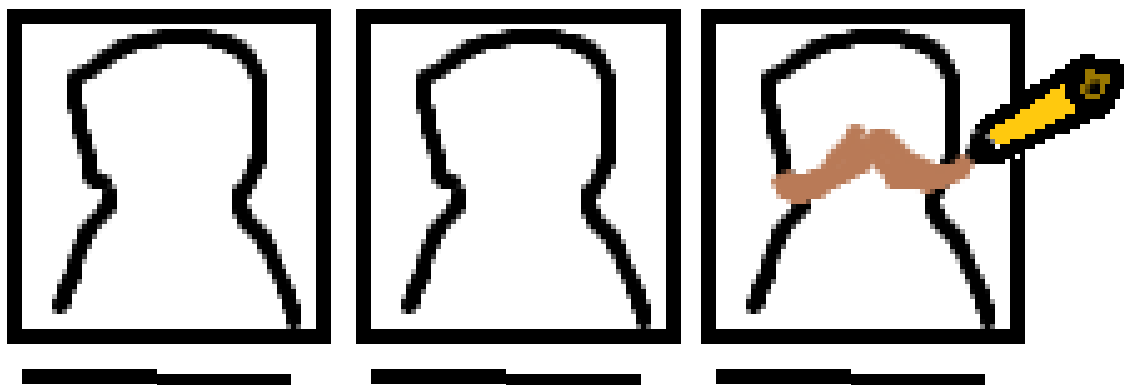


Univerzita sv. Cyrila a Metoda v Trnave
Fakulta Prírodných Vied
Ústav počítačových technológií a informatiky

Fúzatý Prípad
SEMESTRÁLNY PROJEKT



Ročník: 2
Krúžok: 6
Ak. Rok: 2025-2026

Marek Miškolci

Fúzatý Prípád

[Link-Prezentácia]

1. Popis prípadu

1.1. Stručný popis prípadu

Vandalizácia digitálnej publikácie – ročenky pridaním fúzov do jednotlivých obrázkových súborov. Prebehla deň pred tlačou po tlačovej kontrole a spôsobila tlačiarenskej firme materiálnu škodu vo forme mrhania toneru a papiera. Súborný na tlač boli na notebooku, našiel sa pri ňom USB kľúč. Je tu tiež možnosť, že digitálne začmáranie fotiek nebola jediná nekalá vec v rámci tohto prípadu.

1.2. Detailnejší popis

Tlačiarenská firma *PickTheCMYK* (fiktívny názov pre fiktívnu firmu) dostala zakázku na vytlačenie ročeniek. Tlačové súbory boli vypracované v programe Scribus, kde boli samotné obrázkové súbory pridané embedovaním (čo znamená že akákoľvek zmena v súboroch bola okamžite odzrkadlená v súbore na tlač)

Fig.1 – Ilustrovaná reprodukcia pôvodných verzii fotografií v tlačovej publikácii



Deň pred tlačením bola zhotovená posledná tlačová kontrola. Všetko bolo ako má byť.

Avšak v deň tlače bol výsledok tlačeného rozdielny od verzie – portréty vo vytlačenej publikácii boli vandalizované doplnenými fúzmi. Pred tým než bola tlač predčasne zastavená došlo k vytlačeniu dvoch kompletných kópií, čo znamenalo že finančná a materiálna strata bola menej seriózná, no toner lacný nie je, takže je to stále rana do rozpočtu firmy.

Fig.2 – Kresba už znehodnotenej tlačoviny



Na mieste činu, pri notebooku, z ktorého mala byť poslaná finálna verzia tlačového dokumentu sa našlo USB. Je tu tiež isté podozrenie, že vandalizácia fotografií a mrhanie tonerom je v tomto prípade len vrchol ľadovca a notebook mohol byť napadnutý niečím horším – napríklad vírusom.

1.3. 5WH

Who?

-Pravdepodobne niekto z personálu tlačovej firmy

Where?

-V špecifickom oddelení tlačovej firmy

When?

-Deň pred tlačou.

What?

-Manipulácia s obrázkovými dátami, možno sérioznejší útok(ktorý je skrytý popri softvéri použitom na znehodnotenie tlačovej publikácie)

Why?

-Cieľom mohlo pravdepodobne podryť imidž profesionality firmy, poukázať relatívne neškodným útokom na diery v bezpečnosti firmy, mrhať jej prostriedkami, potenciálne prepašovať dodatočný škodlivý softvér do napadnutého zariadenia/lokálnej siete popri „žartíku“.

How?

-Pravdepodobne prostredníctvom softvéru na USB

1.4. Predmet a cieľ vyšetrovania

-izolovať všetky relevantné zariadenia od siete, vytvoriť obraz pamäte notebooku a USB, získať kópiu logov zo zariadenia, čo spravuje zámkový systém firmy, ak sú, kópie záznamov z kamier

-analýza dôkazov, pátranie po potenciálne škodlivých súboroch ktoré sa z USB mohli dostať na notebook

-na základe vyšetrovania zoceliť bezpečnosť tlačiarenskej firmy

-zistiť vinníka, ktorý spôsobil problém a donútiť ho pokryť náklady spojené s pokazenou tlačou/nahradením napadnutého zariadenia

1.5. Odborný príspevok

DFRWS: USB ako platformy pre útoky

<https://dfrws.org/presentation/duck-hunt-memory-forensics-of-usb-attack-platforms/>

2.Hypotézy

A-USB bolo prepašované do budovy firmy zamestnancom, ktorý mal v úmysle spraviť relatívne neškodný žartík, no softvér na USB bol poskytnutý treťou stranou, ktorá zamýšľala niečo iné

B-Išlo o vedomú sabotáž

C-USB a notebook boli skompromitované treťou stranou bez vedomia ostatných potenciálnych podozrivých

D-Na USB bol len program na vandalizáciu fotiek, hoci motivácie/okolnosti s činom spojené sa môžu podobáť hypotézam A-C

-K overeniu jednotlivých hypotéz musíme identifikovať súbory na zabezpečených zariadeniach, analyzovať potenciálne zdroje stôp z bezprostrednej blízkosti miesta činu a na základe výsledkov určiť pravdivosť týchto hypotéz. Hypotézu A sa dá overiť podľa metadát súborov na USB, analógových dôkazov, odchytenej elektronickej komunikácie, resp. zo stôp, čo vinník zanechal. Na základe zistení môžeme odvodiť pravdivosť hypotéz B a C, ktoré sú tiež spojené so špekuláciou o motíve vinníka s predpokladom, že sa nájde dodatočný softvér popri nástroji, ktorý bol použitý na znehodnotenie tlačovej publikácie. Na základe obsahu USB kľúča tiež môžeme určiť, či je hypotéza D pravdivá a na kľúči bol len softvér na vandalizáciu.

Samotný obsah USB môžeme získať prostredníctvom image-u pamäťového média(USB), ideálne s writeblockerom a následne vykonať analýzu obsahu image súbru prostredníctvom forenzného softvéru, napríklad Autopsy. Takto je možné nenarušiť integritu zabezpečených dôkazov a zároveň sa priblížiť k cieľom nášho vyšetrovania.

2.1. Overenie jednotlivých hypotéz

Vďaka značnému nedostatku dôslednosti zo strany páchatel'a sa nám podarilo zaistiť slušné množstvo stôp, ktoré nám umožnia nielen prípad vyriešiť, ale aj určiť pravdivosť našich hypotéz.

Integrita dôkazov je zabezpečená prostredníctvom hash-ov, ktoré boli zapísané v dobe vytvorenia image súborov

V rámci kapitol 5 a 6 sme zachytili počas analýzy stôp z operačnej pamäte a image-ov relevantných úložiskových médií, špecificky USB kľúča nájdeného na mieste činu.

Analýzou image-u USB kľúča, ktorý sme prehliadali cez softvérové programy Exterro FTK Imager a Autopsy (kapitola 6, artefakty 1, 3, 4, 5, a 6) sme zistili jeho obsah, na ktorého základe môžeme vylúčiť, že okrem programu na vandalizáciu fotiek nebol na samotnom USB žiadny ďalší škodlivý softvér (ani nebol medzi vymazanými súbormi, ako môžeme vidieť v kapitole 6, artefakte 3), čo následne vyvracia časť hypotéz A-C, ktoré počítajú s tým, že tam nejaký softvér takéhoto typu bol.

C môžeme kompletne zamietnuť na základe stôp z USB(kapitola 6, artefakty 3, 4) aj z operačnej pamäte(kapitola 5, artefakty 1-4) , keďže je očividné, že šlo o čin vopred plánovaný. Najmä na základe upraveného textového dokumentu so zoznamom zariadení, ktoré firma používa na spracovanie súborov pred tlačou(kapitola 6, artefakt 3) a súbore s vypísanou verziou samotného plánu(kapitola 6, artefakt 4).

Vďaka stopám zanechaných v operačnej pamäti (kapitola 5, artefakty 1-3 + záber uložený z kamery-kapitola 6, artefakt 2) a zachytenej mailovej komunikácii cez Moodle (kapitola 5, artefakt 4) môžeme zúžiť zvyšné čiastočne potvrdené hypotézy na jednu, t.j. hypotézu A, kde sme potvrdili, že sa motív zhoduje s hypotézou, hoci zvyšné okolnosti sedia viac k hypotéze D.

V konečnom dôsledku sme dospeli k takémuto záveru ohľadne samotných hypotéz:

Hypotéza A-čiastočne potvrdená

Hypotéza B-zamietnutá

Hypotéza C-zamietnutá

Hypotéza D-potvrdená

3. Digitálne zariadenia

3.1. Digitálne zariadenia s ktorými sa bude pracovať

- Notebook s kompromitovanými súbormi
- USB čo sa našlo neďaleko notebooku
- záznamy zo smart zámku dverí oddelenia firmy

3.2. Parametre jednotlivých zariadení

USB: Verbatim Slider

- tzv. DFA_usb

- USB 2.0

- 16 GB



(Fig.3-USB)

Notebook: DELL Latitude E7270

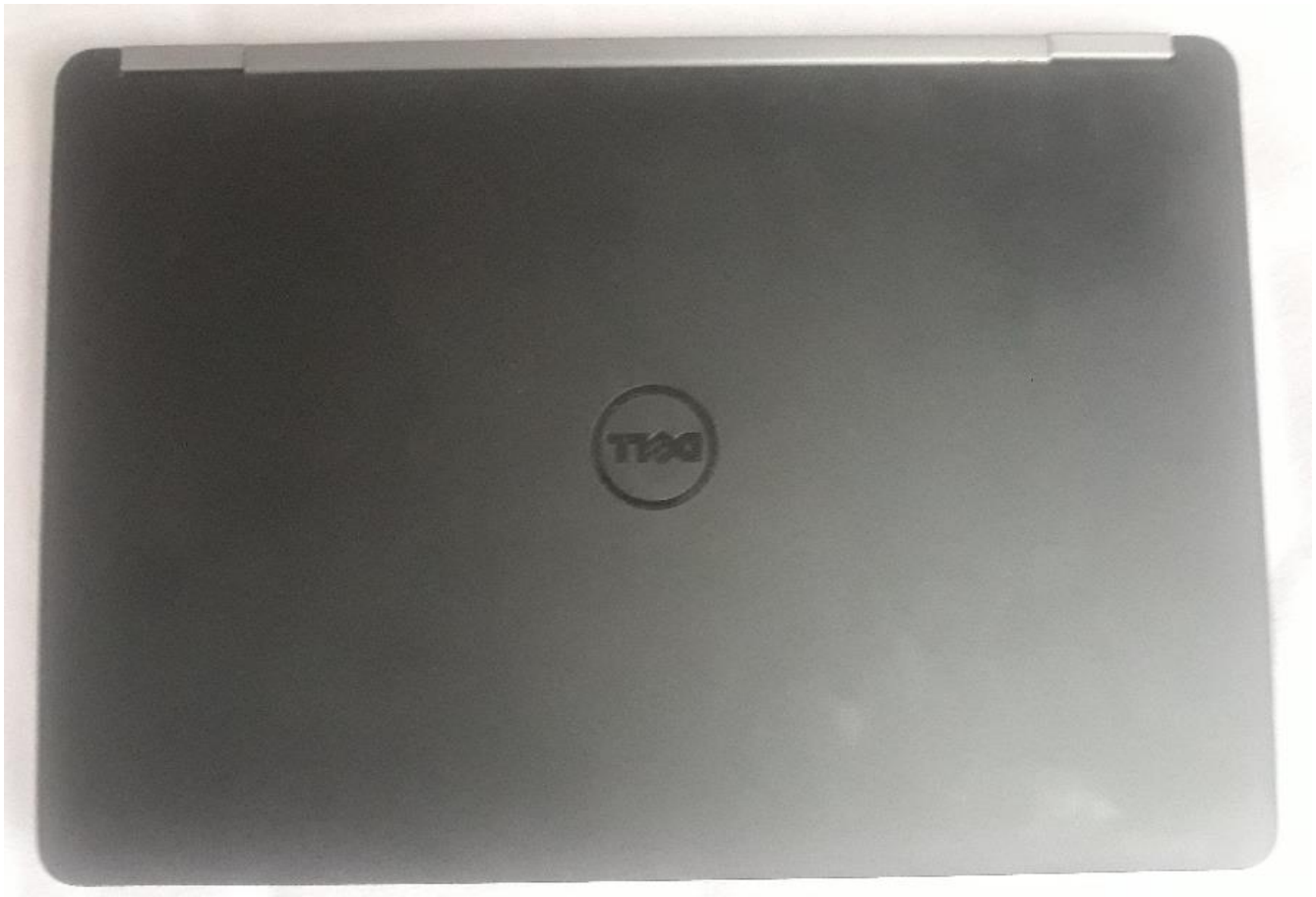
- Úložisko: 252 GB

- OS: Windows 10 Pro

- Procesor: Intel Core i5(2-core, 2.40GHz)

- RAM: 8GB

- GPU: Integrovaný Intel HD Graphics 520(300MHz, 345.6 GFLOPS)



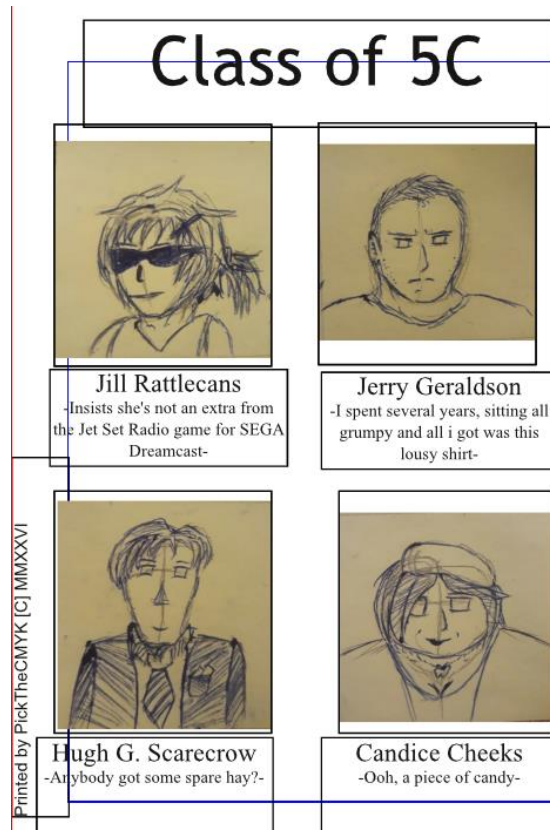
(Fig.4-Notebook)

4.Dáta

4.1. Čo budeme analyzovať(aké súbory)

- Súbory zo zhotoveného imag-u USB(Programy, obrázkové dáta, metadáta obrázkových súborov, programov)
- Súbory z image-u notebooku(Obrázkové súbory a ich metadáta)
- Ak sú. dáta z logov zo smart zámku(Záznamy, časové stopy)
- Súborové metadáta zo spomenutých zariadení

-Ak sú, záznamy z kamier(video súbory)



(Fig.5-strana tlačového dokumentu v programe Scribus – reprodukováaná verzia strany pred znehodnotením)

4.2. Veľkosť dát/datasetu/Dodatočné informácie

- Používané sú 'reálne' dáta(vlastná tvorba) – lokálne uložené, vo veľkosti cca 33.7 MB
- Cca 52 súborov

5. Image RAM, Analýza získaných dôkazov nájdených na RAM

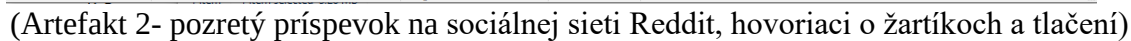
The screenshot displays a memory analysis tool interface. The main window shows a RAM image named 'RAM image miskolci.raw' with a hex dump and decoded text. The decoded text contains several lines of memory data, including a search for the word 'moustache'.

The search results are shown in a table below the main window:

Offset	Excerpt (hex)	Excerpt (text)
2F1BEC1D	23 00 00 55 01 00 00 22 ED 56 FC 0A 00 00 6C 6D 6F 75 73 74 61 63 68 65 00 00 55 01 00 00 CE	#.U.../Vü...lmoustache.U...
2F7093BD	22 48 6F 77 20 64 6F 20 49 20 61 64 64 20 61 20 6D 6F 75 73 74 61 63 68 65 20 74 6F 20 61 20 70	"How do I add a moustache to a p
2F709700	3E 48 6F 77 20 64 6F 20 49 20 61 64 64 20 61 20 6D 6F 75 73 74 61 63 68 65 20 74 6F 20 61 20 70	>How do I add a moustache to a p
306BE388	68 61 72 38 72 6C 6D 38 72 6D 6F 75 73 74 38 72 6D 6F 75 73 74 61 63 68 65 38 72 6E 6D 69 64 38	haz;rm;moust;moustache;mmd;
3261A2C9	68 6F 74 6F 20 65 64 69 74 6F 72 2F 61 64 64 20 6D 6F 75 73 74 61 63 68 65 2D 74 6F 2D 70 68 6F	hoto-editor/add-moustache-to-pho
34786A39	68 6F 74 6F 20 65 64 69 74 6F 72 2F 61 64 64 20 6D 6F 75 73 74 61 63 68 65 2D 74 6F 2D 70 68 6F	hoto-editor/add-moustache-to-pho

The search results show the word 'moustache' appearing in multiple locations, indicating it is a keyword or artifact in the data.

(Artefakt 1-vyhľadavanie, kľúčové slová „ako pridať na fotku fúzy“)



25 marca

09.11

Idem kresliť bajúúzy

Che che che. Do ročenky, che che

Fór storočia...

toto je veľmi inkriminujúca správa.

Každopádne, asi to bude cez USB.

Neviem zatiaľ, zoženiem

-Dežko Páchatel'

AFC2B0

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

.....

AFC2C0

00 00 00 00 00 00 E0 5F B9 71 AD C0 50 EB F6 94

.....f_aq.RPëö"

AFC2D0

2A 85 08 00 45 00 00 34 6F 90 40 00 80 06 00 00

*....E..4o.€.€...

AFC2E0

C0 A8 E1 0C 14 32 49 0B DE 9A 01 BB 62 13 95 2E

Ř"á..2I.Ťš.»b.*.

AFC2F0

D2 80 57 D2 80 10 00 FF FF 18 00 00 01 01 05 0A

ÑewÑe..''.....

AFC300

D2 80 5D 86 D2 80 65 47 50 10 01 FF FD C0 00 00

Ñe]†ÑeeGP..`ýR..

AFC310

06 6D 6F 6F 64 6C 6B 06 66 70 76 75 63 6D 02 73

.moodle.fpvucm.s

AFC320

6B 00 00 1C 00 01 98 F2 97 42 84 F6 80 7D D4 A1

k.....ñ-B,,ö€}Ö~

AFC330

60 FB F0 92 A7 0B 2B 1E 03 56 C6 70 8F 7A 52 10

`úd'S.+..VČpžzR.

AFC340

BE 46 9D E5 36 67 9D 94 60 E1 75 88 37 A9 B5 BF

IFtí6gt`^áu.7@už

AFC350

FD 5E 12 80 50 FC FE 65 00 00 00 00 00 00 00

ý^..€Püťe.....

AFC360

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

.....

AFC370

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

.....

Napísať správu ...

😊

➤

(Artefakt 4-odchytená mailová komunikácia-elektronická pošta prostredníctvom moodlu, samotná správa)

-toto sú vybrané artefakty zo série 14-tich zhotovených z image-u RAM(+z pár starších, robených ešte na hodine)

6. Image zariadení, ktoré sú predmetom vyšetrovania

Robili sme image USB kľúča s veľkosťou 15-16GB, veľkosť image-u 14.49 GB, prostredníctvom softvéru Exterro FTK Imager.

MD5 hash: 8a23fa77df5549bd894f0e71d91336f3

SHA1 hash: 61a2b2879833a68d485c0fccddf234c622f1fc37

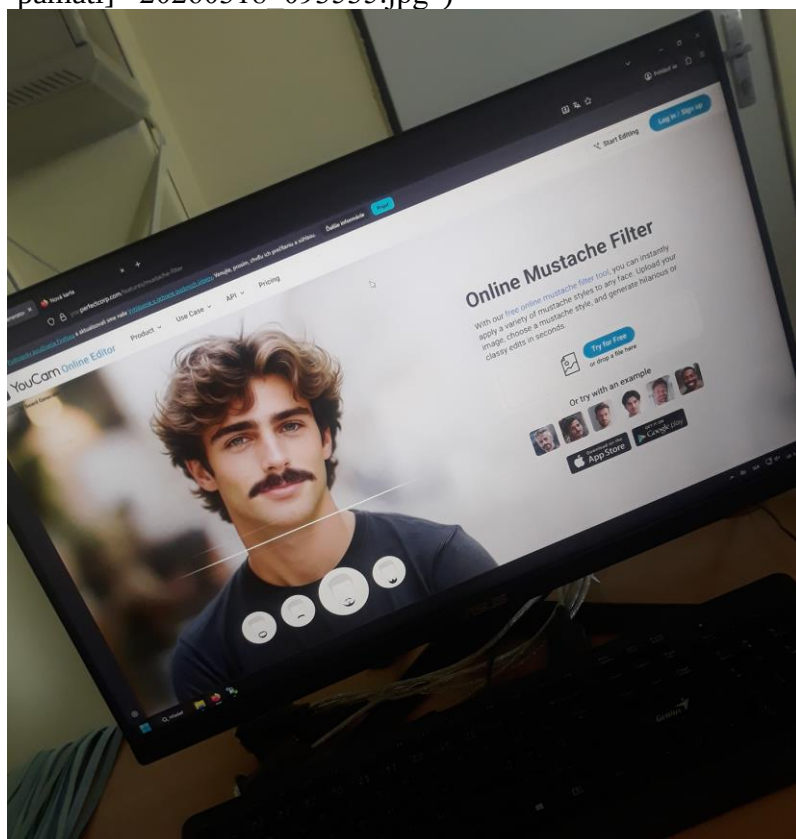
Artefakty(získané prostredníctvom softvérov FTK Imager a Autopsy):

0c000e100	65 00 73 00 00 00 00 00-40 00 00 00 28 00 00 00	e.s....@...(...
0c000e110	00 00 00 00 00 00 04 00-10 00 00 00 18 00 00 00	
0c000e120	8E D8 44 96 C7 25 F1 11-88 E5 E4 A7 A0 77 45 29	0D.Cñ.âs wE)
0c000e130	90 00 00 00 C8 00 00 00-00 04 18 00 00 00 01 00	...E...
0c000e140	A8 00 00 00 20 00 00 00-24 00 49 00 33 00 30 00	...-\$.I.3.0.
0c000e150	30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00	0.....
0c000e160	10 00 00 00 98 00 00 00-98 00 00 00 00 00 00 00	
0c000e170	29 00 00 00 00 00 01 00-78 00 66 00 00 00 00 00	).....x.f....
0c000e180	28 00 00 00 00 00 01 00-C2 92 35 2B 35 BC DC 01	(.....Â.5+5%Ü
0c000e190	D1 37 E9 41 35 BC DC 01-D1 37 E9 41 35 BC DC 01	N7éA5%Ü.N7éA5%Ü
0c000e1a0	D1 37 E9 41 35 BC DC 01-00 00 00 00 00 00 00 00	N7éA5%Ü.....
0c000e1b0	00 00 00 00 00 00 00 00-00 00 00 10 00 00 00 00	
0c000e1c0	12 00 6D 00 6F 00 75 00-73 00 74 00 61 00 63 00	..m.o.u.s.t.a.c.
0c000e1d0	68 00 65 00 20 00 73 00-6F 00 66 00 74 00 77 00	h.e...s.o.f.t.w.
0c000e1e0	61 00 72 00 65 00 00 00-00 00 00 00 00 00 00 00	a.r.e.....
0c000e1f0	10 00 00 00 02 00 00 00-FF FF FF FF 82 79 0A 00	a.r.e.....y..
0c000e200	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
0c000e210	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
0c000e220	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
0c000e230	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
0c000e240	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
0c000e250	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
0c000e260	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
0c000e270	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
0c000e280	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
0c000e290	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
0c000e2a0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
0c000e2b0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
0c000e2c0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	

(USB artefakt 1-na USB nájdený priečinok „Moustache Sofrware/Fúzový Softvér“)

0c000f030	02 00 00 00 00 00 00 00-10 00 00 00 60 00 00 00	
0c000f040	00 00 00 00 00 00 00 00-48 00 00 00 18 00 00 00	H.....
0c000f050	D6 8E 5F 5F 35 BC DC 01-80 65 98 30 B2 B6 DC 01	Ö_5Ü-e-0qÜ-
0c000f060	91 11 3E A4 B4 B6 DC 01-33 24 BA 5F 35 BC DC 01	-->K'qÜ-3q°_5Ü-
0c000f070	20 00 00 00 00 00 00 00-00 00 00 00 00 00 00	
0c000f080	00 00 00 00 00 00 09 01 00 00-00 00 00 00 00 00	
0c000f090	00 00 00 00 00 00 00 00-30 00 00 00 80 00 00 00	0.....
0c000f0a0	00 00 00 00 00 00 02 00-68 00 00 00 18 00 01 00	h.....
0c000f0b0	27 00 00 00 00 00 01 00-D6 8E 5F 5F 35 BC DC 01	'.....Ö_5Ü-
0c000f0c0	D6 8E 5F 5F 35 BC DC 01-D6 8E 5F 5F 35 BC DC 01	Ö_5Ü-Ö_5Ü-
0c000f0d0	D6 8E 5F 5F 35 BC DC 01-00 00 33 00 00 00 00 00	Ö_5Ü--3----
0c000f0e0	00 00 00 00 00 00 00 00-20 00 00 00 00 00 00 00	
0c000f0f0	13 00 32 00 30 00 32 00-36 00 30 00 33 00 31 00	--2-0-2-6-0-3-1-
0c000f100	38 00 5F 00 30 00 39 00-33 00 35 00 33 00 35 00	8--0-9-3-5-3-5-
0c000f110	2E 00 6A 00 70 00 67 00-80 00 00 00 48 00 00 00	.-j-p-g-----H---
0c000f120	01 00 00 00 00 00 01 00-00 00 00 00 00 00 00 00	
0c000f130	2F 03 00 00 00 00 00 00-40 00 00 00 00 00 00 00	/.....@.....
0c000f140	00 00 33 00 00 00 00 00-3F FD 32 00 00 00 00 00	---3-----?ý2----
0c000f150	3F FD 32 00 00 00 00 00-22 30 03 89 11 00 00 00	?ý2-----"0-----
0c000f160	FF FF FF FF 82 79 47 11-00 00 00 00 00 00 00 00	ýýýý-yG-----
0c000f170	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
0c000f180	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
0c000f190	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
0c000f1a0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
0c000f1b0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
0c000f1c0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
0c000f1d0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
0c000f1e0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
0c000f1f0	00 00 00 00 00 00 00 00-00 00 00 00 00 02 00	

(USB Artefakt 2[pre účely premetu snímok z kamerového systému uložený v pamäti]-”20260318 093535.jpg”)



(USB Artefakt 2.1.-snímok”20260318_093535.jpg”, neskôr premenovaný na „stache page screenshot.jpg“)

Fuzaty prípad - Autopsy 4.23.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing

All

Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
list of devices we print from.odt-RF2373fc45.TMP				2026-04-19 10:22:13 SELČ	2026-04-19 10:22:13 SELČ	2026-04-19 10:22:13 SELČ	2026-04-19 10:22:13 SELČ

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Metadata

Name: /img_USB image.001/vol_vo12/DFA files/list of devices we print from.odt-RF2373fc45.TMP

Type: File System

MIME Type: application/octet-stream

Size: 0

File Name Allocation: Unallocated

Metadata Allocation: Unallocated

Modified: 2026-04-19 10:22:13 SELČ

Accessed: 2026-04-19 10:22:13 SELČ

Created: 2026-04-19 10:22:13 SELČ

Changed: 2026-04-19 10:22:13 SELČ

(USB artefakt 3-vymazaný súbor na USB disku, staršia verzia dokumentu (zoznam zariadení z ktorých sa dokumenty tlačia))

Fuzaty pripad - Autopsy 4.23.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Listing Metadata 4 Results

Table Thumbnail Summary Save Table as CSV

Source Name	S	C	O	Version	Date Created	Date Modified	Data Source
</ dfa docpreview.pdf				1.4	2026-03-25 08:34:09 SEČ	2026-03-25 08:34:09 SEČ	USB image.001
</ dfa docpreview.pdf				1.4	2026-03-25 08:34:09 SEČ	2026-03-25 08:34:09 SEČ	USB image.001
</ benign list.odt					2026-04-19 10:09:17 SELČ	2026-04-19 10:13:32 SELČ	USB image.001
</ list of devices we print from.odt					2026-04-19 10:20:35 SELČ	2026-04-19 10:22:13 SELČ	USB image.001

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation

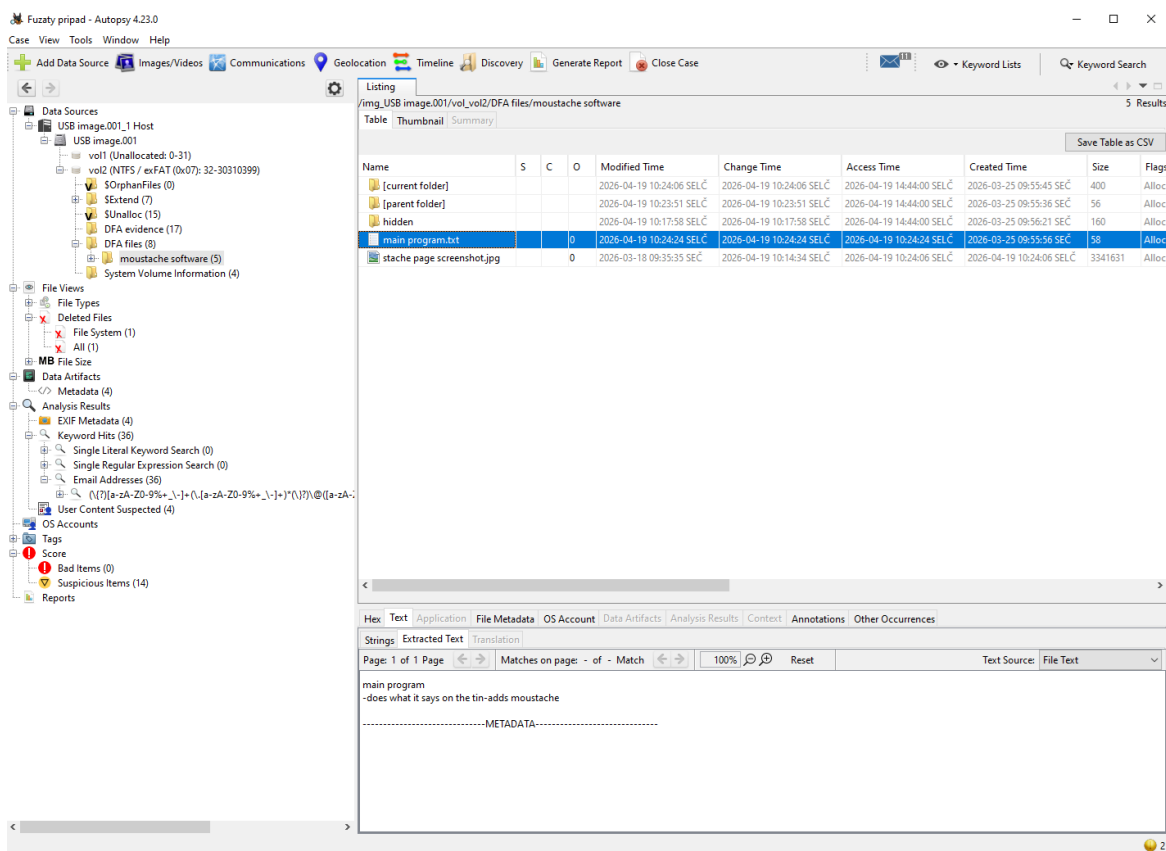
Page: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Source: File Text

Plan zartiku:
 1. pockaj kym Jozko po daco pojde
 2. priplichti sa k notebooku
 3. zapoj USB
 4. zapni softver
 5. ked program dobehne, USB odpoj

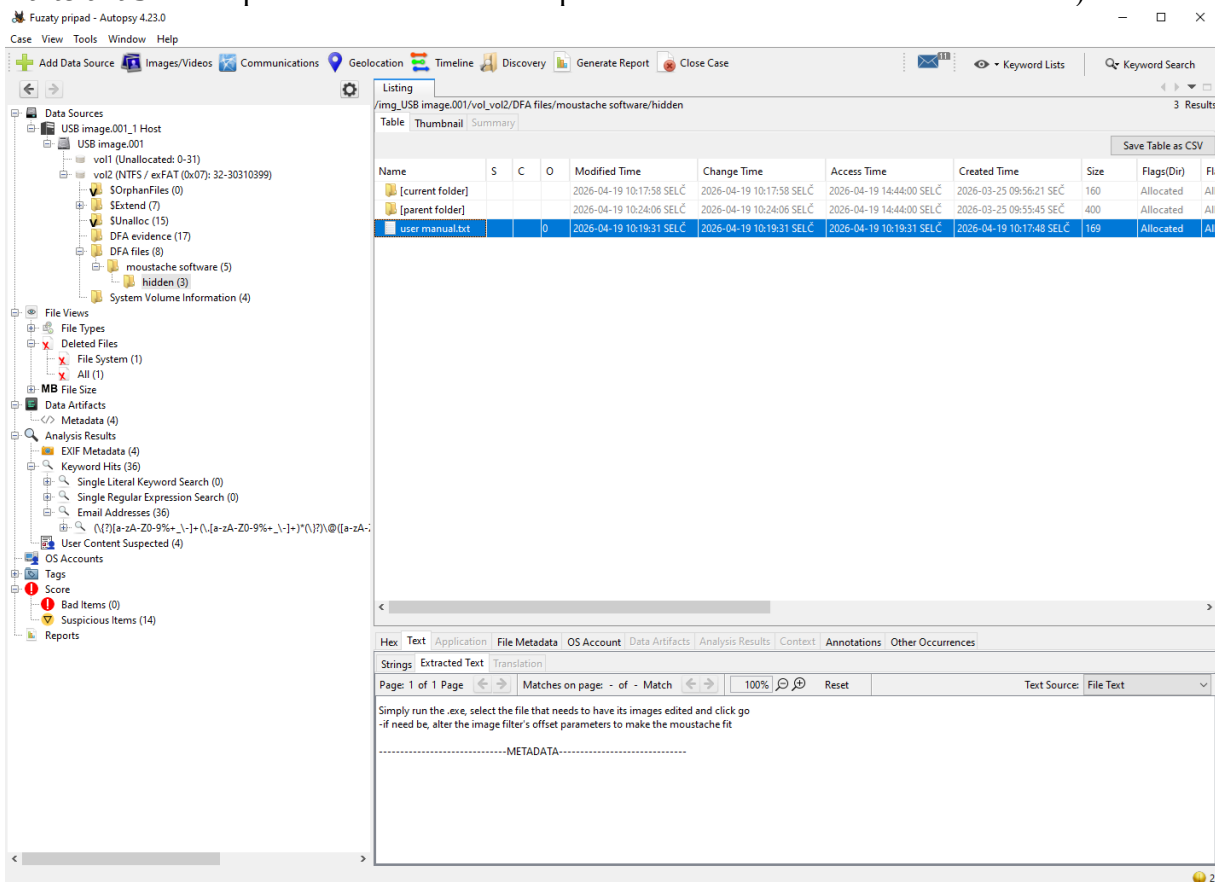
-----METADATA-----

Content-Type: application/vnd.oasis.opendocument.text
 X-TIKA:Parser-Bvc:om.apache.tika.parser.DefaultParser

(USB artefakt 4-textový obsah premenovaného dokumentu + metadáta, nájdená stopa po páchatel'ovi)



(USB artefakt 5-obsah priečinku na USB kľúči-priečinok DFA files/moustache software)



(USB artefakt 6-obsah priečinku na USB kľúči-DFA files/moustache software/hidden)

7.Zoznam použitých softvérových nástrojov a ich použitie

Exterro FTK Imager-Vytvorenie a čítanie image zariadenia spojeného s prípadom

HxD-Prístup ku a prehliadanie image súboru pre RAM

Magnet RAM Capture-Získanie image RAM-ky

LibreOffice Write-na vypísanie dokumentácie

Instability Workbench-spomenutý na hodine ako viac user-friendly ekvivalent HxD

Softvér firmy AXIOM-stiahnutý, ako nástroj na analýzu, no priamo na prípad nepoužitý

Autopsy-nástroj na analýzu dôkazov a ďalšie vyšetovanie

8.Bezpečnostné opatrenia

8.1. Jednotlivé bezpečnostné opatrenia

Zo zariadení nájdených na mieste činu boli vyhotovené image súbory pamäťových úložísk a RAM(v prípade notebooku) pamäte. Tieto boli nielen archivované(uložené na hard disk, ktorý bol zabalený do umelohmotného zatváracieho sáčku, odložený v zamknutej krabici), ale zároveň boli vytvorené zálohy, pre každé jedno, odložené inde. Tieto Image súbory boli zhotovené s pomocou write-blocker nástroja na zachovanie autenticity ich obsahu. Pre image súbory bol vypracovaný chain-of-custody a samotný fyzický USB kľúč je momentálne v úschove oddelenia DFA.

8.2. Chain-of-custody pre jednotlivé zariadenia:

Číslo:	1	Typ súboru:	Image USB, RAM	Obnovený súbor:		Veľkosť:	31GB
Popis prípadu:		Interná vandalizácia tlačovej publikácie, podozrenie, že na npadnutom hardvéri sú potenciálne škodlivé súbory					
Názov súboru:		USB kľúč „DFA_USB“(USB_image.raw), dáta z RAM (RAM_image.raw)					
Miesto získania digitálnej stopy:		Na pravdepodobnom mieste činu, v oddelení tlačovej firmy, z ktorého bola znehodnotená publikácia finalizovaná a posielaná do tlače					
Poznámky:		Image z USB, čo bol Marek kúpiť v nedeľu(8.3.) večer v Alze, zabezpečené v pôvodnom obale, pri notebooku(z ktorého pochádza RAM image)					
Časové pečiatky							
Access:	17:27(9.3.2026)		Modify:	13:20(12.4.2026)		Change:	N/A
Digitáln y odtlačok (heš)	MD5	8a23fa77df5549bd894f0e71d91336f3					
	SHA1	61a2b2879833a68d485c0fccddf234c622f1fc37					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
10:51(11.3.2026)		Spravený image USB kľúča(cez FTK Imager)					
13:20(12.4.2026)		Spravenie image-u RAM pamäte (cez Magnet Forensics RAM Capture)					

Literatúra

DFRWS: O data tamperingu, návrhy na experimenty s data tamperingom

<https://dfrws.org/presentation/prudent-design-principles-for-digital-tampering-experiments/>

DFRWS: USB ako platformy pre útoky

<https://dfrws.org/presentation/duck-hunt-memory-forensics-of-usb-attack-platforms/>

CFREDS: Dataset z DFRWS 2008 Rodeo – USB Images(nepoužité)

<https://cfreds.nist.gov/all/DFRWS2008Rodeo/DFRWS2008USBFlashDriveImages>

DFRWS: Forezná identifikácia modifikovania súborov v pamäti

<https://dfrws.org/presentation/windows-memory-forensics-identification-of-malicious-modifications-in-memory-mapped-image-files/>