

# **UNIVERZITA sv. CYRILA a METODA v TRNAVE**

**FAKULTA PRÍRODNÝCH VIED**

**Prezentácia**

**Nevera**

# 1. Popis prípadu

Predmetom vyšetrovania je podozrenie z mimomanželského vzťahu. Manželka podozrieva manžela z nevery na základe zmeneného správania, zvýšenej ochrany súkromia, častého používania mobilného zariadenia a náhleho fyzického poškodenia jeho elektronických zariadení.

Podľa domienok manželky, manžel úmyselne poškodil alebo zlikvidoval svoje digitálne zariadenia, pravdepodobne s cieľom zabrániť prístupu k potenciálne kompromitujúcim dátam.

## ● 5WH

### 1. Who

- a. Podozrivá osoba: Manžel
- b. Oznamovateľ: Manželka
- c. Potenciálna tretia osoba

### 2. What

- a. Podozrenie z mimomanželského vzťahu
- b. Úmyselné zničenie elektronických zariadení
- c. Možné zahladzovanie digitálnych stôp

### 3. When

- a. Zameranie sa na obdobie zvýšenej digitálnej aktivity

### 4. Where

- a. K nevere pravdepodobne dochádzalo primárne v digitálnej forme, takže väčšina dôkazov sa bude nachádzať v pamäti jednotlivých zariadení či v aplikáciách cez ktoré bola realizovaná komunikácia

### 5. Why

- a. Snaha utajiť mimomanželský vzťah
- b. Ochrana osobných alebo kompromitujúcich informácií
- c. Nešťastná náhoda alebo impulzívna reakcia

### 6. How

- a. Komunikácia pravdepodobne prebiehala cez sociálne siete a mobilné telefóny prostredníctvom telefonických hovorov
- b. K následnému zničeniu notebooku došlo vystavním vode a mobilný telefón bol poškodený fyzickým nárazom

- **Odborný príspevok**

**Názov práce:** Syntactical File Carving and Automated Generation of Reproducible Datasets

**Zdroj:** DFRWS / Forensic Science International: Digital Investigation

**Odkaz:**

<https://dfrws.org/presentation/syntactical-file-carving-and-automated-generation-of-reproducible-datasets/>

**Stručný popis príspevku k prípadu:**

Tento článok sa zaoberá problematikou obnovy dát (file carving), konkrétne v prípadoch, kedy sú súbory na úložisku fragmentované.

## 2. Hypotézy

1. Komunikácia existovala, ale nešlo o fyzickú neveru
  - a. Existovala emocionálna alebo flirtujúca komunikácia, no nedošlo k fyzickému stretnutiu. Poškodenie zariadení bolo reakciou na obavu z konfliktu. - Vyvrátené
2. K nevere došlo, zariadenia boli poškodené úmyselne
  - a. Manžel udržiaval mimomanželský vzťah a po konfrontácii poškodil zariadenia, aby eliminoval dôkazy. - Potvrdené
3. K nevere nedošlo, zariadenia boli poškodené náhodou či z iných dôvodov
  - a. Manžel nezahŕňal tretiu osobu; zariadenia poškodil nedopatrením alebo z dôvodu ochrany iného súkromného obsahu (napr. finančné problémy, osobné údaje). - Vyvrátené

- **Očakávaný výsledok**

- **Technický fakt:**
  - V pamäťových médiách zariadení sa podarí nájsť relevantné dáta
- **Motív:**
  - Obsah komunikácie naznačí existenciu nadštandardného vzťahu s cudzou osobou
- **Súvislosť zariadení:**
  - Obsah USB môže obsahovať zálohy fotografií alebo iné relevantné dáta.
- **Záver o úmysle:**

- Kombinácia fyzického poškodenia notebooku, mobilného telefónu a vyhodenia USB média bude vyhodnotená ako koordinovaný zásah smerujúci k pokusu o znemožnenie prístupu k digitálnym dôkazom.

### 3. Digitálne zariadenia

| Dôkazový materiál                                                        | Potenciálne stopy                | Formáty súborov         |
|--------------------------------------------------------------------------|----------------------------------|-------------------------|
| Notebook -<br>Dell Latitude E5440,<br>320 GB pamäť                       | Multimediálne súbory a dokumenty | .jpg, .docx, EXIF údaje |
| Mobilný telefón -<br>Xiaomi Redmi 6, 64GB<br>pamäť                       | Chatová história, výpisy hovorov | .json, .jpg             |
| USB kľúč -<br>Silicon Power Ultima<br>U02, USB 2.0, USB-A,<br>8 GB pamäť | Zálohy fotografií a súborov      | Všetky uvedené vyššie   |

#### ● Zadržané zariadenia

##### 1. Notebook -

- a. Dell Latitude E5440
- b. 320 GB pamäť
  - Rýchlosť: 80-120 MB/s
  - Prístupová doba: 5-15 ms
- c. 8GB RAM pamäte
  - Rýchlosť: 12-25 GB/s
  - Prístupová doba: 50-70 ns





## 2. Mobilný telefón -

- a. Xiaomi Redmi 6
- b. 64GB pamäť
- c. 4GB RAM pamäte
  - Rýchlosť: 5-15 GB/s
  - Prístupová doba: 50-100 ns



## 3. USB kľúč -

- a. Silicon Power Ultima U02
- b. Typ : USB 2.0, USB-A
- c. 8 GB pamäť
  - Rýchlosť: 15-30 MB/s
  - Prístupová doba: 1 ms



## 4. Dáta

### • Notebook

- Veľkosť datasetu: 1,79 GB
- Veľkosť reálnych dát: 1,79 GB
- Počet súborov: 1704 súborov
- Odkaz na dataset: Používané boli vlastné a generované dáta

### • Mobilný telefón

- Veľkosť datasetu: 533 MB
- Veľkosť reálnych dát: 533 MB
- Počet súborov: 204 súborov
- Odkaz na dataset: Používané boli vlastné a generované dáta

### • USB kľúč

- Veľkosť datasetu: 460 MB
- Veľkosť reálnych dát: 460 MB
- Počet súborov: 227 súborov
- Odkaz na dataset: Používané boli vlastné a generované dáta

## 5. RAM image

| Offset (h) | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | Decoded text     |
|------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------------------|
| 81D121E50  | 72 | 6E | E1 | 20 | 6B | 61 | 6E | 76 | 69 | 63 | 61 | 00 | 00 | 80 | F8 | FF | rná kanvica..Ěř  |
| 81D121E60  | D0 | 00 | 00 | 00 | 0A | 00 | 00 | 00 | 43 | 00 | 68 | 00 | 6C | 00 | 61 | 00 | Ď.....C.h.l.a.   |
| 81D121E70  | 64 | 00 | 6E | 00 | 69 | 00 | 0D | 01 | 6B | 00 | 61 | 00 | 58 | 22 | FE | FF | d.n.i...k.a.X"ť  |
| 81D121E80  | D0 | 04 | 00 | 00 | 11 | 00 | 00 | 00 | 70 | 6F | 77 | 65 | 72 | 2D | 63 | 6F | Ď.....power-co   |
| 81D121E90  | 6E | 73 | 75 | 6D | 70 | 74 | 69 | 6F | 6E | 9A | 72 | 43 | E9 | 1C | FB | FF | nsumptionšrCé.ů  |
| 81D121EA0  | D0 | 04 | 00 | 00 | 12 | 00 | 00 | 00 | 72 | 65 | 66 | 75 | 6E | 64 | 61 | 62 | Ď.....refundab   |
| 81D121EB0  | 6C | 65 | 2D | 64 | 65 | 70 | 6F | 73 | 69 | 74 | 68 | A8 | 77 | 24 | FE | FF | le-deposith"wšť  |
| 81D121EC0  | D0 | 04 | 00 | 00 | 18 | 00 | 00 | 00 | 66 | 6C | 65 | 78 | 20 | 6D | 64 | 3A | Ď.....flex md:   |
| 81D121ED0  | 67 | 61 | 70 | 2D | 78 | 2D | 31 | 32 | 20 | 67 | 61 | 70 | 2D | 78 | 2D | 33 | gap-x-l2 gap-x-3 |
| 81D121EE0  | D0 | 04 | 00 | 00 | 16 | 00 | 00 | 00 | 50 | 65 | 6E | 7A | 69 | F3 | 6E | 20 | Ď.....Penzión    |
| 81D121EF0  | 42 | 65 | 74 | E1 | 6E | 69 | 61 | 20 | 76 | 20 | 6C | 65 | 74 | 65 | 00 | 00 | Betánia v lete.. |
| 81D121F00  | D0 | 04 | 00 | 00 | 13 | 00 | 00 | 00 | 48 | 6F | 74 | 65 | 6C | 20 | 5A | E1 | Ď.....Hotel Zá   |
| 81D121F10  | 74 | 6F | 6B | 61 | 20 | 76 | 20 | 6C | 65 | 74 | 65 | 00 | 00 | 80 | F8 | FF | toka v lete..Ěř  |
| 81D121F20  | D0 | 04 | 00 | 00 | 17 | 00 | 00 | 00 | 41 | 70 | 61 | 72 | 74 | 6D | E1 | 6E | Ď.....Apartmán   |
| 81D121F30  | 79 | 20 | 50 | 75 | 65 | 72 | 74 | 6F | 20 | 76 | 20 | 6C | 65 | 74 | 65 | 00 | y Puerto v lete. |
| 81D121F40  | D0 | 04 | 00 | 00 | 14 | 00 | 00 | 00 | 43 | 68 | 61 | 74 | 61 | 20 | 53 | 65 | Ď.....Chata Se   |
| 81D121F50  | 76 | 65 | 72 | 6B | 61 | 20 | 76 | 20 | 6C | 65 | 74 | 65 | FC | 7F | 00 | 00 | verka v leteü... |
| 81D121F60  | D0 | 04 | 00 | 00 | 12 | 00 | 00 | 00 | 45 | 78 | 70 | 65 | 63 | 74 | 65 | 64 | Ď.....Expected   |
| 81D121F70  | 20 | 61 | 74 | 20 | 6C | 65 | 61 | 73 | 74 | 20 | 4B | 4B | 4B | 4B | 4B | 4B | at least KKKKKK  |
| 81D121F80  | D0 | 04 | 00 | 00 | 11 | 00 | 00 | 00 | 45 | 78 | 70 | 65 | 63 | 74 | 65 | 64 | Ď.....Expected   |
| 81D121F90  | 20 | 61 | 74 | 20 | 6D | 6F | 73 | 74 | 20 | 4B | 4B | 4B | 4B | 4B | 4B | 4B | at most KKKKKKK  |
| 81D121FA0  | D0 | 04 | 00 | 00 | 12 | 00 | 00 | 00 | 75 | 6E | 68 | 61 | 6E | 64 | 6C | 65 | Ď.....unhandle   |
| 81D121FB0  | 64 | 72 | 65 | 6A | 65 | 63 | 74 | 69 | 6F | 6E | 4B | 4B | 4B | 4B | 4B | 4B | drejectionKKKKKK |

*Zápis v pamäti RAM - Vyhľadavanie hotelov*

|            |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |                  |
|------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------------------|
| 7A773BBB0  | 6A | 73 | 5F | 6C | 6F | 63 | 61 | 74 | 69 | 6F | 6E | 5F | 77 | 77 | 77 | 5F | js_location_www_ |
| 7A773BBC0  | 70 | 70 | 5F | 6D | 61 | 70 | 5F | 73 | 65 | 61 | 72 | 63 | 68 | 5F | 69 | 74 | pp_map_search_it |
| 7A773BBDB0 | 65 | 6D | 73 | 5F | 61 | 64 | 64 | 65 | 64 | 5F | 31 | 30 | 00 | 00 | 00 | 00 | ems_added_10.... |
| 7A773BBE0  | 6A | 73 | 5F | 6C | 6F | 63 | 61 | 74 | 69 | 6F | 6E | 5F | 77 | 77 | 77 | 5F | js_location_www_ |
| 7A773BBF0  | 70 | 70 | 5F | 6D | 61 | 70 | 5F | 73 | 65 | 61 | 72 | 63 | 68 | 5F | 69 | 74 | pp_map_search_it |
| 7A773BC00  | 65 | 6D | 73 | 5F | 61 | 64 | 64 | 65 | 64 | 5F | 35 | 00 | 00 | 00 | 00 | 00 | ems_added_5....  |
| 7A773BC10  | 6C | 6F | 63 | 61 | 74 | 69 | 6F | 6E | 42 | 6C | 6F | 63 | 6B | 43 | 6F | 6E | locationBlockCon |
| 7A773BC20  | 74 | 65 | 6E | 74 | 43 | 6F | 6E | 74 | 61 | 69 | 6E | 65 | 72 | 57 | 69 | 74 | tentContainerWit |
| 7A773BC30  | 68 | 4D | 61 | 70 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | hMap.....        |
| 7A773BC40  | 63 | 75 | 73 | 74 | 6F | 6D | 56 | 61 | 6C | 75 | 65 | 20 | 6F | 72 | 20 | 69 | customValue or i |
| 7A773BC50  | 64 | 20 | 6D | 75 | 73 | 74 | 20 | 62 | 65 | 20 | 70 | 72 | 65 | 73 | 65 | 6E | d must be presen |
| 7A773BC60  | 74 | 2E | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | t.....           |
| 7A773BC70  | 5A | 00 | 6F | 00 | 62 | 00 | 72 | 00 | 61 | 00 | 7A | 00 | 69 | 00 | 65 | 01 | Z.o.b.r.a.z.i.e. |
| 7A773BC80  | 20 | 00 | 69 | 00 | 6E | 00 | E9 | 00 | 20 | 00 | 6F | 00 | 74 | 00 | E1 | 00 | .i.n.é. .o.t.á.  |
| 7A773BC90  | 7A | 00 | 6B | 00 | 79 | 00 | 20 | 00 | 28 | 00 | 32 | 00 | 30 | 00 | 29 | 00 | z.k.y. .(.2.0.). |
| 7A773BCA0  | 61 | 70 | 70 | 6C | 69 | 63 | 61 | 74 | 69 | 6F | 6E | 2F | 78 | 2D | 70 | 72 | application/x-pr |
| 7A773BCB0  | 6F | 74 | 6F | 62 | 75 | 66 | 2D | 6A | 73 | 6F | 6E | 2D | 66 | 6F | 72 | 6D | otobuf-json-form |
| 7A773BCC0  | 61 | 74 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | at.....          |
| 7A773BCD0  | 65 | 57 | 48 | 4D | 45 | 4A | 4B | 61 | 45 | 64 | 48 | 49 | 4E | 65 | 43 | 65 | eWHMEJKaEcHINaCe |
| 7A773BCE0  | 51 | 63 | 4A | 5A | 57 | 44 | 62 | 51 | 4D | 64 | 4F | 65 | 57 | 55 | 41 | 65 | QcJZWDbQMdOeWUAe |
| 7A773BCF0  | 63 | 4F | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | cO.....          |
| 7A773BD00  | 68 | 70 | 5F | 64 | 65 | 73 | 6B | 74 | 6F | 70 | 5F | 66 | 61 | 63 | 69 | 6C | hp_desktop_facil |
| 7A773BD10  | 69 | 74 | 69 | 65 | 73 | 5F | 6C | 69 | 73 | 74 | 5F | 63 | 6C | 6F | 73 | 65 | ities_list_close |
| 7A773BD20  | 64 | 5F | 6D | 75 | 6C | 74 | 69 | 70 | 6C | 65 | 5F | 64 | 61 | 74 | 65 | 73 | d_multiple_dates |
| 7A773BD30  | 56 | 79 | 62 | 61 | 76 | 65 | 6E | 69 | 65 | 20 | 2D | 20 | 45 | 6E | 73 | 61 | Vybavenie - Ensa |
| 7A773BD40  | 6E | 61 | 20 | 54 | 68 | 65 | 72 | 6D | 69 | 61 | 20 | 50 | 61 | 6C | 61 | 63 | na Thermia Palac |
| 7A773BD50  | 65 | E5 | E5 | E5 | E5 | E5 | E5 | E5 | E5 | E5 | E5 | E5 | E5 | E5 | E5 | E5 | eiíííííííííííííí |
| 7A773BD60  | 56 | 79 | 62 | 61 | 76 | 65 | 6E | 69 | 65 | 20 | 2D | 20 | 45 | 6E | 73 | 61 | Vybavenie - Ensa |
| 7A773BD70  | 6E | 61 | 20 | 54 | 68 | 65 | 72 | 6D | 69 | 61 | 20 | 50 | 61 | 6C | 61 | 63 | na Thermia Palac |
| 7A773BD80  | 65 | E5 | E5 | E5 | E5 | E5 | E5 | E5 | E5 | E5 | E5 | E5 | E5 | E5 | E5 | E5 | eiíííííííííííííí |

*Zápis v pamäti RAM - Fragment súvisjúci s vyhľadávaním hotelových služieb*

| Offset(h) | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | Decoded text      |
|-----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|-------------------|
| 81494FC70 | 09 | 68 | 74 | 74 | 70 | 73 | 3A | 2F | 2F | 77 | 77 | 77 | 2E | 67 | 6F | 6F | .https://www.goo  |
| 81494FC80 | 67 | 6C | 65 | 2E | 63 | 6F | 6D | 2F | 73 | 65 | 61 | 72 | 63 | 68 | 3F | 63 | gle.com/search?c  |
| 81494FC90 | 6C | 69 | 65 | 6E | 74 | 3D | 66 | 69 | 72 | 65 | 66 | 6F | 78 | 2D | 62 | 2D | lient=firefox-b-  |
| 81494FCA0 | 64 | 26 | 71 | 3D | 6E | 6F | 63 | 6E | 65 | 2B | 73 | 70 | 6F | 6A | 65 | 2B | d&q=nocne+spoje+  |
| 81494FCB0 | 62 | 72 | 61 | 74 | 69 | 73 | 6C | 61 | 76 | 61 | 6E | 6F | 63 | 6E | 65 | 20 | bratislavanocne   |
| 81494FCC0 | 73 | 70 | 6F | 6A | 65 | 20 | 62 | 72 | 61 | 74 | 69 | 73 | 6C | 61 | 76 | 61 | spoje bratislava  |
| 81494FCD0 | 20 | 2D | 20 | 48 | C4 | BE | 61 | 64 | 61 | C5 | A5 | 20 | 47 | 6F | 6F | 67 | - HÄIadaĽÄ Goog   |
| 81494FCE0 | 6C | 6F | 6D | 6D | 6F | 63 | 2E | 65 | 6C | 67 | 6F | 6F | 67 | 2E | 77 | 77 | lommoc.elgoog.w   |
| 81494FCF0 | 77 | 2E | 50 | DB | 00 | 06 | 4D | 49 | 14 | 6D | E2 | 68 | 47 | 42 | 52 | 58 | w.PŮ..MI.mâhGBRX  |
| 81494FD00 | 73 | 50 | 4D | 6A | 41 | 39 | 58 | 6C | 2B | 12 | 47 | B8 | A9 | 59 | 03 | 82 | sPMjA9Xl+.G,©Y.,  |
| 81494FD10 | 1E | AB | 72 | 16 | 00 | 81 | 1D | 45 | 37 | 09 | 08 | 08 | 02 | 06 | 25 | 08 | .«r....E7.....%.  |
| 81494FD20 | 05 | 81 | 09 | 73 | 00 | 02 | 08 | 00 | 09 | 68 | 74 | 74 | 70 | 73 | 3A | 2F | ...s.....https:/  |
| 81494FD30 | 2F | 77 | 77 | 77 | 2E | 64 | 69 | 73 | 6B | 75 | 73 | 6E | 65 | 66 | 6F | 72 | /www.diskusnefor  |
| 81494FD40 | 75 | 6D | 2E | 73 | 6B | 2F | 74 | 65 | 6D | 61 | 2F | 61 | 6B | 6F | 2D | 73 | um.sk/tema/ako-s  |
| 81494FD50 | 70 | 72 | 61 | 76 | 6E | 65 | 2D | 75 | 74 | 61 | 6A | 69 | 74 | 2D | 6D | 69 | pravne-utajit-mi  |
| 81494FD60 | 6C | 65 | 6E | 63 | 61 | 3F | 68 | 6C | 3D | 69 | 6E | 74 | 65 | 72 | 6E | 65 | lenca?hl=interne  |
| 81494FD70 | 74 | 41 | 6B | 6F | 20 | 73 | 70 | 72 | C3 | A1 | 76 | 6E | 65 | 20 | 75 | 74 | tAko sprÄ~vne ut  |
| 81494FD80 | 61 | 6A | 69 | C5 | A5 | 20 | 6D | 69 | 6C | 65 | 6E | 63 | 61 | 6B | 73 | 2E | ajiĽÄ milencaks.  |
| 81494FD90 | 6D | 75 | 72 | 6F | 66 | 65 | 6E | 73 | 75 | 6B | 73 | 69 | 64 | 2E | 77 | 77 | murofensuksid.w   |
| 81494FDA0 | 77 | 2E | 50 | DB | 00 | 06 | 4D | 49 | 11 | FC | A0 | 00 | 76 | 6A | 5F | 65 | w.PŮ..MI.ü .vj_e  |
| 81494FDB0 | 77 | 75 | 71 | 37 | 67 | 75 | 76 | 43 | 2B | 12 | 31 | E3 | 5F | 53 | 53 | 6C | wuq7gucvC+.lä SS1 |
| 81494FDC0 | 6F | 76 | 65 | 6E | 73 | 6B | 6F | 2D | C4 | 8D | 65 | 73 | 6B | C3 | BD | 20 | ovensko-ÄĽeskÄ~   |
| 81494FDD0 | 6E | 65 | 7A | C3 | A1 | 76 | 69 | 73 | 6C | C3 | BD | 20 | 64 | 69 | 73 | 6B | nezÄ~vislä~ disk  |
| 81494FDE0 | 75 | 73 | 6E | C3 | BD | 20 | 73 | 65 | 72 | 76 | 65 | 72 | 20 | 70 | 72 | 65 | usnä~ server pre  |
| 81494FDF0 | 20 | 76 | C5 | A1 | 65 | 74 | 6B | C3 | BD | 63 | 68 | 2E | 68 | 74 | 74 | 70 | vĽ~etkÄ~ch.http   |
| 81494FE00 | 73 | 3A | 2F | 2F | 77 | 77 | 77 | 2E | 64 | 69 | 73 | 6B | 75 | 73 | 6E | 65 | s://www.diskusne  |
| 81494FE10 | 66 | 6F | 72 | 75 | 6D | 2E | 73 | 6B | 2F | 69 | 6D | 61 | 67 | 65 | 73 | 2F | forum.sk/images/  |
| 81494FE20 | 6C | 6F | 67 | 6F | 43 | 72 | 61 | 77 | 6C | 65 | 72 | 2E | 6A | 70 | 67 | 02 | logoCrawler.jpg.  |
| 81494FE30 | 74 | 84 | 11 | AB | 71 | 17 | 00 | 81 | 43 | 53 | 31 | 09 | 08 | 08 | 02 | 06 | t„.«q...CS1.....  |
| 81494FE40 | 25 | 08 | 05 | 84 | 27 | 81 | 0B | 00 | 02 | 08 | 00 | 09 | 68 | 74 | 74 | 70 | %...„'.....http   |
| 81494FE50 | 73 | 3A | 2F | 2F | 77 | 77 | 77 | 2E | 6D | 6F | 64 | 72 | 79 | 6B | 6F | 6E | s://www.modrykon  |
| 81494FE60 | 69 | 6B | 2E | 73 | 6B | 2F | 66 | 6F | 72 | 75 | 6D | 2F | 76 | 7A | 74 | 61 | ik.sk/forum/vzta  |
| 81494FE70 | 68 | 79 | 2D | 6D | 61 | 6E | 7A | 65 | 6C | 73 | 6B | 65 | 2D | 70 | 61 | 72 | hy-manzelske-par  |
| 81494FE80 | 74 | 6E | 65 | 72 | 73 | 6B | 65 | 2D | 70 | 72 | 69 | 61 | 74 | 65 | 6C | 73 | tnerske-priatels  |
| 81494FE90 | 6B | 65 | 2F | 6D | 61 | 6E | 7A | 65 | 6C | 2D | 6D | 61 | 2D | 6D | 69 | 6C | ke/manzel-ma-mil  |
| 81494FEA0 | 65 | 6E | 6B | 75 | 2D | 34 | 2F | 4D | 61 | 6E | C5 | BE | 65 | 6C | 20 | 6D | enku-4/ManĽiel m  |
| 81494FEB0 | C3 | A1 | 20 | 6D | 69 | 6C | 65 | 6E | 6B | 75 | 20 | 2D | 20 | 4D | 6F | 64 | Ä~ milenku - Mod  |
| 81494FEC0 | 72 | C3 | BD | 20 | 6B | 6F | 6E | C3 | AD | 6B | 6B | 73 | 2E | 6B | 69 | 6E | rÄ~ konÄ.kks.kin  |
| 81494FED0 | 6F | 6B | 79 | 72 | 64 | 6F | 6D | 2E | 77 | 77 | 77 | 2E | 50 | DB | 00 | 06 | okyrdom.www.PŮ..  |
| 81494FEE0 | 4D | 49 | 11 | 93 | B0 | B8 | 32 | 6F | 42 | 30 | 6F | 69 | 77 | 41 | 48 | 66 | MI.~°,2oB0oiwAHf  |
| 81494FEF0 | 50 | 46 | 2B | 12 | 23 | 79 | 8B | F9 | 41 | 68 | 6F | 6A | 74 | 65 | 20 | 2C | PF+.#y<ûAhojte ,  |
| 81494FF00 | 4E | 65 | 76 | 69 | 65 | 6D | 20 | C4 | 8D | 69 | 20 | 70 | 6F | 74 | 72 | 65 | Neviem ÄĽi potre  |
| 81494FF10 | 62 | 75 | 6A | 65 | 6D | 20 | 70 | 6F | 6D | 6F | 63 | 2C | 20 | C4 | 8D | 69 | bujem pomoc, ÄĽi  |
| 81494FF20 | 20 | 69 | 62 | 61 | 20 | 76 | 79 | 70 | 6F | C4 | 8D | 75 | 74 | 69 | 65 | 2E | iba vypoÄĽutie.   |
| 81494FF30 | 20 | C4 | 8C | 6F | 20 | 72 | 6F | 62 | 69 | C5 | A5 | 20 | 61 | 6B | 6F | 20 | ÄSo robiĽÄ ako    |
| 81494FF40 | 73 | 61 | 20 | 73 | 20 | 74 | C3 | BD | 6D | 20 | 76 | 79 | 72 | 6F | 76 | 6E | sa s tÄ~m vyrovn  |
| 81494FF50 | 61 | C5 | A5 | 20 | 3F | 20 | 4D | 61 | 6E | 7A | 65 | 6C | 20 | 6D | 61 | 20 | aĽÄ ? Manzel ma   |
| 81494FF60 | 37 | 20 | 72 | 6F | 6B | 6F | 76 | 20 | 6D | 69 | 6C | 65 | 6E | 6B | 75 | 20 | 7 rokov milenku   |
| 81494FF70 | 2C | 20 | 61 | 6E | 69 | 20 | 73 | 6F | 6D | 20 | 74 | 6F | 20 | 6E | 65 | 74 | , ani som to net  |
| 81494FF80 | 75 | C5 | A1 | 69 | 6C | 61 | 20 | 64 | 6F | 6D | 61 | 20 | 62 | 6F | 6C | 6F | uĽ~ila doma bolo  |
| 81494FF90 | 20 | 76 | C5 | BE | 64 | 79 | 20 | 76 | C5 | A1 | 65 | 74 | 6B | 6F | 20 | 72 | vĽIdy vĽ~etko r   |
| 81494FFA0 | 6F | 76 | 6E | 61 | 6B | 6F | 20 | 61 | 20 | 76 | 20 | 70 | 6F | 72 | 69 | 61 | ovnako a v poria  |

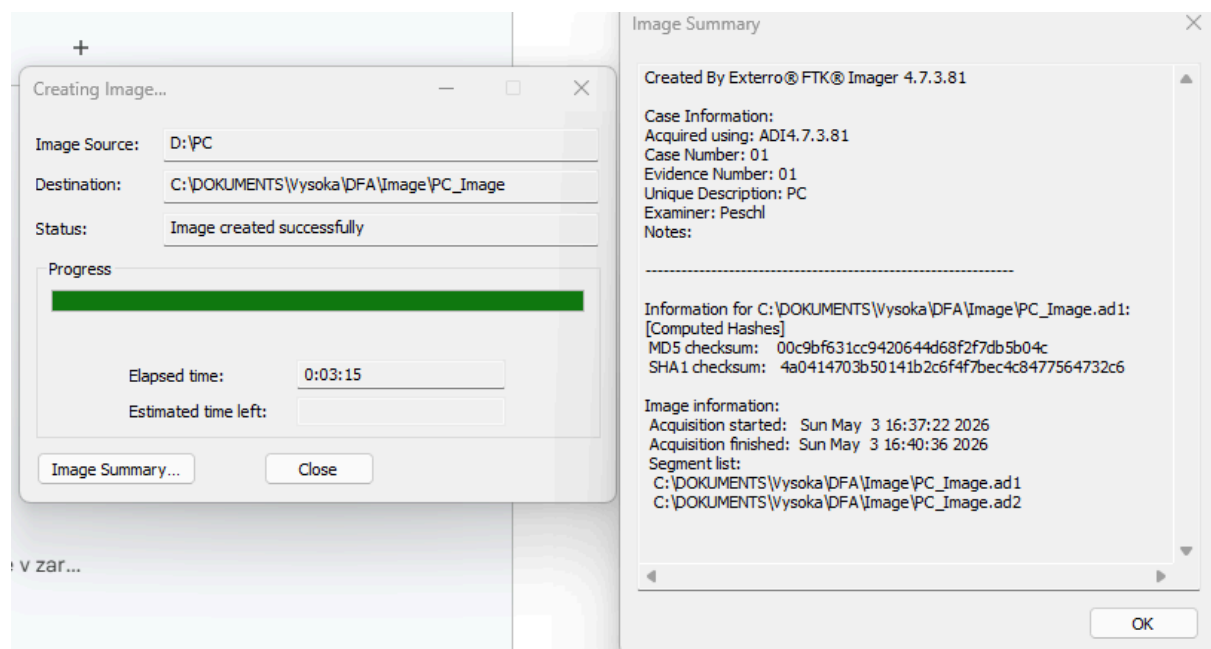
*ZÄpís v pamÄti RAM - VyhĽadÄvanie spÄsobov ako utajit' milenku*

6F 76 6E 61 6B 6F 20 61 20 76 20 70 6F 72 69 61 ovnako a v poria  
64 6B 75 20 2C 20 73 65 78 20 6D 61 6D 65 20 73 dku , sex mame s  
C3 AD 63 65 20 6D 6F C5 BE 6E 6F 20 74 61 6B 20 Ā.ce moĹIno tak  
72 61 7A 20 64 6F 20 6D 65 73 69 61 63 61 20 2C raz do mesiaca ,  
61 6C 65 20 6D 79 73 6C 65 6C 61 20 73 6F 6D 20 ale myslela som  
73 69 20 2C C5 BE 65 20 6A 65 20 74 6F 20 70 6F si ,ĹIe je to po

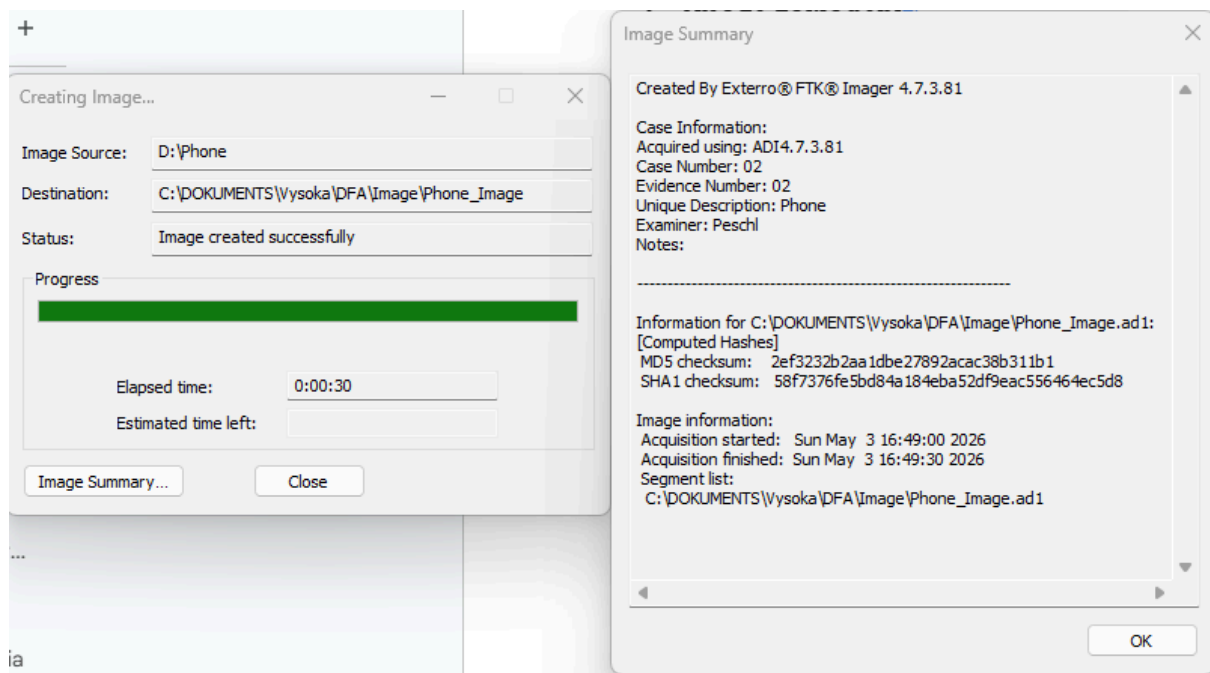
*Zápis v pamäti RAM - Podozrivý záznam so sexuálnym podnetom*

## 6. Image zariadení

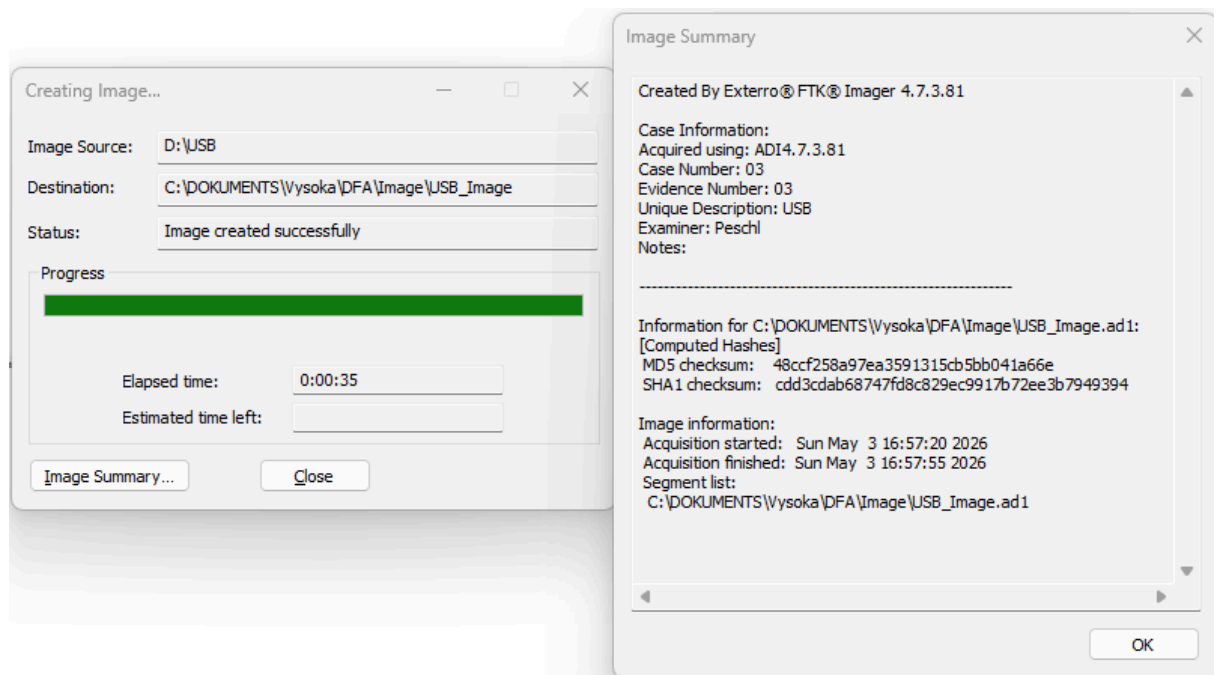
- Notebook



- Mobilný telefón



- USB





- **Dôkazy nájdené v zariadeniach**

- **Notebook - Dell Latitude E5440**

V notebooku sa primárne našli zápisky formou denníku, v ktorých sa pravdepodobne podozrivý snažil vyventilovať, tým, že si všetko spíše.

Listing

Office

TableThumbnailSummary

Page: 1 of 1Pages:Go to Page:

Name

S

C

O

Modified Time

Change Time

Access Time

Zápisky.docx

1

2026-03-25 08:26:00 CET

0000-00-00 00:00:00

2026-03-30 00:00:00 CEST

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Strings

Extracted Text

Translation

Page: 1 of -Page:Matches on page: - of -Match100%Reset

Deň 1 – Pondelok

Neplánoval som, že sa to stane. Aspoň si to tak hovorím. Bola to len správa, potom ďalšia. Nič vážne.

Dnes som si prvýkrát uvedomil, že začínam niečo skrývať. Otočil som telefón displejom dole, keď vošla do miestnosti. Automaticky.

Je zvláštne, ako rýchlo sa z obvyčajnej konverzácie stane tajomstvo.

Deň 2 – Streda

Začal som mazať správy. Najprv len tie „nevinné“, ktoré by mohli vyzeráť zle.

Ale potom som si uvedomil, že aj ich mazanie vyzerá podozrivo.

Digitálne stopy... viem, že úplne nezmiznú. História, zálohy, synchronizácie. Všetko niekde zostáva.

A predsa to robím ďalej.

Deň 3 – Sobota

Zmenil som si heslo na telefóne. Povedal som si, že je to kvôli bezpečnosti.

Nie je.

Keď bola dnes blízko mňa, cítil som zvláštny nepokoj. Ako keby videla cez mňa. Ako keby vedela.

Začínam si uvedomovať, že nežijem jeden život, ale dva. A tie sa raz musia stretnúť.

Deň 4 – Pondelok

Dnes som si dával pozor na čas. Kedy píšem, kedy odpovedám, kde som prihlásený.

Vypol som notifikácie. Skryl aplikáciu do priečinka.

Nikdy by som nepovedal, že budem premýšľať ako niekto, kto sa snaží zakryť digitálne stopy.

Je to ako hra. Lenže s realnými následkami.

Deň 5 – Piatok

Takmer som sa prezradil. Prišla správa, keď sme sedeli spolu.

Rýchlo som ju zmazal, ale ten moment... ten strach...

Začínam byť paranoidný. Každý zvuk notifikácie ma vyruší. Každý jej pohľad analyzujem.

Nie je to už o tom druhom človeku. Je to o tom, čo robím ja.

Deň 6 – Sobota

Dnes som premýšľal, čo by sa stalo, keby sa pozrela do záloh. Do histórie účtu. Do starých dát.

Technológia si pamätá viac než ľudia.

A ja viem, že keby chcela, mohla by nájsť všetko. Stačí vedieť, kde hľadať.

Možno podceňujem, ako ľahko sa dá pravda zrekonštruovať.

Deň 7 – Nedela

Už to nie je vzrušujúce. Už je to len ťažké.

Každý krok je vypočítaný, každé slovo kontrolované.

Stratil som pokoj. A možno aj niečo viac.

Najhoršie je, že viem – keby sa na to niekto pozrel ako na forenzný prípad, všetko by do seba zapadlo. Vzory správania, časové stopy, zmazané dáta.

Pravda tam je. Len ešte nebola odhalená.

METADATA

Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document

X-TIKA:Parsed-By: org.apache.tika.parser.DefaultParser

*Osobné zápisky dokumentujúce úzkosti manžela*

Súpisový.docx

1

2026-03-25 08:49:54 CET

0000-00-00 00:00:00

2026-05-03 00:00:00 CEST

2026-03-30 22:32:39 CEST

7468

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Strings

Extracted Text

Translation

Page: 1 of - Page

Matches on page: - of - Match

100%

Reset

Dnes sme sa mali stretnúť. Celý deň som bol nervózný. Kontroloval som telefón, či som niečo nezabudol vymazať. Správy, históriu, dokonca aj trasu v mapách. Je zvláštne, ako veľa priprav si vyžaduje jedno obyčajné stretnutie. Nie kvôli nej... ale kvôli tomu, aby som to utajil.

Večer

Stretili sme sa na mieste, kde ma nikto nepozná. Aspoň som si to myslel.

Každý zvuk auta ma vyrušil. Každý okoloidúci bol potenciálne riziko. Nedokázal som sa uvoľniť.

Keď som sa pozrel na telefón, uvedomil som si, že ho kontrolujem viac než ju. Či niekto nepísal. Či sa niečo neprezradilo.

Dohodili sme sa na večeri. Vybral som miesto mimo bežných trás. Reštauráciu, kde som nikdy predtým nebol.

Ešte pred odchodom som vypol niektoré notifikácie a skontroloval aplikácie. Premýšľal som, či by niekto vedel spätne zistiť, kde som bol. História polohy, platba kartou... všetko sú stopy.

Aj tak som išiel.

Večer

Sedeli sme pri stole, tmené svetlo, hudba v pozadí. Navonok normálny večer.

Ale ja som sa nedokázal sústrediť. Keď som zaplatil kartou, okamžite mi napadlo, že existuje záznam. Presný čas, presné miesto.

Na chvíľu som oľutoval, že som nepoužil hotovosť.

Každý detail sa mi v hlave mení na potenciálny dôkaz.

METADATA

Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document

X-TIKA:Parsed-By: org.apache.tika.parser.DefaultParser

extended-properties:DocSecurityString: None

*Osobné zápisky dokumentujúce priebeh stretnutí*

- **Mobilný telefón - Xiaomi Redmi 6**  
Mobilný telefón obsahoval súkromné konverzácie, ktoré naznačovali prebiehajúcu neveru, ako aj spoločné fotky z tajných výletov či stretnutí.

| Name           | S | C | O | Modified Time            | Change Time         | Access Time              |
|----------------|---|---|---|--------------------------|---------------------|--------------------------|
| message_2.json |   |   | 0 | 2026-05-02 13:56:04 CEST | 0000-00-00 00:00:00 | 2026-05-03 00:00:00 CEST |

| Hex     | Text           | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other O |
|---------|----------------|-------------|---------------|------------|----------------|------------------|---------|-------------|---------|
| Strings | Extracted Text | Translation |               |            |                |                  |         |             |         |

Page: 1 of - Page ← → Matches on page: - of - Match ← → 100% 🗨 ⌕ Reset

```
{
  "participants": [
    {
      "name": "Martin Novak"
    },
    {
      "name": "NightOwl"
    }
  ],
  "messages": [
    {
      "sender_name": "NightOwl",
      "timestamp_ms": 1684333800000,
      "content": "Si dnes večer voľný?",
      "type": "Generic"
    },
    {
      "sender_name": "Martin Novak",
      "timestamp_ms": 1684333800000,
      "content": "Možno... záleží",
      "type": "Generic"
    },
    {
      "sender_name": "NightOwl",
      "timestamp_ms": 1684333800000,
      "content": "Ále no, však si to spolu užijeme, tak ako minule.",
      "type": "Generic"
    },
    {
      "sender_name": "Martin Novak",
      "timestamp_ms": 1684333800000,
      "content": "Doma je to teraz citlivé. Musíme byť opatrní.",
      "type": "Generic"
    },
    {
      "sender_name": "NightOwl",
      "timestamp_ms": 1684334100000,
      "content": "Vždy sme boli. Ale začína mi to liezť na nervy.",
      "type": "Generic"
    }
  ]
}
```

```

{
  "sender_name": "Martin Novak",
  "timestamp_ms": 1684334100000,
  "content": "Chápem... len nechcem, aby sa na niečo prišlo.",
  "type": "Generic"
},
{
  "sender_name": "NightOwl",
  "timestamp_ms": 1684334100000,
  "content": "Tak potom žiadne správy ako tá posledná. Takto sa to nedá skryť.",
  "type": "Generic"
},
{
  "sender_name": "Martin Novak",
  "timestamp_ms": 1684334100000,
  "content": "Máš pravdu. Vymaž to prosím.",
  "type": "Generic"
},
{
  "sender_name": "NightOwl",
  "timestamp_ms": 1684334160000,
  "content": "Už sa stalo. Zajtra, to isté miesto?",
  "type": "Generic"
},
{
  "sender_name": "Martin Novak",
  "timestamp_ms": 1684334160000,
  "content": "Áno. Ale len na chvíľu.",
  "type": "Generic"
}
]
}

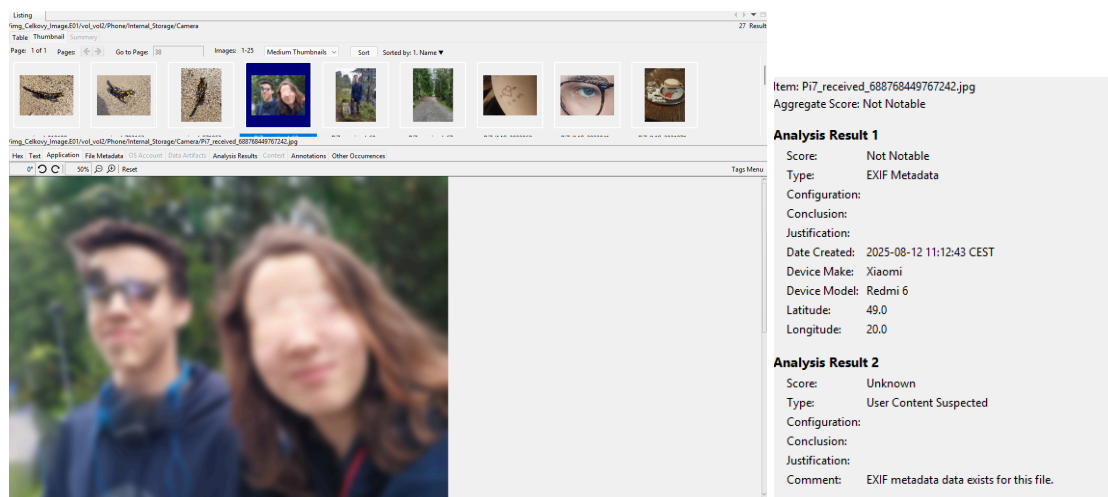
```

*Súkromná konverzácia s cudzou osobou, pravdepodobne ženou, zameraná na tajné stretnutie*  
*Časové obdobie: 17. máj 2023 o 14:35:00*

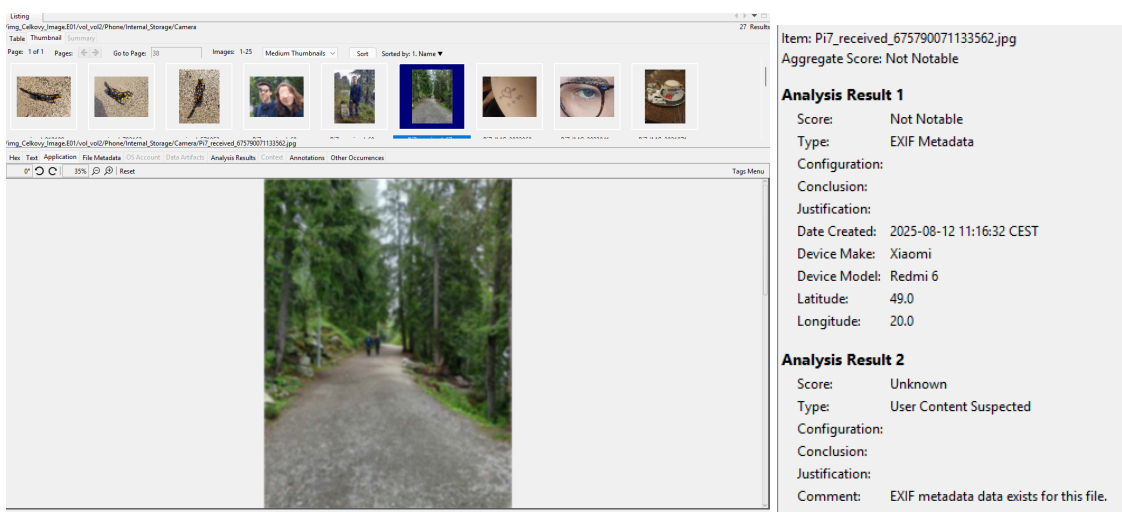


| ▼ Name                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | S              | C           | O             | Modified Time            | Change Time         | Access Time              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-------------|---------------|--------------------------|---------------------|--------------------------|
| message_1.json                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                |             | 0             | 2026-05-02 13:57:10 CEST | 0000-00-00 00:00:00 | 2026-05-03 00:00:00 CEST |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                |             |               |                          |                     |                          |
| Hex                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Text           | Application | File Metadata | OS Account               | Data Artifacts      | Analysis Results         |
| Strings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Extracted Text | Translation | Context       | Annotations              | Other Oc            |                          |
| Page: 1 of - Page   Matches on page: - of - Match   100%   Reset                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                |             |               |                          |                     |                          |
| <pre> {   "participants": [     {       "name": "Martin Novak"     },     {       "name": "J. K."     }   ],   "messages": [     {       "sender_name": "L. K.",       "timestamp_ms": 1685347200000,       "content": "Dobrý deň, chcem sa opýtať na zajtrajšie stretnutie ohľadom \"projektu\".",       "type": "Generic"     },     {       "sender_name": "Martin Novak",       "timestamp_ms": 1685347200000,       "content": "Dobrý deň, áno, platí. Len budem mať obmedzený čas.",       "type": "Generic"     },     {       "sender_name": "L. K.",       "timestamp_ms": 1685347200000,       "content": "Rozumiem. Ako vždy, diskretnosť je pre mňa dôležitá.",       "type": "Generic"     },     {       "sender_name": "Martin Novak",       "timestamp_ms": 1685347200000,       "content": "Samozrejme. Stretneme sa na tom istom mieste ako minule?",       "type": "Generic"     },     {       "sender_name": "L. K.",       "timestamp_ms": 1685347260000,       "content": "Áno, tam kde nás nikto nebude rušiť.",       "type": "Generic"     },     {       "sender_name": "Martin Novak",       "timestamp_ms": 1685347260000,       "content": "Dobre. Len prosím nepoužívaj tento kontakt často.",       "type": "Generic"     },     {       "sender_name": "L. K.",       "timestamp_ms": 1685347260000,       "content": "Neboj sa, dávam si pozor. Minule to bolo... nečakané.",       "type": "Generic"     },     {       "sender_name": "Martin Novak",       "timestamp_ms": 1685347320000,       "content": "Áno, skoro to nevyšlo dobre.",       "type": "Generic"     },     {       "sender_name": "L. K.",       "timestamp_ms": 1685347320000,       "content": "Zajtra budem presná. Nech to nemusíme zbytočne predlžovať.",       "type": "Generic"     },     {       "sender_name": "Martin Novak",       "timestamp_ms": 1685347320000,       "content": "Súhlasím. A tentokrát bez \"chýb\".",       "type": "Generic"     }   ] } </pre> |                |             |               |                          |                     |                          |

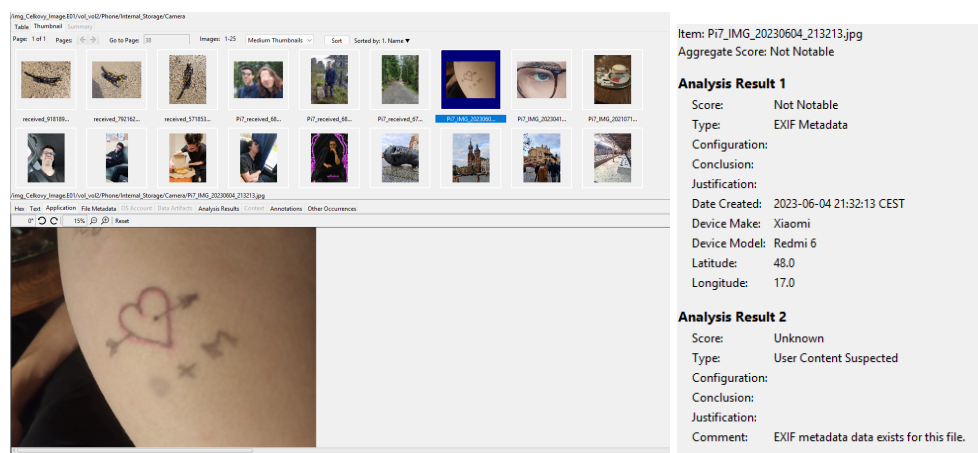
Súkromná konverzácia s cudzou osobou, ženou, zameraná na tajné stretnutie a eliminovanie chýb  
Časové obdobie: 29. máj 2023 o 10:00:00



*Nájdená spoločná fotografia podozrivého s cudzou ženou  
Metadáta ukazujú na dátum 12. august 2025 v čase 11:12:43 s lokalizáciou pri Štrbskom Plese*



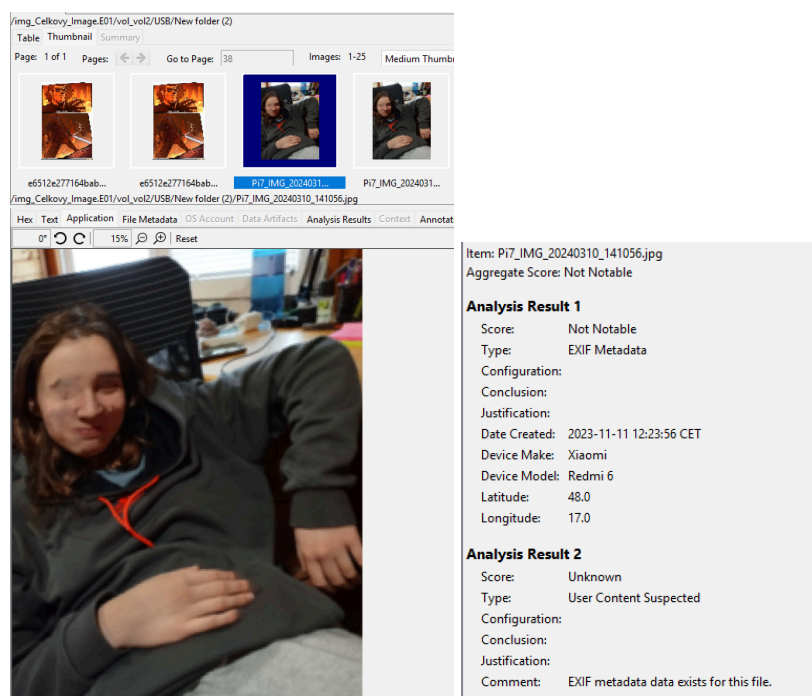
*Nájdená spoločná fotografia scenérie podozrivého s cudzou ženou v úzadi  
Metadáta ukazujú na dátum 12. august 2025 v čase 11:16:32 s lokalizáciou pri Štrbskom Plese*



*Nájdená fotografia ramena, so zjavne ľúbostným nákrešom sprevádzaným iniciálmi cudzej osoby a podozrivého  
Metadáta ukazujú na dátum 04. jún 2023 v čase 21:32:13 s lokalizáciou v rodnom dome podozrivého, v Stupave*

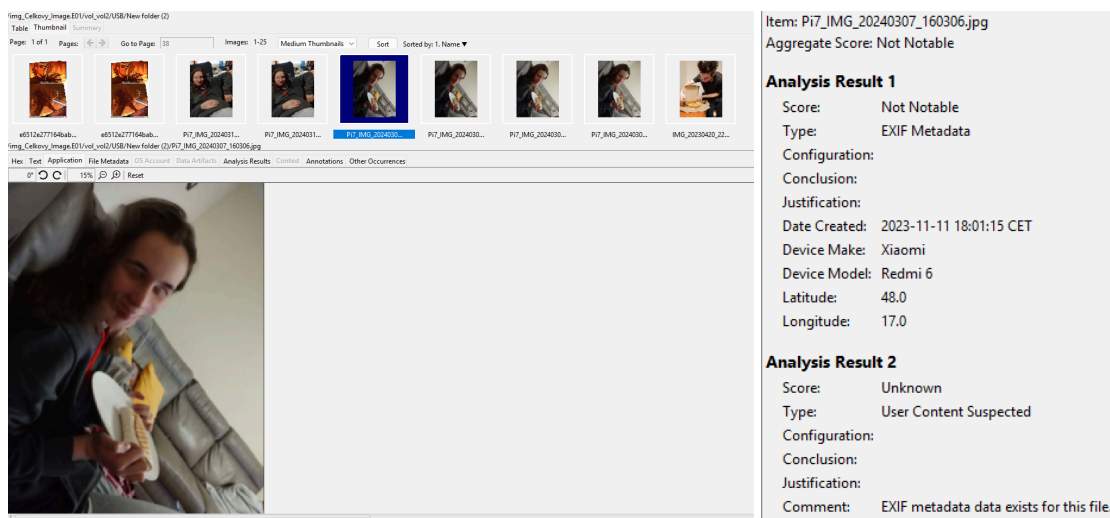
- **USB kľúč - Silicon Power Ultima U02**

Na USB kľúči sa našlo množstvo zálohovaných fotografií, vrátani fotografií, ktoré potvrdzovali manželovu neveru.



*Obrázok zachytáva cudziu ženu*

*Metadáta ukazujú na dátum 11. november 2023 v čase 12:23:56 s lokalizáciou v rodnom dome podozrivého, v Stupave*



*Obrázok zachytáva cudziu ženu*

*Metadáta ukazujú na dátum 11. november 2023 v čase 18:01:15 s lokalizáciou v rodnom dome podozrivého, v Stupave*



*Na základe údajov z časovej osi, vieme aj vyčítať, že došlo k vysokej aktivite v roku 2023, čo sa zhoduje s dátumami v metadátach dôkazov.*

## 7. Použitý Softvér

- FTK Imager
- Autopsy

## 8. Bezpečnostné opatrenia

### • Bitové kópie zariadení

Pomocou softvéru FTK Imager boli zo zaistených zariadení vytvorené bitové kópie. Tento proces zabezpečil identický prepis dát na úrovni sektorov.

#### Prehľad vytvorených obrazov:

- Notebook
- Mobilný telefón
- USB kľúč
- Pamať RAM

Počet kópií: 2

- Pracovná kópia
- Záložná kópia

### • HASH hodnoty

Pri zabezpečovaní integrity dát, boli pre ich kontrolu vypočítané HASH hodnoty (MD5 a SHA1). Tieto hodnoty slúžia na kontrolu integrity dát, a či došlo k ich manipulácii alebo nie.

| Zariadenie      | MD5                              | SHA1                                     |
|-----------------|----------------------------------|------------------------------------------|
| Notebook        | 00c9bf631cc9420644d68f2f7db5b04c | 4a0414703b50141b2c6f4f7bec4c8477564732c6 |
| Mobilný telefón | 2ef3232b2aa1dbe27892acac38b311b1 | 58f7376fe5bd84a184eba52df9eac556464ec5d8 |
| USB kľúč        | 48ccf258a97ea3591315cb5bb041a66e | cdd3cdab68747fd8c829ec9917b72ee3b7949394 |

Tieto hodnoty boli vypočítané po vytvorení bitových kópií a následne overené pred začiatkom samotnej analýzy.

### • Fyzická ochrana zariadení

Zariadenia, ako aj úložné disky, na ktorých boli uložené jednotlivé bitové kópie, boli uložené v antistatických sáčkoch, ktoré boli následne uložené v špecializovaných priestoroch s obmedzeným prístupom.

Originálne zariadenia, z ktorých boli vytvorené bitové kópie sa nevyužívali na analýzu. Analýza prebiehala na pracovných kópiách. Spomínané zariadenia boli chránené pred akýmkoľvek poškodením či neoprávnenou manipuláciou, pričom každá manipulácia bola zaznamenaná v *Chain of Custody*.

- **Chain of Custody**

|                                   |                       |                                                                                 |               |                       |     |          |                       |
|-----------------------------------|-----------------------|---------------------------------------------------------------------------------|---------------|-----------------------|-----|----------|-----------------------|
| Číslo:                            | 01                    | Typ súboru:                                                                     | Binárny súbor | Obnovený súbor:       | Nie | Veľkosť: | 256 GB                |
| Popis prípadu:                    |                       | Nevera                                                                          |               |                       |     |          |                       |
| Názov súboru:                     |                       | PC_Image.ad1                                                                    |               |                       |     |          |                       |
| Miesto získania digitálnej stopy: |                       | Stôl v pracovni pána Martina                                                    |               |                       |     |          |                       |
| Poznámky:                         |                       | Notebook - Dell Latitude E5440                                                  |               |                       |     |          |                       |
|                                   |                       |                                                                                 |               |                       |     |          |                       |
| Časové pečiatky                   |                       |                                                                                 |               |                       |     |          |                       |
| Access:                           | 14.04.2026<br>8:20:54 |                                                                                 | Modify:       | 13.03.2026<br>8:30:34 |     | Change:  | 13.03.2026<br>8:31:02 |
|                                   |                       |                                                                                 |               |                       |     |          |                       |
| Digitálny odtlačok (heš)          | MD5                   | 00c9bf631cc9420644d68f2f7db5b04c                                                |               |                       |     |          |                       |
|                                   | SHA1                  | 4a0414703b50141b2c6f4f7bec4c8477564732c6                                        |               |                       |     |          |                       |
|                                   |                       |                                                                                 |               |                       |     |          |                       |
| Časová pečiatka                   |                       | Akcia vykonaná s digitálnou stopou                                              |               |                       |     |          |                       |
| 12.03.2026<br>13:42:44            |                       | Zaistenie Notebooku, vloženie do antistatického sáčku a označenie štítkom<br>02 |               |                       |     |          |                       |
| 13.03.2026<br>8:30:34             |                       | Vytvorenie bitovej kópie pamäte                                                 |               |                       |     |          |                       |
| 13.03.2026<br>12:22:12            |                       | Odovzdanie digitálneho obrazu na forenznú analýzu                               |               |                       |     |          |                       |
| 14.04.2026<br>8:20:54             |                       | Analýza obsahu a identifikácia relevantného súboru pre prípad                   |               |                       |     |          |                       |

|                                    |                       |                                                                                       |               |                       |     |          |                       |
|------------------------------------|-----------------------|---------------------------------------------------------------------------------------|---------------|-----------------------|-----|----------|-----------------------|
| Číslo:                             | 02                    | Typ súboru:                                                                           | Binárny súbor | Obnovený súbor:       | Nie | Veľkosť: | 64 GB                 |
| Popis prípadu:                     |                       | Nevera                                                                                |               |                       |     |          |                       |
| Názov súboru:                      |                       | Phone_Image.ad1                                                                       |               |                       |     |          |                       |
| Miesto získania digitálnej stopy:  |                       | Stôl v pracovni pána Martina                                                          |               |                       |     |          |                       |
| Poznámky:                          |                       | Mobilný telefón - Xiaomi Redmi 6                                                      |               |                       |     |          |                       |
|                                    |                       |                                                                                       |               |                       |     |          |                       |
| Časové pečiatky                    |                       |                                                                                       |               |                       |     |          |                       |
| Access:                            | 15.04.2026<br>8:05:30 |                                                                                       | Modify:       | 13.03.2026<br>8:15:03 |     | Change:  | 13.03.2026<br>8:15:45 |
|                                    |                       |                                                                                       |               |                       |     |          |                       |
| Digitáln<br>y<br>odtlačok<br>(heš) | MD5                   | 2ef3232b2aa1dbe27892acac38b311b1                                                      |               |                       |     |          |                       |
|                                    | SHA1                  | 58f7376fe5bd84a184eba52df9eac556464ec5d8                                              |               |                       |     |          |                       |
|                                    |                       |                                                                                       |               |                       |     |          |                       |
| Časová pečiatka                    |                       | Akcia vykonaná s digitálnou stopou                                                    |               |                       |     |          |                       |
| 12.03.2026<br>13:51:24             |                       | Zaistenie Mobilného telefónu, vloženie do antistatického sáčku a označenie štítkom 03 |               |                       |     |          |                       |
| 13.03.2026<br>8:15:03              |                       | Vytvorenie bitovej kópie pamäte                                                       |               |                       |     |          |                       |
| 13.03.2026<br>12:22:12             |                       | Odovzdanie digitálneho obrazu na forenznú analýzu                                     |               |                       |     |          |                       |
| 15.04.2026<br>8:05:30              |                       | Analýza obsahu a identifikácia relevantného súboru pre prípad                         |               |                       |     |          |                       |

|                                    |                        |                                                                                 |               |                       |     |          |                       |
|------------------------------------|------------------------|---------------------------------------------------------------------------------|---------------|-----------------------|-----|----------|-----------------------|
| Číslo:                             | 03                     | Typ súboru:                                                                     | Binárny súbor | Obnovený súbor:       | Nie | Veľkosť: | 8 GB                  |
| Popis prípadu:                     |                        | Nevera                                                                          |               |                       |     |          |                       |
| Názov súboru:                      |                        | USB_Image.ad1                                                                   |               |                       |     |          |                       |
| Miesto získania digitálnej stopy:  |                        | Kôš v pracovni pána Martina                                                     |               |                       |     |          |                       |
| Poznámky:                          |                        | USB disk - Silicon Power Ultima U02                                             |               |                       |     |          |                       |
|                                    |                        |                                                                                 |               |                       |     |          |                       |
| Časové pečiatky                    |                        |                                                                                 |               |                       |     |          |                       |
| Access:                            | 15.04.2026<br>15:29:48 |                                                                                 | Modify:       | 13.03.2026<br>8:05:58 |     | Change:  | 13.03.2026<br>8:06:05 |
|                                    |                        |                                                                                 |               |                       |     |          |                       |
| Digitáln<br>y<br>odtlačok<br>(heš) | MD5                    | 48ccf258a97ea3591315cb5bb041a66e                                                |               |                       |     |          |                       |
|                                    | SHA1                   | cdd3cdab68747fd8c829ec9917b72ee3b7949394                                        |               |                       |     |          |                       |
|                                    |                        |                                                                                 |               |                       |     |          |                       |
| Časová pečiatka                    |                        | Akcia vykonaná s digitálnou stopou                                              |               |                       |     |          |                       |
| 12.03.2026<br>13:44:23             |                        | Zaistenie USB kľúča, vloženie do antistatického sáčku a označenie štítkom<br>01 |               |                       |     |          |                       |
| 13.03.2026<br>8:05:58              |                        | Vytvorenie bitovej kópie pamäte                                                 |               |                       |     |          |                       |
| 13.03.2026<br>12:22:12             |                        | Odovzdanie digitálneho obrazu na forenznú analýzu                               |               |                       |     |          |                       |
| 15.04.2026<br>15:29:48             |                        | Analýza obsahu a identifikácia relevantného súboru pre prípad                   |               |                       |     |          |                       |



## 9. Záver

Cieľom tohto vyšetrovania bolo vykonať digitálnu forenznú analýzu v prípade nemanželského vzťahu.

Počas vyšetrovania boli zaistené patričné zariadenia, ktoré boli následne podrobené forenznej analýze. Týmito zariadeniami boli osobný notebook, mobilný telefón ako aj USB kľúč a operačná pamäť RAM. Zo všetkých týchto zariadení boli vytvorené bitové kópie. Každá bitová kópia mala vlastný duplikát v prípade kompromitácie originálnych dát, ako aj pre overenie samotnej integrity dát.

Analýza potvrdila, že k nemanželskému vzťahu skutočne dochádzalo. Na notebooku sa našli zápisky vo forme denníkov, ktoré opisovali čím si podozrivý prechádzal, jeho obavami a zážitkami. Analýza mobilného zariadenia odhalila textové správy s cudzou ženou a spoločné fotografie, ktoré jasne potvrdzujú existenciu mimomanželského pomeru. Následná analýza USB kľúča preukázala prítomnosť záloh dokumentov a fotografií, ktoré obsahovali aj spomínané spoločné snímky.

Na základe získaných dát, bola týmto potvrdená hypotéza č. 2, že si manžel udržiaval mimomanželský vzťah s cudzou osobou.

### DFRWS podklad

- <https://dfrws.org/presentation/syntactical-file-carving-and-automated-generation-of-reproducible-datasets/>