

Univerzita svätého Cyrila a Metóda

Fakulta prírodných vied

Trnavský sériový vrah

Link k prezentácii:

<https://bcstudent.fpvucm.sk/~caliksimon/dfa/prezentacia.pdf>

<https://bcstudent.fpvucm.sk/~caliksimon/dfa/prezentacia.pptx>

Šimon Čalik

2. ročník

2024/2025

Trnavský sériový vrah

Trnavský sériový vrah, má na svedomí 10 obetí, ktorým odrezal hlavu, ktorú ako jedínú našla polícia. Doposiaľ o vrahovi nie sú žiadne známe informácie, avšak pri novej nájdennej hlave sa v jej ústach našiel USB-kľúč, ktorý sa zaistil a odovzdal digitálnym forenzným analytikom.

Na danom USB-kľúči by sa mohli nachádzať informácie o obetiach, vrahovi, svedkoch, motívoch vedúce k dolapeniu páchatel'a alebo jeho identifikácii.

5WH:

„Kto?“ – Žiadne známe osoby súvisiace s prípadom. Žiadny svedkovia.

„Kde?“ – Obete boli nájdené vždy na verejných miestach bez kamier.

- USB sa nachádza v ústach poslednej nájdennej hlavy.

„Kedy?“ – Obete boli nájdené v skorých ranných hodinách medzi 4:00 až 8:00

„Čo?“ – Odrezané ľudské hlavy ľudí, nájdené USB v poslednej z hláv.

„Prečo?“ – Motivácie páchatel'a nie sú známe. Z vytvoreného profilu páchatel'a sa dá diskutovať o tom že ide o páchatel'a s ťažkou narušenou sadistickou myslou a nájdené USB môže naznačovať že túži po pozornosti.

„Ako?“ – Obetiam boli odrezané hlavy v miestne krčných stavcov C4 až C5, následne boli odnesené na verejné miesto bez žiadnych ďalších stôp, až pri poslednej obeti sa našiel USB-kľúč.

Cieľ vyšetovania:

1. Chytiť vraha
2. Zistiť totožnosť vraha
3. Zaistiť digitálne stopy spojené s prípadom
4. Analyzovať digitálne stopy
5. Identifikovať osoby súvisiace s prípadom

Hypotézy:

Hypotéza 1:

Vlastníkom USB-kľúča je vrah.

Z dát na USB zariadení (z fotografií, na ktorých sú obeť, vrah, ...)

Analýza fotografií

Hypotéza 2:

Vlastníkom USB-kľúča je niekto iný ako vrah.

Opak hypotézy 1

Hypotéza 3:

Na kľúči sa nachádzajú digitálne stopy vedúce k dolapeniu páchatel'a.

Analýza všetkých dát + vymazané dáta, ...

Hypotéza 4:

Na kľúči sa nachádzajú informácie o obetiach.

Prehľadávanie dát a fotografií súvisiace nejak s obetami

Hypotéza 5:

USB kľúč slúži na odpútanie pozornosti.

Pozmenené dáta (metadata)

Všetky hypotézy sa budú potvrdzovať / vyvracať pomocou analýzy dát USB zariadenia, či sa dané údaje nachádzajú, respektíve nenachádzajú na zariadení.

Softvérové nástroje využité počas prípadu:

Exterro FTK imager

Autopsy 4.21.0

HxD

Zariadenie:	
Kľúčové parametre produktu	
Typ	USB
Model zariadenia	SanDisk 3.2Gen1
Farba	čierna
Rozhranie	USB 3.0
Výška	4 mm
Konektivita	
Podporované operačné systémy Windows	Áno
Podporované operačné systémy Mac	Áno
Dátové úložisko	
Kapacita	32 GB
Rýchlosť čítania	150 MB/s
Ďalšie vlastnosti	
Spracovanie	Štandardný
Značka	SanDisk
Cylindre	3740
Stopy na cylinder	255
Sektory na stopy	63
Bajty na sektor	512
Počet sektorov	60 088 320
Sériové číslo	04018f34f43c4e04e244
Vymeniteľný disk	Áno



Obrázok 1 - USB - Dôkaz č.: 01

Hľadané súbory: png, jpeg, mov

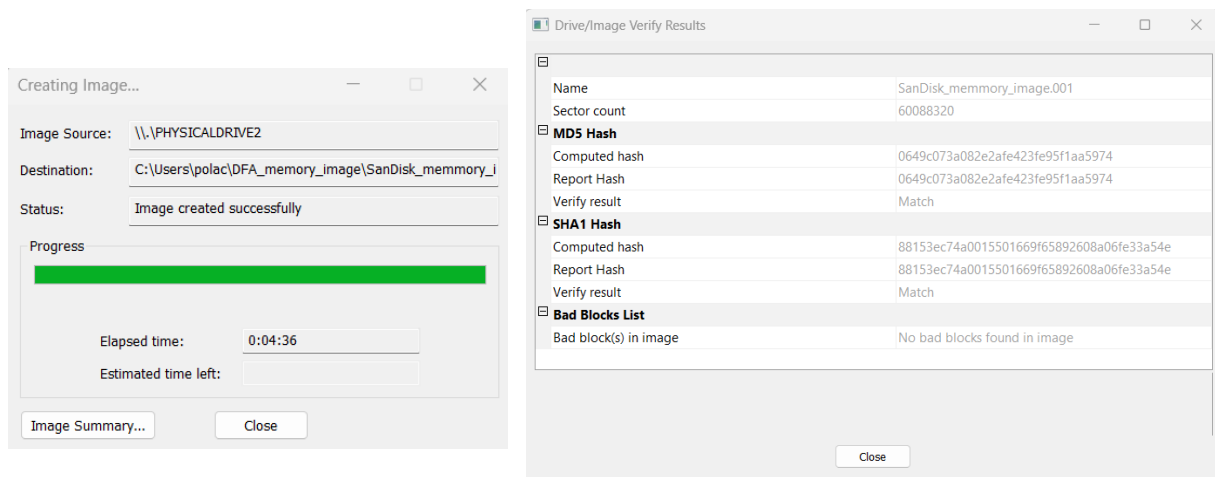
Dáta:

- (Dáta z voľne dostupných datasetov zo stránky <https://cfreds.nist.gov>)
- Manipulated Image Dataset => autor = Jiwon Lee / Dongguk University, veľkosť = 2,3 GB
- dfrws-2007-challenge.img => veľkosť = 330 MB
- bridge-far_qcif.yuv => veľkosť = 76,1 MB
- Manipulated-Image-Dataset-master => veľkosť = 2,49 GB
- 4cam_splc => veľkosť = 315 MB
- 4cam_auth => veľkosť = 479 MB

- o dáta telefónu sú zo stránky <https://cfreds.nist.gov>
- o Veľkosť = 61 925 376 B

Bezpečnostné opatrenia: Zariadenie bolo bezpečne prevezené do laboratória polície príslušným orgánom.

- Vytvorili sa 3 obrazy USB zariadenia pomocou softvéru FTK imager, pre prípad, že by sa niečo stalo s jednou kópiou, tak aby sa nemuselo manipulovať s originálnym zariadením.
- Originálne zariadenie nájdené na mieste činu, digitálni forenzní analytici zaistili, zariadenie umiestnili do hermeticky nepriepustného trezora v odolnom puzdre proti nárazom, prachu, vode a elektromagnetickému signálu, zapečatený plombou aby sa zabránilo manipulovaniu so zariadením počas vyšetrovania.



Informácie o vykonaní obrazu USB zariadenia z Exterro FTK imageru:

Created By Exterro® FTK® Imager 4.7.3.81

Case Information:

Acquired using: ADI4.7.3.81

Case Number: 01

Evidence Number: 01

Unique description: USB sanDisk

Examiner: Simon Calik

Notes: Disk image

Information for C:\Users\polac\DFA_memory_image\SanDisk_memmory_image:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 3 740

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 60 088 320

[Physical Drive Information]

Drive Model: USB SanDisk 3.2Gen1 USB Device

Drive Serial Number: 04018f34f43c4e04e244

Drive Interface Type: USB

Removable drive: True

Source data size: 29340 MB

Sector count: 60088320

[Computed Hashes]

MD5 checksum: 0649c073a082e2afe423fe95f1aa5974

SHA1 checksum: 88153ec74a0015501669f65892608a06fe33a54e

Image Information:

Acquisition started: Wed Mar 5 08:48:05 2025

Acquisition finished: Wed Mar 5 08:52:41 2025

Segment list:

C:\Users\polac\DFA_memory_image\SanDisk_memory_image.001

COMPUTED HASH : 0649c073a082e2afe423fe95f1aa5974

COMPUTED HASH : 88153ec74a0015501669f65892608a06fe33a54e

Image Verification Results:

Verification started: Wed Mar 5 08:52:41 2025

Verification finished: Wed Mar 5 08:53:51 2025

MD5 checksum: 0649c073a082e2afe423fe95f1aa5974 : verified

SHA1 checksum: 88153ec74a0015501669f65892608a06fe33a54e : verified

Chain of custody:

Číslo:	01	Typ súboru:	Jpeg png mov	Obnovený súbor:	Nie	Veľkosť:	29340 MB
opis prípadu:		Trnavský sériový vrah					
Názov súboru:		SanDisk_memmory_image.001					
Miesto získania digitálnej stopy:		Krajské riaditeľstvo Policajného zboru v Trnave					
Poznámky:		Digitálna kópia USB, nájdeného v hlave obeti Trnavského sériového vraha. Created By Exterro® FTK® Imager 4.7.3.81					
Časové pečiatky							
Access:	05.03.2025 08:53:51		Modify:	08:53:51		Change:	08:53:51
Digitálny odtlačok (heš)	MD5	0649c073a082e2afe423fe95f1aa5974					
	SHA1	88153ec74a0015501669f65892608a06fe33a54e					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
05.03.2025 08:48:05		Vytváranie obrazu USB zariadenia pomocou FTK imager					
05.03.2025 08:52:41		Verifikácia hešov MD5 a SHA1					

V ranných hodinách 15.3.2025 sa opäť našla ďalšia odrezaná hlava na verejnom priestranstve cukrovaru Trnava. Polícia okrem hlavy našla aj zapnuté telefónne zariadenie, ktoré okamžite polícia zaistila do hermeticky nepriepustného igelitu a previezla do laboratória. Následne digitálny forenzný analytici vykonali memory capture = vytvorili digitálnu kópiu operačnej pamäti, pretože sa na nej nachádzajú volatilné dáta ktoré by sa mohli stratiť a môžu na nej byť dôležité dáta.

Na zaistenie dát z operačnej pamäti sa využil program Exterro FTK imager.

Bezpečnostné opatrenie:

Zo zariadenia sa vykonala memory capture operačnej pamäte a 2 bitové kópie sekundárnej pamäte

Zariadenie sa uzavrelo do trezora v puzdre proti nárazom, prachu, vode a elektromagnetickému signálu zapečatený plombou proti manipulácii so zariadením.

Zariadenie:

Výrobca	Samsung
Model	Galaxy A71
Operačný systém	Android
Rozlíšenie displeja	1080x2400 (FHD+)
Veľkosť RAM	6GB
Interná pamäť	128 GB
MicroSD	Do 512 GB
Frekvencia procesora	2.2 GHz
Počet jadier	8
Typ displeja	Super AMOLED Plus
Rozmery:	
Displej	169,5 mm
Výška	163,6 mm
Šírka	76 mm
Hrúbka	7,7 mm
Hmotnosť	179 g
Zadný fotoaparát	64 Mpx + 12 Mpx + 5 Mpx + 5 Mpx
Predný fotoaparát	32 Mpx
Rozlíšenie nahrávania videa	UHD 4K (3840 x 2160) @ 30fps
Počet SIM kariet	Dual-SIM
USB Interface	USB-C
Verzia USB	USB 2.0
Konektor na slúchadlá	3,5 mm stereo
NFC	Áno
Kapacita batérie	4500

Fotografia Zariadenia:



Chain of custody:

Číslo:	01	Typ súboru:	txt	Obnovený súbor:	Nie	Veľkosť:	18 000 MB
Popis prípadu:		Trnavský sériový vrah					
Názov súboru:		Samsung Galaxy A71					
Miesto získania digitálnej stopy:		Krajské riaditeľstvo Policajného zboru v Trnave					
Poznámky:		Digitálna kópia operačnej pamäte a sekundárnej pamäte zariadenia Samsung A71, nájdeného v pri obeti Trnavského sériového vraha. pomocou Exterro® FTK® Imager 4.7.3.81					
Časové pečiatky							
Access:	15.03.2025 14:57:32		Modify:	15:06:16		Change:	15:06:16
Digitálny odtlačok (heš)	MD5	ed2a458e9551d17ac580a33cb25701e6					
	SHA1	fa3aec5de3b2c9136a83d0ad7513ec2ac3780d30					
Časová pečiatka							
15.03.2025 14:57:32		Vytváranie zachytenia operačnej pamäti zariadenia pomocou FTK imager					
15.03.2025 15:06:16		Verifikácia hešov MD5 a SHA1					
31.03.2025 10:33:25		Vytvorenie bitovej kópie sekundárnej pamäte pomocou FTK imageru					
31.03.2025 10:33:26		Verifikácia hešov MD5 a SHA1					

Vytvorenie memdump:

Created By Exterro® FTK® Imager 4.7.3.81

Case Information:

Case Number:

Evidence Number:

Unique Description:

Examiner:

Notes:

Information for C:\Users\polac\DFA_memory_image\memcapture.ad1:

[Computed Hashes]

MD5 checksum: d5b0f8cbcfab749d7c870ec7f22343da

SHA1 checksum: b2ee5949989e5397e2583b50e086dd39d46e3e5d

Image information:

Acquisition started: Sat Mar 15 14:57:32 2025

Acquisition finished: Sat Mar 15 15:06:16 2025

Segment list:

C:\Users\polac\DFA_memory_image\memcapture.ad1

C:\Users\polac\DFA_memory_image\memcapture.ad2

C:\Users\polac\DFA_memory_image\memcapture.ad3

Vytvorenie bitovej kópie sekundárnej pamäte:

Created By Exterro® FTK® Imager 4.7.3.81

Case Information:

Acquired using: ADI4.7.3.81

Case Number: 02

Evidence Number:

Unique Description:

Examiner: Šimon Čálik

Notes:

Information for C:\Users\polac\DFA_mobile_image_FTK_imager\mobile_image:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Logical

[Drive Geometry]

Bytes per Sector: 512

Sector Count: 120 948

[Image]

Image Type: Raw (dd)

Source data size: 59 MB

Sector count: 120948

[Computed Hashes]

MD5 checksum: ed2a458e9551d17ac580a33cb25701e6

SHA1 checksum: fa3aec5de3b2c9136a83d0ad7513ec2ac3780d30

Image Information:

Acquisition started: Mon Mar 31 10:33:25 2025

Acquisition finished: Mon Mar 31 10:33:25 2025

Segment list:

C:\Users\polac\DFA_mobile_image_FTK_imager\mobile_image.001

COMPUTED HASH : ed2a458e9551d17ac580a33cb25701e6

COMPUTED HASH : fa3aec5de3b2c9136a83d0ad7513ec2ac3780d30

Image Verification Results:

Verification started: Mon Mar 31 10:33:25 2025

Verification finished: Mon Mar 31 10:33:26 2025

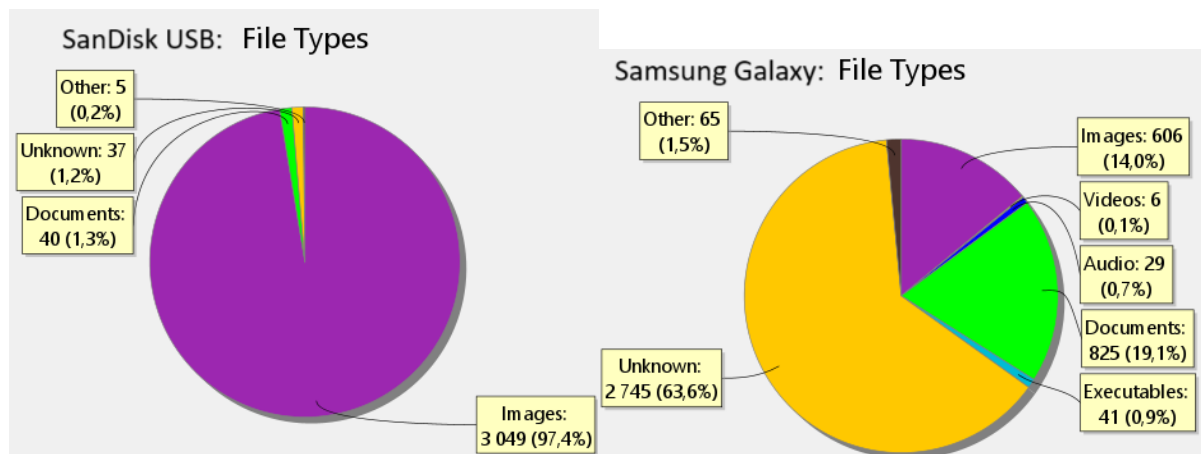
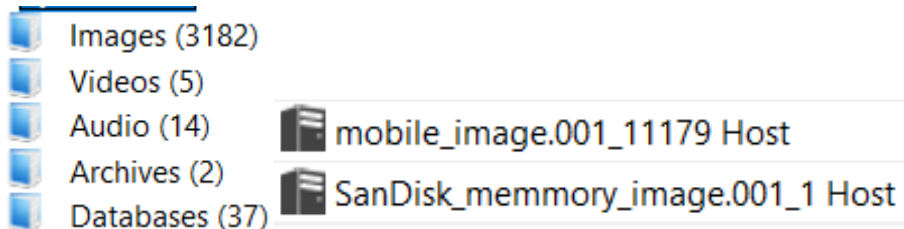
MD5 checksum: ed2a458e9551d17ac580a33cb25701e6 : verified

SHA1 checksum: fa3aec5de3b2c9136a83d0ad7513ec2ac3780d30 : verified

Skúmané dáta:

Všetky dáta z USB zariadenia a sekundárnej pamäte mobilného zariadenia som uložil na môj pracovný notebook, aby som vedel prehľadávať všetky dáta naraz pomocou nástroja autopsy.

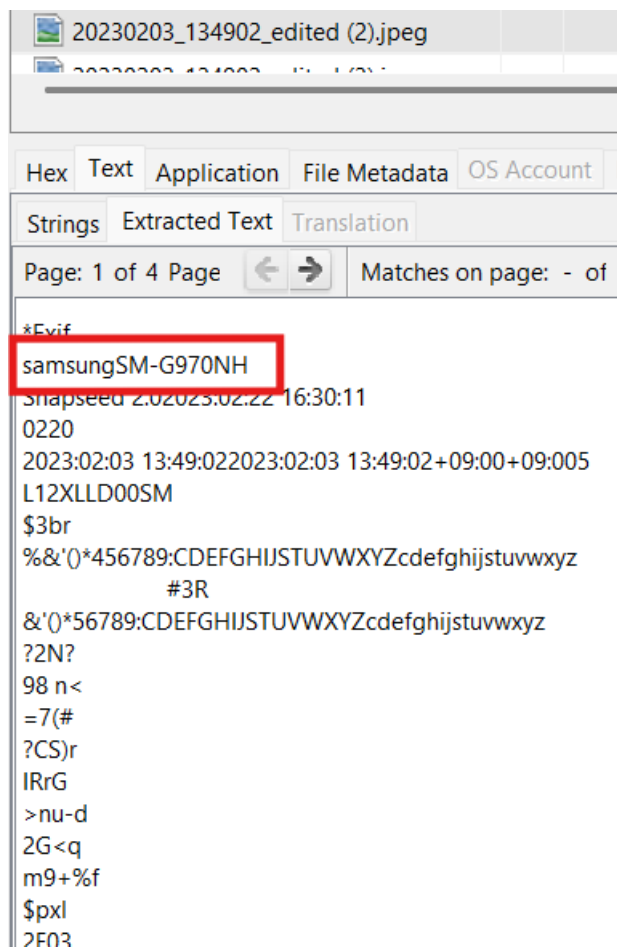
Zistilo sa že na najviac dát je obrázkov formátu png, jpeg a tiff.



Prehľadované dáta:

.jpg, .jpeg, .png, .psd, .nef, .tiff, .bmp, .tec, .tif, .webp
.aaf, .3gp, .asf, .avi, .m1v, .m2v, .m4v, .mp4, .mov, .mpeg, .mpg, .mpe, .mp4, .rm, .wmv, .mpv, .flv, .swf
.aiff, .aif, .flac, .wav, .m4a, .ape, .wma, .mp2, .mp1, .mp3, .aac, .mp4, .m4p, .m1a, .m2a, .m4r, .mpa, .m3u, .mid, .midi, .ogg
.zip, .rar, .7zip, .7z, .arj, .tar, .gzip, .bzip, .bzip2, .cab, .jar, .cpio, .ar, .gz, .tgz, .bz2
.db, .db3, .sqlite, .sqlite3
'htm', '.html', '.doc', '.docx', '.odt', '.xls', '.xlsx', '.ppt', '.pptx', '.pdf', '.txt', '.rtf'
'exe', '.msi', '.cmd', '.com', '.bat', '.reg', '.scr', '.dll', '.ini'

Z exif dát fotografií sa zistilo že fotografie z USB boli vytvorené pomocou nájdeného Samsung mobilného zariadenia.

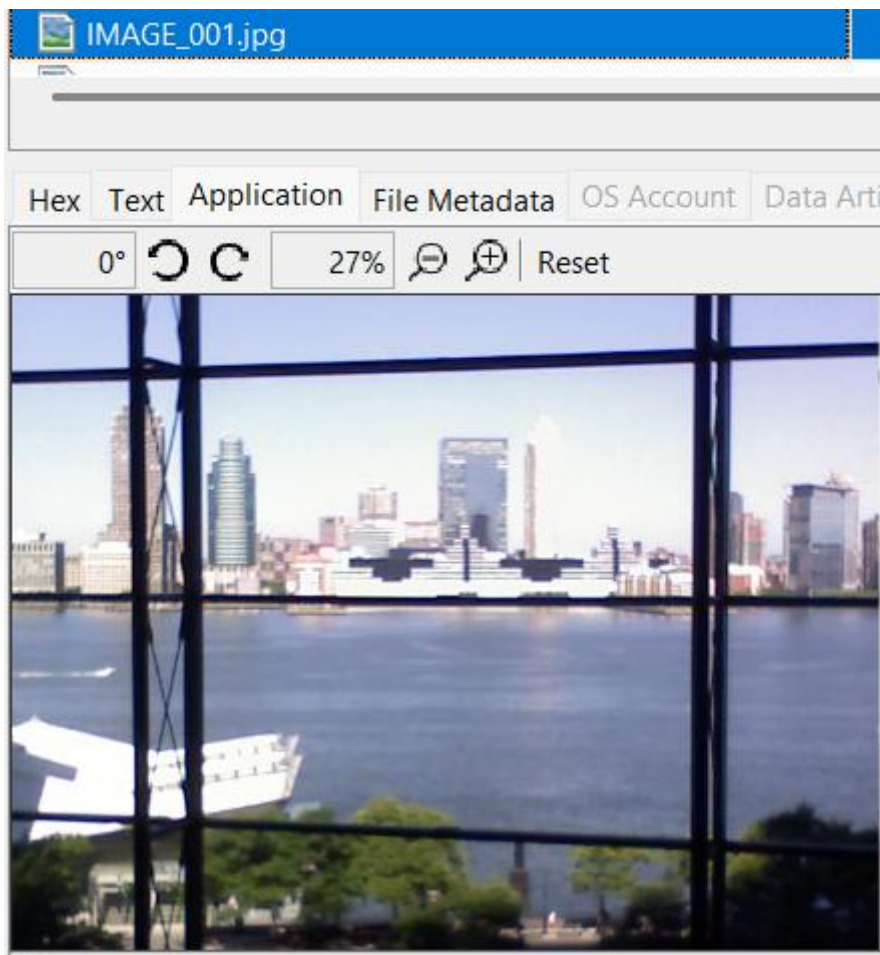


Hypotéza 1 – Vlastníkom USB je vrah - Potvrdená

Z týchto fotografií zozbieraných z USB a mobilného zariadenia vyplýva, že vlastníkom USB zariadenia je naozaj vrah. Ide o fotografie zo súkromného života normálneho človeka ale sú tam medzi nimi fotografie bydlísk obetí, odfotohrované pred ich vraždou, ktoré zavraždil Trnavský sériový vrah.

A exif dáta fotografií uviedli že fotky boli robené telefónom ktorý sa tiež našiel pri obeti, čo prispieva k tejto hypotéze

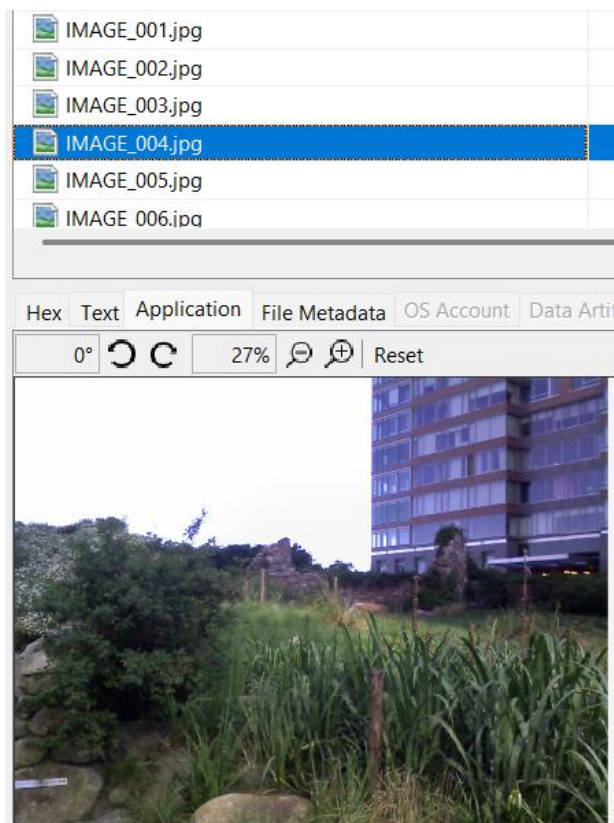
Osobná fotografia z dovolenky:



Z času vytvorenia, je zrejme že fotografia je vierohodná a nijak nezmenená, z času vytvorenia fotografie vyplýva že vrah mal USB v osobnom vlastníctve už dlhú dobu.

Modified Time	Change Time	Access Time	Created Time
2009-07-19 10:51:52 SELČ	0000-00-00 00:00:00	2009-07-19 01:00:00 SELČ	2009-07-19 10:51:52 SELČ

Na ďalšej fotografii je odфотографovaný dom z jednej z obetí sériového vraha v čase pred jej vraždou, čo je priamym dôkazom že vrah mal naplánovanú vraždu tejto osoby a vopred ju sledoval. Podobných fotografií je viac



Na ďalšej fotografii je vidieť jednu z obetí, ide o muža odфотографovaného tesne pred jeho vraždou. Z tohto usudzujem so 100 % istotou že vlastníkom USB kľúča je vrah.



Ďalšie fotografie zavraždených osôb z USB

Analysis ResultsContextAnnotationsOther Occurrences

Analysis ResultsContextAnnotationsOther Occurrences




Modified Time	Change Time	Access Time	Created Time
2009-07-22 17:29:18 SELČ	0000-00-00 00:00:00	2009-07-22 01:00:00 SELČ	2009-07-22 17:29:18 SELČ

Čas vytvorenia každej fotografie je len pár hodín pred ich zavraždením.

Ďalej forenzný psychiater z fotografií z USB podobným rorschachovým obrázkom, usúdil že ide o osobu s vraždňými, deviantnými myšlienkami a že ide o osobu s poruchou osobnosti.

	0	2006-11-03 20:40:12 SEČ	0000-00-00 00:00:00	2025-03-05 01:00:00 SEČ	20
	0	2005-12-23 07:06:38 SEČ	0000-00-00 00:00:00	2025-03-05 01:00:00 SEČ	20
	0	2006-11-03 20:40:20 SEČ	0000-00-00 00:00:00	2025-03-05 01:00:00 SEČ	20
	0	2005-12-23 07:08:08 SEČ	0000-00-00 00:00:00	2025-03-05 01:00:00 SEČ	20
	0	2006-11-03 20:40:34 SEČ	0000-00-00 00:00:00	2025-03-05 01:00:00 SEČ	20
	0	2005-12-23 07:09:38 SEČ	0000-00-00 00:00:00	2025-03-05 01:00:00 SEČ	20
	0	2006-11-03 20:40:46 SEČ	0000-00-00 00:00:00	2025-03-05 01:00:00 SEČ	20
	0	2005-12-23 07:11:10 SEČ	0000-00-00 00:00:00	2025-03-05 01:00:00 SEČ	20
	0	2006-11-03 20:40:58 SEČ	0000-00-00 00:00:00	2025-03-05 01:00:00 SEČ	20
	0	2005-12-23 07:12:50 SEČ	0000-00-00 00:00:00	2025-03-05 01:00:00 SEČ	20

HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences

0°42%Reset



Hypotéza 2 – Vlastníkom USB kľúča je niekto iný ako vrah – Vyvrátená

Z vyvodenia Hypotézy 1 je táto hypotéza automaticky vyvrátená, a nenašli sa žiadne informácie o opaku.

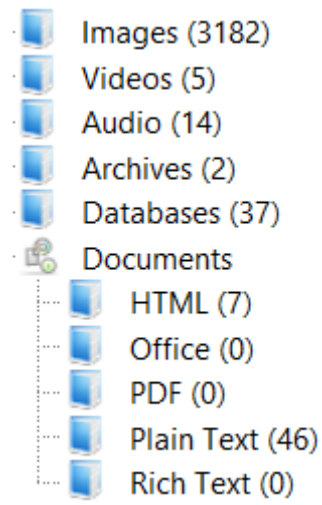
Ďalšou informáciou podporujúcu vyvrátenie tejto hypotézy je web história zariadenia. Ide o vedecké stránky zaoberajúce sa anatómiou ľudského tela a hlavne to najdôležitejšie je že tieto stránky popisujú ako sa vykonáva rez krku medzi stavcami C4 a C5 tak aby sa odrezala hlava, presne tak ako to vykonáva Trnavský sériový vrah.

	index.dat		0	http://www.foxnews.com/css/story.css?1246481129	2009-07-22 20:28:45 SELČ
	index.dat		0	http://seehuhn.de/media/icon/left.png	2009-07-22 20:23:02 SELČ
	index.dat		0	http://www.foxnews.com/js/init_story.js?1233034464	2009-07-22 20:28:49 SELČ
	index.dat		0	http://www.foxnews.com/i/new/hottopics.gif	2009-07-22 20:28:58 SELČ
	index.dat		0	http://web.adblade.com/css/adTemplates/adType1_zon	2009-07-22 20:29:36 SELČ
	index.dat		0	http://i.cdn.turner.com/cnn/.element/js/2.0/main.js	2009-07-24 13:43:22 SELČ
	index.dat		0	http://i.cdn.turner.com/cnn/.element/img/2.0/mosaic/ba	2009-07-24 13:40:38 SELČ
	index.dat		0	http://www.foxnews.com/js/fsoverlay.js?1233034323	2009-07-22 20:28:14 SELČ
	index.dat		0	http://images.intellitxt.com/ast/js/foxnews/foxnews_itx...	2009-07-22 20:29:41 SELČ
	index.dat		0	http://i.cdn.turner.com/cnn/.element/img/2.0/content/p.	2009-07-24 13:40:43 SELČ
	index.dat		0	http://i.cdn.turner.com/cnn/.element/img/2.0/global/dr..	2009-07-24 13:36:13 SELČ

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations
Result: 3 of 291 Result  								
Visit Details								
Date Accessed: 2009-07-22 20:28:49 SELČ								
Domain: foxnews.com								
URL: http://www.foxnews.com/js/init_story.js?1233034464								
Program Name: Internet Explorer Analyzer								

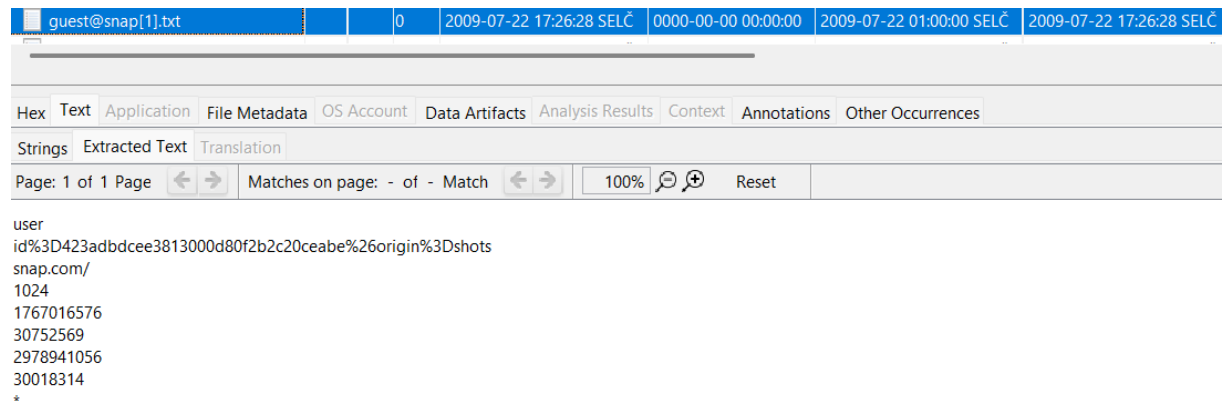
Hypotéza 3 – Na kľúči sa nachádzajú digitálne stopy vedúce k dolapeniu páchatel'a – Vyvrátená

Po dôkladnej analýze všetkých dát:



Sa nedokázalo nájsť žiadne informácie vedúce k dolapeniu vraha, preto je táto hypotéza vyvrátená.

Nenašli sa žiadne zaujímavé dáta, iba pár nezmyselných textov, ktoré boli nepodstatné:



Hypotéza 4 – Na kľučí sa nachádzajú informácie o obetiach – Potvrdená

Na fotografiách sa našli fotografie obetí, ktoré odfotil vrah.

File Name	Count	Date	Time	Action	Date	Time	Action
black_hair_girl.jpg	0	2007-04-19 13:00:50	SELČ		2007-04-19 01:00:00	SELČ	
black_hair_guy.jpg	0	2007-04-19 13:00:50	SELČ		2007-04-19 01:00:00	SELČ	
brunette_girl.jpg	0	2007-04-19 13:00:50	SELČ		2007-04-19 01:00:00	SELČ	
diva_girl.jpg	0	2007-04-19 13:00:50	SELČ		2007-04-19 01:00:00	SELČ	

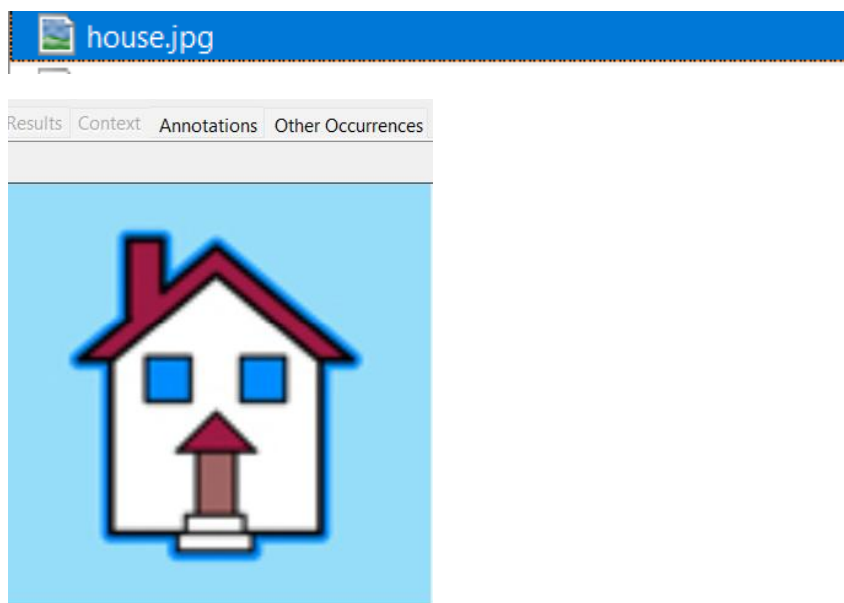
sis Results Context Annotations Other Occurrences



Results Context Annotations Other Occurrences



Ďalej sa tam nachádza táto podozrivá fotografia domu, ktoré je však polícií neznáma pretože nesúvisí so žiadnou známou obetou vraha. Preto sa polícia domnieva že môže ísť o dom budúcej obete, ktorú chce vrah zabiť.



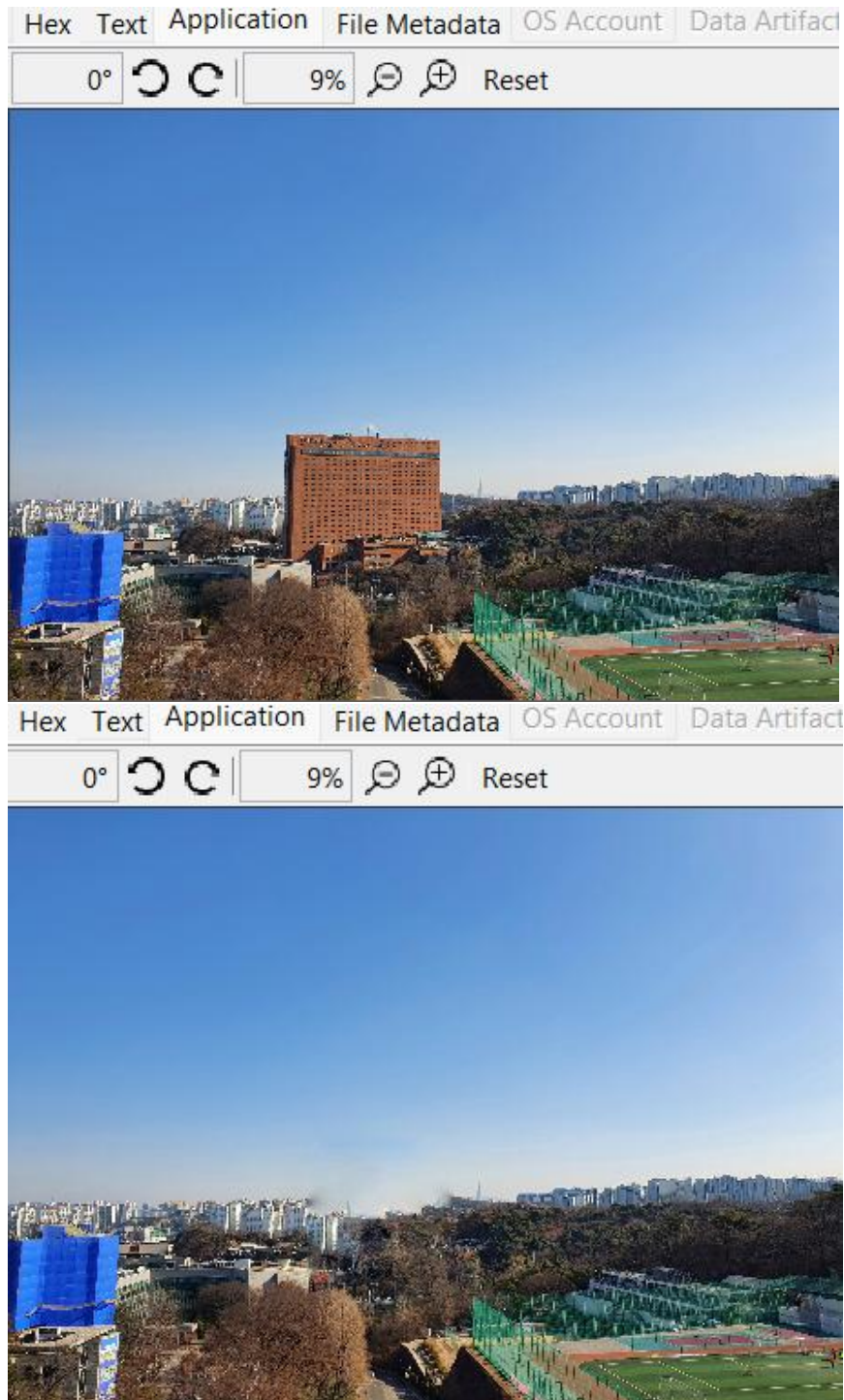
Tieto dáta potvrdzujú túto hypotézu

Hypotéza 5 – USB kľúč slúži na odpútanie pozornosti -

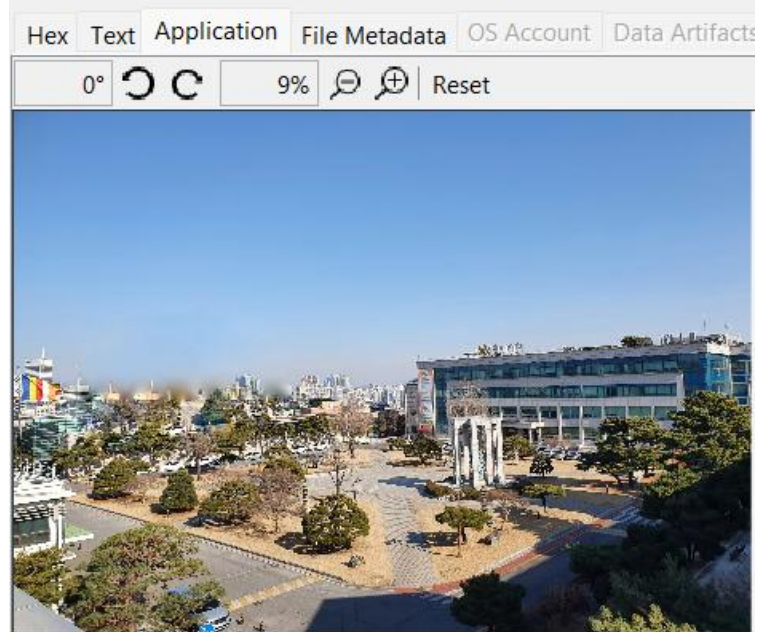
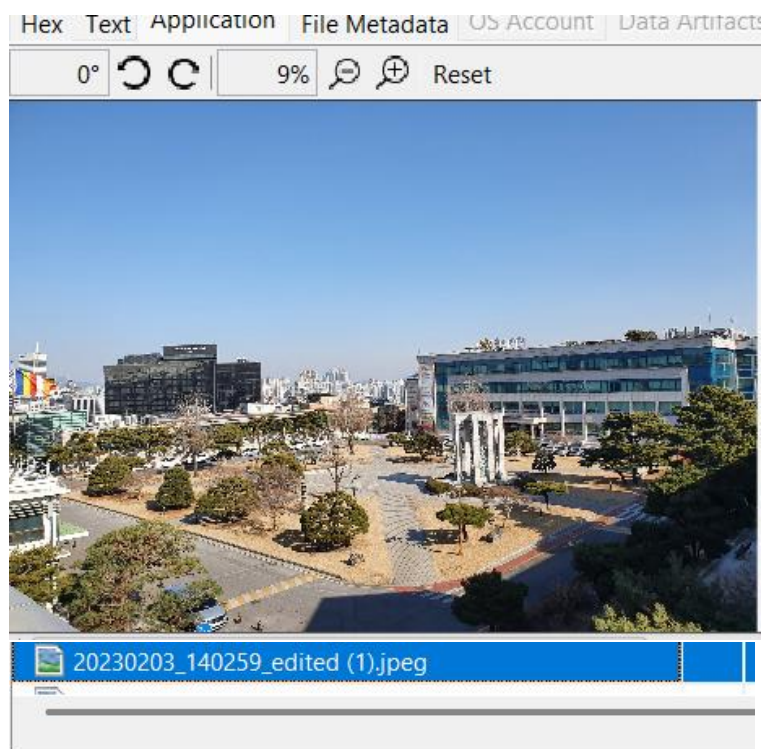
Potvrdená

Našli sa fotografie, ktoré boli zmanipulované, Forezný tím dokázal nájsť originálne fotografie a fotografie, ktoré boli zmenené vrahom, preto túto hypotézu posudzujem ako potvrdenú. Nevie sa prečo toto vrah zamýšľal, možno chcel len získať čas navyše a aby sa polícia zaoberala nepodstatnými dátami a lokáciami.

(Prvá fotka je originál)



(Prvá fotografia je originál)



Na týchto fotografiách je vidieť že páchatel odstránil z uvedených miest objekty, aby zhoršil lokáciu daného miesta. (zrejme polícia toto miesto nenašla a nenašla tam niečo)

Z týchto metadát fotografie:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
20230203_140210.jpg			1	2023-08-11 08:34:20 SELČ	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
20230203_140259.jpg			1	2023-08-11 08:34:20 SELČ	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
20230203_140858.jpg			1	2023-08-11 08:34:20 SELČ	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
20230203_141154.jpg			1	2023-08-11 08:34:20 SELČ	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

Je isté že sú zmanipulované.

Analýza operačnej pamäte zariadenia

Z dát operačnej pamäti mobilného zariadenia nájdeného pri obeti, digitálni forenzní analytici sa snažili, v programe HxD na vyhľadávanie a dekodovanie informácií, pomocou niekoľkých kľúčových slov, nájsť dáta spojené s prípadom.

Pomocou kľúčového slova „**Trnava**“ sa v operačnej pamäti nachádzalo množstvo dát, môže ísť o miesta, v ktorých sa páchateľ najčastejšie pohybuje. Forenzní analytici porovnali tieto lokácie s nájdenými obetami, pričom sa 100% zhodovali:

Checksum	Search (2693 hits)	
Offset	Excerpt (hex)	Excerpt (text)
324ADCF	5A 7E A0 6C 47 21 5C 8B AF 7B D2 1D 21 D5 2A 14 54 72 6E 61 76 61 2C 2C 48 6F 73 70 6F 64 C3 A1	Z- IG\Z(NJO*.Trnava..HospodA
324AF95	62 26 52 65 73 74 61 75 72 61 6E 74 C2 B4 73 20 54 72 6E 61 76 61 18 01 20 EA 7A 20 03 1A 0E 0A	bRestaurantA's Trnava..ez
3E361C0	61 6C 5F 33 2F 53 4B 2F 74 6F 70 5F 55 43 4D 5F 54 52 4E 41 56 41 5F 67 72 61 79 2E 70 6E 67 00	al_3/SK/top_UCM_TRNAVA_gray.png.
429B1EA	37 39 32 25 32 46 37 2C 2B 39 31 37 2B 30 31 2B 54 72 6E 61 76 61 2F 40 34 38 2E 33 37 36 33 39	792%2F7,+917+01+Trnava/@48.37639
429B2C7	20 37 37 39 32 2F 37 2C 20 39 31 37 20 30 31 20 54 72 6E 61 76 61 20 E2 80 93 20 4D 61 70 79 20	7792/7, 917 01 Trnava a€" Mapy
429B82C	37 39 32 25 32 46 37 2C 2B 39 31 37 2B 30 31 2B 54 72 6E 61 76 61 2F 40 34 38 2E 33 37 36 33 39	792%2F7,+917+01+Trnava/@48.37639
429BF2E	37 39 32 25 32 46 37 2C 2B 39 31 37 2B 30 31 2B 54 72 6E 61 76 61 2F 40 34 38 2E 33 37 36 33 39	792%2F7,+917+01+Trnava/@48.37639
464C9D7	0A 14 4F 42 49 20 70 72 65 64 61 6A C5 88 61 20 54 72 6E 61 76 61 20 E0 46 20 03 1A 0E 0A 0A 0A	..OBI predajLa Trnava rF
464CA3B	12 14 4F 42 49 20 70 72 65 64 61 6A C5 88 61 20 54 72 6E 61 76 61 C2 D2 96 99 01 0B 0A 09 10 15	..OBI predajLa Trnava AN~
464CC52	08 4B 61 75 66 6C 61 6E 64 20 E0 72 0A 16 0A 0F 54 72 6E 61 76 61 2D 4A 75 68 20 4E 6F 76 61 18	..Kaufland fr....Trnava-Juh Nova.

Pomocou slova „**zbrane**“ sa takisto našli 4 výskyty v operačnej pamäti, no však nemali žiadnu spojitosť s prípadom a išlo o chybové hlásenia a systémové správy súvisiace s miniaplikáciami (widgets) vo Windowse.

8D 65 6B 2E 20 4D 6F 72 64 61 20 62 6F 73 74 65	Ĥek. Morda boste
20 6D 6F 72 61 6C 69 20 7A 6E 6F 76 61 20 6E 61	morali znova na
6D 65 73 74 69 74 69 20 61 70 6C 69 6B 61 63 69	mestiti aplikaci
6A 6F 2E 00 44 6F 64 61 6A 20 70 72 69 70 6F 6D	jo..Dodaj pripom
6F C4 8D 65 6B 00 00 00 5A 61 70 72 69 00 00 00	oAĤek...Zapri...
50 6F 69 C5 A1 C4 8D 69 20 76 65 C4 8D 20 70 72	PoiĤ~AĤi veAĤ pr
69 70 6F 6D 6F C4 8D 6B 6F 76 00 00 50 72 69 70	ipomoAĤkov..Prip
6E 69 00 00 50 72 69 70 6E 69 20 6E 61 6D 69 7A	ni..Pripni namiz
6E 65 20 70 72 69 70 6F 6D 6F C4 8D 6B 65 00 00	ne pripomoAĤke..
50 61 6B 65 74 20 6C 6F 6B 61 6C 6E 69 68 20 69	Paket lokalnih i
7A 6B 75 C5 A1 65 6E 6A 20 57 69 6E 64 6F 77 73	zkuĤ~enj Windows
00 00 00 00 49 7A 62 72 61 6E 65 67 61 20 70 72	Izbranega pr
69 70 6F 6D 6F C4 8D 6B 61 20 74 72 65 6E 75 74	ipomoAĤka trenut
6E 6F 20 6E 69 20 62 69 6C 6F 20 6D 6F 67 6F C4	no ni bilo mogoA
8D 65 20 64 6F 64 61 74 69 2E 00 00 4E 61 70 61	Ĥe dodati...Napa
6B 61 20 70 72 69 20 64 6F 64 61 6A 61 6E 6A 75	ka pri dodajanju
20 70 72 69 70 6F 6D 6F C4 8D 6B 61 00 00 00 00	pripomoAĤka....
4E 61 20 76 6F 6C 6A 6F 20 6A 65 20 70 6F 73 6F	Na voljo je poso

Search (4 hits)

Offset	Excerpt (hex)	Excerpt (text)
2C	72 61 6E 6A 65 6E 4F 64 73 74 72 61 6E 69 20 69 7A 62 72 61 6E 65 20 65 6C 65 6D 65 6E 74 65 53	ranjenOdstrani izbrane elementeS
9A	70 69 73 65 20 76 20 C5 BE 69 76 6F 20 76 20 69 7A 62 72 61 6E 65 6D 20 6A 65 7A 69 6B 75 2E 00	pise v Ľivo v izbranem jeziku..
76	70 69 73 65 20 76 20 C5 BE 69 76 6F 20 76 20 69 7A 62 72 61 6E 65 6D 20 6A 65 7A 69 6B 75 2E 00	pise v Ľivo v izbranem jeziku..
ID5	65 6E 6A 20 57 69 6E 64 6F 77 73 00 00 00 00 49 7A 62 72 61 6E 65 67 61 20 70 72 69 70 6F 6D 6F	enj Windows....Izbranega pripomo

V operačnej pamäti sa našlo niekoľko výskytov slova „vrah“, čo bolo veľkým prínosom k dolapeniu páchateľa.

Checksum	Search (117 hits)	
Offset	Excerpt (hex)	Excerpt (text)
386FE562	73 00 65 00 72 00 69 00 6F 00 76 00 79 00 5F 00 76 00 72 00 61 00 68 00 2F 00 00 00 00 00 00	sériový.vrah./.....
50B8C714	73 00 E9 00 72 00 69 00 6F 00 76 00 FD 00 20 00 76 00 72 00 61 00 68 00 2E 00 00 00 54 00 FD 00	sériový.vrah....Tý.
128B60494	73 00 E9 00 72 00 69 00 6F 00 76 00 FD 00 20 00 76 00 72 00 61 00 68 00 2E 00 00 00 54 00 FD 00	sériový.vrah....Tý.
130E1C50C	73 00 E9 00 72 00 69 00 6F 00 76 00 FD 00 20 00 76 00 72 00 61 00 68 00 2E 00 00 00 54 00 FD 00	sériový.vrah....Tý.
166E3F68C	73 00 E9 00 72 00 69 00 6F 00 76 00 FD 00 20 00 76 00 72 00 61 00 68 00 2E 00 00 00 54 00 FD 00	sériový.vrah....Tý.
169334748	73 00 E9 00 72 00 69 00 6F 00 76 00 FD 00 20 00 76 00 72 00 61 00 68 00 2E 00 00 00 54 00 FD 00	sériový.vrah....Tý.
17465B1CC	73 00 E9 00 72 00 69 00 6F 00 76 00 FD 00 20 00 76 00 72 00 61 00 68 00 2E 00 00 00 54 00 FD 00	sériový.vrah....Tý.
17F983DDC	73 00 E9 00 72 00 69 00 6F 00 76 00 FD 00 20 00 76 00 72 00 61 00 68 00 2E 00 00 00 54 00 FD 00	sériový.vrah....Tý.
19B8CC018	70 00 72 00 6F 00 66 00 69 00 6C 00 65 00 20 00 76 00 72 00 61 00 68 00 61 00 2E 00 20 00 20 00	profile.vrah.....
19B8CC039	20 00 0A 00 0A 00 39 00 2E 00 20 00 2A 00 2A 00 56 00 72 00 61 00 68 00 20 00 63 00 68 00 63 00	Vrah.chc.
1AFE5E2EC	73 00 E9 00 72 00 69 00 6F 00 76 00 FD 00 20 00 76 00 72 00 61 00 68 00 2E 00 00 00 54 00 FD 00	sériový.vrah....Tý.
18C2575B8	A9 00 72 00 69 00 6F 00 76 00 02 01 DD 02 20 00 76 00 72 00 61 00 68 00 2E 00 00 00 0A 00 54 00	@riov...Y.vrah.....T.
1C25CB714	A9 00 72 00 69 00 6F 00 76 00 02 01 DD 02 20 00 76 00 72 00 61 00 68 00 2E 00 00 00 0A 00 54 00	@riov...Y.vrah.....T.
1C914C93C	73 00 E9 00 72 00 69 00 6F 00 76 00 FD 00 20 00 76 00 72 00 61 00 68 00 2E 00 00 00 54 00 FD 00	sériový.vrah....Tý.
1C56BEE0	A9 00 72 00 69 00 6F 00 76 00 02 01 DD 02 20 00 76 00 72 00 61 00 68 00 2E 00 00 00 0A 00 54 00	@riov...Y.vrah.....T.
1CAAFA325	7A 00 6F 00 6D 00 2A 00 2A 00 20 00 13 20 20 00 76 00 72 00 61 00 68 00 20 00 6D 00 F4 00 7E 01	zom"...vrah.mó~.
1CAAFA307	20 00 0A 00 0A 00 38 00 2E 00 20 00 2A 00 2A 00 56 00 72 00 61 00 68 00 20 00 6D 00 61 00 70 00	Vrah.nap.
1CAAFA419	70 00 72 00 6F 00 66 00 69 00 6C 00 65 00 20 00 76 00 72 00 61 00 68 00 61 00 2E 00 20 00 20 00	profile.vrah.....
1CAAFA437	20 00 0A 00 0A 00 39 00 2E 00 20 00 2A 00 2A 00 56 00 72 00 61 00 68 00 20 00 63 00 68 00 63 00	Vrah.chc.
1D97A64C8	73 00 65 00 72 00 69 00 6F 00 76 00 79 00 5F 00 76 00 72 00 61 00 68 00 2F 00 4D 00 6F 00 64 00	sériový.vrah./Mod.
1D97A64C8	73 00 65 00 72 00 69 00 6F 00 76 00 79 00 5F 00 76 00 72 00 61 00 68 00 2F 00 4D 00 6F 00 64 00	sériový.vrah./Mod.
1DBCC2578	73 00 E9 00 72 00 69 00 6F 00 76 00 FD 00 20 00 76 00 72 00 61 00 68 00 2E 00 00 00 54 00 FD 00	sériový.vrah....Tý.
1E6E1268C	73 00 E9 00 72 00 69 00 6F 00 76 00 FD 00 20 00 76 00 72 00 61 00 68 00 2E 00 00 00 54 00 FD 00	sériový.vrah....Tý.
1E71D7EE0	A9 00 72 00 69 00 6F 00 76 00 02 01 DD 02 20 00 76 00 72 00 61 00 68 00 2E 00 00 00 0A 00 54 00	@riov...Y.vrah.....T.
1ECF0650C	73 00 E9 00 72 00 69 00 6F 00 76 00 FD 00 20 00 76 00 72 00 61 00 68 00 2E 00 00 00 54 00 FD 00	sériový.vrah....Tý.
1F82F60A0	A9 00 72 00 69 00 6F 00 76 00 02 01 DD 02 20 00 76 00 72 00 61 00 68 00 2E 00 00 00 0A 00 54 00	@riov...Y.vrah.....T.
2108B70AC	73 00 E9 00 72 00 69 00 6F 00 76 00 FD 00 20 00 76 00 72 00 61 00 68 00 2E 00 00 00 0A 00 54 00	sériový.vrah.....Tý.
2108B752C	73 00 E9 00 72 00 69 00 6F 00 76 00 FD 00 20 00 76 00 72 00 61 00 68 00 2E 00 00 00 54 00 FD 00	sériový.vrah....Tý.
21C22D848	A9 00 72 00 69 00 6F 00 76 00 02 01 DD 02 20 00 76 00 72 00 61 00 68 00 2E 00 00 00 0A 00 54 00	@riov...Y.vrah.....T.
227538BCC	00 00 65 00 72 00 69 00 6F 00 76 00 79 00 5F 00 76 00 72 00 61 00 68 00 5C 00 4D 00 6F 00 64 00	@riov...Y.vrah./Mod.
22B84ED40	A9 00 72 00 69 00 6F 00 76 00 02 01 DD 02 20 00 76 00 72 00 61 00 68 00 2E 00 00 00 0A 00 54 00	@riov...Y.vrah.....T.

V.o.l.á.m. .s.a.
.P.i.a.t.a. .L.
a.k.a.t.o.a. .a.
.s.o.m. .T.r.n.
a.v.s.k.ý. .s.é.
r.i.o.v.ý. .V.r.h.
s.h....T.ý.m.t.
o. .s.a. .p.r.i.
z.n.á.v.a.m. .k.
u. .v.a.e.t.k.ý.
m. .o.b.e.t.i.a.
m. .k.t.o.r.é. .
p.o.l.i.c.i.a. .
n.a.a.l.á....M.
o.j.i.m. .m.o.t.
i.v.o.m. .k. .p.
á.c.h.a.n.i.u. .
v.r.á~d. .b.o.
l.o. .~e. .m.á.
m. .n.e.o.d.o.l.
a.t.e.>.n.ú. .c.
h.t.i... .p.á.c.
h.a.e. .v.r.a.~.
d.y. .a. .z.a.b.
i.j.a.e., .z.r.
e.j.m.e. .s.o.m.
.p.s.y.c.h.i.c.
k.y. .c.h.o.r.ý.
.a. .c.h.c.e.l.
.s.o.m. .p.o.z.
o.r.n.o.s.e. .m.
é.d.i.i. .t.a.k.

Z uvedených dát sa dal dekódovať obsahujúci text:

„Volám sa Pišta Lakatoš a som Trnavský sériový vrah.

Týmto sa priznávam ku všetkým obetiam ktoré polícia našla.

Mojím motívom k páchaniu vražd bolo že mám neodolateľnú chť páchať vraždy a zabíjať, zrejme som psychicky chorý a chcel som pozornosť médií tak som odtrhával obetiam hlavy, bolo to pre mňa neopojateľná vec, ktorú som nevedel zastaviť. Tento dokument slúži ma moje dochytenie. Opäť chcem aby to bolo medializované, čo určite aj bude. Budem vraždiť ešte viac dokým ma nedolapíte a nebudem mať pokoj.

Nájdete ma na 48° 22' 0.3068598" N 17° 34' 1.9929199" E“

Záver:

Vďaka vykonaniu obrazu USB zariadenia, ktoré sa našlo v ústach obeti Trnavského vraha, a následnému vykonaniu analýzy pomocou softvéru Autopsy, sa podarilo spojiť telefóny prístroj, ktorý sa neskôr našiel pri ďalšej obeti s páchatelom.

Vďaka analýze obrázkov a exif dát fotografií sa potvrdila Hypotéza 1, že vlastníkom USB-kľúča je vrah, a tým sa nám vylúčila hypotéza číslo 2, že vlastníkom USB zariadenia nie je vrah.

Taktiež sa potvrdila hypotéza číslo 4 – Na fotografiách na USB-kľúči sa nachádzali informácie / fotografie obetí.

Nesmierne dôležitými dátami boli tie z operačnej pamäte, na ktorých sa vrah priznal a povedal svoje ďalšie postupy, to znamená že by pokračoval vo vraždení až dokým by neprišla polícia na dané súradnice.

S istotou teraz vieme kto je páchatelom. Je to Pišta Lakatoš, ktorý napísal vo svojom zariadení priznanie na jeho dolapenie.

Polícia prišla na dané miesto, páchatel sa tam nachádzal. Polícia ho zadržala a následne priviedla na Krajské riaditeľstvo Policajného zboru v Trnave, kde ho vypočula, páchatel sa ku všetkému priznal. Dňa 5.5.2025 sa uskutoční súd, na ktorom sudca vysloví posledné slovo o jeho vinne a jeho uväznení.

Literatúra:

[2010 USA pres-secure usb bypassing tool.pdf](#)

Tento dokument rieši Secure USB Flash disk, ktoré majú zabudované bezpečnostné funkcie na ochranu dát. Väčšina týchto „bezpečných USB diskov“ využíva šifrovanie alebo nejaký druh overovania, aby zabránila neoprávnenému prístupu k súborom. No autori zistili, že mnohé z týchto ochranných mechanizmov nie sú až také spoľahlivé, pretože niektoré USB kontroléri majú špecifické príkazy, ktoré umožňujú ochranu jednoducho obísť.

[Open Source Data Extraction Tools: Best 18 Tools | Data Stack Hub](#)

Stránka ukazuje 18 najlepších open-source nástrojov na extrakciu dát. Tieto nástroje sú navrhnuté na získavanie a spracovanie dát z rôznych zdrojov, ako sú napríklad webové stránky, databázy, dokumenty a podobne. Medzi uvedené nástroje patria napríklad Apache Nutch, Scrapy, BeautifulSoup, Octoparse a WebHarvy, pričom každý z nich je stručne opísaný aj spolu s jeho vlastnosťami a výhodami.