Master IT-Sicherheit und Forensik
Kolloquium zur Master-Thesis

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

1. Betreuer: Prof. Dr.-Ing. habil. Andreas Ahrens
2. Betreuer: Prof. Dr.-Ing. Antje Raab-Düsterhöft

Vortragender: J. Müller

Agenda

- Motivation
- Problemstellung
- Zielsetzung
- Vorgehensweise und Methoden
- Ergebnisse
- Möglichkeiten und Grenzen
- Diskussion

Motivation

- Weiterhin **ansteigende Nutzung von Kryptowährungen** wie Bitcoin als anerkanntes Zahlungsmittel
- **Kryptowährungen** dienen auch für **illegale Handlungen**, wie Erpressungen nach Ransomware Attacken oder zur **Geldwäsche** von **Einkünften aus illegalen Geschäften**

Bild: mk1one/Shutterstock.com

Studie: Geldwäsche mit Kryptowährungen 2021 um 30 Prozent gestiegen

„Cyberkriminelle haben laut einer Studie des Blockchain-Analysehauses Chainalysis 2021 Kryptogeld im Wert von rund 8,6 Milliarden US-Dollar gewaschen.“

Quelle: https://www.heise.de/news/Studie-Geldwaesche-mit-Kryptowaehrungen-2021-um-30-Prozent-gestiegen-6341024.html

- Relevanz für Banken, Behörden & Unternehmen einen **Nachweis der Nutzung von Kryptowährungen** zu führen
- Im Mittelpunkt der **Problematik** stehen die **Finanztransaktionen** sowie die **handelnden Akteure zu ermitteln**

Problemstellung

- **Verfolgung von Geldflüssen gestaltet sich schwierig!**
  - **Konten** (Wallets) liegen **nicht zentralisiert** in der Administration **regulierter Banksysteme**
  - **Wallets** werden **dezentral** in **Peer-2-Peer Netzwerken** geführt
  - **Ein- und Auszahlungen** von Kryptowährungen können **ohne Identitätsnachweise** durchgeführt werden
  - **Sender bzw. Empfänger Adressen** können fortlaufend erneuert werden

---

- **Zahlungstransaktionen** von Kryptowährungen sind aber **keineswegs vollständig anonym**!
- Eingesetzte **Blockchain-Technologien**, die als **dezentrale Buchungssysteme** fungieren sowie der **Einsatz von Open Source Intelligence (OSINT)**, ergeben Ansätze Zahlungsflüsse nachvollziehen zu können.

Zielsetzung

- Untersuchung wie **IT-forensische Methoden** der **Datenakquise- und Datenanalyse** unter Zuhilfenahme von **Open Source Intelligence**, bei der **Ermittlung** von **Zahlungsflüssen blockchain-basierter Kryptowährungen**, eingesetzt werden können
- Ermittlung der Stellen des **Nutzungsprozess,** an denen **Spuren** anfallen und wie diese bei einer **IT-forensischen Untersuchung** genutzt werden können
- **Definition von Testszenarien** in denen unter **Einsatz der etablierten IT-forensischer Softwaretools** (AXIOM, Autopsy, Bulk Extraktor) relevante Spuren **ermittelt** und **ausgewertet** werden
- **Datenauswertung** der Testszenarien und **Bewertung der Erkennungsleistung der eingesetzten Tools**
- **Gefundene Spuren** im Rahmen von **Datenanalysen** und mithilfe von **Open Source Intelligence** (OSINT) miteinander in Verbindung bringen
- Aufzeigen der **aktuellen Möglichkeiten und Grenzen** einer **Nachweisführung** und **Nachverfolgung**
- **Abschließende Handlungsempfehlung**

Vorgehensweise und Methoden

Szenarien
- Erstellung realitätsnaher Szenarien

Testfälle
- Definition Szenarien basierter Testfälle

Ausführung
- Erzeugung der lokalen Spuren auf Endgeräte

Auswertung
- Datenakquise
- Datenauswertung IT-forensischer Spuren

Datenanalyse
- Untersuchung Auswertungs-möglichkeiten
- Einsatz von OSINT-Diensten

Fachpresse

Lageberichte

ELECTRUM

bitcoin

coinbase

BINANCE

VirtualBox

ubuntu Linux

Windows 10

iPhone

Ledger Nano S

AUTOPSY DIGITAL FORENSICS

MAGNET AXIOM

The Sleuth Kit DIGITAL FORENSIC TOOL

bulk_extractor

Blockchain.com

WalletExplorer.com

BLOCKCHAIR

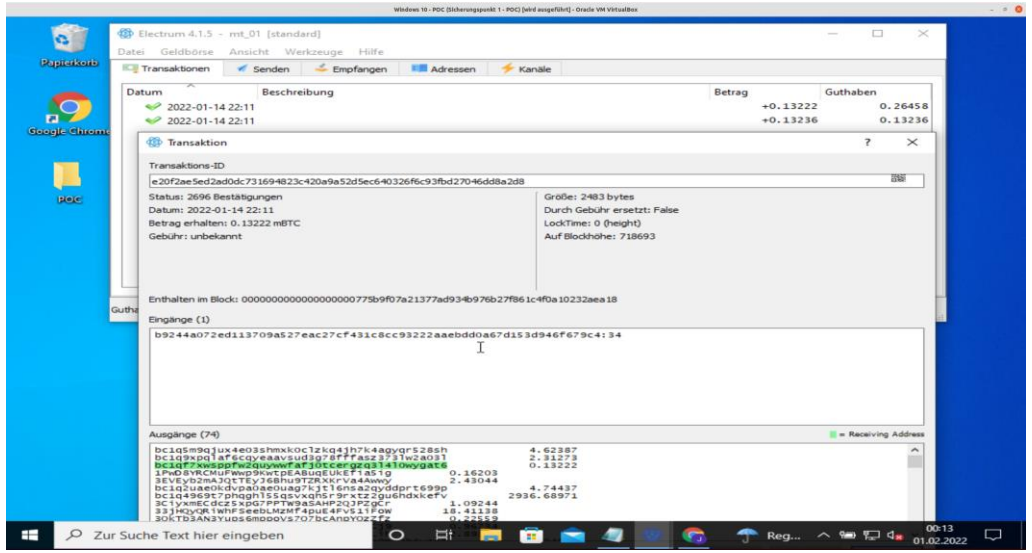
OXT

MALTEGO

BitcoinAbuse

Proof of Concept

VirtualBox Windows10 ELECTRUM bitcoin



MALTEGO


```
Terminal (als Systemverwalter)
Datei  Bearbeiten  Darstellung  Suchen  Terminal  Hilfe
   IW   /media/sf_forensik_shared/bulk_out3/bitcoin.txt
# BANNER FILE NOT PROVIDED (-b option)
# BULK_EXTRACTOR-Version: 1.6.0 ($Rev: 10844 $)
# Feature-Recorder: bitcoin
# Filename: Windows10_poc02
# Feature-File-Version: 1.1
227938339    bc1q5477rflmrrxavynqswlpqw6fhhljf52vxarcha    y": {\x0D\x0A    "bc1q5477rflmrrxavynqswlpqw6fhhljf52vxarcha": [],\x0D\x0A
227938398    bc1q5cf5syt3u878dl5dz3ytaph9memsze5tmussg8    : [],\x0D\x0A    "bc1q5cf5syt3u878dl5dz3ytaph9memsze5tmussg8": [],\x0D\x0A
227938457    bc1q5cugcqa0smhql6f68utjhs2rd6mz0q3uzrgveq    : [],\x0D\x0A    "bc1q5cugcqa0smhql6f68utjhs2rd6mz0q3uzrgveq": [],\x0D\x0A
227938516    bc1q5lrem4vsqpre0yqcze2xm5ugsag2n70q3ph4sr    : [],\x0D\x0A    "bc1q5lrem4vsqpre0yqcze2xm5ugsag2n70q3ph4sr": [],\x0D\x0A
227938575    bc1q7kz9n7a9m2sttp22wcthnjxgxnqutn6hv399v5    : [],\x0D\x0A    "bc1q7kz9n7a9m2sttp22wcthnjxgxnqutn6hv399v5": [],\x0D\x0A
227938634    bc1q7rk6gpkkpvk4a5422mn0mpkgaj09zt6gf6e656    : [],\x0D\x0A    "bc1q7rk6gpkkpvk4a5422mn0mpkgaj09zt6gf6e656": [],\x0D\x0A
227938693    bc1q7y8jlr22yxapmgayger7dguhzksdzfqd2af8kh    : [],\x0D\x0A    "bc1q7y8jlr22yxapmgayger7dguhzksdzfqd2af8kh": [],\x0D\x0A
227938752    bc1qe0qz92fq9lswgn0hx0apkhlzkfmr3l5leetqe0    : [],\x0D\x0A    "bc1qe0qz92fq9lswgn0hx0apkhlzkfmr3l5leetqe0": [],\x0D\x0A
227938811    bc1qf7xwsppfw2quywwfafj0tcergzq3l4l0wygat6    : [],\x0D\x0A    "bc1qf7xwsppfw2quywwfafj0tcergzq3l4l0wygat6": [\x0D\x0A
```

ubuntu Linux

The Sleuth Kit DIGITAL FORENSIC TOOL

bulk_extractor

Szenario 1: Handel mit illegalen Waren und Dienstleistungen

- Auf **illegalen Marktplätzen** werden von **anonymen Anbietern** Waren und Dienstleistungen angeboten
- **Handel mit illegalen Waren** wird auf **virtuellen Marktplätzen** u.a. im **Darknet (Tor-Netzwerk)** durchgeführt
- BKA konnte 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]

- **Schwierige Verfolgung,** da durch **Nutzung von Kryptowährungen** und des **Tor-Netzwerks Spuren verwischt werden**

Testfall – T1

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

Datenauswertung Testfall – T1

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 (Klartext)	N	Y	N	Nur AXIOM konnte das genutzte Coinbase Passwort in Klartext anzeigen.
Binance Google Suche	Suche	Y	Y	Y	Alle Tools konnten die Google-Suche nach Binance 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.

Teils unterschiedliche Erkennungsleistung, AXIOM besonders stark!

Vergleichbare Erkennungsleistung aller Tools.

Keine automatisierte Erkennung von Bitcoin Tx-IDs & Adressen in Autopsy.

Datenauswertung Testfall – T1

Artefakt	Aktion	Autopsy	AXIOM	Bulk Extractor	Kommentierung
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.

OSINT-Analyse | Testfall – T1 | Maltego Community Edition mit Tatum

(1) Coinbase Account – Auszahlungsadresse – (Kunde)

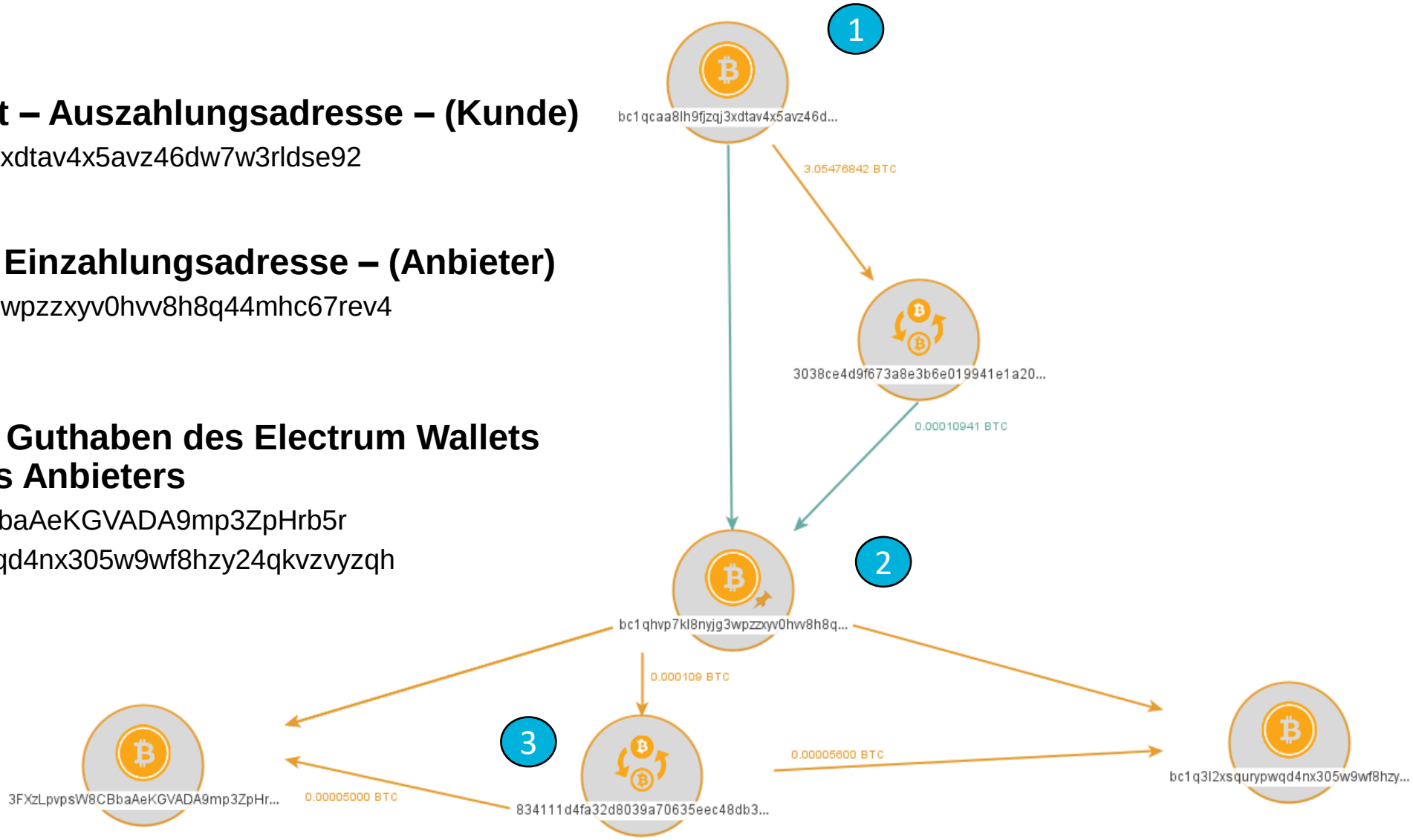
- bc1qcaa8lh9fjzqj3xdtav4x5avz46dw7w3rldse92

(2) Electrum Wallet – Einzahlungsadresse – (Anbieter)

- bc1qhvp7kl8nyjg3wpzzxyv0hvv8h8q44mhc67rev4

(3) Weiterleitung von Guthaben des Electrum Wallets an zwei Adressen des Anbieters

- 3FXzLpvpsW8CBbaAeKGVADA9mp3ZpHrb5r
- bc1q3l2xsqurypwqd4nx305w9wf8hzy24qkvzvyzqh



Szenario 2: Ransomware und Erpressung

Fokus auf Transaktionen, die im Kontext zu **Ransomware Erpressungen** ausgeführt wurden.

> *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. [1, S. 39]*

Für die Analyse dieses Szenarios wurden **zwei Handlungsstränge** verfolgt:

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

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

Testfall – T2

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

Datenauswertung Testfall – T2 (Autopsy | AXIOM)

Artefakt	Autopsy	AXIOM	Kommentierung
E-Mail-Kommunikation in Thunderbird zwischen Erpresser und Opfer (inkl. Bitcoin-Adresse)	Y	Y	Vollständige Offenlegung; vergleichbare Erkennungsleistung
Aufgerufene Webseiten (Web-History)	Y	Y	Vollständige Offenlegung; vergleichbare Erkennungsleistung
Websuchen	Y	Y	Vollständige Offenlegung; vergleichbare Erkennungsleistung
Nutzung Blockchain-Explorer	Y	Y	Vollständige Offenlegung; vergleichbare Erkennungsleistung
Electrum Soft Wallet Nutzung	Y	Y	**Autopsy** - keine Listung von Electrum unter "Installed Programs“ - Sichtbar im Standardpfad für Programm-Installationen - Anzeige einer Prefetch-Datei - „Interesting Files > Cyrptocurrency Wallets“ > Wallet-Datei muss aber manuell gesucht werden **AXIOM** - Nachweisbar über die installierten Programmen - Artefakte in der NTUSER.DAT (App-Switch Counter) - Anzeige des Wallet-Files (Anzeige lokaler Zugriffe)
Einsatz der Keyword Suche (Hits)	Y	Y	Verwendung einer statischen Keyword-Liste ergab eine Vielzahl von Treffern in Autopsy und AXIOM
Reguläre Ausdrücke ([13]|bc1)[A-HJ-NP-Za-km-z1-9]{27,34})	N	Y	**Autopsy:** Systemwarnung und Absturz bei Einsatz des Regulären Ausdrucks **AXIOM:** Performante Prozessierung; jedoch hohe Menge an False-Positives

Datenauswertung Testfall – T2 (Bulk Extraktor)

- **Extraktion von Bitcoin-Adressen funktionierte mit Bulk Extractor überzeugend**

- In der Datenextraktion befand sich u.a. die Datei **bitcoin.txt** mit der vom Erpresser verwendeten Empfangsadresse: bc1q0yetwase0pcctlkseuzg8sanlg5lsjlzt4493l

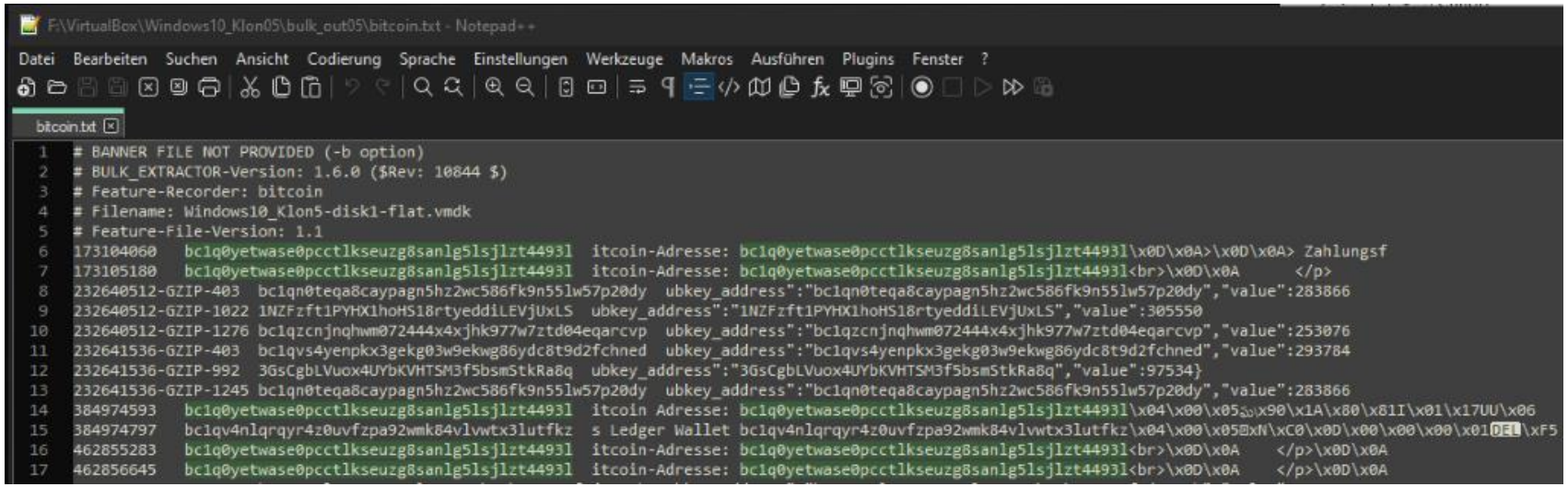


Bild 14: Bulk Output der Bitcoin-Adressen des Bulk Extractors [39]

- Anzahl False-Positives deutlich geringer als im Vergleich zur Suche über Reguläre Ausdrücke in AXIOM

OSINT-Analyse | Testfall – T2

Tabelle 11: Kryptowährungs-Objekte aus Testfall - T2

Sender	Bitcoin-Adresse	Transaktion	Zahlungsbetrag	Bitcoin-Adresse	Empfänger
Opfer	bc1qx8est 8urgs2lxfv ul4r5ax5yf mt483w08 dwf2e	bd7a8dc1c6a287 ca468f02799da4 203da67137cf7d 5765d3c3dc5257 ea0857b6	0.0007 BTC (zzgl. Gebühren)	bc1q0yet wase0pc ctlkseuzg 8sanlg5ls jlzt4493l	Erpresser

OSINT-Analyse | Testfall – T2

2 Transaktion des Opfers zum Erpresser

Bitcoin-Explorer unter Blockchain.com

Transactions

Fee	0.00000200 BTC (0.901 sat/B - 0.357 sat/WU - 222 bytes) (1.418 sat/vByte - 141 virtual bytes)	-0.00080000 BTC
Hash	bd7a8dc1c6a287ca468f02799da4203da67137cf7d5765d3c3dc5257ea0857b6	2022-06-04 21:39
bc1qx8est8urgs2lxfvul4r5ax5yfmt483w08dwf2e	0.00080000 BTC	bc1qpf5wqqra24h2rz3kpupj4vlhpv9cudl48jhgea 0.00009800 BTC bc1q0yetwase0pcctlkseuzg8sanlg5lsjlzt4493l 0.00070000 BTC

Bitcoin-Adresse des Erpresser

Fee	0.00010640 BTC (21.028 sat/B - 6.270 sat/WU - 506 bytes) (25.035 sat/vByte - 425 virtual bytes)	+0.00080000 BTC
Hash	3641dc13d600747e69293e41f07f0b659e2bf4857c773b1a6c00006fb8524a44	2022-06-04 21:30
bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h	0.46697970 BTC	bc1q6w8l0vd2utjhrnfxt35e82rk8qcn8j5kwthyuu 0.33639307 BTC bc1qpvrn0ph3c699dyxlfff7r380suxufj9xjctu3w 0.00143180 BTC bc1qgefsyhasqu3aqmwdgcel38akwn3f72s9wuy2tp 0.01174000 BTC 3HJLNe8FuAucuPS8mExVTPgLHyBcpRN4LE 0.00080000 BTC 3FyDSSMVqNJUBriL5mvTuHEA1GBK1ccdk8 0.00176432 BTC 3NGgHXdKggAj71f1ciQTc8fUDaZ33b8G8N 0.00180000 BTC 3A74xGG2Vb1knhSdonjsNanmiw2SWgBjpN 0.02480000 BTC bc1qcqwnxyr7drm87ncsdaetfrl4wfzun0zrgejzgx 0.00249069 BTC bc1qx8est8urgs2lxfvul4r5ax5yfmt483w08dwf2e 0.00080000 BTC 3EN1L7upRpZ8LgdqAhe62h6JA56E1MyF5k 0.00471000 BTC Load more outputs... (1 remaining)

1 Initiale Transaktion des Opfers für Befüllung des eigenen Wallets

Bitcoin-Adresse des Opfers

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

OSINT-Analyse | Testfall – T2

Bitcoin-Explorer unter Blockchain.com

Address

USD | BTC

This address has transacted 436,253 times on the Bitcoin blockchain. It has received a total of 30,655,794.75981625 BTC ($657,448,772,788.23) and has sent a total of 30,607,707.48648983 BTC ($656,417,485,911.38). The current value of this address is 48,087.27332642 BTC ($1,031,286,876.85).

Address	bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h
Format	BECH32 (P2WPKH)
Transactions	436,253
Total Received	30655794.75981625 BTC
Total Sent	30607707.48648983 BTC
Final Balance	48087.27332642 BTC

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

Am 19.08.2022 betrug der Wert der Bitcoin-Adresse zwischenzeitlich 48.087.27332642 BTC (1.028.024.155.35 $) mit insgesamt 436253 durchgeführten Transaktionen, weshalb bei dieser Bitcoin-Adresse von einem Finanzdienstleister bspw. einer Kryptowährungs-Börse ausgegangen werden konnte.

OSINT-Analyse | Testfall – T2

Bitcoin-Explorer unter OXT.me

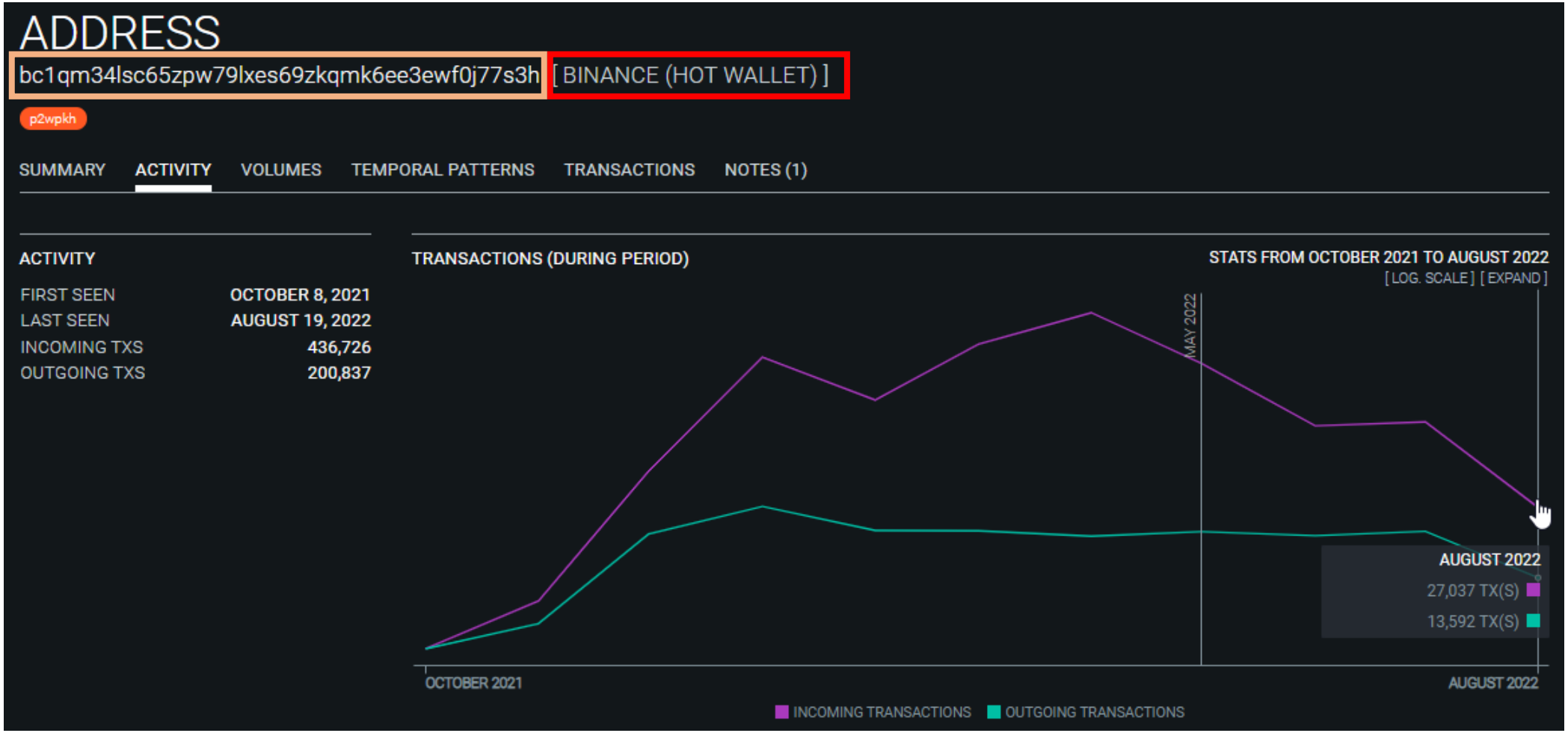


Bild 35: Verlaufskurven über eingehende und ausgehende Transaktionen einer Binance zugeordneten Bitcoin-Adresse [47]

Testfall – T3

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)

Datenauswertung Testfall – T3

Artefakt	Autopsy	AXIOM	Kommentierung

Hardware-Wallet
Ledger Nano S
	Y	Y	**Autopsy**
			- Nachweis der Nutzung des Ledger Nano S
			  - Download der Software
			  - Installation Ledger Live (Windows Registry)
			  - Listung in Interesting Files > Cryptocurreny Wallets
			- Keine Offenlegung konkreter Kryptowährungs-Objekte wie Adressen oder Transaktionen
			
			AXIOM
			- Nachweis der Nutzung des Ledger Nano S
			  - Download der Software
			  - Installation Ledger Live (Windows Registry)
			  - Anschluss des Hardware-Wallets an den USB-Port
			  - Anwendungsnutzung genutzte Funktion com.ledger.live
			  - App-Switch in der NTUSER.DAT
			- Keine Offenlegung konkreter Kryptowährungs-Objekte wie Adressen oder Transaktionen

Kryptowährungs-Objekte verblieben verschlüsselt auf dem Ledger Nano S

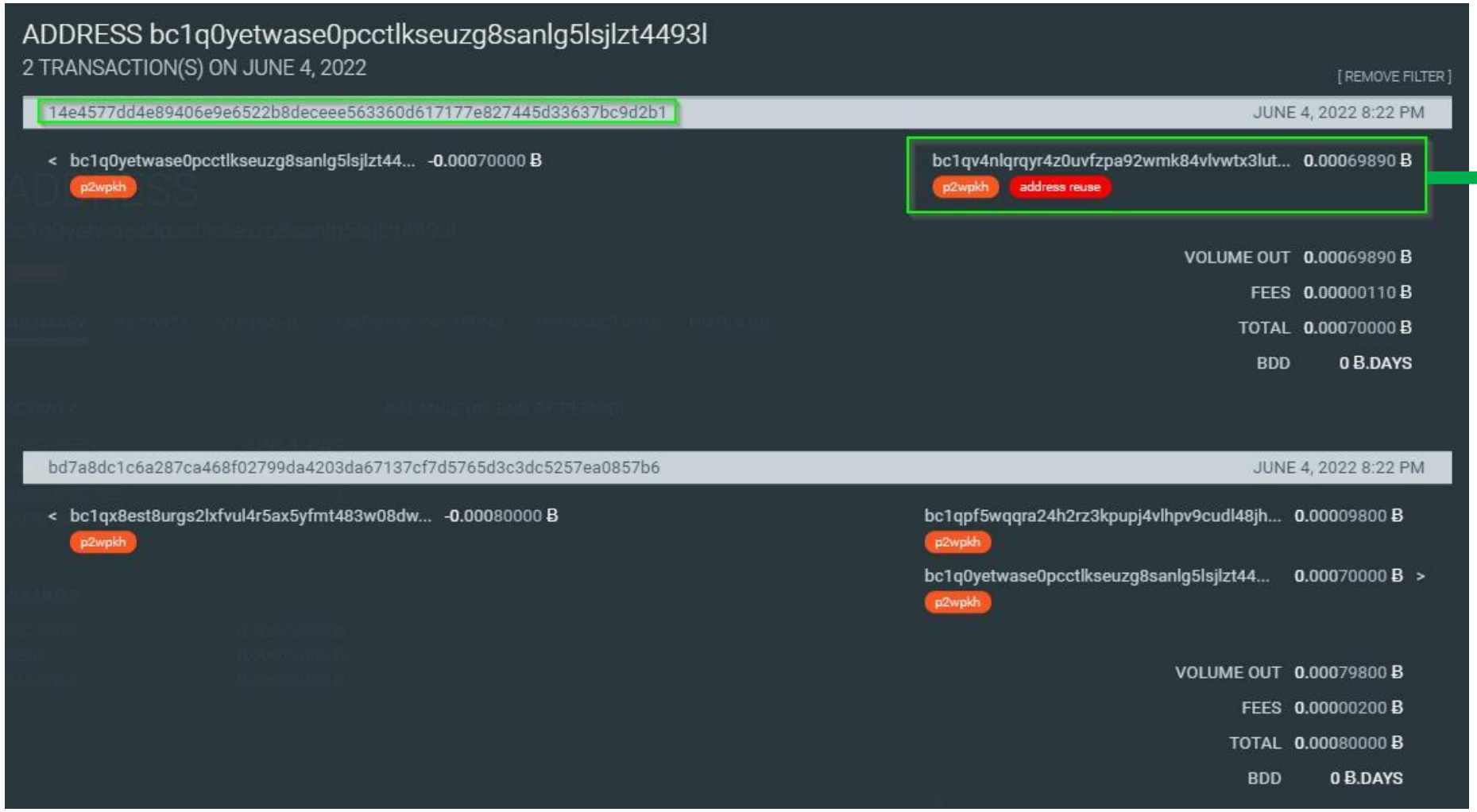
OSINT-Analyse | Testfall – T3

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 

OSINT-Analyse | Testfall – T3

Bitcoin-Explorer unter OXT.me



Ledger Nano S

Bild 37: Transaktionen einer Bitcoin-Adresse des Erpressers

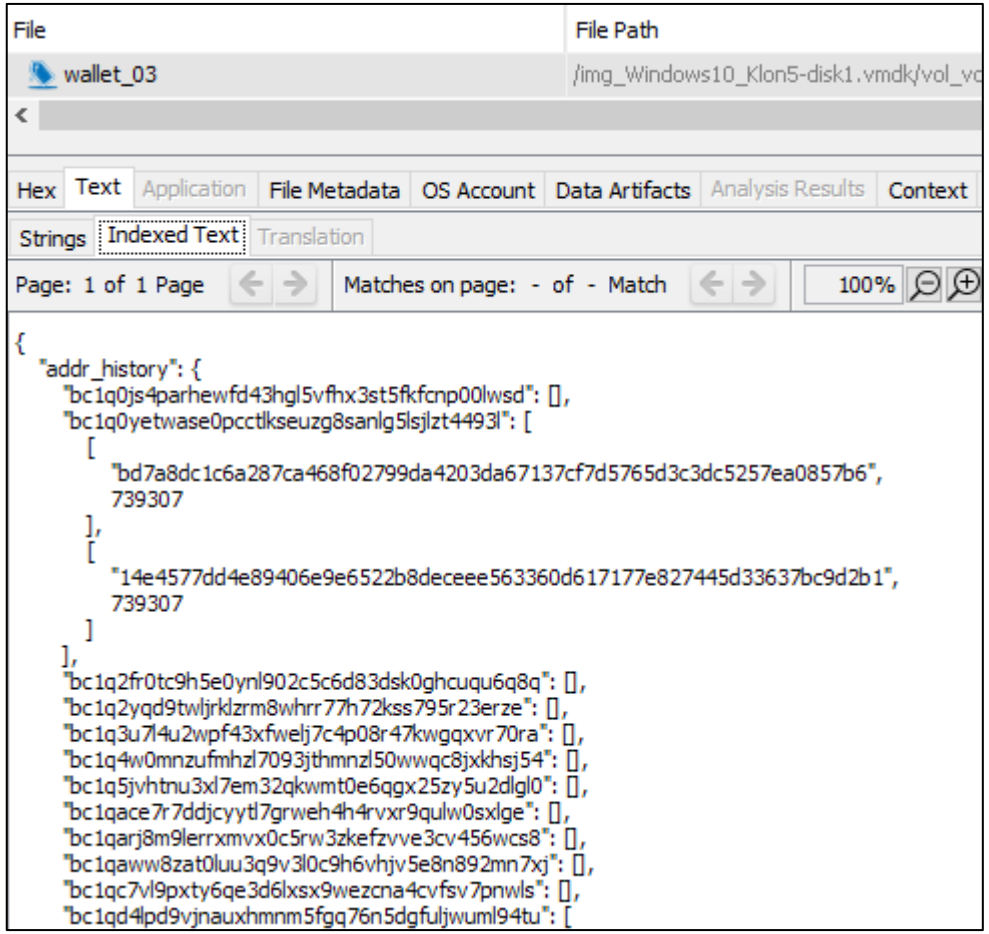
Weitere Erkenntnisse aus der Datenauswertung | Testfälle T0 - T3

Einsatz <u>unverschlüsselter</u> Electrum Wallets

- Generell gilt **Electrum als eine sichere Wallet-Lösung**, jedoch muss **vor Nutzung** dies auch **sicher konfiguriert** werden, d.h. es muss 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.

Kryptowährungs-Objekte der Wallet-Datei in Klartext auslesbar



Weitere Erkenntnisse aus der Datenauswertung | Testfälle T0 - T3

Webhistorie, Webcache und genutzte Web-Formulare

- **Microsoft EDGE und Google Chrome** hinterließen untersuchungsrelevante **Spuren**
  - Nutzung von Kryptowährungs-Diensten erzeugte **Einträge in der Webhistorie**
  - Durch **Ausführung des User-Logins** konnten **Artefakte aus dem Login-Vorgang** gewonnen werden:
    - **Login-Name in Klartext** (E-Mail-Adresse)
    - Password (verschlüsselt in SQLite-DB)

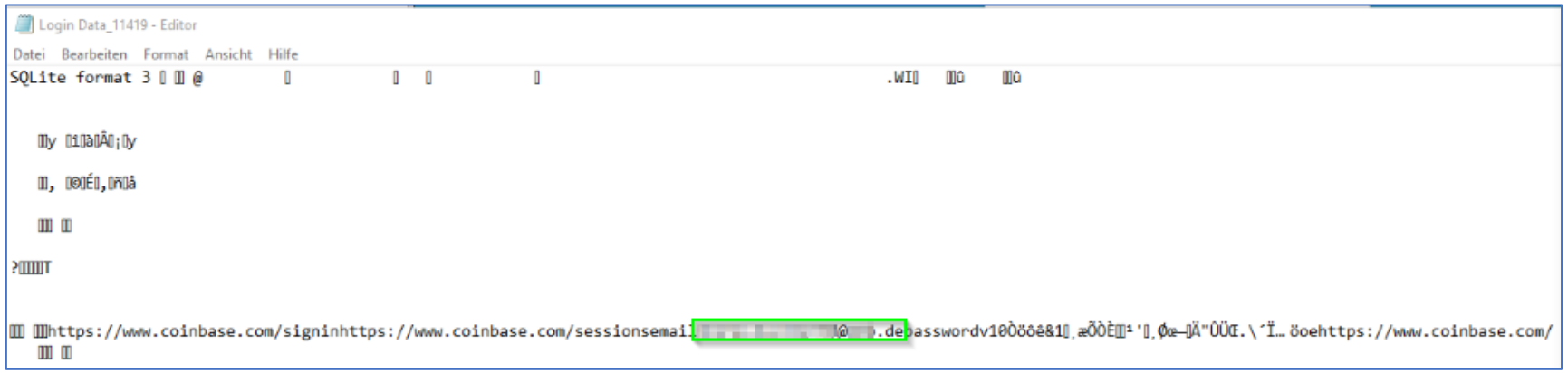


Bild 22 Auszug SQLite: Link zu Coinbase-Login, Login-Name (E-Mail-Adresse) in Klartext

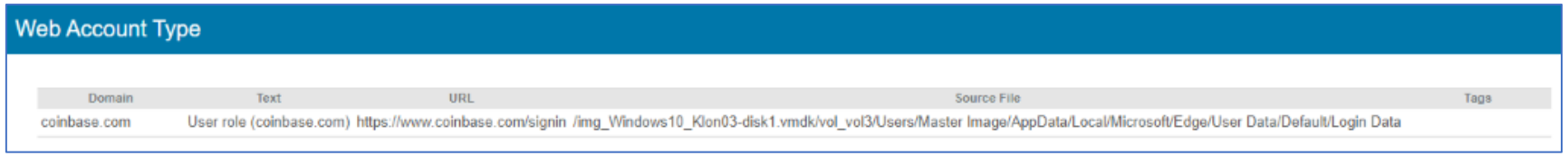
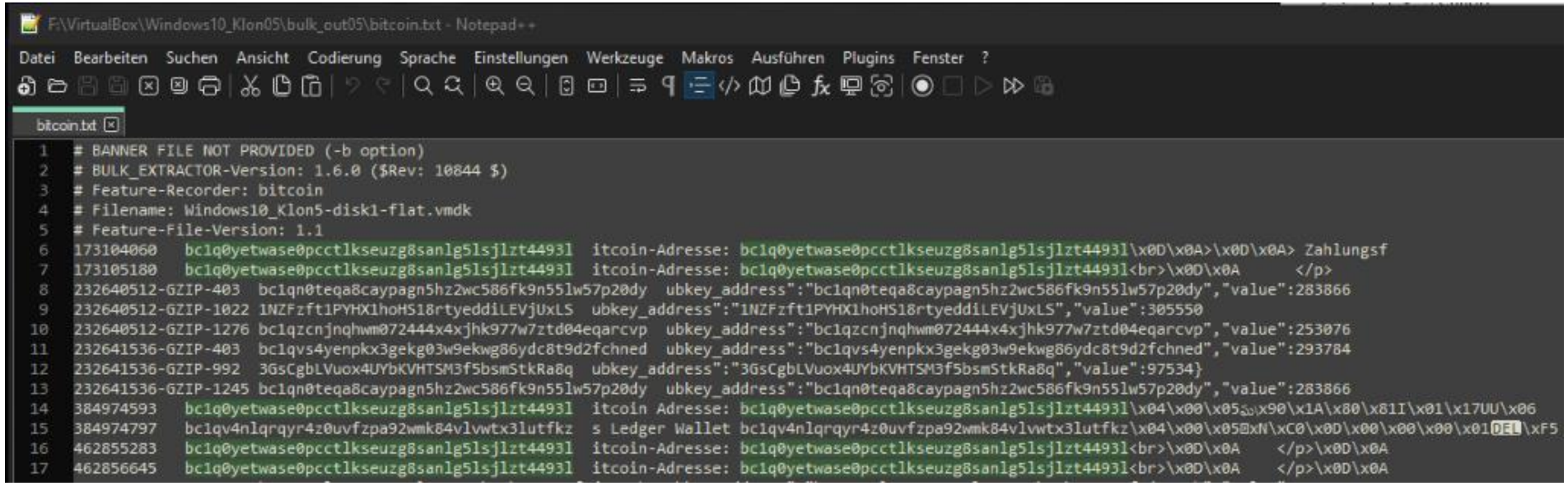


Bild 23: Auswertung des Web Account Type über Autopsy mit Anzeige von coinbase.com

Auswertung Bulk Extractor Exporte

- Bulk Extractor lieferte als Ergebnis TXT-Dateien im CSV Format



- Analyse über Datenimport in Excel für Suchen in der Ergebnismenge, Entfernen von Doubletten sowie Pivot-Funktionen zur Analyse

- Einsatz Python um TXT-Dateien zu validieren oder auszuwerten

Auswertung Bulk Extractor Exporte mit Python | Validierung

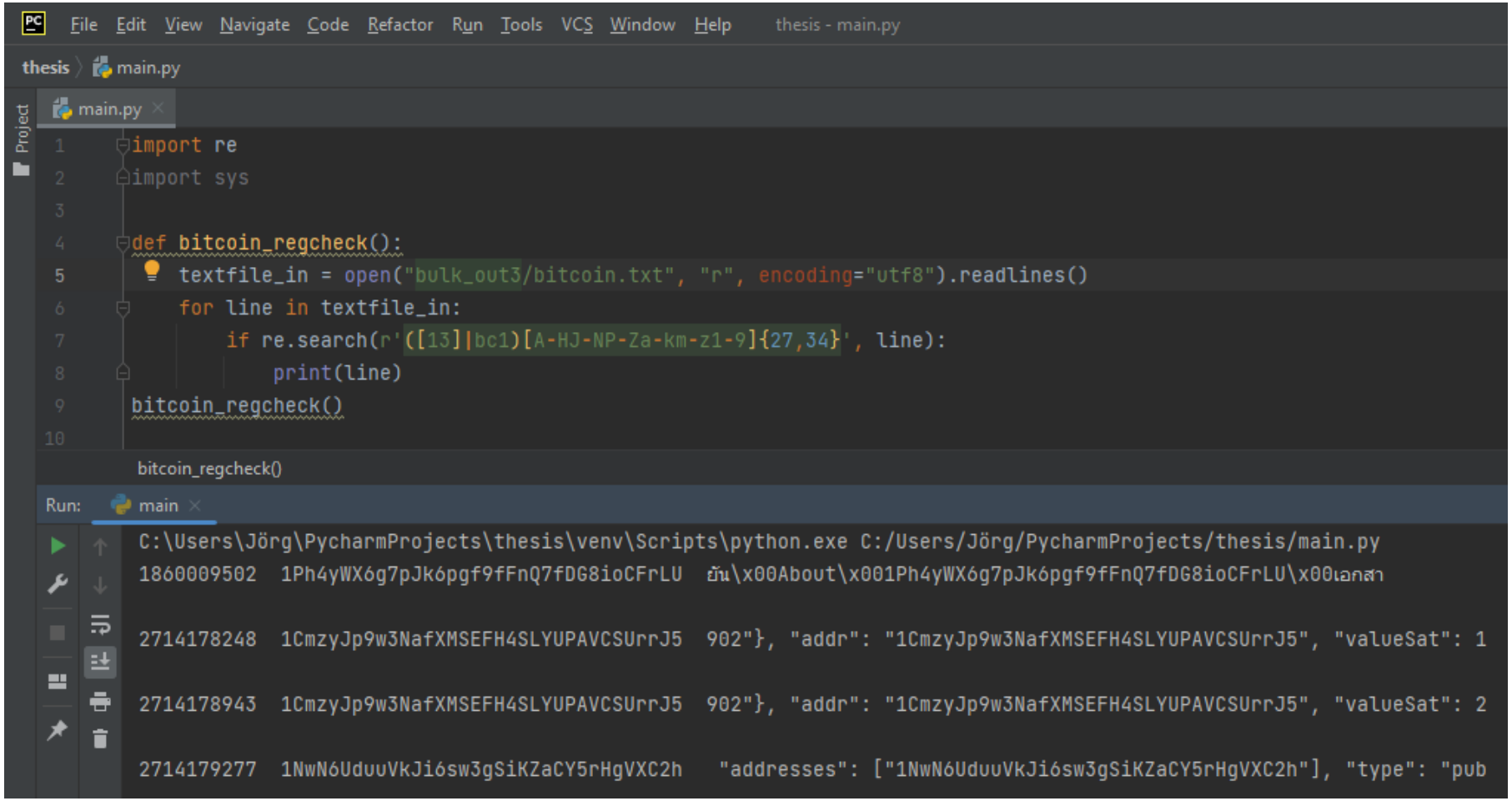


Bild 26: Ausführung Python Script zur Validierung von Bitcoin-Adressen in einer TXT-Datei unter Anwendung von Regulären Ausdrücken

Auswertung Bulk Extractor Exporte mit Python | Keyword-Suche

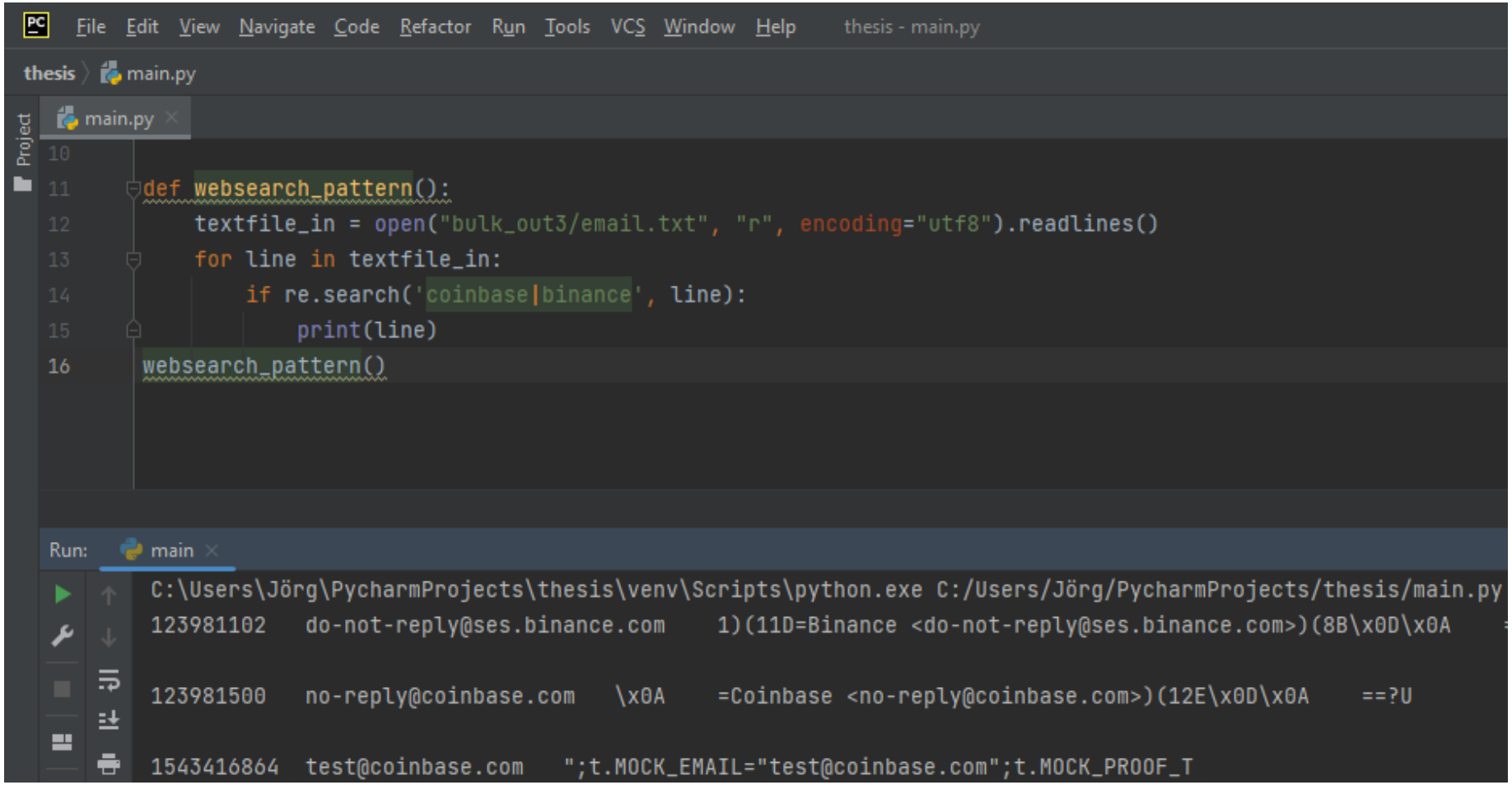


Bild 27: Ausführung Python Script zur Suche nach Keywords in einer TXT-Datei

Testfall – T4

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

OSINT-Analyse | Testfall – T4

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	d599f920f0af831271dabd390afdf94d220a1c7c36606960ccd1d9fff2c188f2
2018-10-03 12:45:30	+0.03920691	0.04670691	15cba769a4a73304a68f11b7fa581b6966fe139733723a25a0dcf01a110fce905
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	9118ca462a6ee14608e00ae018e4a1eb1f28241c2bd2083617cd656059b3b9d8
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	f99399b9ffa1da38b9cab71b9b1b7ff38957a7a77330be373f2c6ab27faaf284
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	a336905bae0f14835789 0cc51168e875b00c6bbe78f9b1efccf0980b1ba3667b
2018-04-07 17:53:23	+0.001144	0.08350943	1f2f5d44a4fb0a14b594e71a6b1a0c6b0e402fc0b2caa4eac709c7806cce1315
2018-04-06 15:00:04	+0.07003	0.08236543	e9503225722 0cebd566d0adf09b710046e423db0ab123e17869b81fe7c4bc813
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	6e462a0f6018ba298fd9136e83fed4c4afa7f075173a8b2cb04db19700 3c6573
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]

- **WalletExplorer** fasst mehrere Bitcoin-Adressen in einer Wallet-ID zusammen
- Suchergebnis Wallet-ID [c13d678521] enthält die verdächtige Bitcoin-Adresse: **12HaVrpXkLr2UnkMf6X9bY11cuNrZUdUnV**
- **Transaktionsdaten** konnten in eine **CSV-Datei** für die weitere Analyse exportiert werden

OSINT-Analyse | Testfall – T4

Zahlungen mutmaßlicher Opfer

	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.[illegible].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 [48]

Transaktionen mutmaßlicher Erpresser

	#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	[illegible]20493	000020335711d767	0	acff23f787680dbb863f12725918c9cdb858e841d782d4bff2761f5d9f11cd92
24	13.04.201[illegible]	0,083	000020335711d767	0,00043153	a336905bae0f148357890cc51168e875b00c6bbe78f9b1efccf0980b1ba3667b
[illegible]	[illegible]8 22:53	0,0570865	000167562aa67dd3	0,00142477	5dce9daa94fb202249841c385d28c4086e376390e452c2a958b9ac38cccef6e6
[illegible]	[illegible].11.2017 23:38	0,0027	0000723b95aa0c34	0,03319845	458a046c7c68f6b33fa4da2e981a1419991471951e9ce7c4843549f4f7cb8fdf
45	09.11.2017 01:24	0,02954797	7d34a2a8ab9eb7bf	0,00130477	b8ea0395355282d733b33ab8cbb5060576cd32166181f6b2b849e2153e742288
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]

Bewertung eingesetzter IT-Forensik-Tools

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	+++	+	+++

- **Erkennungsleistung war in den folgenden Aspekten gleichwertig**
  - 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 unverschlüsselten **Electrum Wallets**
  - Stabile Prozessierung der **Keyword-Suche über Reguläre Ausdrücke**
  - Anteilig **logische Datenakquise auf Apple IPhone SE**
  - AXIOM konnte gegenüber Autopsy insgesamt **bessere Resultate** liefern

- **Bulk Extractor konnte Informationen performant in TXT-Dateien extrahieren**
  - **Bitcoin-Adressen**
  - **E-Mail-Adressen**
  - **Web-Domains & URLs**

Bewertung eingesetzter OSINT-Dienste

OSINT-Dienst	Blockchain.com	OXT.me	WalletExplorer.com	Bitcoinabuse.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.

Möglichkeiten einer Nachweisführung

- **Methoden der IT-Forensik** können Spuren aus der Nutzung von Kryptowährungs-Diensten **auf lokalen Endgeräten nachweisen**

- **Offensichtliche Spuren** waren insbesondere **Kryptowährungs-Objekte**:
  - **Wallets**
  - **Bitcoin-Adressen**
  - **Bitcoin-Transaktionen**

- **E-Mail-Adressen** aus Kommunikationsverläufen & Nutzung als **User-Login** (Kryptowährungs-Dienste)

- **Unverschlüsselte Wallet-Inhalte** können als **Klartext ausgelesen** werden (Electrum)

- **Aufrufe von Suchmaschinen** und **Krypto-Webseiten** mit entsprechenden **Abfragen zu Suchbegriffen**, **Kryptowährungs-Adressen bzw. Transaktionen**, teils in den **Links der Browser-Historie** auffindbar

- **Weitere Artefakte**
  - **Anschluss von Hardware-Wallets** wie bspw. dem Ledger Nano S
  - **Softwarekomponenten** wie das **Electrum Wallet, Ledger Live**
  - **Kryptowährungs-Apps** wie **Binance** oder **Coinbase**

Grenzen einer Nachweisführung

iPhone

- **Datenakquise von Apple IPhone Smartphones**
  - ausschließlich AXIOM war im Stande, eine logische Datensicherung auf Teilen des Endgeräts durchzuführen um diese nachfolgend auszuwerten

---

- **Verschlüsselungen, die das Auslesen von Dateien in Klartext verhindern**
  - Verschlüsselt konfigurierte Electrum Wallets
  - Generell verschlüsselte Ledger Nano S Wallets

Möglichkeiten und Grenzen einer Nachverfolgung

- **OSINT unterstützt Ermittlungen im Bereich von Kryptowährungen**
  - **Blockchain-Explorer** können die **Transaktionen**, deren **Eingangs- und Ausgangsadressen** und **Zahlungsbeträge** ausweisen > Transaktionen lassen sich generell nachvollziehen
  - **Bedeutet nicht**, dass sich alleinig hierdurch die **Identität der Akteure** ableiten lässt!

- **Weiterführende Ermittlungen**, die der Offenlegung von Identitäten handelnder Akteure dienen, zeigten beim alleinigen OSINT-Einsatz Grenzen

- **Transaktionen der Bitcoin-Blockchain** sind als **pseudonym** anzusehen

- Um 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 zwei Handlungsweisen heraus, die bei einer Ermittlung im Bereich von Kryptowährungen anwendbar sind.

Ermittlungsansätze im Bereich von Kryptowährungen

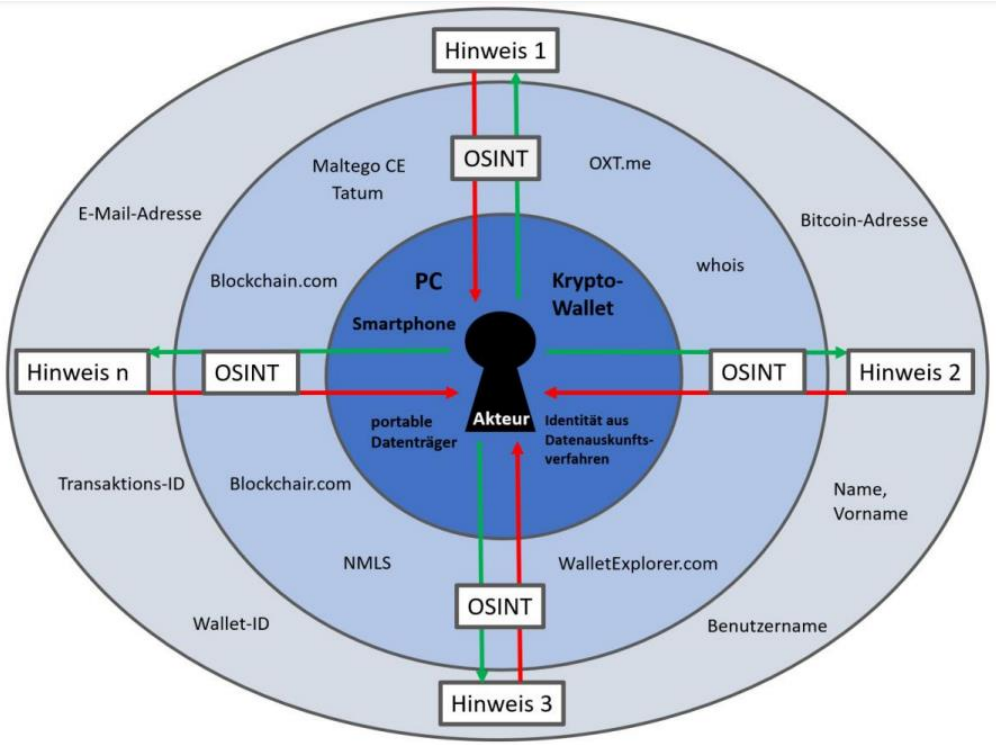


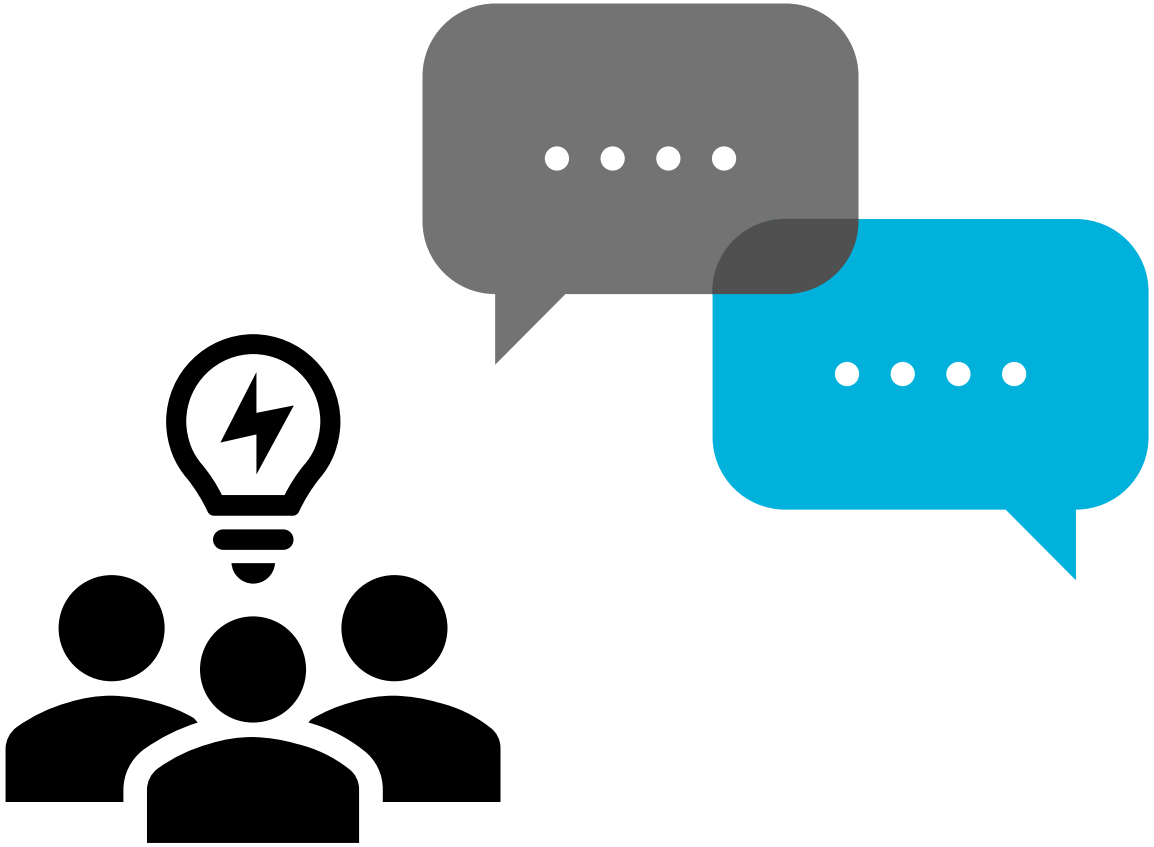
Bild 51: Modell zum Nachweis Blockchain-basierter Kryptowährungen und Nachverfolgungen von Zahlungsflüssen unter Einsatz von Open Source Intelligence

(1) Einsatz von OSINT auf Basis IT-forensischer Spuren
OSINT-Dienste ausgehend von IT-forensischen Spuren gezielt abfragen, um **neue Hinweise oder Informationen** zu erlagen.

(2) Freie Auswertung von OSINT-Diensten
- beginnt mit einem **Hinweis oder losen Information**
- **Recherche** kann u.U. eine **Verbindung zum Akteur** herstellen:
  Bspw. Nutzung einer E-Mail-Adresse, die als Login-Name für eine Kryptowährungs-Börse dient, einzelne Transaktion, deren Ein- oder Auszahlungspunkt ein offiziell registrierter Finanzdienstleister ist.
- **Nachfolgende Initiierung** entsprechender **Datenauskunftsverfahren** kann ggf. die **Identität des Kunden** offenlegen.
- Nach **Feststellung der Identität** kann eine **IT-forensische Sicherung** der Endgeräte des betroffenen Akteurs erfolgen.

Ansätze (1) und (2) lassen sich im Verlauf einer Ermittlung auch wechselseitig anwenden und bieten damit eine Methodik, lose Spuren aus der Nutzung von Kryptowährungen zu konkreten Transaktionen zusammenzuführen um so die handelnden Akteure zu ermitteln.

Diskussion



Vielen Dank für Ihre Aufmerksamkeit!