

UNIVERZITA SV. CYRILA A METODA V TRNAVE
FAKULTA PRIRODNÝCH VIED

Vražda v Orient Expresse v 21. Storočí

prezentacia

Semestrálna práca

Obsah

1. Prípád a zhrnutie	1
1.1. Digitálne stopy	1
1.2. Digitálne zariadenia	1
1.2.1. Mobil obete – Samuela Ratchetta	1
1.2.2. Mobil Hectora MacQueena	2
1.2.3. Mobil Pierra Michela	3
1.3. Hypotéza	3
1.3.1. Hypotéza 1 – Finančný motív	3
1.3.2. Hypotéza 2 – Pokus o získanie prístupu	4
1.3.3. Hypotéza 3 – Digitálna manipulácia po smrti	5
1.4. 5W + H	6
1.5. Ciele vyšetrovania	7
1.6. Postup vyšetrovania	7
1.7. Literatúra	8
1.8. Dáta	9
1.9. Image RAM	10
1.9.1. Dôkaz č. 1 – pokus o prihlásenie identifikácia	10
1.9.2. Dôkaz č. 2 – aktivita kryptomenovej aplikácie	10
1.9.3. Dôkaz č. 3 – Kryptomenová transakcia	11
1.10. Image Zariadení	11
1.10.1. Dôkaz č. 1 – Email komunikácia	11
1.10.2. Dôkaz č. 2 – nájdený súbor	12
1.10.3. Dôkaz č. 3 – Logy prihlásenia do zariadenia	12
1.10.4. Dôkaz č. 4 – Transakčný záznam	13
1.10.5. Dôkaz č. 5 – Zmenené záznamy	13
1.10.6. Dôkaz č. 6 – Zaujímavé komunikácie	13
1.10.7. Dôkaz č. 7 – Cache a dočasné súbory aplikácie	14
1.11. SW nástroje použité	14
1.11.1. FTK Imager	14
1.11.2. RAM Capturer	15
1.11.3. HxD	15
1.11.4. Autopsy	15
1.12. Bezpečnostné opatrenia	16
1.13. Chain of Custody	17
1.14. Záver	20

1. Prípád a zhrnutie

Práca sa zaoberá digitálnou forenznou analýzou prípadu vraždy v uzavretom priestore vlaku Orient Express v 21. storočí. Cieľom je analyzovať digitálne zariadenia, identifikovať relevantné digitálne stopy a rekonštruovať časovú os udalostí, na základe získaných dôkazov sú overené stanovené hypotézy, pričom hlavná hypotéza sa zameriava na pokus o neoprávnený prístup ku kryptopeňaženke obete.

1.1. Digitálne stopy

Vyšetovanie sa zameriava iba na:

- Logy prihlásenia do notebooku obete
- Čas poslednej aktivity smartfónu
- Históriu e-mailovej komunikácie
- Záznam poslednej kryptomenovej transakcie
- Systémové logy operačného systému

1.2. Digitálne zariadenia

- Všetci okrem Edwarda Mastermana mali smartfón pri sebe

Obet' mala navyše prístup k svojej digitálnej kryptopeňaženke. Smartfón obete bol po nájdení mierne fyzicky poškodený (rozbitý displej), ale zariadenie sa zapína.

1.2.1. Mobil obete – Samuela Ratchetta



Model: Samsung Galaxy S10

Farba: Modrá

Interné úložisko: 64 GB

RAM: 8 GB

Operačný systém: Android

Pripojenie: Wi-Fi, LTE, Bluetooth, USB-C

Typ úložiska: UFS 2.1

Prenosová rýchlosť: do 500 MB/s (čítanie), cca 150–200 MB/s (zápis)

Prístupová doba: približne 0.1 ms

1.2.2. Mobil Hectora MacQueena



Model: HTC U23 Pro

Farba: Biela

Interné úložisko: 256 GB

RAM: 12 GB

Operačný systém: Android

Pripojenie: Wi-Fi, LTE, Bluetooth, USB-C

Typ úložiska: UFS 3.1

Prenosová rýchlosť: do 1200 MB/s, cca 500-700 MB/s(zápis)

Prístupová doba: približne 0.05 ms

1.2.3. Mobil Pierra Michela



Model: Samsung Galaxy A17 5G

Farba: Biela

Interné úložisko: 128 GB

RAM: 4 GB

Operačný systém: Android

Pripojenie: Wi-Fi, LTE, Bluetooth, USB-C

Typ úložiska: UFS 2.2

Prenosová rýchlosť: do 600 MB/s (čítanie), cca 200–300 MB/s (zápis)

Prístupová doba: približne 0.08 ms

1.3.Hypotéza

1.3.1. Hypotéza 1 – Finančný motív

Jeden z cestujúcich prišiel o finančné prostriedky a konal z pomsty.

Digitálne stopy:

- História e-mailovej komunikácie

- Záznam poslednej kryptomenovej transakcie
- Systémové logy operačného systému

Zariadenia:

- smartfón obete
- smartfón podozrivého (dataset)

Nástroje:

- FTK Imager – analýza e-mailov a súborov, vyhľadávanie reťazcov (wallet, bitcoin)

Postup overenia:

1. Analýza e-mailovej komunikácie medzi obeťou a podozrivými
2. Identifikácia konfliktov alebo finančných sporov
3. Preskúmanie kryptomenovej transakcie pred smrťou
4. Overenie súvislosti medzi komunikáciou a transakciou

Výsledok:

potvrdená

1.3.2. Hypotéza 2 – Pokus o získanie prístupu

Páchateľ sa pokúsil získať prístup k notebooku alebo kryptopeňaženke obete.

Digitálne stopy:

- Logy prihlásenia do notebooku obete
- Systémové logy operačného systému
- Záznam poslednej kryptomenovej transakcie
- Čas poslednej aktivity smartfónu

Zariadenia:

- smartfón obete
- smartfóny podozrivých (dataset 1, 2, 3)

Nástroje:

- FTK Imager – analýza logov a dát
- RAM Capturer – získanie RAM

Postup overenia:

- Analýza logov prihlásenia do zariadenia obete
- Identifikácia podozrivej aktivity v čase smrti
- Porovnanie časových údajov medzi jednotlivými digitálnymi stopami
- Analýza kryptomenovej transakcie
- Vyhľadanie artefaktov v RAM (napr. prístup k aplikácii)

Výsledok:

potvrdená

1.3.3. Hypotéza 3 – Digitálna manipulácia po smrti

Po smrti obete niekto manipuloval s jej zariadeniami, aby vytvoril falošnú časovú os.

Digitálne stopy:

- Čas poslednej aktivity smartfónu
- Systémové logy operačného systému
- Logy prihlásenia do notebooku obete

Zariadenia:

- smartfón obete
- notebook obete

Nástroje:

- FTK Imager – analýza časových pečiatok a logov
- HxD – kontrola integrity dát a vyhľadávanie reťazcov
- RAM Capturer – získanie RAM (overenie aktívnych procesov v čase incidentu)

Postup overenia:

- Identifikácia poslednej zaznamenanej aktivity smartfónu
- Analýza časových pečiatok v systémových logoch
- Porovnanie logov prihlásenia do notebooku
- Overenie, či existuje aktivita zariadenia po poslednej zaznamenanej aktivite
- Kontrola RAM pamäte na prítomnosť aktívnych procesov

Výsledok:

zamietnutá

1.4. 5W + H**WHO(Kto?)**

Obeťou je Samuel Ratchett, investor do kryptomien. V uzavretom vozni sa nachádzali traja cestujúci, ktorí predstavujú jediný okruh podozrivých..

WHAT(Čo?)

Obeť bola nájdená mŕtva vo svojej kajute krátko po zaznamenanej digitálnej aktivite (prihlásenie do zariadenia a kryptomenová transakcia).

WHEN(Kedy?)

Čas smrti sa odhaduje medzi 00:00 – 01:15 na základe systémových logov a digitálnych stôp.

WHERE(Kde?)

Incident sa stal v uzavretom vozni vlaku počas nočnej izolácie bez možnosti vstupu cudzích osôb.

WHY(Prečo?)

Možným motívom je finančný konflikt súvisiaci s kryptomenami alebo snaha získať prístup k digitálnym aktívam.

HOW(Ako?)

Predpokladá sa kombinácia fyzického útoku a následnej manipulácie s digitálnymi zariadeniami s cieľom zakryť dôkazy.

1.5.Ciele vyšetrovania

Cieľom digitálnej forenznej analýzy je:

- Poskytnúť polícii technickú analýzu v oblasti analýzy digitálnych zariadení
- Overiť autenticitu digitálnych alibi podozrivých
- Identifikovať prípadnú manipuláciu so zariadeniami

1.6. Postup vyšetrovania

- Zaistenie zariadení a izolácia od siete
- Vytvorenie bitovej kópie diskov a výpočet has hodnoty
- Analýza digitálnych stôp (systémové logy, e-mailová komunikácia)
- Rekonštrukcia časovej osi

1.7. Literatúra

<https://dfrws.org/wp-content/uploads/2025/05/Forensic-recovery-via-chip-transplantation-in-samsung-smartphones.pdf>

Odborný článok sa zameriava na pokročilé metódy mobilnej digitálnej forenziky, konkrétne na obnovu dát zo smartfónov Samsung prostredníctvom transplantácie hardvérových čipov. Príspevok vysvetľuje technické obmedzenia štandardnej extrakcie dát pri fyzicky poškodených alebo silne šifrovaných zariadeniach a popisuje metodiku umožňujúcu obnovu prístupu k digitálnym dôkazom. Štúdia predstavuje praktickú aplikáciu hardvérovej forenziky v trestnom konaní.

<https://cfreds.nist.gov/all/>

National Institute of Standards and Technology (NIST). Computer Forensic Reference Data Sets (CFReDS). Referenčné dátové sady pre testovanie nástrojov digitálnej forenznej analýzy.

Christie, A. (1934). Vražda v Orient exprese.

Literárne dielo predstavuje klasický model vyšetrovania v uzavretom priestore („locked-room mystery“), v ktorom je páchatel' obmedzený na okruh cestujúcich. Slúži ako naratívny základ modernizovaného forenzného prípadu zasadeného do 21. storočia s dôrazom na digitálne dôkazy.

1.8. Dáta

Analyzovaný dataset pozostáva z forenzných obrazov mobilných zariadení získaných v rámci vyšetrovania. Dáta boli uložené vo forme archivovaných súborov (ZIP, TAR), ktoré obsahujú kompletne obrazy úložiska zariadení.

Typy súbor v mojich stiahnutých dátasetoch sú systémové logy operačného systému, aplikáčne dáta, databázové súbory, textové súbory, záznamy komunikácie, cache a dočasné súbory.

Veľkosť dátasetov je nasledovná: Dataset 1 – 14,2 GB; Dataset 2 – 8GB; Dataset 3 – 5,4GB. Celková veľkosť je približne teda 27,6GB.

Zdroj dátasetov:

- NIST CFReDS (Computer Forensic Reference Data Sets)

<https://cfreds.nist.gov/all/>

1.9. Image RAM

1.9.1. Dôkaz č. 1 – pokus o prihlásenie identifikácia

```
00000000 74 69 6D 65 73 74 61 6D 70 3A 20 30 30 3A 35 31 timestamp: 00:51
00000010 3A 31 32 20 20 0D 0A 4C 6F 67 69 6E 20 61 74 74 :12 ..Login att
00000020 65 6D 70 74 3A 20 46 41 49 4C 45 44 20 20 0D 0A empt: FAILED ..
```

Analýza:

V dekódovanom texte RAM pamäte bol identifikovaný čitateľný reťazec obsahujúci časovú pečiatku a informáciu o prihlásení. Reťazec „Login attempt: FAILED“ indikuje neúspešný pokus o prístup do zariadenia.

Význam dôkazu:

Dôkaz poukazuje na pokus o neoprávnený prístup k zariadeniu obete. Časová pečiatka umožňuje zaradiť udalosť do časovej osi incidentu. Podporuje hypotézu o pokuse o získanie prístupu ku kryptopeňaženke.

1.9.2. Dôkaz č. 2 – aktivita kryptomenovej aplikácie

```
00000030 0D 0A 4C 61 73 74 20 61 63 74 69 76 69 74 79 3A ..Last activity:
00000040 20 30 30 3A 35 32 3A 30 38 20 20 0D 0A 41 70 70 00:52:08 ..App
00000050 6C 69 63 61 74 69 6F 6E 3A 20 43 72 79 70 74 6F lication: Crypto
00000060 20 57 61 6C 6C 65 74 20 20 0D 0A 0D 0A 54 72 61 Wallet ....Tra
```

Analýza:

V dekódovanom texte RAM pamäte bol identifikovaný reťazec obsahujúci „Last activity: 00:52:08“. Súčasne bol zistený názov aplikácie „Application: Crypto Wallet“, čo poukazuje na aktívne používanie kryptomenovej aplikácie.

Význam dôkazu:

Naznačuje, že zariadenie bolo aktívne krátko pred incidentom. Použitie kryptomenovej aplikácie súvisí s finančným motívom prípadu. Podporuje hypotézu o pokuse o prístup ku kryptopeňaženke obete.

1.9.3. Dôkaz č. 3 – Kryptomenová transakcia

```
00000060 20 57 61 6C 6C 65 74 20 20 0D 0A 0D 0A 54 72 61  Wallet ....Tra
00000070 6E 73 61 63 74 69 6F 6E 20 74 69 6D 65 3A 20 30  nsaction time: 0
00000080 30 3A 35 33 3A 32 31 20 20 0D 0A 53 74 61 74 75  0:53:21 ..Statu
00000090 73 3A 20 50 45 4E 44 49 4E 47 20 20 0D 0A 0D 0A  s: PENDING ....
```

Analýza:

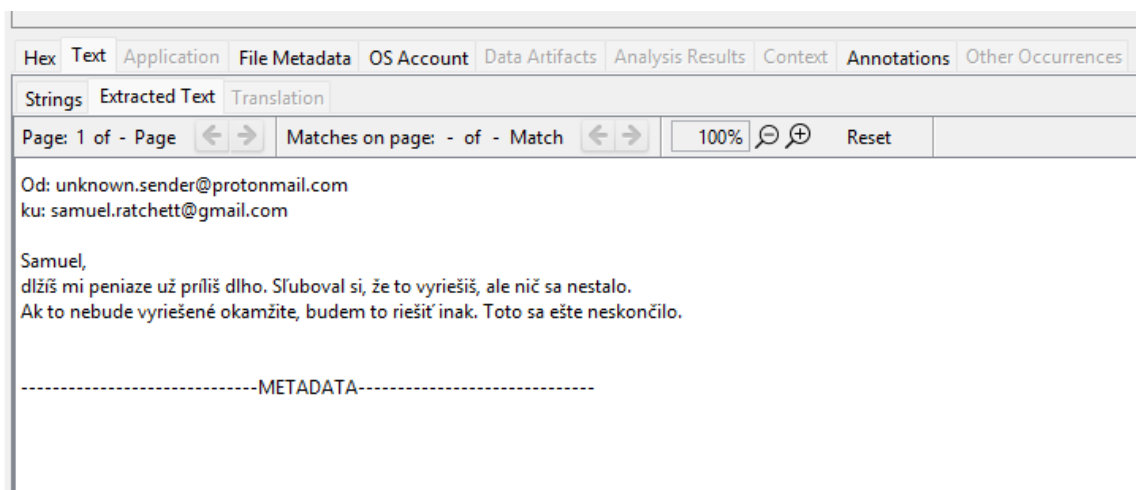
V dekódovanom texte RAM pamäte bol identifikovaný reťazec „Transaction time: 00:53:21“. Súčasne bol zistený stav transakcie „Status: PENDING“, čo naznačuje prebiehajúcu alebo nedokončenú operáciu.

Význam dôkazu:

Naznačuje manipuláciu s kryptomenovými prostriedkami krátko pred incidentom. Čas transakcie nadväzuje na predchádzajúce aktivity zariadenia. Výrazne podporuje hypotézu o pokuse o získanie prístupu ku kryptopeňaženke.

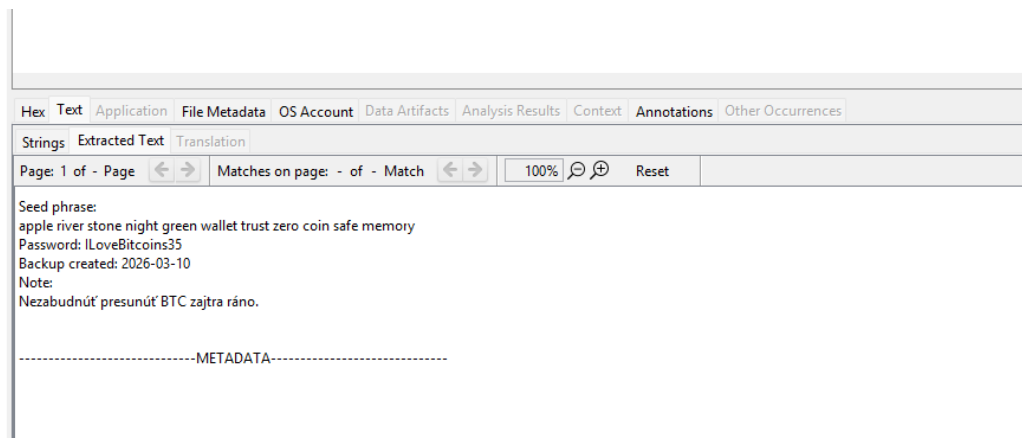
1.10. Image Zariadení

1.10.1. Dôkaz č. 1 – Email komunikácia



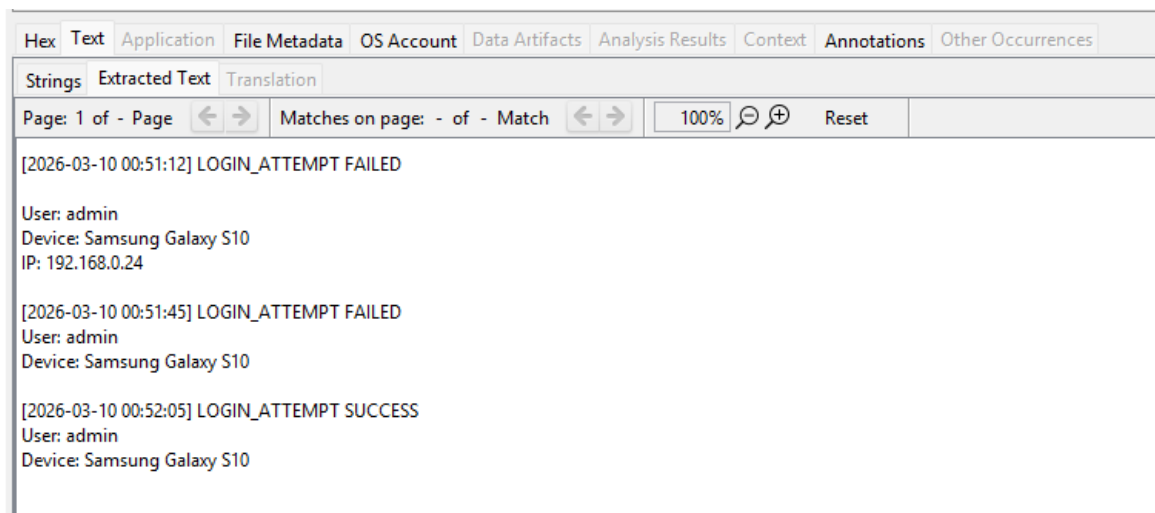
Tento dôkaz poukazuje na existenciu finančného konfliktu. Naznačuje možný motív trestného činu. Podporuje hypotézu finančného motívu

1.10.2. Dôkaz č. 2 – nájdený súbor



Poukazuje na existenciu kryptopeňaženky a prístupových údajov. Naznačuje možnosť neoprávneného prístupu k finančným prostriedkom. Podporuje hypotézu o pokuse o získanie prístupu ku kryptopeňaženke.

1.10.3. Dôkaz č. 3 – Logy prihlásenia do zariadenia



Naznačuje pokus o prelomenie prístupu do zariadenia. Indikuje možný neoprávnený prístup po viacerých neúspešných pokusoch. Silne podporuje hypotézu o pokuse o získanie prístupu k zariadeniu obeť.

1.10.4. Dôkaz č. 4 – Transakčný záznam

The screenshot shows a forensic analysis tool interface. At the top, there are tabs: Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The 'Text' tab is selected. Below it, there are sub-tabs: Strings, Extracted Text, and Translation. The 'Extracted Text' sub-tab is active. The main area displays transaction details: Transaction ID: 8f3a9c2d4b7e1a56, Date: 2026-03-10, Time: 00:53:21, From Wallet: bc1qxy...ratchett01, To Wallet: bc1qzz...unknown99, Amount: 0.75 BTC, Fee: 0.0001 BTC, Status: PENDING, Confirmation: 0/6. Below this, there is a section labeled '-----METADATA-----'.

Poukazuje na pokus o presun finančných prostriedkov. Naznačuje možnú neoprávnenú manipuláciu s kryptopeňaženkou. Silne podporuje hypotézu o pokuse o získanie prístupu ku kryptopeňaženke.

1.10.5. Dôkaz č. 5 – Zmenené záznamy

Save Table as CSV			
Icon	Date/Time	Description	Event Type
	2020-03-23 00:00:05	/MUS_Android.tar/data/data/com.joeykrim.rootcheck...	File Modified
	2020-03-23 00:00:05	/MUS_Android.tar/data/data/com.joeykrim.rootcheck...	File Modified

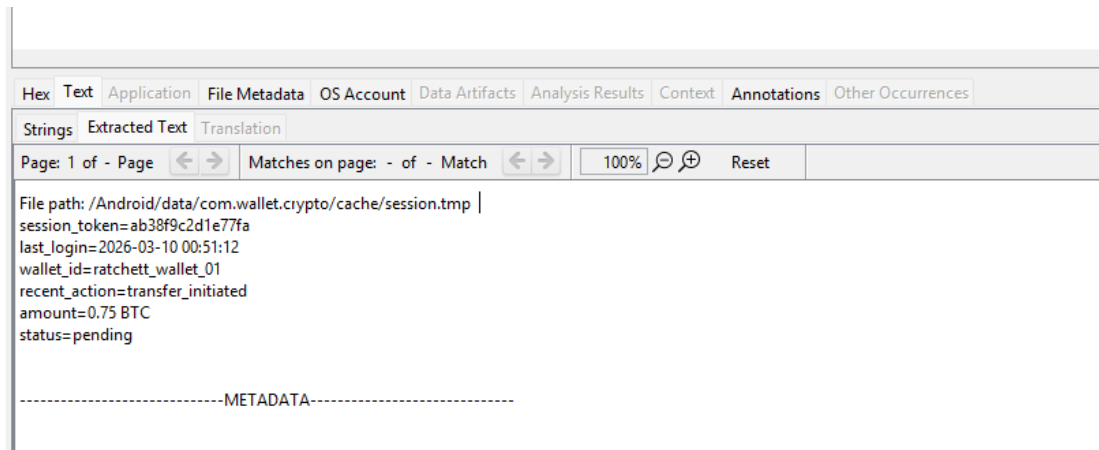
Pomocou nástroja Autopsy bola analyzovaná časová os súborového systému zariadenia. V sledovanom období boli identifikované viaceré udalosti typu „File Modified“, ktoré poukazujú na aktívnu prácu so súbormi.

1.10.6. Dôkaz č. 6 – Zaujímavé komunikácie

	dokazyOhrozenia.txt		
	email_backup.txt		
	Funds_backup.txt		
	Logs_backup.txt		
	POMOC!.txt		
	session_backup.txt		
	vyhrazanie.txt		
	wallet_backup.txt		

Pomocou nástroja Autopsy boli identifikované textové súbory obsahujúce komunikáciu s výhražným charakterom. Súbory boli uložené v adresári: /komunikacia/. Dôležité sú preto, lebo poukazujú existenciu konfliktu medzi obeťou a inou osobou. Silne podporuje hypotézu finančného alebo osobného motívu.

1.10.7. Dôkaz č. 7 – Cache a dočasné súbory aplikácie



Potvrďuje používanie kryptomenovej aplikácie v čase incidentu. Obsahuje informácie o prebiehajúcej finančnej operácii. Podporuje hypotézu o neoprávnenom prístupe ku kryptopeňaženke

1.11. SW nástroje použité

1.11.1. FTK Imager

Nástroj FTK Imager bol použitý na vytváranie a analýzu forenzných obrazov dátových nosičov. Umožňuje prehliadanie súborového systému bez zmeny pôvodných dát a poskytuje základné funkcie digitálnej forenznej analýzy.

Použitie v práci:

- vytvorenie bitovej kópie dát (image)
- výpočet hash hodnôt (MD5, SHA1) na overenie integrity dát
- analýza súborov a systémových logov
- vyhľadávanie reťazcov pomocou funkcie „Find“

1.11.2. RAM Capturer

RAM Capturer bol použitý na získanie obrazu operačnej pamäte (RAM) zariadenia. Tento nástroj umožňuje zachytiť volatilné dáta, ktoré sa po vypnutí zariadenia strácajú.

Použitie v práci:

- vytvorenie obrazu RAM pamäte
- získanie dočasných dát (napr. aktívne procesy, textové reťazce)
- zabezpečenie dôkazov nachádzajúcich sa iba v pamäti

1.11.3. HxD

HxD je hexadecimálny editor, ktorý bol použitý na analýzu surových dát získaných z RAM pamäte. Umožňuje zobrazenie dát v hexadecimálnej aj textovej podobe a vyhľadávanie konkrétnych reťazcov.

Použitie v práci:

- analýza obrazu RAM pamäte na úrovni surových dát
- identifikácia textových reťazcov (napr. login, wallet, transaction)
- kontrola obsahu pamäte a interpretácia nájdených artefaktov

1.11.4. Autopsy

Autopsy je open-source nástroj na digitálnu forenznú analýzu, ktorý umožňuje prehliadanie a analýzu dátových obrazov zariadení. Poskytuje funkcie ako analýza časovej osi (timeline), prehliadanie súborov, vyhľadávanie artefaktov a identifikáciu používateľskej aktivity.

Použitie v práci:

- analýza časovej osi (timeline) zariadenia
- identifikácia súborov a komunikácie (napr. textové súbory s výhražným obsahom)
- analýza systémových a aplikačných dát
- vyhľadávanie relevantných digitálnych stôp v datasetoch

1.12. Bezpečnostné opatrenia

Počas digitálneho forenzného vyšetrovania boli dodržané základné bezpečnostné opatrenia na zabezpečenie integrity a dôveryhodnosti dôkazov.

Zo všetkých zaistených zariadení boli vytvorené minimálne dve bitové kópie (forenzné obrazy dát). Jedna kópia bola použitá na samotnú analýzu a druhá bola uložená ako záložná kópia pre prípad potreby opakovanej analýzy.

Integrita dát bola overená pomocou hash funkcií MD5 a SHA1. Vypočítané hash hodnoty boli porovnané pred a po analýze, čím sa zabezpečilo, že nedošlo k zmene dát.

Zariadenia boli po zaistení izolované od siete, aby sa zabránilo vzdialenému prístupu alebo manipulácii s dátami. Následne boli uchovávané v zabezpečenom prostredí s obmedzeným prístupom.

Počas celého vyšetrovania bol vedený chain of custody, ktorý zaznamenáva manipuláciu s dôkazmi, časové pečiatky a vykonané úkony.

1.13. Chain of Custody

Číslo:	01	Typ súboru:	zip	Obnovený súbor:	Nie	Veľkosť:	14.2 GB
Popis prípadu:		Vražda v Orient Expresse v 21. storočí					
Názov súboru:		3 Samsung.GSM SM-G973F DS Galaxy S10.zip					
Miesto získania digitálnej stopy:		Forenzný dataset – mobilné zariadenie (CFReDS)					
Poznámky:							
Časové pečiatky							
Access:	10.3.2026 --8-20-23--		Modify:	10.3.2026 --8-30-55--		Change:	17.3.2026 --11-25-25--
Digitálny odtlačok (heš)	MD5	57062f09f04cb0666502159217fa6fa2					
	SHA1	f99df4e7e34efb1c9ec81657f7d6934d632edded					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
10.3.2026 9:15		Zaistenie mobilného zariadenia					
10.3.2026 10:02		Vytvorenie forenzného obrazu dát (dump)					
10.3.2026 10:30		hash hodnoty (MD5, SHA1)					
10.3.2026 11:00		Import obrazu do forenzného nástroja					

Číslo:	02	Typ súboru:	tar	Obnovený súbor:	Nie	Veľkosť:	8 GB
Popis prípadu:		Vražda v Orient Expresse v 21. storočí					
Názov súboru:		MUS_Android.tar					
Miesto získania digitálnej stopy:		Forenzný dataset – mobilné zariadenie (CFReDS)					
Poznámky:							
Časové pečiatky							
Access:	10.3.2026 --8-20-23--		Modify:	10.3.2026 --8-30-55--		Change:	17.3.2026 --11-25-25--
Digitálny odtlačok (heš)	MD5	57062f09f04cb0666502159217fa6fa2					
	SHA1	f99df4e7e34efb1c9ec81657f7d6934d632edded					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
10.3.2026 11:20		Zaistenie mobilného zariadenia					
10.3.2026 11:35		Vytvorenie forenzného obrazu dát (dump)					
10.3.2026 11:55		hash hodnoty (MD5, SHA1)					
10.3.2026 12:15		Import obrazu do forenzného nástroja					

Číslo:	03	Typ súboru:	tar	Obnovený súbor:	Nie	Veľkosť:	5,4 GB
Popis prípadu:		Vražda v Orient Expresse v 21. storočí					
Názov súboru:		Android_8.tar					
Miesto získania digitálnej stopy:		Forenzný dataset – mobilné zariadenie (CFReDS)					
Poznámky:							
Časové pečiatky							
Access:	10.3.2026 --8-20-23--		Modify:	10.3.2026 --8-30-55--		Change:	17.3.2026 --11-25-25--
Digitálny odtlačok (heš)	MD5	57062f09f04cb0666502159217fa6fa2					
	SHA1	f99df4e7e34efb1c9ec81657f7d6934d632edded					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
10.3.2026 12:30		Zaistenie mobilného zariadenia					
10.3.2026 12:55		Vytvorenie forenzného obrazu dát (dump)					
10.3.2026 13:20		hash hodnoty (MD5, SHA1)					
10.3.2026 13:45		Import obrazu do forenzného nástroja					

1.14. Záver

Na základe vykonanej digitálnej forenznej analýzy bolo možné rekonštruovať priebeh udalostí a identifikovať kľúčové digitálne stopy súvisiace s incidentom. Analýza RAM pamäte odhalila pokusy o prihlásenie do zariadenia, následnú aktivitu používateľa a iniciovanie kryptomenovej transakcie, čo poukazuje na možný neoprávnený prístup k zariadeniu obete.

Tieto zistenia boli ďalej podporené analýzou dát zariadení pomocou nástroja Autopsy, kde boli identifikované súbory obsahujúce komunikáciu s výhražným charakterom, systémové logy prihlásenia, ako aj záznamy o aktivitách aplikácií. Zvlášť významné boli textové súbory uložené v adresári komunikácie, ktoré poukazujú na existenciu konfliktu a možný motív konania.

Analýza transakčných záznamov a cache súborov aplikácie potvrdila, že v čase incidentu prebiehala operácia s kryptomenovou peňaženkou, pričom stav transakcie bol „pending“, čo naznačuje nedokončený pokus o presun finančných prostriedkov. Tieto dôkazy sú časovo zosúladené s aktivitami identifikovanými v RAM pamäti aj časovej osi zariadenia.

Na základe všetkých analyzovaných dôkazov bola potvrdená hypotéza o neoprávnenom prístupe k zariadeniu a hypotéza finančného motívu. Naopak, hypotéza o manipulácii so zariadením po smrti obete nebola potvrdená, keďže nebola identifikovaná žiadna relevantná aktivita po predpokladanom čase incidentu.

Výsledky analýzy potvrdzujú význam digitálnej forenznej analýzy pri vyšetrovaní incidentov, keďže umožňuje identifikovať, analyzovať a prepojiť rôzne digitálne stopy do logického celku.