

UNIVERZITA SV. CYRILA A METODA V TRNAVE
FAKULTA PRIRODNÝCH VIED

Ústav počítačových technológií a informatiky

Vražda študenta

Semestrálna práca

2. Ročník, UPTI 05

Matej Červenec

2024/2025

Obsah

1	Identifikácia	4
1.1	Prípad	4
1.2	Digitálne stopy	4
1.3	Digitálne zariadenia	4
1.4	Hypotézy	5
1.5	5 WH	5
1.6	Ciele vyšetrovania	5
1.7	Postup vyšetrovania	6
1.8	Literatúra	6
2	Zaist'ovanie a zber	7
2.1	SMARTFÓN	7
2.2	NOTEBOOK	8
2.3	Vytvorenie disk imagu	10
3	Uchovanie	12
3.1	Vytvorenie kópií	12
3.2	Používané nástroje	12
3.3	Používané dáta	12
4	Vyt'azovanie	15
4.1	Kategórie a počet súborov	15
5	Analýza	17
5.1	Analýza RAM pamäte	17
5.2	Hypotéza 1	18
5.3	Hypotéza 2	20

5.4	Hypotéza 3	21
Záver		24

Obsah obrázkov

Obr. č. 1: Fotografia mobilného zariadenia	8
Obr. č. 2: Fotografia notebooku	10
Obr. č. 3: Disk image 1. kópia	10
Obr. č. 4: Disk image 2. kópia	11
Obr. č. 5: CHOC č. 1	13
Obr. č. 6: CHOC č. 2	14
Obr. č. 7: Obnovené súbory	15
Obr. č. 8: Graf typov obnovených dát	16
Obr. č. 9: RAM image č. 1	17
Obr. č. 10: RAM image č. 2	17
Obr. č. 11: Kamerový záznam z párty	18
Obr. č. 12: Metadáta kamerového záznamu z party	18
Obr. č. 13: Kamerový záznam pred bytom	19
Obr. č. 14: Metadáta kamerového záznamu z ulice pred bytom	19
Obr. č. 15: Textový súbor 900123.txt	20
Obr. č. 16: Textový súbor 900120.txt	21
Obr. č. 17: Fotografia rodiny obete (dataset 900.zip)	22
Obr. č. 18: Fotografia obete (dataset 900.zip)	22
Obr. č. 19: Vyhľadané IMEI číslo	23

1 Identifikácia

Prezentácia - <https://bcstudent.fpvucm.sk/~cervenecmatej/dfa/prezentacia.pdf>

1.1 Prípád

V piatok 21. 2. 2025 bola spáchaná vražda študenta, ktorý bol nájdený mŕtvy vo svojom prenajatom byte. Obet' nemala žiadne známe priestupky ani spojitost' s nelegálnou činnosťou. Pri čine neboli nájdení žiadni svedkovia, avšak je známe, že obet' v ten deň navštívila bar v meste, kde sa konala študentská párty. Na mieste činu sa našli smartfón a notebook, ktoré pravdepodobne patrili obeti. Zariadenia neboli zabezpečené heslom. Hlavným podozrivým je kamarát obete, ktorý mal byť s ním údajne na skorej spomenutej party

1.2 Digitálne stopy

Na zariadeniach je vyhľadávanie sústredené na komunikačné, multimediálne a GPS stopy. Medzi takéto stopy patria posledné správy SMS alebo e-maily, fotografie a videá a informácie o pohybe obete. V prípade nutnosti vyšetrovateľa môžu zväžiť záznamy mestských kamier.

Multimediálne súbory - Fotografie alebo videá z daného dňa/týždňa, ktoré by objasnili okolnosti trestného činu. Multimediálne súbory na moderných smartfónoch obsahujú taktiež dôležité metadáta, z ktorých vieme zistiť lokáciu a čas kde sa obet' nachádzala v čase vytvorenia fotografie alebo videa.

Komunikačné záznamy – SMS správy alebo rôzne internetové chaty nám môžu pomôcť s tým obet' komunikovala naposledy, na základe čoho môžeme vytvoriť zoznam prípadných podozrivých. Je možné objaviť aj rôzne nekalé aktivity obete, ktoré vyhrotili v tento čin, čo nám môže poskytnúť potencionálny motív vraždy.

GPS stopy – Pokiaľ obet' mala zapnuté geolokačné služby môžeme nájsť archívy lokácie obete spolu s časom aby sme zistili kedy a kde sa obet' nachádzala pred smrťou.

1.3 Digitálne zariadenia

Notebook – Na mieste činu bol nájdený notebook predpokladane patril obeti avšak bol objavený vo veľmi poškodenom stave. Poškodenie sa vyskytlo pravdepodobne pri zápase s útočníkom, keďže aj stôl vedľa notebooku bol prekotený. Notebook bol bezpečne zaistený, ale nebude z neho možné čerpať ani analyzovať dáta kvôli rozsiahlemu poškodeniu.

Smartfón – Na mieste činu bolo nájdené mobilné zariadenie blízko obeti z čoho odhadujeme že zariadenie pravdepodobne patrilo obeti. Toto zariadenie môže obsahovať dôležité záznamy z dňa trestného činu.

1.4 Hypotézy

Hypotéza 1 - Obet' bola zabitá kamarátom, s ktorým údajne bola na párty. Na zariadeniach sa nenašli žiadne multimediálne súbory ani správy z toho večera, takže sa predpokladá že mohli byť vymazané. Motivácia vraždy je neznáma.

Hypotéza 2 - Obet' mohla byť zapojená do nelegálnej činnosti. Pri takejto hypotéze sa vysvetľujú pravdepodobne vymazané fotografie a chaty z dôvodu bezpečnosti

Hypotéza 3 - Zariadenia nepatria obeti a mohli byť boli odcudzené čo by viedlo k motivácii útoku od pôvodného vlastníka

1.5 5 WH

WHO/KTO – zavraždený študent, kamarát študenta

WHERE/KDE – byt študenta, party v meste

WHEN/KEDY – zariadenia boli nájdené pri prehliadke bytu forenznými analytikmi, zosnulý bol objavený odhadovane 3 hodiny po smrti

WHAT/ČO - napadnutie a vražda, objavenie smartfónu a notebooku

WHY/PREČO – dôvody činu nie sú zatiaľ známe avšak čas usmrtenia je zdanlivo premyslený aby bol čin najmenej nápadný

HOW/AKO – podľa zostatkov obete išlo o násilnú vraždu, kde sa obet' pokúšala brániť, na tele sú jasné známky po boji s útočníkom, po ktorom obet' skončila uškrtená. Predpokladá sa že útočník vymazal prípadné digitálne stopy, ktoré by ho usvedčili z činu

1.6 Ciele vyšetovania

1. **Identifikácia** – Cieľom je identifikácia zaobstaraných zariadení a ich stavu. Hlavným cieľom je zistenie možnosti obnovy dát a posledného majiteľa týchto digitálnych zariadení, keďže nie je úplne jasné komu patria.

2. **Odhalenie páchatel'a** – Cieľom bude zistenie kto je skutočným vinníkom tohto trestného činu. Na objavenie reálneho páchatel'a je potrebný reálny, vernostný a takzvané nepriestrelný dôkaz preukazujúci jeho vinu
3. **Motív trestného činu** – Vyšetrovanie sa bude sústrediť na možné motívy, ktoré mohli viesť k tomuto trestnému činu.

1.7 Postup vyšetrovania

1. Bezpečné zaistenie digitálnych zariadení z miesta činu
2. Vytvorenie kópii diskov zaobstaraných zariadení
3. Zanalyzovanie diskov a prípadná obnova zmazaných dát
4. Vyhľadávanie údajov spojených s trestným činom
5. Vytvorenie analytického dokumentu s obsahom objavených dát slúžiacich ako dôkaz
6. Súdny proces alebo uzavretie vyšetrovania

1.8 Literatúra

Key Steps in Forensic Phone Analysis

<https://www.salvationdata.com/knowledge/forensic-phone-analysis/>

Tento článok hovorí o postupoch forenznej analýzy na mobilných zariadeniach. Autor článku rozoberá komplexnosť analýzy na kľúčové postupy od samotného zabavenia zariadenie až po forenznú správu, ktorá sa prezentuje pri súdnom konaní. Taktiež spomína software ako je SPF Pro pretože je spoľahlivý a jednoduchý na používanie. K článku je aj pridaný odkaz na investigatívne nástroje, ktoré môžu pomôcť vyšetrovaniu. Odkaz: <https://www.salvationdata.com/work-tips/the-top-20-open-source-digital-forensic-tools-for-2024/>

Detailed Forensic Procedure for Laptop computers

<https://www.giac.org/paper/gsec/3024/detailed-forensic-procedure-laptop-computers/105045>

Odborný článok sa zaoberá problematikou analyzovania prenosných počítačových zariadení. Autor vysvetľuje dôležitosť správneho spracovania digitálnych dôkazov aby boli právne prijateľné. Autor taktiež vysvetľuje postupy forenznej analýzy a rôzne nástrahy na ktoré je potrebné dbať.

2 Zaist'ovanie a zber

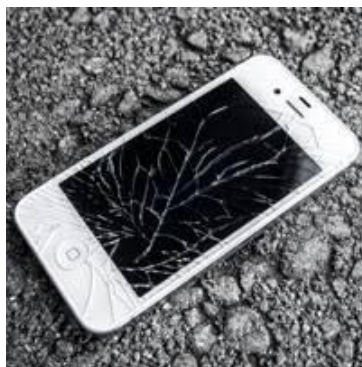
Vyšetrované zariadenia

- Smartfón
- Notebook

2.1 SMARTFÓN

Názov zariadenia	iPhone 4S
Vydanie	2011
Operačný systém	iOS 5 (aktualizovateľný na iOS 9.3.6)
Úložisko	64 GB
Displej	3.5 palca Retina
Rozlíšenie displeja	640 x 960 px
Procesor	Apple A5, Dual-core 1.0 GHz Cortex-A9
Pamäť RAM	512 MB
Fotoaparát	8 MP, autofokus, LED blesk
Predná kamera	VGA
Batéria	1432 mAh
Senzory	Akcelerometer, gyroskop, kompas, proximita, GPS
Rozmery	115.2 x 58.6 x 9.3 mm
Hmotnosť	140 g
Životnosť batérie	1432 mAh (až 8 hodín hovoru, 200 hodín v pohotovostnom režime)

Rýchlosť čítania/zápisu	(Nedostupné)
Prístupová doba	Rýchlosť prístupu k pamäti RAM (Nedostupné)
Čas nabíjania	Približne 2 hodiny na plné nabitie
Architektúra procesora	ARM Cortex-A9 (32-bit), dual-core
Poznámky	Zariadenie je v mierne poškodenom stave, hardvér zariadenia je plne funkčný, vonkajší obal, konkrétne displej zariadenia má stredne veľké praskliny



Obr. č. 1: Fotografia mobilného zariadenia

2.2 NOTEBOOK

Názov zariadenia	Acer Aspire (odhadovaný model z rokov 2000-2010)
Vydanie	Odhadované roky 2000-2010
Operačný systém	Windows Vista alebo Windows 7 (v závislosti od roku výroby)
Úložisko	160 GB až 320 GB HDD
Displej	15.4-palcový LCD

Rozlíšenie displeja	1280x800 px
Procesor	Intel Pentium Dual-Core
Pamäť RAM	4 GB DDR3 RAM
Grafická karta	Integrovaná grafická karta Intel GMA 4500MHD
Optická mechanika	DVD-RW mechanika
Pripojenie	Wi-Fi 802.11 b/g/n, Ethernet 10/100 Mbps, USB 2.0, VGA, audio porty
Batéria	6-článková lítium-iónová batéria (životnosť batérie sa líšila v závislosti od modelu a používania)
Hmotnosť	Približne 2.5 kg
Životnosť batérie	(Nedostupné, líši sa v závislosti od modelu a používania)
Rýchlosť čítania/zápisu	(Nedostupné)
Prístupová doba	Rýchlosť prístupu k pamäti RAM (Nedostupné)
Čas nabíjania	(Nedostupné)
Poznámky	Zariadenie je v ťažko poškodenom stave, pri skonfiškovaní nebolo možné presne určiť niektoré parametre zariadenia avšak je známe že nebude z neho možné analyzovať dáta.

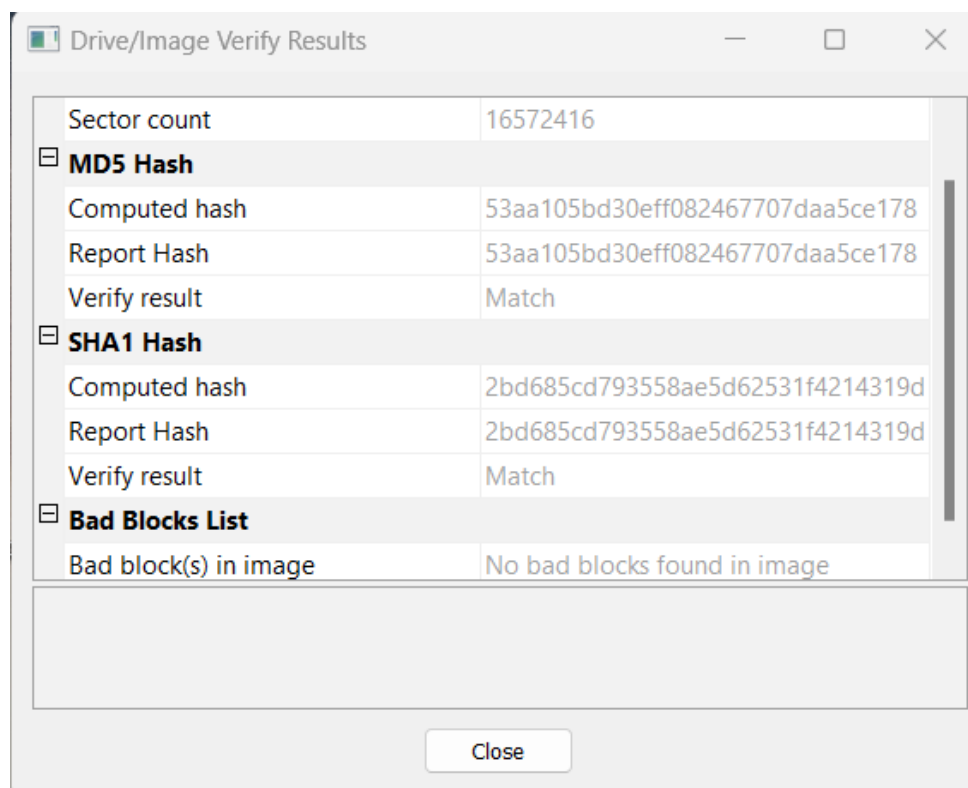


Obr. č. 2: Fotografia notebooku

2.3 Vytvorenie disk imagu

Drive/Image Verify Results	
Name	xxx.001
Sector count	16572416
MD5 Hash	
Computed hash	c72fce527de9f31d261006d77e5267f1
Report Hash	c72fce527de9f31d261006d77e5267f1
Verify result	Match
SHA1 Hash	
Computed hash	09116747272e71315f87ea55f8a6fec721fa0f69
Report Hash	09116747272e71315f87ea55f8a6fec721fa0f69
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image
Close	

Obr. č. 3: Disk image 1. kópia



Obr. č. 4: Disk image 2. kópia

3 Uchovanie

3.1 Vytvorenie kópií

Po zaistení smartfónu sme urobili 2 bitové kópie disku, ktoré boli uložené na náš pracovný disk pre tento konkrétny prípad. Aby sme zaistili konzistentnosť a pravdivosť dôkazov, tak bolo nutné vytvoriť aspoň 2 kópie v prípade poškodenia alebo zničenia tej prvej. Originálny disk je zapečatený vo vodotesnom a prachu-vzdornom boxe, ktorý je uložený v izolovanej miestnosti s dôkazmi kam má prístup len personál na ich vlastné služobné číslo. Táto miestnosť má prísny zákaz magnetických materiálov aby sa zabránilo akejkoľvek manipulácii s originálnymi dôkazmi.

3.2 Použité nástroje

Na vyšetrowanie digitálnych stôp súvisiacich s vraždou používame viacero nástrojov ako sú:

- FTK imager – Tento nástroj nám poslužil na vytvorenie kópií disku a taktiež na získanie RAM imagu, ktorý sme analyzovali
- HxD – S týmto nástrojom sme vykonávali analýzu a vyhľadávanie informácií v získanom RAM imagi
- Autopsy – Tento nástroj nám slúži na analýzu súborov získaných z disku, kde nám bude veľmi nápomocný v konečných krokoch vyšetrowania
- FotoForensics – online webový nástroj na skúmanie metadát obrázkov

3.3 Použité dáta

Dáta vyšetrowaného prípadu sú čerpané z internetu za pomoci stiahnutých datasetov. Datasetsy boli stiahnuté z: <https://cfreds.nist.gov/search/tag/>.

Odkazy na stiahnutie datasetov:

- <https://digitalcorpora.s3.amazonaws.com/corpora/files/govdocs1/zipfiles/902.zip> - veľkosť 285
- <https://digitalcorpora.s3.amazonaws.com/corpora/files/govdocs1/zipfiles/900.zip> - veľkosť 339 MB
- <https://sipi.usc.edu/database/aerials.zip> - veľkosť 81,8 MB
- <https://sipi.usc.edu/database/textures.zip> - veľkosť 28-3 MB
- https://web.archive.org/web/20160402084138if_/http://dfrws.org/2006/challenge/dfrws-2006-challenge.zip - veľkosť 40,6 MB
- https://s3.amazonaws.com/cftt.cfreds.nist.gov/cfreds/mobile/CHIPOFF/LG+K7/Mobile+Device+Data+Population_LGK7.docx – veľkosť 1,49 MB

- <https://web.archive.org/web/20160404195654if/http://dfrws.org/2007/challenge/dfrws-2007-challenge.zip> - veľkosť 299 MB
- Pre analýzu hypotézy č. 1 boli použité vlastné dáta – obrázky (11, 13)
- Pre analýzu hypotézy č. 3 boli použité vlastné dáta – obrázok (19)

Číslo:	02	Typ súboru:	001	Obnovený súbor:	Nie	Veľkosť:	8 GB
Popis prípadu:		Vražda študenta					
Názov súboru:		xxx.001					
Miesto získania digitálnej stopy:		Smartfón nájdený na mieste činu					
Poznámky:		Zo smartfónu boli extrahované potrebné informácie, na základe ktorých bude pokračovať vyšetrovanie					
Časové pečiatky							
Access:	10.03.2025 10:20:36		Modify:	10.03.2025 10:32:42		Change:	
Digitáln y odtlačok (heš)	MD5	c72fce527de9f31d261006d77e5267f1					
	SHA1	09116747272e71315f87ea55f8a6fec721fa0f69					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
10.03.2025 10:04:00		Zistenie MD5 hash – úspešne vykonané					
10.03.2025 10:04:00		Zistenie SHA1 hash – úspešne vykonané					

Obr. č. 5: CHOC č. 1

Číslo:	03	Typ súboru:	001	Obnovený súbor:	Nie	Veľkosť:	8 GB
Popis prípadu:		Vražda študenta					
Názov súboru:		Disk_image.001					
Miesto získania digitálnej stopy:		Smartfón nájdený na mieste činu					
Poznámky:		Zo smartfónu boli extrahované potrebné informácie, na základe ktorých bude pokračovať vyšetrovanie					
Časové pečiatky							
Access:	15.03.2025 13:49:18		Modify:	15.03.2025 14:01:09		Change:	
Digitáln y odtlačok (heš)	MD5	53aa105bd30eff082467707daa5ce178					
	SHA1	2bd685cd793558ae5d62531f4214319d					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
15.03.2025 13:49:18		Zistenie MD5 hash – úspešne vykonané					
15.03.2025 13:49:18		Zistenie SHA1 hash – úspešne vykonané					

Obr. č. 6: CHOC č. 2

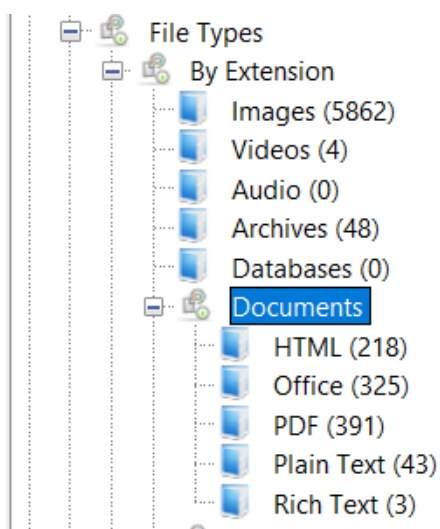
4 Vyt'azovanie

4.1 Kategórie a počet súborov

Súborový systém analyzovaného zariadenia – FAT32

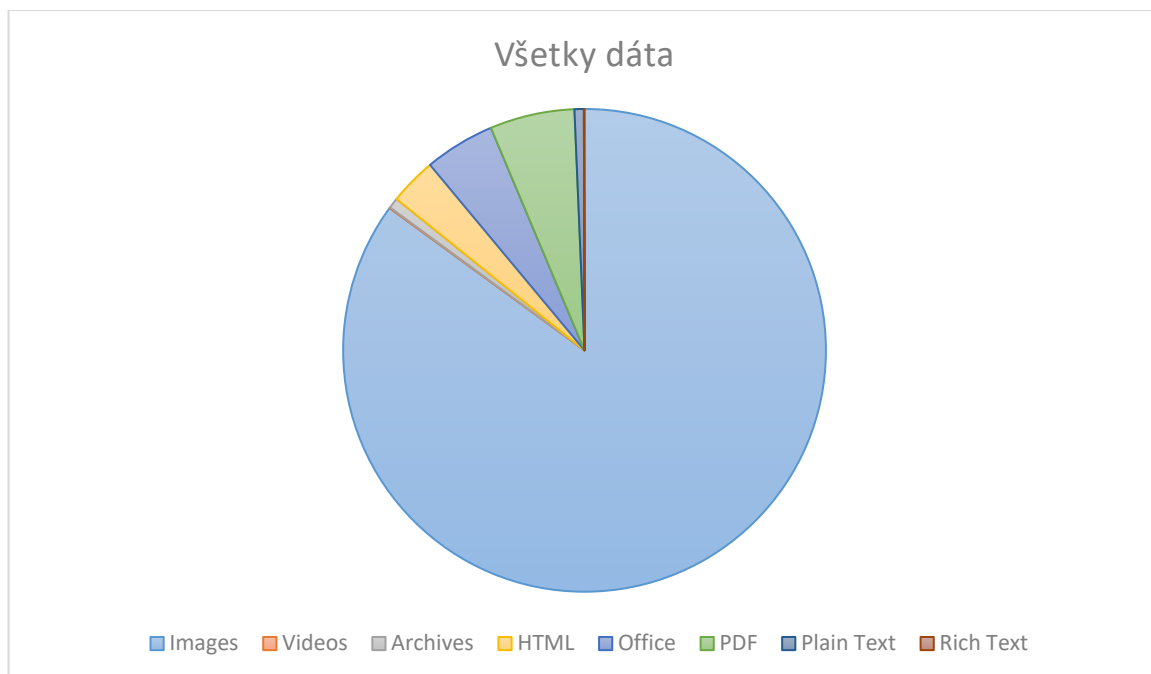
Na disku boli objavené tieto typy dát:

- Images: 5862
- Videos: 4
- Archives: 48
- HTML: 218
- Office: 325
- PDF: 391
- Plain Text: 43
- Rich Text: 3



Obr. č. 7: Obnovené súbory

Pri našej analýze sa budeme sústrediť na hľadanie súvisiacich obrázkov s prípadom, ktoré by nám mohli pomôcť vystaviť zoznam podozrivých osôb.



Obr. č. 8: Graf typov obnovených dát

5 Analýza

5.1 Analýza RAM pamäte

V RAM pamäti sme sa pokúšali nájsť bežné textové výrazy, ktoré by nám odhalili správy z daného dňa. Išlo o správy typu: „ahoj“, „stretneme sa“, „vecer“, „party“. Bohužiaľ neboli nájdené žiadne súvisiace výsledky z týchto hľadaných výrazov. Následne sme dali vyhľadávať meno kamaráta obeti s ktorým mala byť údajne v ten večer na párty „michal“.

```
07948F9C0 03 02 82 01 04 9E 20 01 2F 4A 61 3A 20 70 C4 82 ...,,ž ./Ja: pĀ,  
07948F9D0 C2 B4 6A 64 65 6D 65 20 6B 75 20 6D 6E 65 20 64 Ā'jdeme ku mne d  
07948F9E0 6F 20 62 79 74 75 20 70 6F 20 70 61 72 74 79 3F o bytu po party?  
07948F9F0 0D 0A 0D 0A 4D 69 63 68 61 6C 3A 20 41 6E 6F 20 ....Michal: Ano  
07948FA00 61 20 6F 20 6B 6F 6C 6B 65 6A 20 70 72 65 73 6E a o kolkej presn  
07948FA10 65 20 61 73 69 20 3F 0D 0A 0D 0A 4A 61 3A 20 6F e asi ?....Ja: o  
07948FA20 20 33 3A 30 30 20 63 63 61 0D 0A 0D 0A 4D 69 63 3:00 cca....Mic  
07948FA30 68 61 6C 3A 20 6F 6B 65 6A 20 64 6F 68 6F 64 6E hal: okej dohodn  
07948FA40 75 74 65 19 04 03 02 2C 04 9E 20 02 55 40 0A 60 ute....,,ž .U@.'
```

Obr. č. 9: RAM image č. 1

Vo výsledkoch sme našli konverzáciu obete so spomínaným kamarátom, kde konverzácia naznačuje že sa mali stretnúť na mieste činu v daný čas kedy bola obeť usmrtená. Ďalšie výsledky ukázali konverzáciu obete s neznámym pravdepodobne kamarátom, kde bolo spomenuté že hlavný podozrivý bol dlžný obeti 5000 Eur a deň vraždy mal byť posledný deň na splatenie dlhu.

```
003CAEFF0 68 63 D0 7F 80 02 00 00 68 63 D0 7F 80 02 00 00 hcD.€...hcD.€...  
003CAF000 4A 61 3A 20 4D 69 63 68 61 6C 6F 76 69 20 64 6E Ja: Michalovi dn  
003CAF010 65 73 20 64 61 76 61 6D 20 64 6E 65 73 20 70 6F es davam dnes po  
003CAF020 73 6C 65 64 6E 75 20 6D 6F 7A 6E 6F 73 74 20 6D slednu moznost m  
003CAF030 69 20 70 65 6E 69 61 7A 65 20 76 72 61 74 69 74 i peniaze vratit  
003CAF040 0D 0A 0D 0A 53 61 6D 6F 3A 20 41 20 6B 6F 6C 6B ....Samo: A kolk  
003CAF050 6F 20 74 69 20 64 6C 7A 69 0D 0A 0D 0A 4A 61 3A o ti dlzi....Ja:  
003CAF060 20 75 7A 20 35 30 30 30 20 65 75 72 0D 0A 0D 0A uz 5000 eur....  
003CAF070 53 61 6D 6F 3A 20 66 75 68 61 20 74 61 6B 20 68 Samo: fuha tak h  
003CAF080 61 64 61 6D 20 74 69 20 74 6F 20 76 72 61 74 69 adam ti to vrati  
003CAF090 0D 0A 0D 0A 00 00 00 00 00 00 00 00 00 00 00 00
```

Obr. č. 10: RAM image č. 2

Po týchto výsledkoch sme sa pokúsili hľadať ďalej súvisiace informácie ako výhražné správy a podobne, ale nenašli sme žiadne ďalšie výsledky, ktoré by boli prípadu nápomocné avšak na základe zistených informácií sa bude prihliadať na 1. hypotézu a hlavného podozrivého.

5.2 Hypotéza 1

„Hypotéza 1 - Obeť bola zabitá kamarátom, s ktorým údajne bola na párty. Na zariadeniach sa nenašli žiadne multimediálne súbory ani správy z toho večera, takže sa predpokladá že mohli byť vymazané. Motivácia vraždy je neznáma.“

Ako prvé sme skúmali obraz RAM pre akékoľvek súvisiace informácie, na základe čoho sa nám podarilo nájsť konverzáciu, ktorá by mala potvrdzovať účasť obete s kamarátom na party. Aby sme vedeli túto časť hypotézy potvrdiť, skúmali sme kamerové záznamy, kde bol nájdený kamerový záznam obete s kamarátom, pár hodín pred smrťou obete.



Obr. č. 11: Kamerový záznam z párty

Property	Value
Filename	Cam1.png
Filetime	2025-02-20 23:42:40
File Type	image/png
Dimensions	1478x991
Color Channels	4
Unique Colors	415046
File Size	2,113,192 bytes
MD5	fccb6160019d754a8924d3e0070472f3
SHA1	7d91a73b08e296f839ebf145a3772647304761db
SHA256	945c93b45e7015cb2ad64ea72766dab35a9531a9ce264fd471745762f4096d78
First Analyzed	2025-04-12 14:57:53 GMT

Obr. č. 12: Metadáta kamerového záznamu z party

Ďalším krokom bolo sústrediť vyšetrovanie na kamerové záznamy pred bytom obete aby sme potvrdili prítomnosť podozrivého v čase vraždy na tomto mieste, kde sa nám podarilo potvrdiť túto časť hypotézy.



Obr. č. 13: Kamerový záznam pred bytom

Property	Value
Filename	10cb0ac7433d487ab52e52a74798241b.jpg
Filetime	2025-02-21 2:58:32
File Type	image/jpeg
Dimensions	1024x1024
Color Channels	3
Unique Colors	47702
File Size	59,501 bytes
MD5	fc32a8bfe9311d56bbf59b3b9bcd4e4
SHA1	69dd646985f3e6827332cb195838d1cca77a278e
SHA256	5cdd8eccb9af2f67fc6daebc3d2fb2ff8e3faf9656f42b669b867b3a481a5f81
First Analyzed	2025-04-12 15:19:54 GMT

Obr. č. 14: Metadáta kamerového záznamu z ulice pred bytom

Na základe všetkých získaných dôkazov môžeme s určitosťou potvrdiť hypotézu 1, kde sa ako motivácia odhaduje peňažný dlh.

5.3 Hypotéza 2

„Hypotéza 2 - Obeť mohla byť zapojená do nelegálnej činnosti. Pri takejto hypotéze sa vysvetľujú pravdepodobne vymazané fotografie a chaty z dôvodu bezpečnosti“

Pri tejto hypotéze sme analyzovali podozrivé textové súbory, ktoré boli obnovené. V prvom súbore „900123.txt“ sme našli zvláštne číselné kódy, ktoré na prvý pohľad boli podozrivé, ale pri analýze sa ukázali ako neškodné meteorologické logy vďaka nadpisom každého stĺpca, čo sme potvrdili na základe nadpisov jednotlivých stĺpcov a štandardizovanej štruktúry údajov.

The screenshot shows a file explorer interface with a list of files and a detailed view of file 900123.txt. The file list includes columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), and Flags(Meta). The file 900123.txt is highlighted. Below the file list, the 'Strings' tab is selected, showing the extracted text of the file. The text contains various alphanumeric codes and timestamps, including 'FOUS90 KWNO 201200', 'OUTPUT FROM NGM 12Z JUL 20 04', and several lines of data with timestamps and coordinates.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
900120.txt				2006-08-23 02:12:40 SELC	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	483701	Allocated	Allocated
900123.txt				2004-07-20 16:00:46 SELČ	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2011	Allocated	Allocated
900319.txt				2004-12-17 23:03:31 SEČ	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	332	Allocated	Allocated
900339.txt				2002-09-09 14:17:59 SELČ	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	348	Allocated	Allocated

FOUS90 KWNO 201200
OUTPUT FROM NGM 12Z JUL 20 04
TTPTR1R2R3 VVVL PSDDFF HHT1T3T5 TTPTR1R2R3 VVVL PSDDFF HHT1T3T5
BRW//863130 -1006 092108 51111003 BTI//958552 -0801 111508 54100902
06000944841 -1210 113112 47030602 06000688147 00601 092105 54131002
12000755344 -0810 143014 44030101 12000497243 00400 080304 56171102
18000735641 -0611 163011 42010000 18000637047 -0301 100110 54141002
24000856249 -1412 182909 41000000 24000987652 00301 163514 49040801
30000826366 -0913 202704 41000000 30000947450 -1102 183207 47030600
36000576165 -1113 213005 45040200 36000726546 -0603 203605 48070400
42000495873 -1711 201102 47060501 42000735449 -0905 210702 48060500
48000455782 -0910 201611 49080702 48000815253 -0607 221904 48050500

BTT//727953 -0601 093003 56130801 FAI//597143 -1001 083506 58161002
06000647446 00301 093202 55140801 06000587244 -0800 080103 58171002
12000476549 00300 083006 57181001 12008487254 00498 073406 61201203
18000456149 -0300 083609 57181000 18009517561 -0798 070110 61191203
24000505549 -0900 100209 55161000 24000537871 00398 093304 60181202

Obr. č. 15: Textový súbor 900123.txt

Ďalším podozrivým súborom bol 900120.txt, v ktorom analýza odhalila oceánografické údaje, nijak nesúvisiace s našou hypotézou ani vyšetrovaním

Listing

Plain Text

43 Results

Table

Thumbnail

Summary

Page: 1 of 1

Pages: < >

Go to Page:

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
900120.txt				2006-08-23 02:12:40 SELČ	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	483701	Allocated	Allocated
900123.txt				2004-07-20 16:00:46 SELČ	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2011	Allocated	Allocated
900319.txt				2004-12-17 23:03:31 SELČ	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	332	Allocated	Allocated
900339.txt				2002-09-09 14:17:59 SELČ	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	348	Allocated	Allocated

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Strings

Extracted Text

Translation

Page: 1 of 16 Page

Matches on page: - of - Match

100%

Reset

Text Source: File Text

Group/Ship,Cruise_ID,JD_GMT,Date_MM/DD/YY,Date_DDMMYYYY,Time,Latitude,Longitude,xCO2eq_ppm,xCO2atm_ppm,xCO2air_ave_ppm,Press_equ_mbar,Teq_°C,SST_°C,Salinity,H2O_flow_l/min,IR_gas_flow_ml/min,Temp_IR_°C,fCO2sw_uatm,fCO2atm_uatm,dfCO2_uatm,QC Flag,Subflag
PMEL/Waikato,cw2005_04,110.1367245,04/19/05,19042005,3:16:53,-36.4272,175.0088,376.5589971,1022.8,20.69,20.3449,35.4518,1.2,91.7,34.61,,,2,
PMEL/Waikato,cw2005_04,110.1375,04/19/05,19042005,3:18:00,-36.4213,175.0068,376.7584374,1022.8,20.67,20.28,35.4524,1.2,71.8,34.68,,,2,
PMEL/Waikato,cw2005_04,110.138287,04/19/05,19042005,3:19:08,-36.4156,175.0043,376.6594222,1022.8,20.87,20.241,35.4503,1.2,74.4,34.76,,,2,
PMEL/Waikato,cw2005_04,110.1390741,04/19/05,19042005,3:20:16,-36.4098,175.0016,376.46091,1022.8,20.92,20.2383,35.4502,1.2,79.4,34.83,,,2,
PMEL/Waikato,cw2005_04,110.1398843,04/19/05,19042005,3:21:26,-36.4038,174.9991,376.5608873,1022.8,20.9,20.2088,35.4498,1.2,85.2,34.9,,,2,
PMEL/Waikato,cw2005_04,110.1406829,04/19/05,19042005,3:22:35,-36.3978,174.9967,376.461868,1022.8,20.9,20.1449,35.4477,1.2,70.5,34.96,,,2,
PMEL/Waikato,cw2005_04,110.1414699,04/19/05,19042005,3:23:43,-36.3918,174.9945,376.561836,1022.8,20.87,20.1362,35.4463,1.2,87.3,35.02,,,2,
PMEL/Waikato,cw2005_04,110.1422569,04/19/05,19042005,3:24:51,-36.3857,174.9924,376.5623069,1022.8,20.85,20.0619,35.448,1.2,87.5,35.09,,,2,
PMEL/Waikato,cw2005_04,110.1430671,04/19/05,19042005,3:26:01,-36.3795,174.9899,376.463288,1022.8,20.83,20.0168,35.4484,1.2,82.6,35.14,,,2,
PMEL/Waikato,cw2005_04,110.1438426,04/19/05,19042005,3:27:08,-36.3734,174.9875,376.5632557,1022.8,20.79,20.0486,35.4452,1.2,80.8,35.2,,,2,
PMEL/Waikato,cw2005_04,110.1477083,04/19/05,19042005,3:32:42,-36.344,174.9759,391.891114,376.5611209,1022.8,20.66,19.8812,35.4431,1.2,55.6,35.45,373.2959427,370.3816
424.2,914300313,2,
PMEL/Waikato,cw2005_04,110.1485069,04/19/05,19042005,3:33:51,-36.338,174.9734,390.3991518,376.5405113,1022.8,20.62,19.8372,35.437,1.2,51.35,371.8315841,370.383604
2,1.447979876,2,
PMEL/Waikato,cw2005_04,110.1493056,04/19/05,19042005,3:35:00,-36.3319,174.9709,388.4095184,376.5199017,1022.8,20.59,19.7917,35.4325,1.2,55.4,35.54,369.7190568,370.38
62716,-0.667214743,2,

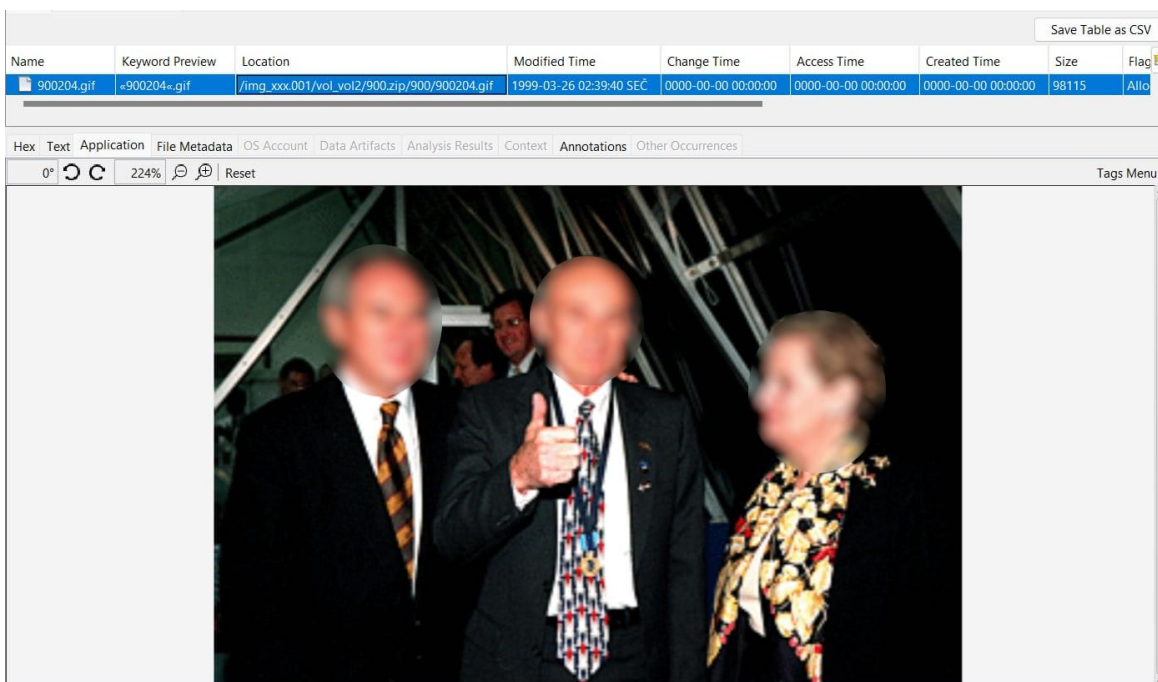
Obr. č. 16: Textový súbor 900120.txt

Na základe analyzovaných údajov súvisiacich s prípadom a nedostatkom dôkazov nevieme hypotézu ani potvrdiť, ani vyvrátiť.

5.4 Hypotéza 3

„Hypotéza 3 - Zariadenia nepatria obeti a mohli byť boli odcudzené čo by viedlo k motivácii útoku od pôvodného vlastníka“

Pre overenie hypotézy či zariadenie patrí obeti sme sa zamerali na obnovené fotografie v zariadení, kde boli nájdené fotografie rodiny aj samotnej obete za mlada.



Obr. č. 17: Fotografia rodiny obete (dataset 900.zip)



Obr. č. 18: Fotografia obete (dataset 900.zip)

Aby sme s istotou potvrdili vlastníka mobilu na zariadení bolo vyhľadané IMEI(International Mobile Equipment Identity) číslo na zariadení, s ktorým bolo pomocou operátora daného telefónu možné určiť že naozaj vlastníkom bola obeť.

General About	
Model	993-14379LL/A
Serial Number	X0XX0XXXX0X
Wi-Fi Address	XX:XX:0X:XX:X0
Bluetooth	XX:XX:0X:XX:XX
IMEI	01 234567 890123 4
ICCID	0123456789012345678
MEID	01 234567 890123
Modem Firmware	-
SEID	>
Legal	>

Obr. č. 19: Vyhľadané IMEI číslo

Pomocou získaných dôkazov vieme vyvrátiť hypotézu číslo 3, ktorá tvrdí že zariadenia nepatrili obeti.

Záver

Vyšetrením sme dokázali potvrdiť vinníka z vraždy študenta, a to kamaráta Michala, ktorým bola obeť na párty. Na potvrdenie tohto záveru nám pomohli chatové komunikácie medzi kamarátmi, kamerové záznamy potvrdzujúce časové zhody obvineného na mieste činu. Taktiež bol zistený motív vraždy z RAM imagu, kde motívom bol vysoký dlh peňazí

Hypotézy	Potvrdená	Vyvrátená	Nepotvrdená
Hypotéza 1	X		
Hypotéza 2			X
Hypotéza 3		X	