Es konnten die Bitcoin-Adresse, txid, firstbits (erste Adresszeichen), erste txid-Zeichen, interne Wallet-ID oder Dienstname zur Suche verwendet werden.

8.3.1 Analyse Testfall – T0

Die kryptografischen Spuren aus der IT-forensischen Untersuchung ließen sich mit dem WalletExplorer.com weiter zusammensetzen und verfolgen. Als Ausgangspunkt wurden die Kryptowährungs-Objekte des Electrum-Wallets angewendet, die aus der Spurenauswertung des Testfalls T0 ermittelt werden konnten.

Tabelle 16: Kryptowährungs-Objekte aus Testfall - T0

Sender	Bitcoin-Adresse	Transaktion	Zahlungsbetrag	Bitcoin-Adresse	Empfänger
Kunde	bc1q34hcaqa95lchs5f4nkrk0vsrwvnx8vwmku9r6r	71a997ef103972d3787458c6b294a6d189ba90c8bf56c6e80daaae921afc6f50	0.0002 BTC (zzgl. Gebühren)	bc1qwtkutllfdf0duhdyez8wcq6xulq94d55q7xznz	Anbieter

Ausgangspunkt für eine Zahlungsflussanalyse konnte im WalletExplorer eine Transaktions-ID, Sender- oder Empfängeradresse, interne Wallet-ID, XPUB/YPUB/ZPUB oder ein Service Name sein. [48]

Wie im folgenden Bild 39 zu sehen ist, ergab die Suche nach der vom Kunden genutzten Bitcoin-Adresse im WalletExplorer einen Treffer:

bc1q34hcaqa95lchs5f4nkrk0vsrwvnx8vwmku9r6r

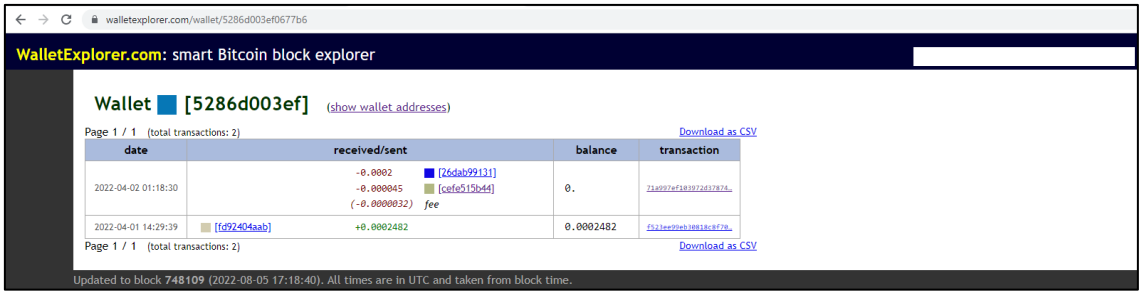


Bild 39: WalletExplorer.com - Suchtreffer bc1q34hcaqa95lchs5f4nkrk0vsrwvnx8vwmku9r6r [48]

Der WalletExplorer bildete eine WalletID ab; im vorliegenden Fall war es die ID [5286d003ef], die auf die bekannte Bitcoin-Adresse des Kunden bc1q34hcaqa95lchs5f4nkrk0vsrwvnx8vwmku9r6r auflöste. Eine Suche nach WalletID oder Bitcoin-Adresse führte hierbei zum gleichen Ergebnis. Neben dem Ausführungsdatum wurden die mit der Transaktion gesendeten Bitcoins, entstandene Gebühren und die Balance nach Ausführung durch den WalletExplorer ausgegeben. Über die Transaktions-ID

71a997ef103972d3787458c6b294a6d189ba90c8bf56c6e80daaae921afc6f50

war ersichtlich, wohin der ausgewiesene Betrag von 0.0002 BTC geflossen ist.

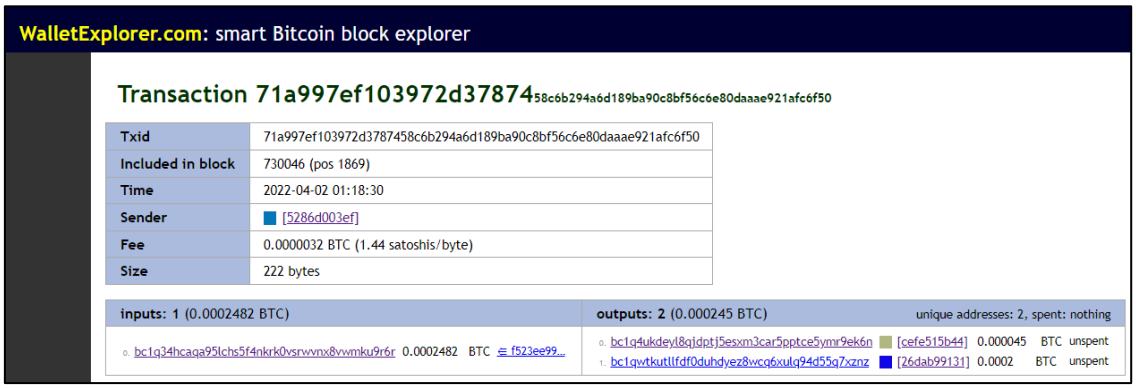


Bild 40: Transaktion mit Input des Kunden und Output an Anbieter [48]

Die Darstellung im WalletExplorer ermöglichte es, ausgehend von der Zahlung des Kunden, über die Transaktion an die Bitcoin-Adresse des Anbieters zu gelangen. In folgenden Bild 41 findet sich das Wallet des Anbieters der illegalen Waren.

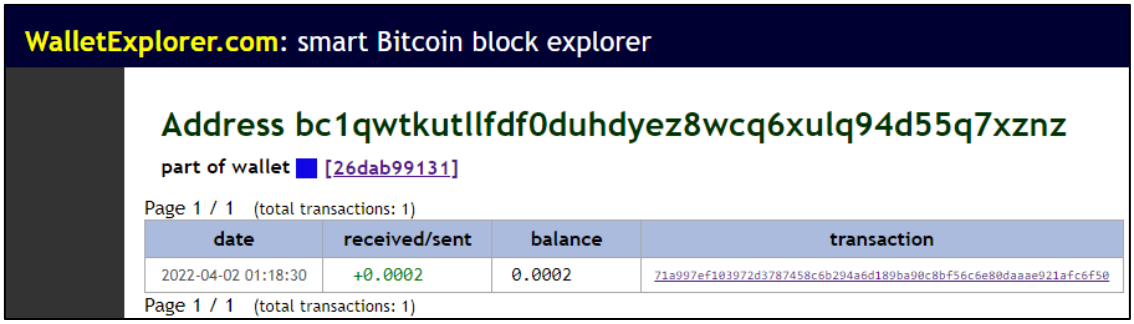


Bild 41: Wallet des Anbieters bc1qwtkutllfdf0duhdyez8wcq6xulq94d55q7xznz mit Eingangsbuchung des Kunden [48]

8.3.2 Analyse Testfall – T4

Nach Eingabe der als verdächtig eingestuften Bitcoin-Adresse 12HaVrpXkLr2UnkMf6X9bY11cuNrZUdUnV in die WalletExplorer Suchmaske ergaben sich aus dem Suchergebnis verschiedene Möglichkeiten der Analyse. Anzumerken ist, dass auch der Download als CSV-Datei angeboten wurde, um die Transaktionen in einem externen Tool zur Datenanalyse weiter auszuwerten. Der WalletExplorer fasst mehrere Bitcoin-Adressen zu einem Wallet zusammen, weshalb als Suchergebnis die Wallet-ID [c13d678521] ausgegeben wurde wovon eben die Adresse 12HaVrpXkLr2UnkMf6X9bY11cuNrZUdUnV zugeordnet ist. Wie auf dem folgenden Bild 42 ersichtlich wurde, ist im vorliegenden Wallet ausschließlich die oben genannte Adresse zugeordnet worden.

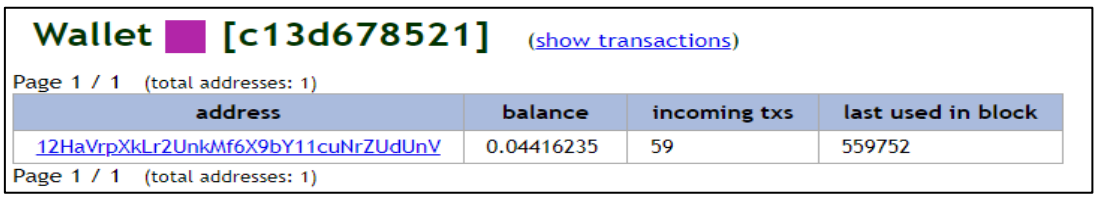
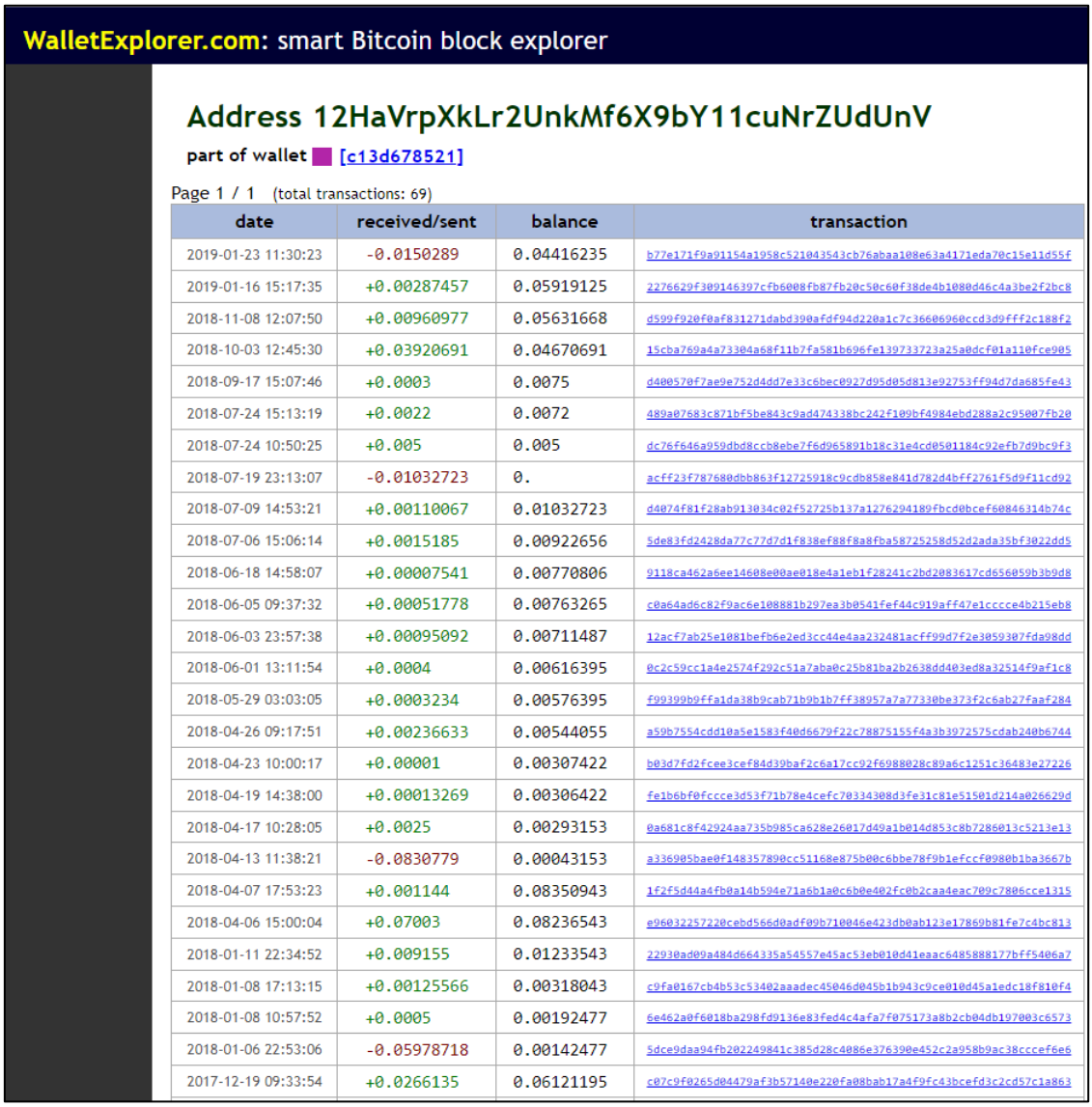


Bild 42: Wallet [c13d678521] nutzte ausschließlich die Bitcoin-Adresse 12HaVrpXkLr2UnkMf6X9bY11cuNrZUdUnV [48]

Dem Wallet [c13d678521] waren insgesamt 69 Transaktionen zugeordnet, wovon 59 als eingehende und 10 als ausgehende Transaktionen gewertet werden konnten. In folgenden Bild 43 findet sich ein Auszug dieser Transaktionen:



WalletExplorer.com: smart Bitcoin block explorer

Address 12HaVrpXkLr2UnkMf6X9bY11cuNrZUdUnV

part of wallet [c13d678521]

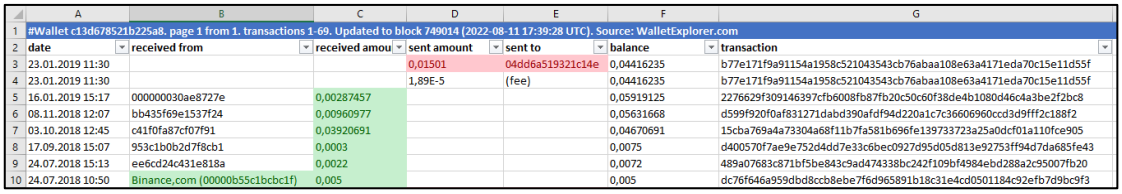
Page 1 / 1 (total transactions: 69)

date	received/sent	balance	transaction
2019-01-23 11:30:23	-0.0150289	0.04416235	b77e171f9a91154a1958c521043543cb76abaa108e63a4171eda70c15e11d55f
2019-01-16 15:17:35	+0.00287457	0.05919125	2276629f309146397cfb6008fb87fb20c50c60f38de4b1080d46c4a3be2f2bc8
2018-11-08 12:07:50	+0.00960977	0.05631668	d599f920f0af831271dabd390afdf94d220a1c7c36606960ccd3d9fff2c188f2
2018-10-03 12:45:30	+0.03920691	0.04670691	15cba769a4a73304a68f11b7fa581b696fe139733723a25a0dcf01a110fce905
2018-09-17 15:07:46	+0.0003	0.0075	d400570f7ae9e752d4dd7e33c6bec0927d95d05d813e92753ff94d7da685fe43
2018-07-24 15:13:19	+0.0022	0.0072	489a07683c871bf5be843c9ad474338bc242f109bf4984ebd288a2c95007fb20
2018-07-24 10:50:25	+0.005	0.005	dc76f646a959dbd8ccb8ebe7f6d965891b18c31e4cd0501184c92efb7d9bc9f3
2018-07-19 23:13:07	-0.01032723	0.	acff23f787680dbb863f12725918c9cdb858e841d782d4bff2761f5d9f11cd92
2018-07-09 14:53:21	+0.00110067	0.01032723	d4074f81f28ab913034c02f52725b137a1276294189fbcd0bcef60846314b74c
2018-07-06 15:06:14	+0.0015185	0.00922656	5de83fd2428da77c77d7d1f838ef88f8a8fba58725258d52d2ada35bf3022dd5
2018-06-18 14:58:07	+0.00007541	0.00770806	0118ca462a6ee14608e00ae018e4a1eb1f28241c2bd2083617cd656059b3b9d8
2018-06-05 09:37:32	+0.00051778	0.00763265	c0a64ad6c82f9ac6e108881b297ea3b0541fef44c919aff47e1ccccc4b215eb8
2018-06-03 23:57:38	+0.00095092	0.00711487	12acf7ab25e1081befb6e2ed3cc44e4aa232481acff99d7f2e3059307fda98dd
2018-06-01 13:11:54	+0.0004	0.00616395	0c2c59cc1a4e2574f292c51a7aba0c25b81ba2b2638dd403ed8a32514f9af1c8
2018-05-29 03:03:05	+0.0003234	0.00576395	f99399b9ffa1da38b9cab71b9b1b7ff38957a7a7730be373f2c6ab27faaf284
2018-04-26 09:17:51	+0.00236633	0.00544055	a59b7554cdd10a5e1583f40d6679f22c78875155f4a3b3972575cdab240b6744
2018-04-23 10:00:17	+0.00001	0.00307422	b03d7fd2fcee3cef84d39baf2c6a17cc92f6988028c89a6c1251c36483e27226
2018-04-19 14:38:00	+0.00013269	0.00306422	fe1b6bf0fccce3d53f71b78e4cefc70334308d3fe31c81e51501d214a026629d
2018-04-17 10:28:05	+0.0025	0.00293153	0a681c8f42924aa735b985ca628e26017d49a1b014d853c8b7286013c5213e13
2018-04-13 11:38:21	-0.0830779	0.00043153	a336905bae0f148357890cc51168e875b00c6bbe78f9b1efccf0980b1ba3667b
2018-04-07 17:53:23	+0.001144	0.08350943	1f2f5d44a4fb0a14b594e71a6b1a0c6b0e402fc0b2caa4eac709c7806cce1315
2018-04-06 15:00:04	+0.07003	0.08236543	e96032257220cebd566d0adf09b710046e423db0ab123e17869b81fe7c4bc813
2018-01-11 22:34:52	+0.009155	0.01233543	22930ad09a484d664335a54557e45ac53eb010d41eaac6485888177bff5406a7
2018-01-08 17:13:15	+0.00125566	0.00318043	c9fa0167cb4b53c53402aaadec45046d045b1b943c9ce010d45a1edc18f810f4
2018-01-08 10:57:52	+0.0005	0.00192477	6e462a0f6018ba298fd9136e83fed4c4afa7f075173a8b2cb04db197003c6573
2018-01-06 22:53:06	-0.05978718	0.00142477	5dce9daa94fb202249841c385d28c4086e376390e452c2a958b9ac38cccef6e6
2017-12-19 09:33:54	+0.0266135	0.06121195	c07c9f0265d04479af3b57140e220fa08bab17a4f9fc43bcefd3c2cd57c1a863

Bild 43: Auszug der 69 Transaktionen von Wallet [c13d678521] [48]

Aus der exportierten CSV-Datei, die alle Transaktionsdaten des Wallets enthielt, ließ sich für die weitere Datenanalyse ein Daten-Import in Excel durchführen.

In folgenden Bild 44 findet sich ein Auszug einer beispielhaften Datenanalyse durch Datenimport und -auswertung in Excel.



	A	B	C	D	E	F	G
1	#Wallet c13d678521b225a8. page 1 from 1. transactions 1-69. Updated to block 749014 (2022-08-11 17:39:28 UTC). Source: WalletExplorer.com						
2	date	received from	received amou	sent amount	sent to	balance	transaction
3	23.01.2019 11:30			0,01501	04dd6a519321c14e	0,04416235	b77e171f9a91154a1958c521043543cb76abaa108e63a4171eda70c15e11d55f
4	23.01.2019 11:30			1,89E-5	(fee)	0,04416235	b77e171f9a91154a1958c521043543cb76abaa108e63a4171eda70c15e11d55f
5	16.01.2019 15:17	000000030ae8727e	0,00287457			0,05919125	2276629f309146397cfb6008fb87fb20c50c60f38de4b1080d46c4a3be2f2bc8
6	08.11.2018 12:07	bb435f69e1537f24	0,00960977			0,05631668	d599f920f0af831271dabd390afdf94d220a1c7c36606960ccd3d9fff2c188f2
7	03.10.2018 12:45	c41f0fa87cf07f91	0,03920691			0,04670691	15cba769a4a73304a68f11b7fa581b696fe139733723a25a0dcf01a110fce905
8	17.09.2018 15:07	953c1b0b2d7f8cb1	0,0003			0,0075	d400570f7ae9e752d4dd7e33c6bec0927d95d05d813e92753ff94d7da685fe43
9	24.07.2018 15:13	ee6cd24c431e818a	0,0022			0,0072	489a07683c871bf5be843c9ad474338bc242f109bf4984ebd288a2c95007fb20
10	24.07.2018 10:50	Binance.com (00000b55c1bcbc1f)	0,005			0,005	dc76f646a959dbd8ccb8ebe7f6d965891b18c31e4cd0501184c92efb7d9bc9f3

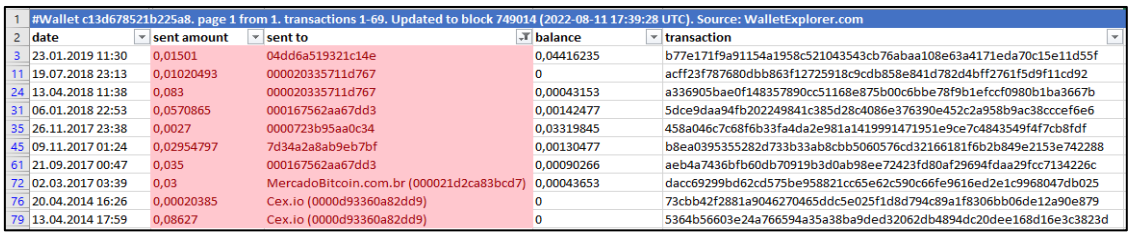
Bild 44: Excel-basierte Datenanalyse auf Basis von Daten des WalletExplorer

Die gesamte Datenanalyse befindet sich in der Anlage 6: S2.2_T4_walletexplorer-c13d678521b225a8-1.xlsx

Aus der vorangegangenen Datenauswertung konnten verschiedene Erkenntnisse gewonnen werden.

Die initiale Transaktion, aus der die vorliegende Bitcoin-Adresse Zahlungen erhielt, wurde durch sog. CoinJoin Transaktionen durchgeführt. Coinjoin ist eine sog. On-Chain-Lösung für Bitcoin mit dem Ziel der Verbesserung der Privatsphäre. Das Konzept wurde erstmals 2013 von Gregory Maxwell vorgeschlagen. Es wurde entwickelt, um die “Common-Input-Ownership-Heuristic” (Gemeineigentums-Heuristik) zu brechen. Diese geht davon aus, dass alle Inputs einer Transaktion der gleichen Entität gehören. [49]

Durch die Nutzung von CoinJoin Transaktionen wurden involvierte Entitäten weiter verschleiert und eine Nachverfolgbarkeit zu der handelnden Identität zusätzlich erschwert. Die Opfer der Erpressung nutzten zur Zahlung des Lösegelds u.a. den Zahlungsdienstleister Binance.com. Von besonderem Interesse ist jedoch die Erkenntnis, dass die Abgänge der Transaktion teilweise an andere Währungsbörsen gingen:



1	#Wallet c13d678521b225a8. page 1 from 1. transactions 1-69. Updated to block 749014 (2022-08-11 17:39:28 UTC). Source: WalletExplorer.com				
2	date	sent amount	sent to	balance	transaction
3	23.01.2019 11:30	0,01501	04dd6a519321c14e	0,04416235	b77e171f9a91154a1958c521043543cb76abaa108e63a4171eda70c15e11d55f
11	19.07.2018 23:13	0,01020493	000020335711d767	0	acff23f787680dbb863f12725918c9cdb858e841d782d4bff2761f5d9f11cd92
24	13.04.2018 11:38	0,083	000020335711d767	0,00043153	a336905bae0f148357890cc51168e875b00c6bbe78f9b1efccf0980b1ba3667b
31	06.01.2018 22:53	0,0570865	000167562aa67dd3	0,00142477	5dce9daa94fb202249841c385d28c4086e376390e452c2a958b9ac38cccef6e6
35	26.11.2017 23:38	0,0027	0000723b95aa0c34	0,03319845	458a046c7c68f6b33fa4da2e981a1419991471951e9ce7c4843549f4f7cb8fdf
45	09.11.2017 01:24	0,02954797	7d34a2a8ab9eb7bf	0,00130477	b8ea0395355282d733b33ab8cbb50605760cd32166181f6b2b849e2153e742288
61	21.09.2017 00:47	0,035	000167562aa67dd3	0,00090266	aeb4a7436bfb60db70919b3d0ab98ee72423fd80af29694fdaa29fcc7134226c
72	02.03.2017 03:39	0,03	MercadoBitcoin.com.br (000021d2ca83bcd7)	0,00043653	dacc69299bd62cd575be958821cc65e62c590c66fe9616ed2e1c9968047db025
76	20.04.2014 16:26	0,00020385	Cex.io (0000d93360a82dd9)	0	73cbb42f2881a9046270465ddc5e025f1d8d794c89a1f8306bb06de12a90e879
79	13.04.2014 17:59	0,08627	Cex.io (0000d93360a82dd9)	0	5364b56603e24a766594a35a38ba9ded32062db4894dc20dee168d16e3c3823d

Bild 45: Zahlungsausgänge an andere Wallets und Kryptowährungs-Dienste [48]

Bei CEX.io handelte es sich um ein offiziell registriertes Unternehmen, gegründet 2013 in London, Großbritannien. Ursprünglich war es ein Cloud-Mining-Anbieter, der den GHash.io-Mining-Pool besaß. 2014 war GHash einer der größten Mining-Pools der Welt. Anfang 2015 wurde von CEX.io beschlossen, die Cloud-Mining-Dienstleistungen einzustellen. CEX.io wird seither ausschließlich als Kryptowährungs-Austauschplattform betrieben. [50]

Eine weitere Krypto-Börse, an die aus dem vorliegenden Wallet Bitcoins abgeflossen sind, ist MercadoBitcoin.com.br. Diese Krypto-Börse behauptet von sich selbst zu den 25 vertrauenswürdigsten Börsen der Welt zu gehören und die größte Plattform für Kryptowährungen und digitale Vermögenswerte in Lateinamerika zu sein, mehr als 3 Millionen Kunden sollen dort registriert sein. [51]

Aus Sicht einer Ermittlung fanden sich damit Ansätze, die realen Identitäten, die als Empfänger der ausgehenden Transaktionen begünstigt wurden, aufzudecken. Da es sich bei den genannten Kryptowährungs-Dienstanbietern um registrierte Unternehmen handelte, könnten generell Datenauskunftsverfahren gegenüber diesen Finanzdienstleistern ausgelöst werden, um ggf. die dahinterliegenden Personen offenzulegen, die für die Konten bei Eröffnung registriert wurden.

8.3.3 Bewertung für den OSINT-Einsatz

Basierend auf den vorangegangenen Analysen der Testfälle T0 und T4 ergab sich folgende Bewertung für den WalletExplorer.

Tabelle 17: WalletExplorer.com - Bewertung für den OSINT-Einsatz

Kriterium	Bewertung	Kommentierung
Verfügbarkeit	+++	Der Dienst war während der Nutzung 100% verfügbar.
Neutralität	+++	Der Dienst selbst ist Non-Profit orientiert. Anzumerken ist, dass auf der Webseite steht, dass der Entwickler Ales Janda mittlerweile bei dem kommerziellen Anbieter Chainalysis als Programmierer und Analyst arbeitet. Es bleibt zu hoffen, dass der Dienst weiterhin neutral und Non-Profit orientiert arbeitet.
Hauptfunktionen	++	Der Dienst bietet eine Zusammenfassung von verschiedenen Adressen zu einem Wallet an. Das ist nützlich, da die Adressen oft wechseln können und somit u.U. dennoch einem Wallet zugeordnet werden können. Der Mechanismus war in Teilen vom Autor beschrieben unter den FAQ nachzulesen. Die dargestellten Funktionen zur Suche nach verschiedenen Kriterien funktionierten stabil, auch eine JSON-API könnte auf Nachfrage bereitgestellt werden. Die Darstellung der Webseite ist nicht intuitiv und wirkte nicht mehr zeitgemäß, hier könnte durch ein Update des User-Interface noch mehr Akzeptanz hergestellt werden.

Aktualität	++	Die Daten waren nicht in Real-Time verfügbar, sondern wurden ca. alle 1-2 Tage aktualisiert.
Qualität	+++	In den Testfällen konnten keine Abweichungen zu den gesicherten Transaktionsdaten festgestellt werden.
Quantität	+++	Zwar waren die Funktionen auf das wichtigste beschränkt, d.h. Suche und Analyse, jedoch bot der Dienst auch eine Vielzahl von Daten zu aktuellen und historischen „Top-Wallets“ an, die realen Entitäten wie Krypto- Börsen, Pools, Services sowie Glückspielanbietern zugeordnet sind.
Kosten	+++	Der Dienst konnte zum Zeitpunkt der Erstellung dieser Arbeit vollkommen kostenfrei genutzt werden.

8.4 Datenbank: Bitcoinabuse.com

Aus Sicht von Akteuren, die beabsichtigen, Bitcoin-Transaktionen durchzuführen, ist ein wichtiges Kriterium noch vor der Transaktion zu wissen, ob die Empfänger-Adresse vertrauenswürdig erscheint. Daher sind Bitcoin-Adressen, die in der Vergangenheit bei anderen Personen bereits negativ aufgefallen sind, von hohem Interesse. Der Dienst Bitcoinabuse.com setzt an dieser Stelle an und bietet im Wesentlichen eine öffentlich zugängliche Datenbank mit spezifischen Bitcoin-Adressen, die vor Betrügern, Hackern und anderen kriminellen Akteuren warnen sollen. Ziel ist es, Personen vor Betrügern zur warnen, deren Bitcoin-Adressen im Zusammenhang mit kriminellen Aktivitäten stehen.

Hauptfunktionen von Bitcoinabuse.com:

- Meldung von verdächtigen Bitcoin-Adressen
- Möglichkeit, lokale Strafverfolgungsbehörden durch eine Meldung zu informieren
- Abfrage von verdächtigen Bitcoin-Adressen aus der Datenbank
- Monitoring verdächtiger Bitcoin-Adressen
- Angebot einer API, die folgende Funktionen beinhaltet:
    - Bitcoin-Adresse melden
    - Nachschlagen von Arten des Bitcoin-Missbrauchs
    - Suche nach bestimmten Meldungen
    - Eine Adresse überprüfen
    - Alle Meldungen herunterladen

8.4.1 Analyse von BitcoinAbuse.com

Die öffentlich zugängliche Datenbasis besteht aus Selbstmeldungen, beispielsweise von betroffenen Betrugsopfern. In folgendem Bild 46 ist das Formular zur Meldung betrügerischer Adressen dargestellt:

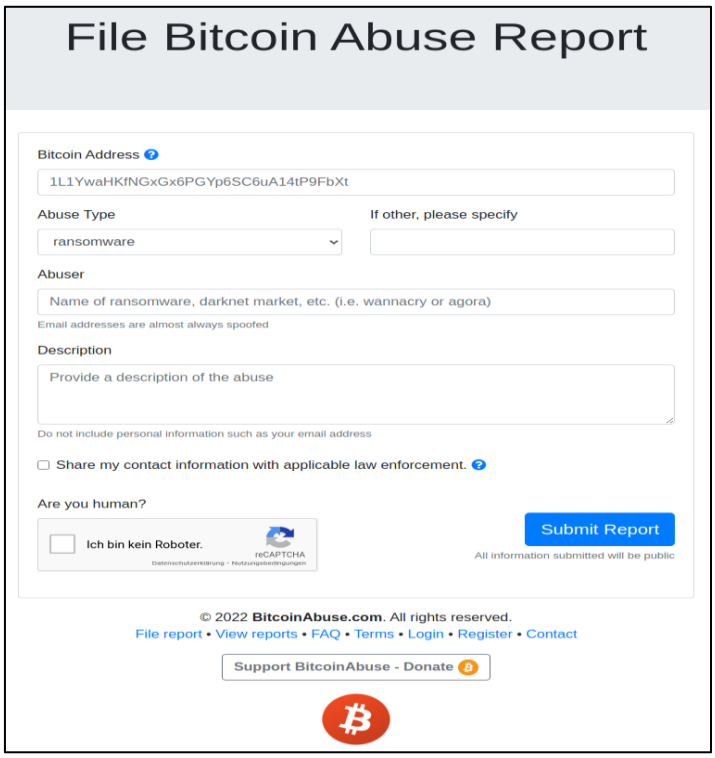


Bild 46: Formular zur Eingabe von potentiell betrügerischen Bitcoin-Adressen [52]

Eine Abfrage von verdächtigen Adressen ergab am Beispiel der Bitcoin-Adresse 1CFPa4vNQGS14UB3TZAeH6cWadSBcYiaaQ, die im folgenden Bild 47 dargestellten Information:

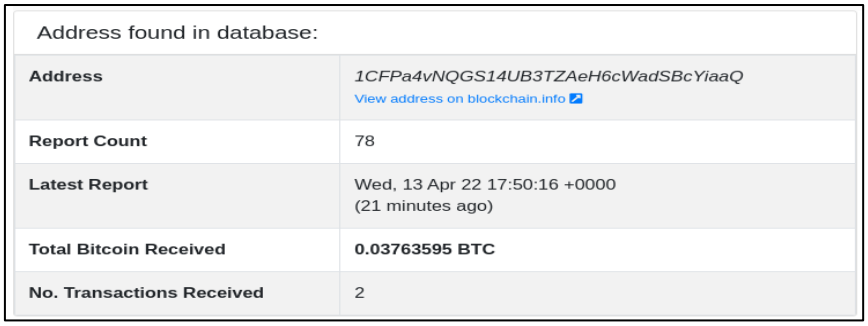


Bild 47: Ausgabe eines Abfrage-Treffers der BitcoinAbuse.com Datenbank [52]

Die betreffende Bitcoin-Adresse wurde insgesamt 78-mal gemeldet, wobei zum Zeitpunkt der Sichtung die letzte Meldung am 13. April 2022 um 17:50:16, d.h. 21 Minuten vor Erstellung des obigen Bild 47 erfolgt war. Die Gesamtmenge der Transaktionen und erhaltenen Bitcoins wurde hierbei auch ausgewiesen.

Die Verwendung des Dienstes ließ schnell Fragen zur Datenqualität aufkommen, denn durch das Angebot der schnellen und formlosen Betrugsmeldung erschienen auch Falschmeldungen nicht ausgeschlossen zu sein. Eine weitere Recherche nach dem Betreiber des Dienstes verlief teils spurlos. Über eine whois Abfrage der Domain BitcoinAbuse.com ließen sich keine Hintergrundinformationen zum Anbieter erkennen.

In der Ausgabe von Bild 48 sind die entsprechenden Felder, die einen Rückschluss auf den Diensteanbieter geben würden, anonymisiert worden.

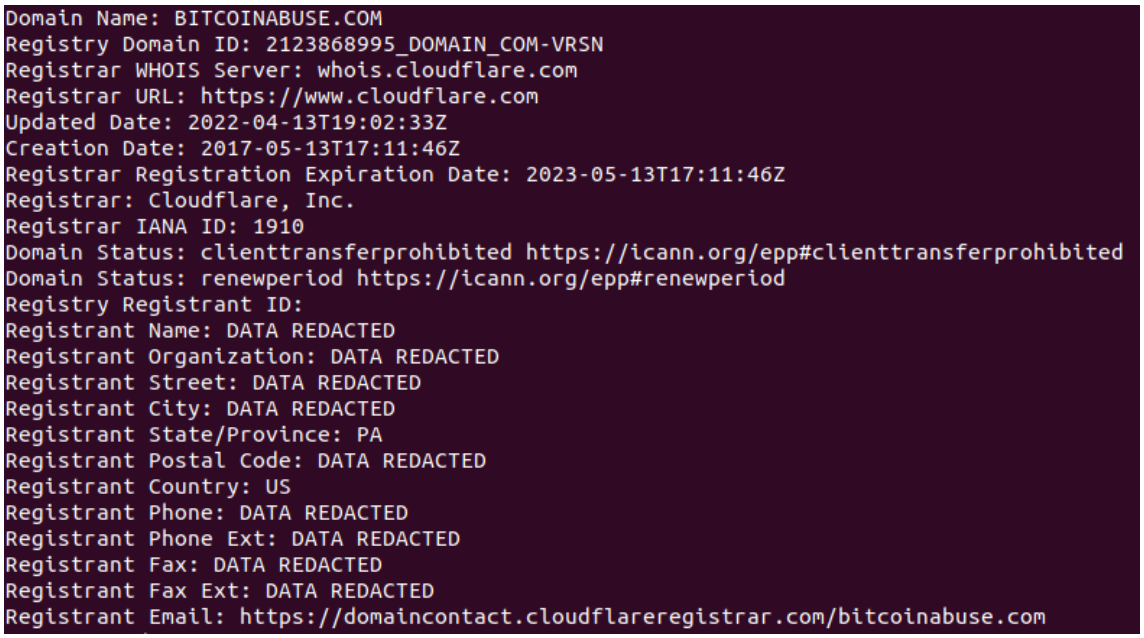


Bild 48: Ergebnis der Whois-Abfrage für die Domain bitcoinabuse.com [52]

Inwiefern sich der Dienst zukünftig entwickelt, ist aktuell schwer zu prognostizieren, denn die Anzahl der Betrugsmeldungen hatte bereits in 2020 mit jährlich 102233 Meldungen einen Peak. In 2021 war die Anzahl mit 55040 Meldungen rückläufig. Seit Beginn des laufenden Jahres 2022 sind es 12726 Meldungen (Stand: 15. April 2022) mit 121 pro Tag leicht unter Vorjahresniveau.

In der folgenden Grafik in Bild 49, die auf BitcoinAbuse am 15. April 2022 abrufbar war, konnte der rückläufige Trend von Betrugsmeldungen erkannt werden:

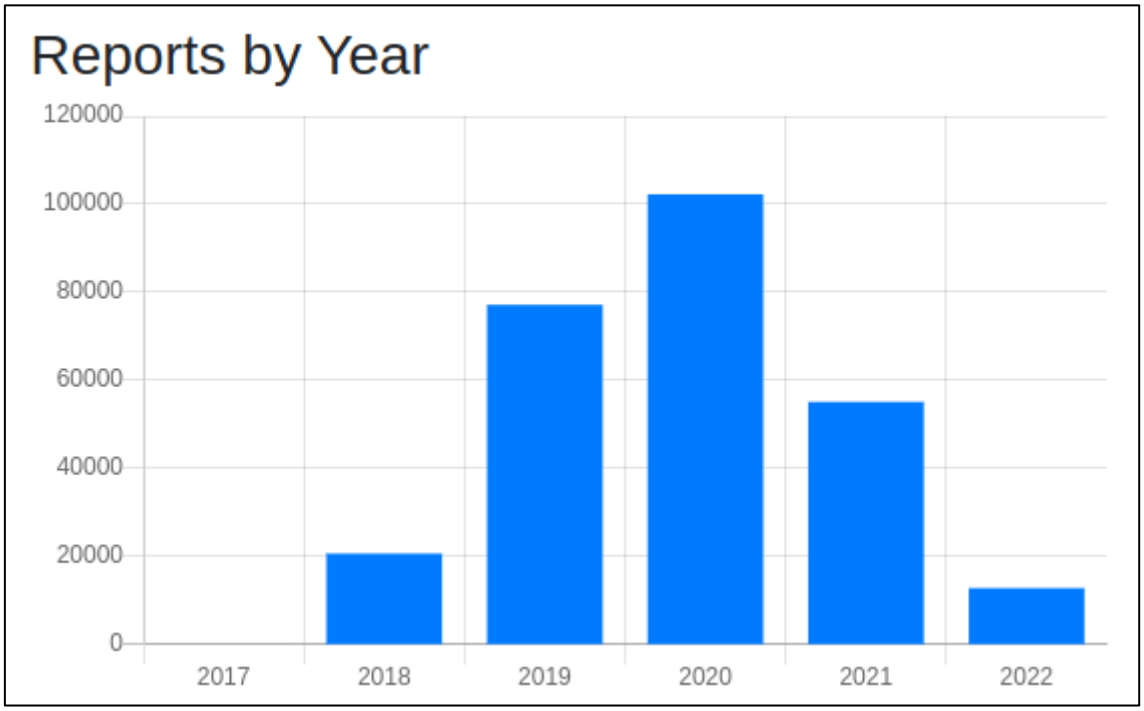


Bild 49: Verlauf der Betrugsmeldungen von 2017 bis 2022 (Stand: 15.04.2022) [52]

8.4.2 Bewertung für den OSINT-Einsatz

Aus der Analyse in Kapitel 8.4.1 ergab sich folgende Bewertung für den Dienst.

Tabelle 18: BitcoinAbuse.com - Bewertung für den OSINT-Einsatz

Kriterium	Bewertung	Kommentierung
Verfügbarkeit	+++	Der Dienst war während der Nutzung 100% verfügbar, dazu führt er seit 2017 eigene Statistiken, die einen durchgängigen Service dokumentieren.
Neutralität	+	Der Dienst selbst ist Non-Profit orientiert. Anzumerken ist, dass sich nicht ermitteln ließ, welche Organisation oder Person für die Webseite verantwortlich ist. Eine Anfrage zur Klärung der Identität des Dienstanbieters, die im Rahmen dieser Arbeit am 15.04.2022 über das Kontaktformular gestellt worden ist, blieb bis 30.10.2022 unbeantwortet.
Haupt-funktionen	++	Funktionen zur Meldung und Abfrage von Bitcoin-Adressen sind enthalten. Zum Zeitpunkt der Analyse wurde nur die Kryptowährung Bitcoin unterstützt.
Aktualität	+++	Die erfassten Daten waren nach Eingabe direkt verfügbar, erkennbar über Zeitstempel vorangegangener Meldungen.
Qualität	+	Während der Nutzung konnten weder False-Positive noch False-Negative Treffer gesichtet werden. Eine bewusste Manipulation des Dienstes erschien aber leicht möglich, indem man eine Bitcoin-Adresse meldet, die überhaupt nicht negativ aufgefallen ist. Ob und wie die Meldungen von BitcoinAbuse.com validiert werden, ist nicht transparent. Die Daten können, nachdem diese durch das Melde-formular abgegeben worden sind, nicht verändert werden.
Quantität	+	Fokus war alleinig Bitcoin und die Anzahl eingegangener Betrugsmeldungen war Stand 04/2022 eher rückläufig.
Kosten	+++	Der Dienst konnte zum Zeitpunkt der Erstellung dieser Arbeit vollkommen kostenfrei genutzt werden.

8.5 Analyse-Tool: Maltego Community Edition

Maltego ist ein grafisches Open-Source-Informations- und Link-Analyse-Tool zum Sammeln und Verbinden von Informationen für Ermittlungsaufgaben. Maltego ist eine Java-Anwendung, die auf Windows, Mac und Linux läuft. [53]

Die Maltego Community Edition bietet zur Nachverfolgung von Zahlungsströmen verschiedener Kryptowährungen unter anderem den Tatum Blockchain Explorer. Stand Mai 2022 werden dabei die Kryptowährungen Bitcoin, Bitcoin Cash, Ethereum, Litecoin und in Teilen DogeCoin unterstützt.

Tatum ist eine Blockchain-Entwicklungsplattform, die über 40 Blockchain-Protokolle und über 2000 digitale Assets unterstützt. Ihr Ziel ist es, Entwicklern zu helfen, Blockchain-Anwendungen zu erstellen und die Masseneinführung der Blockchain-Technologie zu erleichtern. Die Integration von Tatum in Maltego hilft Ermittlern, die Blockchain-Infrastruktur für fünf Blockchains - Bitcoin, Ethereum, Litecoin, Bitcoin Cash und Dogecoin - zu durchforsten, und ermöglicht es, Kontext und Einblicke in den Transaktionen zu erhalten. Maltego kündigte außerdem an, in Zukunft noch weitere Blockchains hinzuzufügen, sofern die API-Unterstützung von Tatum für diese auf den neuesten Stand gebracht wird. [26]

8.5.1 Analyse Testfall – T1

Die kryptografischen Spuren aus der IT-forensischen Untersuchung ließen sich in Maltego CE weiter zusammensetzen und verfolgen.

Ausgangspunkt für eine Zahlungsflussanalyse konnte in Maltego CE eine Transaktions-ID sowie Sender- oder Empfängeradresse sein.

Folgende IT-forensische Artefakte konnten aus der Datenakquise und Datenauswertung gewonnen werden. Diese konnten in der Zahlungsflussanalyse mit Tatum weiter verifiziert und damit die Transaktion transparent gemacht werden.

(1) Coinbase Account – Auszahlungsadresse – (Kunde)
- bc1qcaa8lh9fjzqj3xdtav4x5avz46dw7w3rldse92

(2) Electrum Wallet – Einzahlungsadresse – (Anbieter)
- bc1qhvp7kl8nyjg3wpzzxyv0hvv8h8q44mhc67rev4

(3) Weiterleitung von Guthaben des Electrum Wallets an zwei Adressen
- 3FXzLpvpsW8CBbaAeKGVADA9mp3ZpHrb5r
- bc1q3l2xsqurypwqd4nx305w9wf8hzy24qkvzvyzqh

Der folgende Graph zeigt die Zahlungsflüsse des Szenarios S1 - Testfall T1 erstellt unter Anwendung von Maltego CE. Die Darstellung war im Tool variabel anpassbar und konnte entweder ausschließlich Adressen aber auch Transaktionen enthalten. Im vorliegen Graphen kann der Fluss des Geldes über die verschiedenen Bitcoin-Adressen sowie die damit verbundenen Transaktions-IDs erkannt werden.

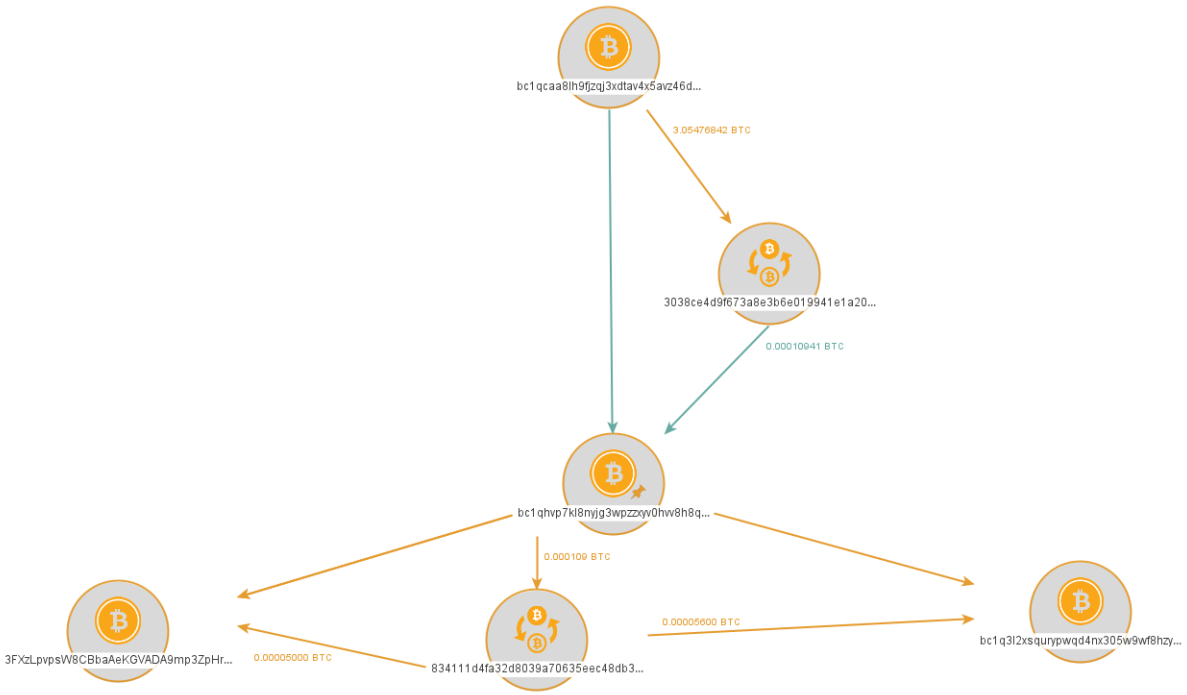


Bild 50: Grafische Darstellung der Bitcoin-Geldflüsse in Maltego CE

8.5.2 Bewertung für den OSINT-Einsatz

Basierend auf den vorangegangenen Analysen des Testfalls T1 ergibt sich folgende Bewertung für das Tatum Modul in Maltego CE.

Tabelle 19: Maltego CE mit Tatum Modul - Bewertung für den OSINT-Einsatz

Kriterium	Bewertung	Kommentierung
Verfügbarkeit	+++	Der Dienst war während der Nutzung 100% verfügbar und lief auf dem genutzten Client stabil.
Neutralität	+++	Maltego handelt als Unternehmen gewinn-orientiert. Die Neutralität erschien nach Sichtung des Maltego Webauftritts und weiterer Recherchen als gegeben.
Haupt-funktionen	+++	Funktionsumfänge in Maltego CE waren im Vergleich zur kostenpflichtigen Vollversion nur eingeschränkt verfügbar. Durch Nutzung des Tatum-Moduls konnten Kryptowährungs-Transaktionen einbezogen werden und in einem spezifischen Graphen abgebildet werden. Die Oberfläche für die grafische Link-Analyse wirkte intuitiv, zeitgemäß und gut nutzbar. Die Anbindung verschiedener Datenquellen und die Nutzungsmöglichkeit weiterer, teils kostenpflichtiger Module erweitern den möglichen Funktionsumfang.
Aktualität	+++	Daten des Tatum-Moduls in Maltego CE waren augenscheinlich tagesaktuell verfügbar.
Qualität	+++	In den Testfällen konnten keine Abweichungen zu den gesicherten Transaktionsdaten festgestellt werden.
Quantität	+++	Maltego CE bot im Vergleich zu den rein webbasierten Blockchain-Explorern u.a. die Möglichkeit, weitere Datenquellen in die Analyse einzubinden.
Kosten	++	Maltego CE und Tatum konnten zum Zeitpunkt der Erstellung dieser Arbeit kostenfrei genutzt werden. Für den vollen Funktionsumfang müssten jedoch kostenpflichtige Lizenzen erworben werden.

9 Zusammenfassende Bewertung

Das Ziel dieser Arbeit war, neue Erkenntnisse bezüglich des kombinierten Einsatzes von Methoden und Tools der IT-Forensik sowie dem Einsatz von Open Source Intelligence, für Ermittlungen im Zusammenhang mit Kryptowährungen, bereitzustellen.

Um abschließend eine Handlungsempfehlung abgeben zu können wurden hierzu auf Basis aktueller Bedrohungslagen Szenarien entwickelt, Testfälle abgeleitet, ausgeführt und IT-forensisch ausgewertet. Die Ergebnisse wurden unter Anwendung von Open Source Intelligence weiterverfolgt und aus Sicht einer Ermittlungstätigkeit bewertet.

Auf Basis der Auswertung der End-2-End Szenarien basierten Testfälle T0 – T4 ließen sich innerhalb dieser Arbeit verschiedene Erkenntnisse gewinnen, die für Ermittlungen im Zusammenhang mit Kryptowährungen relevant sind.

In Kapitel 9 werden nachfolgend die eingesetzten IT-Forensik-Tools sowie OSINT-Dienste zusammenfassend bewertet.

Es werden die Möglichkeiten und Grenzen aufgezeigt, die beim Nachweis Blockchain-basierter Kryptowährungen und deren Nachverfolgung von Zahlungsflüssen unter Einsatz von Open Source Intelligence beobachtet wurden.

9.1 Bewertung eingesetzter IT-Forensik-Tools

Alle drei eingesetzten Forensik-Tools (Autopsy, AXIOM, Bulk Extractor) konnten im Rahmen der vorliegenden Arbeit effektiv eingesetzt werden. Die Ergebnisse der Datenauswertungen aus den Testfällen finden sich im Detail in Kapitel 7.

Im Einzelnen ergaben sich dennoch Unterschiede in der zugrundliegenden Datenakquise und der Erkennungsleistung, auf die im Folgenden eingegangen wird.

Die Erkennungsleistung der eingesetzten Tools war in den folgenden Aspekten jeweils gleichwertig geben:

- Besuchte Kryptowährungs-Webseiten (URLs)
- Durchgeführte Google-Suchen
- Aufruf der Coinbase Wallet Extension
- Aufruf des Coinbase Tresors
- Ermittlung Coinbase Benutzername
- Durchgeführte Downloads von Software (u.a. Wallets)

Besondere Leistungen von AXIOM

- Darstellung des genutzten Coinbase Passworts in Klartext
- Erkennung der Bitcoin-Adressen und Transaktionen des Electrum Wallets
- Stabile Prozessierung der Keyword-Suche über Reguläre Ausdrücke
- Anteilig logische Datenakquise auf Apple IPhone SE

AXIOM konnte bei den Erkennungsleistungen gegenüber Autopsy insgesamt bessere Resultate liefern. Dazu sind die Möglichkeiten zur Darstellung, Filterung und Suche in der GUI von AXIOM vielseitiger als in Autopsy. Der Bulk Extraktor wurde ohne GUI, rein über die Kommandozeile angewendet.

Besondere Leistungen von Autopsy

Autopsy konnte, innerhalb der ausgewerteten Testfälle, bei der Datenakquise- und Erkennung gegenüber AXIOM keine besonderen Leistungen erbringen. Im Vergleich zum Bulk Extractor bot Autopsy aber insgesamt den größeren Funktionsumfang für eine fallbasierte Bearbeitung und Darstellung mehrerer Datenquellen. Dazu bot Autopsy auch eine statische Keyword-Suche, die mit AXIOM vergleichbar ist jedoch von Bulk Extractor in dieser Form nicht angeboten wurde.

Besondere Leistungen von Bulk Extractor

Die besondere Leistung des Bulk Extractor war die performante Extraktion relevanter Informationen aus den zugeführten Images in TXT-Dateien, hierzu zählten für die vorliegende Arbeit die Extraktion folgender Artefakte:

- Bitcoin-Adressen
- E-Mail-Adressen
- Web-Domains & URLs

Die von Bulk Extraktor erzeugten TXT-Dateien konnten nachfolgend mit Scripten weiter prozessiert werden um relevante Daten zu validieren oder durch Suchen weiter einzugrenzen.

Ansätze hierzu wurden in Kapitel 7.5.9 bis 7.5.11 aufgezeigt und im Detail beschrieben.

In der nachfolgenden Tabelle 20 wurden die gewonnenen Erkenntnisse in einer zusammenfassenden Bewertung dargestellt.

Tabelle 20: Bewertung eingesetzter IT-Forensik-Tools

IT-Forensik-Tool	Autopsy	AXIOM	Bulk Extractor
Erkennungsleistungen	Bewertungen		
Durchgeführte Google-Suchen	+++	+++	+++
Besuchte Kryptowährungs-Webseiten (URLs)	+++	+++	+++
Suche über Reguläre Ausdrücke	+	++	++
Suche über statische Keyword-Liste	+++	+++	+
Datenakquise Apple IPhone SE	-	++	-
Durchgeführte Downloads	+++	+++	+++
Coinbase Wallet Extension, Tresor, Benutzername	+++	+++	+++
Anzeige Coinbase Passwort in Klartext	-	+++	-
Bitcoin-Adressen, Transaktionen (Electrum Wallet)	+	+++	++
Performante TXT-Extraktion von Bitcoin-Adressen, E-Mail-Adressen, URLs	-	-	+++
Allgemeine Einsatzkriterien	Bewertungen		
Nutzung über GUI	++	+++	-
Kosten	+++	+	+++

9.2 Möglichkeiten und Grenzen der IT-Forensik

Die IT-Forensik bot durch ihre Methoden der Datenakquise und Datenauswertung einen idealen Einstiegspunkt, relevante Spuren aus der Nutzung von Kryptowährungs-Diensten auf lokalen Endgeräten gewinnen zu können.

Als offensichtliche Spuren waren insbesondere Kryptowährungs-Objekte wie Wallets, Bitcoin-Adressen, Bitcoin-Transaktionen aber generell auch E-Mail-Adressen aus relevanten Kommunikationsverläufen oder der Nutzung als User-Login bei entsprechenden Kryptowährungs-Diensten zu finden.

Sofern beim Betroffenen keine Verschlüsselung der Wallet-Informationen vorgenommen wurde, konnten diese als Klartext ausgelesen werden, siehe Kapitel 7.5.2.

Auch der Aufruf von Suchmaschinen und Krypto-Webseiten mit entsprechenden Abfragen zu Suchbegriffen oder Kryptowährungs-Adressen bzw. Transaktionen wurden teils in den Links der Browser-Historie gespeichert, siehe Kapitel 7.5.4.

Als weniger offensichtliche Artefakte waren aber auch indirekte Kryptowährungs-Spuren, die sich aus der Nutzung von relevanten Hard- und Softwarekomponenten ermitteln ließen von Bedeutung. Zur Hardware zählten hierbei der Anschluss von Hardware-Wallets wie bspw. dem Ledger Nano S, der sich in der Windows-Registry als USB-Device nachvollziehen ließ, siehe Kapitel 7.5.3.

Softwarekomponenten wie das Electrum Wallet (Kapitel 7.5.2) oder auch Ledger Live, welches für die Nutzung des Hardware-Wallets Ledger Nano S benötigt wurden, ließen sich als relevante indirekte Spuren auslesen, siehe Kapitel 7.5.3.

Grenzen bei der Datenakquise und Auswertung traten während dieser Arbeit bei dem genutzten Smartphone Apple IPhone SE auf. Von den betrachteten IT-Forensik-Tools war ausschließlich AXIOM im Stande, eine logische Datensicherung auf Teilen des Endgeräts durchzuführen und diese nachfolgend auszuwerten, siehe Kapitel 7.5.1.

Eine weitere Grenze bei der Datenakquise und Auswertung bildeten naturgemäß Verschlüsselungen, die das Auslesen von Dateien in Klartext verhinderten. Hierbei gilt festzuhalten, dass aus dem unverschlüsselten Electrum Wallet Kryptowährungs-Spuren ausgelesen werden konnten, siehe Kapitel 7.5.2 aber eben aus dem verschlüsselten Ledger Nano S Wallet nicht, siehe Kapitel 7.5.3.

9.3 Bewertung eingesetzter OSINT-Dienste

Insgesamt wurden innerhalb dieser Arbeit fünf Dienste untersucht, die durch ihre Eigenschaften als offen zugängliche Informationsquelle als OSINT-Dienste angesehen werden konnten.

Durch den Fokus auf die Nachverfolgung Blockchain-basierter Kryptowährungstransaktionen wurden hierbei primär webbasierte Blockchain-Explorer untersucht. Zusätzlich wurde ein Szenario mit Testfall mit dem client-basierten OSINT-Analyse-Tool Maltego CE und dessen Modul Tatum ausgewertet.

Aus Kostengründen wurden ausschließlich frei verfügbare Anteile der jeweiligen Dienste untersucht. Zusätzlich wurden während der Arbeit weitere Datenquellen, u.a. für Hintergrundrecherchen zu den Dienstanbietern einbezogen. Hierzu zählten whois-Abfragen zur Ermittlung von Domain-Registraren, NMLS-Datenbankabfragen zu offiziell registrierten US-Finanzdienstleistern sowie auch die direkte Kontaktanfrage des Dienstes.

Basierend auf den Einzelbewertungen jedes OSINT-Dienstes erfolgt nachfolgend eine zusammenfassende Bewertung durch Beleuchtung der wichtigsten Aspekte.

Recherche und Analyse von Bitcoin-Transaktionen

Alle untersuchten webbasierten Blockchain-Explorer konnten die in den Testfällen erzeugten Bitcoin-Transaktionen mit den Basisdaten Transaktions-ID, Absender- und Empfängeradresse und Zahlungsbetrag einsehbar machen. Auch die Verfügbarkeit war bei allen Blockchain-Explorern durchweg gegeben.

Im Detail ergaben sich jedoch Unterschiede im Funktionsumfang, die bei einer Ermittlungstätigkeit im Umfeld von Kryptowährungen Relevanz tragen.

Zuordnung von Bitcoin-Adressen zu realen Entitäten

Die beiden Blockchain-Explorer OXT.me und WalletExplorer.com konnten als Einzige innerhalb der analysierten Testfälle einzelne Bitcoin-Adressen realen Entitäten zuordnen. Hierzu zählten u.a. die Zuordnung einer Bitcoin-Adresse zur Kryptowährungs-Börse Binance durch OXT.me, siehe Kapitel 8.2.1 sowie die Zuordnung mehrerer Entitäten wie CEX.io und MercadoBitcoin.com.br, in einem mehrstufigen Transaktionsverlauf, siehe Kapitel 8.3.2.

Die Datenbasis von WalletExplorer.com bot die umfassendste Anzahl an Zuordnungen von Bitcoin-Adressen zu realen Entitäten. Gepaart mit der Möglichkeit, die Daten von der Weboberfläche als TXT-Datei zu exportieren, bietet dieser OSINT-Dienst ein nutzbares Werkzeug bei der Ermittlungstätigkeit. Durch die Erstellung eindeutiger Wallet-IDs verfügt WalletExplorer.com auch über die Zuordnung mehrerer Bitcoin-Adressen zu einem Wallet, siehe Kapitel 8.3.1 und 8.3.2.

Generell muss festgehalten werden, dass die Zuordnung der realen Entitäten durch die Dienste selbst erfolgte, daher kann es nur ein Indikator für die Ermittlungstätigkeit sein und hat alleinstehend keineswegs Beweischarakter.

Visualisierung von Transaktionen

Der Dienst OXT.me bot neben der aktuellen Datenbasis auch Funktionen zur Visualisierung und Kennzeichnung von Bitcoin-Transaktionen, kann Aktivitäten und Volumen grafisch darstellen und mit Kommentaren versehen, siehe Kapitel 8.2.1.

Grenzen webbasierter Blockchain-Explorer

Alle der untersuchten webbasierten Blockchain-Explorer stoßen an ihre Grenzen, wenn es darum geht, mehrstufige Transaktionsketten darzustellen.

Generell stellte sich in diesem Fall ein grafisch basiertes Link-Analyse-Tool wie Maltego CE in Verbindung mit dem Modul Tatum als die bessere Wahl dar.

Die webbasierten Blockchain-Explorer boten damit eher einen Einstieg, um einzelne Transaktionen einer Blockchain zu prüfen. Wenn es aber darum geht, einen Zahlungsfluss über mehrere Adressen hinweg zu verfolgen, konnte keiner der untersuchten webbasierten Blockchain-Explorer die Leistung von Maltego CE in diesem Aspekt erreichen.

Datenqualität

Insgesamt war die Datenqualität aus den untersuchten Transaktionen der Testfälle über alle Dienste hinweg fehlerfrei was auf die Validierungsmechanismen der zugrundeliegenden Blockchain-Technologie zurückführen war.

Einzig der Dienst Bitcoinabuse.com erwies sich als weniger nutzbar, da dieser augenscheinlich keine Validierung der gemeldeten Bitcoin-Adressen vornimmt, d.h. die Qualität der Datenbasis war hier in Frage zu stellen. Schadhafte Falschmeldungen innerhalb des Dienstes sind einfach zu produzieren und daher sehr wahrscheinlich, siehe Kapitel 8.4.1.

In der nachfolgenden Tabelle 21 werden die gewonnenen Analyseergebnisse aus Kapitel 8 in einer zusammenfassenden Bewertung dargestellt.

Tabelle 21: Bewertung eingesetzter OSINT-Dienste

OSINT-Dienst	Blockchain.com	OXT.me	Wallet Explorer.com	Bitcoin-abuse.com	Maltego CE Tatum
Verfügbarkeit	+++	+++	+++	+++	+++
Neutralität	+++	++	+++	+	+++
Hauptfunktionen	++	++	++	++	+++
Aktualität	+++	+++	++	+++	+++
Qualität	+++	+++	+++	+	+++
Quantität	+	+++	+++	+	+++
Kosten	+++	+++	+++	+++	++
Eignung	Schnelle Recherche von Bitcoin-Adressen und Einzeltransaktionen.	Zuordnung einzelner Bitcoin-Adressen zu Krypto-Diensten. Erweiterte Möglichkeiten zur Visualisierung von Transaktionen.	Zuordnung mehrerer Bitcoin-Adressen zu einem Wallet. Im Vergleich beste Datenbasis für die Zuordnung von Bitcoin-Adressen zu Krypto-diensten.	Weniger nutzbar, keine Validierung eingegebener Bitcoin-Adressen.	Grafisch basiertes Link-Analyse-Tool für die umfassende Untersuchung von Transaktionsketten.

9.4 Möglichkeiten und Grenzen von OSINT

OSINT bot im Rahmen dieser Arbeit verschiedenste Dienste, die eine Ermittlung im Bereich von Kryptowährungen unterstützen. In erster Linie sind hierbei die Blockchain-Explorer zu nennen, die je nach unterstützter Kryptowährung jede Transaktion, deren Eingangs- und Ausgangsadressen und Zahlungsbeträge ausweisen. Somit ließen sich die Transaktionen generell nachvollziehen, wenngleich das nicht zwangsläufig bedeutete, dass sich die Identität der Akteure daraus ableiten ließ. Für weiterführende Ermittlungen, die der Offenlegung von Identitäten handelnder Akteure dienen, zeigten sich beim alleinigen OSINT-Einsatz Grenzen. Um neben den rein pseudonym anzusehenden Daten aus der Blockchain einen Bezug zu realen Identitäten zu bilden, bedarf es der Kombination aus den Möglichkeiten der IT-Forensik sowie der Recherche und Analyse über OSINT. Es stellten sich während der Arbeit daher zwei grundlegende Handlungsweisen heraus, die im Falle einer Ermittlung sinnvoll erscheinen:

(1) Einsatz von OSINT auf Basis IT-forensischer Spuren

Bei diesem Ansatz wird auf Basis von IT-forensischen Spuren eine OSINT-Recherche und Analyse durchgeführt. Dieses Vorgehen ist sehr zielgerichtet, da hier bereits Spuren von Kryptowährungen vorliegen, die zum einen direkt in die Ermittlung einbezogen werden können und des Weiteren u.U. auch konkreten Identitäten zugordnet werden können. Diese Möglichkeit stellt den Idealfall dar. Jedoch werden in der Realität gerade am Anfang einer Ermittlung u.U. keine IT-forensischen Spuren vorliegen, hier kann die initiale Recherche mit OSINT den Einstieg in die Ermittlung bilden.

(2) Freie Auswertung von OSINT-Diensten

Sofern aus anderen Quellen Informationen wie E-Mail-Adressen, Login-Namen oder ggf. Wallets vorliegen, kann eine Ermittlung auch auf Basis von OSINT-Diensten begonnen werden. Dabei kann in Konstellationen, in denen unterschiedliche Datenquellen und Artefakte vorliegen, auch der Einsatz eines OSINT-Analyse-Tools wie Maltego zur Sammlung und Darstellung unterschiedlicher Datentypen hilfreich sein.

10 Ausblick und Handlungsempfehlung

Der Beginn einer Ermittlung mit Bezug zu Kryptowährungen kann eine IT-forensische Datenakquise darstellen, indem auf dem Endgerät eines Betroffenen entsprechende Spuren der Nutzung von Kryptowährungs-Diensten gesichert und ausgewertet werden.

Dieser Ansatz birgt den Vorteil, dass bereits zu Beginn der Ermittlung potentielle Informationen zur Identität des Betroffenen oder weiterer Beteiligten vorliegen können. Hierbei kann in einem ersten Schritt festgestellt werden, ob der Betroffene durch Anschluss bzw. Installation entsprechende Wallets oder Kryptowährung assoziierte Dienste aktiviert hat.

Die weitere Nutzung dieser Komponenten hinterlässt dann konkrete Spuren in Form von Kryptowährungs-Objekten, die sich je nach Sicherungs- oder Verschleierungsmaßnahmen des Betroffenen für die weitere Analyse getätigter Transaktionen anwenden lassen.

Besonders im Falle von unverschlüsselten Wallets, lokal abgelegten Transaktionsdaten wie bspw. Bitcoin-Adressen oder Transaktions-ID können Mithilfe von OSINT-Diensten wie Blockchain-Explorern Zahlungsflüsse nachvollzogen werden.

Durch die weitere Hinzunahme von OSINT-Tools zur grafisch orientierten Transaktionsanalyse wie bspw. Maltego oder Chainalysis lassen sich weitere Datenmengen, Entitäten und Identitäten in der Analyse herausbilden. Schwieriger gestaltet sich eine Recherche und Analyse mit OSINT, wenn zu Beginn der Ermittlung keine gesicherten IT-forensischen Spuren vorliegen.

Im folgenden Bild 51 werden die zwei grundlegenden Ermittlungsansätze aus Kapitel 9.4 abschließend in einem Modell zusammengeführt.

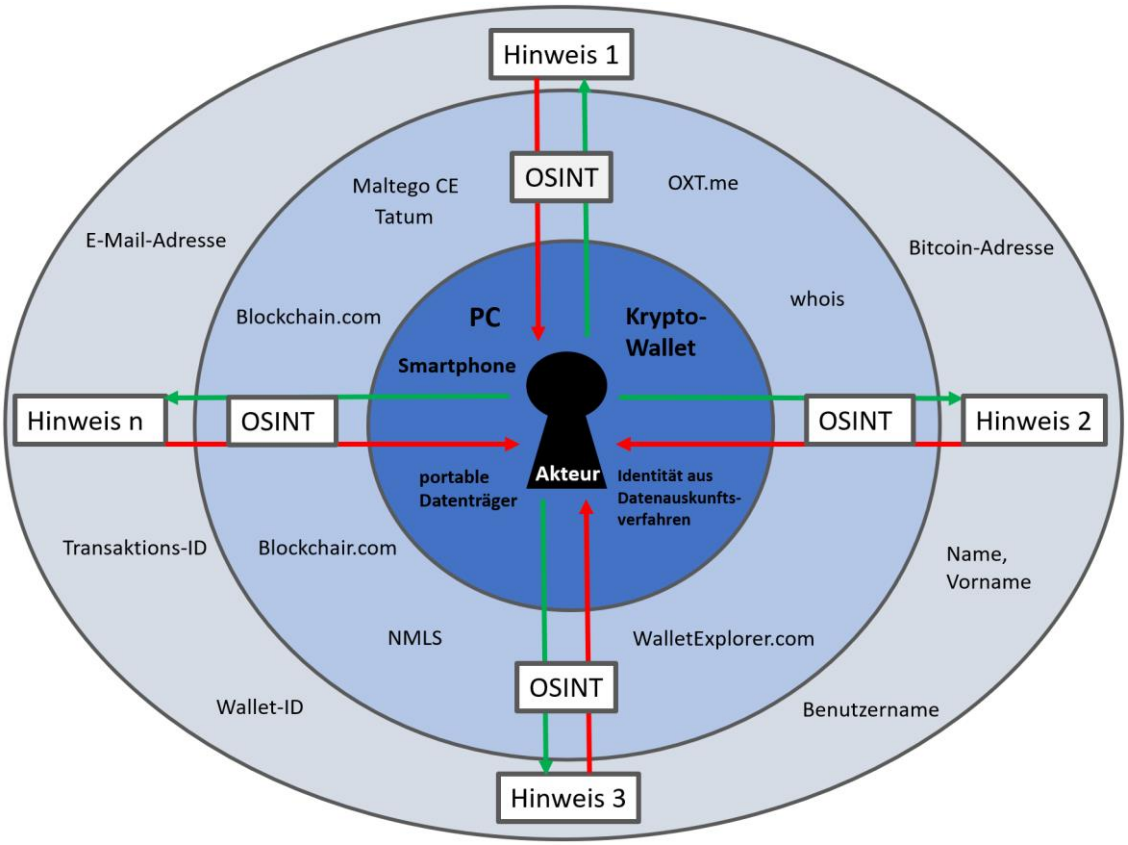


Bild 51: Modell zum Nachweis Blockchain-basierter Kryptowährungen und Nachverfolgungen von Zahlungsflüssen unter Einsatz von Open Source Intelligence

Aus dem in Bild 51 dargestellten Modell lassen sich die zwei Ermittlungsansätze zum Nachweis Blockchain-basierter Kryptowährungen und der Nachverfolgung von Zahlungsflüssen abschließend wie folgt beschreiben:

(1) Einsatz von OSINT auf Basis IT-forensischer Spuren

Einsatz von OSINT auf Basis IT-forensischer Spuren hat das Ziel, die OSINT-Dienste ausgehend von IT-forensischen Spuren gezielt abzufragen, um neue Hinweise oder Informationen zu erlagen, siehe grüne Pfeile in Bild 51. Hierbei werden die zuvor von Datenträgern gesicherten und ausgewerteten Spuren von Kryptowährungen genutzt, um gezielte Suchen in den OSINT-Diensten durchzuführen. Im Ergebnis kann es weitere Hinweise oder Information geben, die u.U. dem eingangs ermittelten Akteur zugeschrieben werden können.

(2) Freie Auswertung von OSINT-Diensten

Eine freie Auswertung von OSINT-Diensten beginnt mit einem Hinweis oder einer losen Information, die zum jeweiligen Sachverhalt gehören um damit eine OSINT-basierte Recherche durchzuführen. Durch die Recherche kann u.U. eine Verbindung zu einem Akteur hergestellt werden, siehe rote Pfeile in Bild 51. Dies kann bspw. durch die Nutzung einer E-Mail-Adresse, die einem Akteur als Login-Name für eine Kryptowährungs-Börse dient, geschehen oder auch eine einzelne Transaktion sein, deren Ein- oder Auszahlungspunkt ein offiziell registrierter Finanzdienstleister ist. Durch die nachfolgende Initiierung entsprechender Datenauskunftsverfahren kann ggf. die Identität des Kunden offenlegt werden. Nach Feststellung der Identität sind weitere Maßnahmen denkbar, die dann eine IT-forensische Sicherung der Endgeräte des betroffenen Akteurs vorsehen.

Beide Ansätze lassen sich im Verlauf einer Ermittlung auch wechselseitig anwenden und bieten damit eine Methodik, um lose Spuren aus der Nutzung von Kryptowährungen zu konkreten Transaktionen zusammenzuführen und so die handelnden Akteure zu ermitteln.

Literaturverzeichnis

[1] Chainalysis: The 2022 Crypto Crime Report: Original data and research into cryptocurrency-based crime. https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf, 18.03.2022

[2] Luber, Stefan; Schmitz, Peter: Definition IT-Forensik: Was ist IT-Forensik? https://www.security-insider.de/was-ist-it-forensik-a-774063, 23.07.2022

[3] Vogel Communications Group: Definition OSINT (Open Source Intelligence): Was ist Open Source Intelligence (OSINT)? https://www.security-insider.de/was-ist-open-source-intelligence-osint-a-929161, 23.07.2022

[4] Mitschele, Andreas: Gabler Wirtschaftslexikon: Definition Blockchain. https://wirtschaftslexikon.gabler.de/definition/blockchain-54161/version-277215, 10.06.2022

[5] David Furlonger; Uzureau, Christophe: Was ist Blockchain? https://www.gartner.de/de/artikel/was-ist-blockchain, 05.06.2022

[6] Bundesanstalt für Finanzdienstleistungsaufsicht: Blockchain-Technologie. https://www.bafin.de/dok/9224766, 05.06.2022

[7] Berghoff, Christian; Gebhardt, Ute; Lochter, Manfred: Blockchain sicher gestalten: Konzepte, Anforderungen, Bewertungen. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf, 10.06.2022

[8] Hellwig, D.; Karlic, G.; Huchzermeier, A.: Blockchain-Grundlagen: Entwickeln Sie Ihre eigene Blockchain. Berlin, Heidelberg: Springer Gabler, 2021.

[9] Seregin, Kirill: Distributed Ledger Technologie (DLT) ist mehr als Blockchain. https://blockchainwelt.de/dlt-distributed-ledger-technologie-ist-mehr-als-blockchain, 10.06.2022

[10] Robin, W.; Kons, Alexandra: Konsensmechanismus: Der ultimative Guide zum zentralen Element der Blockchain. https://de.beincrypto.com/konsensmechanismus-der-ultimative-guide-zum-zentralen-element-der-blockchain, 11.06.2022

[11] The Bitcoin Foundation: Wie funktioniert Bitcoin?: Transaktionen - private Schlüssel. https://bitcoin.org/de/wie-es-funktioniert, 29.06.2022

[12] Was ist die Bitcoin Blockchain? https://help.coinbase.com/de/coinbase/getting-started/crypto-education/what-is-the-bitcoin-blockchain, 26.06.2022

[13] Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf, 29.06.2022

[14] The Bitcoin Foundation: Bitcoin Developer Guide: Block Chain Overview. https://developer.bitcoin.org/devguide/block_chain.html, 26.06.2022

[15] Schmitz, Peter: Definition Mining: Was ist Mining? https://www.blockchain-insider.de/was-ist-mining-a-875590, 22.07.2022

[16] Centre for Alternative Finance: Cambridge Bitcoin Electricity Consumption Index: Bitcoin Mining Map. https://ccaf.io/cbeci/mining_map, 28.08.2022

[17] Schiller, Kai: Die Rolle der Kryptographie innerhalb der Blockchain-Technologie. https://blockchainwelt.de/kryptographie-innerhalb-der-blockchain-technologie, 12.06.2022

[18] National Institute of Standards and Technology: Glossary: hashing. https://csrc.nist.gov/glossary/term/hashing, 26.06.2022

[19] Constantin, Lucian: Was ist Hashing? https://www.computerwoche.de/a/was-ist-hashing,3550630, 26.06.2022

[20] Bundesamt für Sicherheit in der Informationstechnik: Blockchain macht Daten praktisch unveränderbar: Was sind Kryptowährungen? https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Blockchain-Kryptowaehrung/blockchain-kryptowaehrung_node.html, 29.06.2022

[21] Breeden II, John; Maier, Florian: Open Source Intelligence: Die besten OSINT Tools. https://www.computerwoche.de/a/wie-viel-wissen-hacker-ueber-sie,3548786, 27.05.2022

[22] Kaspersky: encyclopedia by Kaspersky: OSINT (Open-Source Intelligence). https://encyclopedia.kaspersky.com/glossary/osint, 27.05.2022

[23] Deutsche Hochschule der Polizei: Vernetzungsprojekt SENTINEL: Open Source Intelligence. https://www.dhpol.de/departements/departement_II/FG_II.2/vernetzungsprojekt-sentinel.php, 27.05.2022

[24] Lesavre, L.; Varin, P.; Yaga, D.: Blockchain Networks: Token Design and Management Overview. Gaithersburg: National Institute of Standards and Technology, 2021.

[25] BLOCKCHAIR: Datenbank-Dumps. https://blockchair.com/de/dumps#database, 26.05.2022

[26] Maltego Technologies: Tatum Blockchain Explorer. https://www.maltego.com/transform-hub/tatum-blockchain-explorer, 08.05.2022

[27] Maltego Technologies: Maltego Desktop Client Editions: Which Maltego edition is right for me? https://www.maltego.com/maltego-desktop-client-versions, 31.07.2022

[28] Chainalysis: Chainalysis Reactor Certification (CRC). https://www.chainalysis.com/crc, 31.07.2022

[29] Elliptic Forensics: Crypto Investigations: Elliptic Investigator. https://www.elliptic.co/solutions/crypto-investigations, 31.07.2022

[30] blockstream.info: Blockstream Explorer. https://blockstream.info, 12.09.2022

[31] Blockchain.com: Blockchain Explorer. https://www.blockchain.com/, 08.08.2022

[32] Bitpanda GmbH: Was ist eine Wallet? https://www.bitpanda.com/academy/de/lektionen/was-ist-eine-wallet-und-wo-bekomme-ich-eine, 28.08.2022

[33] BISON: Was ist eine Bitcoin Wallet Adresse? https://bisonapp.com/bitcoin-wallet/#:~:text=Hand%20in%20Hand.-,Was%20ist%20eine%20Bitcoin%20Wallet%20Adresse%3F,um%20Zahlungen%20empfangen%20zu%20k%C3%B6nnen., 29.08.2022

[34] Joko: Welchen Bitcoin-Adresstyp sollte ich verwenden? https://shiftcrypto.ch/blog/was-sind-bitcoin-adressen, 28.08.2022

[35] BKA: Illegaler Darknet-Marktplatz „Hydra Market“ abgeschaltet. https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2022/Presse2022/220405_PM_IllegalerDarknetMarktplatz.html, 08.05.2022

[36] Dalal, Siddhartha; Wang, Zihe; Sabharwal, Siddhanth: IDENTIFYING RANSOMWARE ACTORS IN THE BITCOIN NETWORK. https://arxiv.org/ftp/arxiv/papers/2108/2108.13807.pdf, 30.05.2022

[37] Carrier, Brian: Open Source Digital Forensics. https://www.sleuthkit.org/index.php, 10.05.2022

[38] Carrier, Brian: Analysis Features. https://www.sleuthkit.org/autopsy/features.php, 10.05.2022

[39] Garfinkel, Simson L.: README.md. https://github.com/simsong/bulk_extractor, 10.05.2022

[40] Magnet Forensics: MAGNET AXIOM: Recover & Analyze Your Evidence in One Case. https://www.magnetforensics.com/products/magnet-axiom, 11.05.2022

[41] Raab-Düsterhöft, Antje: IT-Forensik Wiki: Magnet Axiom. https://it-forensik.fiw.hs-wismar.de/index.php/Magnet_Axiom, 11.05.2022

[42] Kim Jong Cracks: Jailbreak for iPhone 5s through iPhone X, iOS 12.0 and up. https://checkra.in, 01.07.2022

[43] Reality Net System Solutions: iOS - Triage: Bash script to extract data from a "checkra1ned" iOS device. https://github.com/RealityNet/ios_triage, 01.07.2022

[44] Voegtlin, Thomas; SomberNight: Electrum: Bitcoin Wallet. https://electrum.org/#home, 06.08.2022

[45] NMLS Consumer Access: Blockchain.com, Inc. https://www.nmlsconsumeraccess.org/EntityDetails.aspx/COMPANY/2024031, 19.08.2022

[46] Blockchain.com. https://www.blockchain.com, 19.08.2022

[47] OXT.me: ABOUT OXT. https://oxt.me/about, 19.08.2022

[48] Janda, Ales: WalletExplorer.com: smart Bitcoin block explorer. https://www.walletexplorer.com, 06.08.2022

[49] BitcoinQnA: Coinjoin Q+A Einfache Antworten auf die häufigsten Coinjoin-Fragen. https://bitcoiner.guide/qna/de/coinjoin/#:~:text=Was%20ist%20Coinjoin%3F,Gemeineigentums%2DHeuristik)%20zu%20brechen., 12.08.2022

[50] Küster, Felix: CEX.io Test und Erfahrungen – Wie gut ist diese Bitcoin Börse? https://kryptozeitung.com/cexio-boerse-testbericht, 12.08.2022

[51] MercadoBitcoin: We were born to create the new digital economy. https://www.mercadobitcoin.com.br/en/quem-somos, 12.08.2022

[52] Bitcoinabuse.com. https://www.bitcoinabuse.com, 07.08.2022

[53] Maltego Technologies: What is Maltego. https://www.maltego.com/product-features, 11.05.2022

Bilderverzeichnis

Bild 1: Vereinfachte Darstellung der Bitcoin-Blockchain in Anlehnung an Nakamoto [13] 13

Bild 2: Übersicht über Maltego Lizenzen und Funktionen [27] 22

Bild 3: Screenshot Elliptic Investigator [29] 23

Bild 4: Anzeige einer Bitcoin-Transaktion im Explorer von Blockstream.info [30] 25

Bild 5: Bitcoin-Adressen einer Transaktion im Explorer Blockchain.com [31] 26

Bild 6: Erzeugung eines neuen Falls in AXIOM [40] 44

Bild 7: Erzeugung eines Bulk Outputs mit Bulk Extractor [39] 45

Bild 8: Electrum Wallet auf Windows 10 VM 46

Bild 9: Ansicht der initialen Transaktion in Blockchain Explorer (blockstream.info) [30] 47

Bild 10: Autopsy Keyword Listing [38] 53

Bild 11: Globale Keywordsuche – Reguläre Ausdrücke [38] 54

Bild 12: Systemwarnung Autopsy bei Einsatz des Regulären Ausdrucks [38] 54

Bild 13: Auswertung Regulärer Ausdrücke in AXIOM [40] 57

Bild 14: Bulk Output der Bitcoin-Adressen des Bulk Extractors [39] 58

Bild 15: Sichtbarkeit des Benutzernamen (E-Mail-Adresse) aus Login in Binance APP [40] 60

Bild 16: Sichtbarkeit der Installation der Coinbase APP [40] 61

Bild 17: Analyse einer unverschlüsselten Electrum Wallet Datei [44] 65

Bild 18: Electrum config Datei zeigte den Pfad der zuletzt genutzten Wallet-Datei 66

Bild 19: Ansicht des Verzeichnisses mit der Datei wallet_01 66

Bild 20: Eintrag Ledger Nano S in der Windows-Registry unter SYSTEM 68

Bild 21: Nachweis des Aufrufs der Ledger Live Software 69

Bild 22 Auszug SQLite: Link zu Coinbase-Login, Login-Name (E-Mail-Adresse) in Klartext 70

Bild 23: Auswertung des Web Account Type über Autopsy mit Anzeige von coinbase.com 71

Bild 24: Übersicht der zuletzt vom Anwender aufgerufenen Dokumente 72

Bild 25: Electrum Wallet in der Interesting Files Liste in Autopsy 73

Bild 26: Ausführung Python Script zur Validierung von Bitcoin-Adressen in einer TXT-Datei unter Anwendung von Regulären Ausdrücken 75

Bild 27: Ausführung Python Script zur Suche nach Keywords in einer TXT-Datei 76

Bild 28: Auszug aus der NMLS-Registrierung der Blockchain.com, Inc. als anerkannter US-Finanzdienstleister [45] 77

Bild 29: Explorer-Dienst auf Blockchain.com [46] 78

Bild 30: Suchergebnis Bitcoin-Explorer über Transaktionen des Opfers [46] 80

Bild 31: Die Bitcoin-Adresse, von der das Opfer eine initiale Zahlung erhielt, zeigte eine hohe Aktivität [46] 80

Bild 32: Ergebnis des whois Abfrage von OXT.ME 83

Bild 33: Übersicht der Transaktionen des Opfers in OXT.me [47] 84

Bild 34: Initiale Einzahlung auf das Electrum Wallet des Opfers erfolgte von einem Binance-Account [47] 85

Bild 35: Verlaufskurven über eingehende und ausgehende Transaktionen einer Binance zugeordneten Bitcoin-Adresse [47] 86

Bild 36: Anzeige des Guthabens einer Bitcoin-Adresse des Erpressers 87

Bild 37: Transaktionen einer Bitcoin-Adresse des Erpressers 88

Bild 38: Anzeige des Guthabens einer weiteren Bitcoin-Adresse des Erpressers 88

Bild 39: WalletExplorer.com - Suchtreffer bc1q34hcaqa95lchs5f4nkrk0vsrwvnx8vwmku9r6r [48] 92

Bild 40: Transaktion mit Input des Kunden und Output an Anbieter [48] 92

Bild 41: Wallet des Anbieters bc1qwtkutllfdf0duhdyez8wcq6xulq94d55q7xznz mit Eingangsbuchung des Kunden [48] 93

Bild 42: Wallet [c13d678521] nutzte ausschließlich die Bitcoin-Adresse 12HaVrpXkLr2UnkMf6X9bY11cuNrZUdUnV [48] 93

Bild 43: Auszug der 69 Transaktionen von Wallet [c13d678521] [48] 94

Bild 44: Excel-basierte Datenanalyse auf Basis von Daten des WalletExplorer 95

Bild 45: Zahlungsausgänge an andere Wallets und Kryptowährungs-Dienste [48] 95

Bild 46: Formular zur Eingabe von potentiell betrügerischen Bitcoin-Adressen [52] 100

Bild 47: Ausgabe eines Abfrage-Treffers der BitcoinAbuse.com Datenbank [52] 100

Bild 48: Ergebnis der Whois-Abfrage für die Domain bitcoinabuse.com [52] 101

Bild 49: Verlauf der Betrugsmeldungen von 2017 bis 2022 (Stand: 15.04.2022) [52] 102

Bild 50: Grafische Darstellung der Bitcoin-Geldflüsse in Maltego CE 105

Bild 51: Modell zum Nachweis Blockchain-basierter Kryptowährungen und Nachverfolgungen von Zahlungsflüssen unter Einsatz von Open Source Intelligence 119

Tabellenverzeichnis

Tabelle 1: Übersicht webbasierter Blockchain-Explorer 19

Tabelle 2: Übersicht clientbasierter Tools zur Analyse von Kryptowährungs-Transaktionen 21

Tabelle 3: Testfallbeschreibung - T0 34

Tabelle 4: Testfallbeschreibung - T1 35

Tabelle 5: Testfallbeschreibung - T2 36

Tabelle 6: Testfallbeschreibung - T3 37

Tabelle 7: Testfallbeschreibung - T4 38

Tabelle 8: Übersicht eingesetzter Software mit deren Hauptfunktionen 40

Tabelle 9: Vergleich der Erkennungsleistung von Autopsy, AXIOM und Bulk Extractor nach unterschiedlichen Artefakten 48

Tabelle 10: Auswertung der Web-Cookies über Autopsy mit Treffern für binance.com und coinbase.com 71

Tabelle 11: Kryptowährungs-Objekte aus Testfall - T2 79

Tabelle 12: Blockchain.com - Bewertung für den OSINT-Einsatz 81

Tabelle 13: Kryptowährungs-Objekte aus Testfall - T2 84

Tabelle 14: Transaktion zur Weiterleitung der erpressten Bitcoins auf ein Ledger Nano S 89

Tabelle 15: OXT.me - Bewertung für den OSINT-Einsatz 89

Tabelle 16: Kryptowährungs-Objekte aus Testfall - T0 91

Tabelle 17: WalletExplorer.com - Bewertung für den OSINT-Einsatz 97

Tabelle 18: BitcoinAbuse.com - Bewertung für den OSINT-Einsatz 103

Tabelle 19: Maltego CE mit Tatum Modul - Bewertung für den OSINT-Einsatz 106

Tabelle 20: Bewertung eingesetzter IT-Forensik-Tools 110

Anlagenverzeichnis

Aufgrund der Art und des Umfangs der Anlagen befinden sich alle aufgeführten Anlagen auf der beigefügten CD im Innenband dieser Arbeit.

Anlage 1:	S2.1-Auswertung_Autopsy.xlsb
Anlage 2:	S2.1-Auswertung_AXIOM.xlsb
Anlage 3:	Python-Script
Anlage 4:	S2_keyword_list 20220616
Anlage 5:	mixed HTML Report 04-29-2022-17-26-55
Anlage 6:	S2.2_T4_walletexplorer-c13d678521b225a8-1.xlsx

Verzeichnis der Abkürzungen

BAFIN	Bundesanstalt für Finanzdienstleistungsaufsicht
BKA	Bundeskriminalamt
BTC	Bitcoin
CPU	Central Processing Unit
DLT	Distributed-Ledger-Technologie
DPoS	Delegated Proof-of-Stake
FAQ	Frequently Asked Questions
GUI	Graphical User Interface
ID	Identification
iOS	iPhone Operating System
Maltego CE	Maltego Community Edition
MBOX	Mailbox
mBTC	Millibitcoin - tausendstel eines Bitcoins
MIME	Multipurpose Internet Mail Extensions
MIT	Massachusetts Institute of Technology
NIST	National Institute of Standards and Technology
NIST	National Institute of Standards and Technology
OSINT	Open Scource Intelligence
P2P	Peer-to-Peer
P2PKH	Pay-to-PubKey-Hash
P2SH	Pay-to-Script-Hash
P2TR	Pay-to-Taproot
P2WPKH	Pay-to-Witness-Public-Key-Hash
PoS	Proof-of-Stake
PoW	Proof-of-Work
RAM	Random Access Memory
SSD	Solid State Drive
Tx	Transaction
URL	Uniform Resource Locator
USB	Universal Serial Bus
VDI	Virtual Desktop Infrastructure
VHD	Virtual Hard Disk Format
VM	Virtuelle Maschine
VMDK	Virtual Machine Disk
ZIT	Zentraler Informations- und Fahndungsdienst

Thesen

Kryptowährungen wie Bitcoin können nicht als vollständig anonymes Zahlungsmittel angesehen werden, denn durch Anwendung von OSINT-Diensten wie Blockchain-Explorern können Transaktionen eingesehen werden. Da die hinterlegenden Identitäten der Sender- und Empfängeradressen aber nicht direkt einsehbar sind, kann von einem pseudonymisierten Zahlungssystem ausgegangen werden.

Zur Verknüpfung von pseudonymisierten Transaktionen auf der Blockchain mit konkreten Identitäten dienen Ansätze aus der IT-Forensik, um entsprechende Spuren zu sichern und nachfolgend auszuwerten.

Durch Zuordnungen einzelner Kryptowährungs-Adressen zu Entitäten, die in OSINT-Diensten wie OXT.me oder WalletExplorer.com einzusehen sind und dabei auch zu offiziell registrierten Finanzdienstleistungsunternehmen führen, bestehen generell Möglichkeiten, durch entsprechende Auskunftsverfahren die Identitäten der Akteure zu ermitteln.

Einen limitierten, aber durchaus anwendbaren Rahmen für die Datenakquise und Auswertung bilden, je nach vorliegenden Endgeräten und Datenspeichern, die Open-Source Forensik-Tools Autopsy und Bulk Extraktor. AXIOM bietet im Vergleich dazu erweiterte Funktionen, wie die anteilig logische Datenakquise aus Apple IPhone Geräten und eine bessere Unterstützung bei der Suche über Reguläre Ausdrücke.

Neben den frei zugänglichen OSINT-Diensten und den grafisch orientierten Analyse-Tools wie Maltego CE sind für Ermittlungen im Umfeld von Kryptowährungen verschiedene kommerzielle Angebote wie Reactor von Chainalysis und Elliptic Investigator verfügbar. Besonders Reactor stellte sich bei den Recherchen als vielversprechendes Produkt dar.

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe.
Die Stellen der Arbeit, die anderen Quellen im Wortlaut oder dem Sinn nach entnommen wurden, sind durch Angaben der Herkunft kenntlich gemacht. Dies gilt auch für Zeichnungen, Skizzen, bildliche Darstellungen sowie für Quellen aus dem Internet.

Ich erkläre ferner, dass ich die vorliegende Arbeit in keinem anderen Prüfungsverfahren als Prüfungsarbeit eingereicht habe oder einreichen werde.

Die eingereichte schriftliche Fassung entspricht der auf dem Medium gespeicherten Fassung.

Ort, Datum (Unterschrift)