

**UNIVERZITA SV. CYRILA A METODA V TRNAVE**

**FAKULTA PRIRODNÝCH VIED**

**Katedra aplikovanej informatiky a matematiky**

# **Únik tajných fotiek z exkluzívneho photoshoot pre magazín**

**Digitálna Forenzná Analýza**

# Obsah

|                                                       |    |
|-------------------------------------------------------|----|
| Prípád: .....                                         | 3  |
| Objektívy pre vyšetrenie: .....                       | 3  |
| Hypotézy: .....                                       | 3  |
| 5WH.....                                              | 4  |
| Používané programy: .....                             | 4  |
| Zariadenia .....                                      | 5  |
| 1. USB kľúč nájdený v koši z jednej v kancelárií..... | 5  |
| 2. Notebook manažéra projektu .....                   | 7  |
| Vytvorenie kópií a zabezpečenie .....                 | 9  |
| Chain of Custody .....                                | 9  |
| Analýza dát .....                                     | 13 |
| Čo vieme zatiaľ ešte mimo analýzy? .....              | 13 |
| Autopsy dátová analýza .....                          | 14 |
| RAM analýza .....                                     | 15 |
| Analýza pripojených zariadení.....                    | 17 |
| Analýza prehľadávaných stránok.....                   | 18 |
| Analýza USB zariadenia .....                          | 20 |
| Analýza fotiek a ich metadát.....                     | 21 |
| Analýza databázy zamestnancov .....                   | 22 |
| Analýza e-mailovej komunikácie.....                   | 23 |
| Overenie hypotéz .....                                | 25 |
| Literatúra:.....                                      | 26 |
| Pripravené dáta a použité datasety:.....              | 26 |
| Záver .....                                           | 27 |

# Únik tajných fotiek z exkluzívneho photoshoot pre magazín

Alex Budinský, skupina 05, 2. ročník

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

## Prípady:

Známy magazín mali exkluzívny photoshoot s vysoko-profilovými ľuďmi pre nadchádzajúcu edíciu magazínu. Fotky a ilustrácie mali byť dôverné až do oficiálneho vydania. No na internete sa týždeň pred vydaním zobrazili fotky, ktoré neboli upravené na vydanie a obsahovali aj tie vyhodnené zábery alebo alternatívne zábery – tieto fotky sa rozšírili sociálnymi sieťami a aj na stránkach klebiet a povier.

Spoločnosť sa domnieva v interný únik fotiek ale nemajú tuha, ako sa na prvom mieste ocitli na internete. Jediné dôkazy, ktoré boli nájdené a sú podozrivé sú:

- **Pracovný notebook** zabezpečený spoločnosťou používaný marketingovým tímom
- **USB kľúč** nájdený v koši v jednej z kancelárií

## Objektívny pre vyšetrovanie:

- **Zistiť spôsob úniku dát** – bol to interný únik dát alebo externý (hacknutie)?
- **Analýza USB a notebooku**
- **Extrahovať údaje z poškodeného USB**
- **Zistiť zdroj úniku dát cez zverejnené dáta na internete** – nájsť informácie v metadátach vo zverejnených obrázkoch

## Hypotézy:

### Hypotéza 1:

Podľa opísanej situácie vieme, že sa jedná o nejakú celebritu alebo osobnosť – dedukujem, že sa jedná o interný únik dát. Domnievam sa, že manažér, ktorý sa staral o celý tento projekt, bol v skutočnosti veľký fanúšik alebo nenávidel túto osobnosť a chceli zverejniť ich fotky buď na osvedčenie že sú fenoménny alebo hrozný v realite.

### Hypotéza 2:

Naša osoba sa napojila do notebooku a cez USB vložila skript na odomknutie prístupu na všetky stránky internetu – za normálnych okolností majú vo firemnej sieti zablokovaný prístup na všetky stránky okrem firmou povolených. Toto USB sa po použití zničilo a zahodilo v snahe sa zbaviť dôkazov.

### Hypotéza 3:

Notebook nebol správne nakonfigurovaný a odišli odtiaľ fotky cez nejaký externý útok – cez internet.

### Hypotéza 4:

Jedná sa o externý únik dát – pozvaný fotograf, dizajnér setu a iní ľudia, ktorý nepatrili pod spoločnosť a mali prístup ku akýmkoľvek dátam.

## **5WH**

### **Kto?**

Osoba, ktorá to nahrala na internete, zamestnanec – ktorý nemusí byť ani priamo spojený s projektom, ľudia ktorý boli súčasťou projektu.

### **Kde?**

Únik informácií sa stal na internete ale miesto činu je zatiaľ firemná budova.

### **Kedy?**

Únik dát na internet sa stal týždeň pred vydaním magazínu.

### **Čo?**

Citlivé dáta a fotky, ktoré mali byť súkromné až do vydania magazínu. Medzi tieto fotky patria aj neupravené fotky, grafika a nejaký text – ktorý sa mal nachádzať v článkoch pri fotkách.

### **Prečo?**

Nemáme presnú motiváciu ale medzi motivácie môže byť, že chceli poškodiť profil osobnosti, odhaliť nejaké veci o danej osobnosti alebo môže byť aj to, že boli veľkým fanatikom a chceli zverejniť ich fotky – aby spravili dôraz na to, že aký sú majestátny bez retušovania a iných úprav.

### **Ako?**

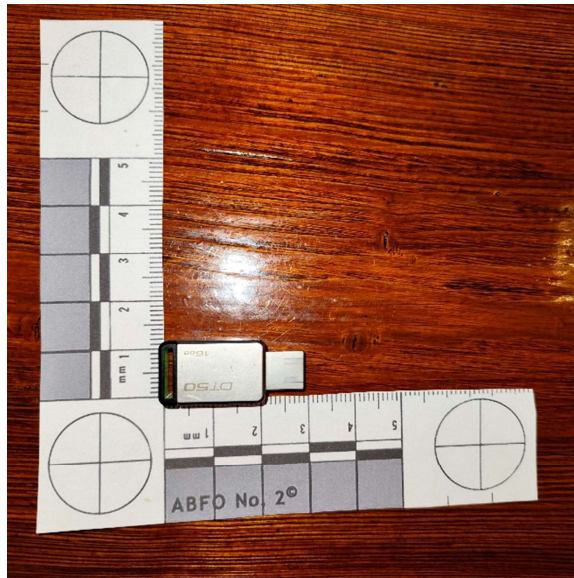
Predpokladá sa, že došlo k internému úniku informácií ale zase mohlo dôjsť aj ku externému úniku informácií.

## **Použité programy:**

- USBDeview
- Autopsy
- MS Excel
- FTK Imager (verzia: 4.7.1.2)
- Magnet RAM Capture (verzia: 1.2.0).
- Exiftool
- Google Earth
- BrowsingHistoryView (verzia: 2.60)

## Zariadenia

### 1. USB kľúč nájdený v koši z jednej v kancelárii



Obrázok 1: nájdený USB kľúč

- USB bolo nájdené v koši v otvorenej kancelárii – majiteľa USB bude ťažšie upresniť keďže oblasť okolo kôšu je veľmi frekventovaná oblasť
- **Parametre zaradenia:**

|                         |                                                              |
|-------------------------|--------------------------------------------------------------|
| <b>Značka</b>           | Kingstone                                                    |
| <b>Model</b>            | Kingston DataTraveler 3.0 USB Device DT50 (Silver and green) |
| <b>Serial Number</b>    | 0S 8028271                                                   |
| <b>Rozmery</b>          | 44.9mm x 20mm x 9.2mm                                        |
| <b>Hmotnosť</b>         | 10 g                                                         |
| <b>Kapacita</b>         | 14755 MB (píše sa 16GB)                                      |
| <b>Rozhranie</b>        | USB 3.1                                                      |
| <b>Podporované OS</b>   | Windows 8 – 11, Mac OS, Linux, Chrome OS                     |
| <b>Rýchlosť čítania</b> | 30 MB/s                                                      |
| <b>Rýchlosť zápisu</b>  | 5 MB/s                                                       |

- **Informácie o USB získané z FTK Imager:**

Created By AccessData® FTK® Imager 4.7.1.2

Case Information:

Acquired using: ADI4.7.1.2

Case Number: 01

Evidence Number: 01

Unique description: usb\_kingstone\_dt50\_16\_GB

Examiner: Alex Budinský

Notes: sede usb s zelenym privesom

-----  
Information for C:\Users\Alex Wolfie\Documents\2\_rocnik\letny\Digitalna Forenzna Analyza\captured disk\usb\_kingstone\_dt50\_16\_GB:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 1.881

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 30.218.842

[Physical Drive Information]

Drive Model: Kingston DataTraveler 3.0 USB Device

Drive Serial Number: \_\_\_\_\_0

Drive Interface Type: USB

Removable drive: True

Source data size: 14755 MB

Sector count: 30218842

[Computed Hashes]

MD5 checksum: dccebbe84c46f00353e75531a31498c0

SHA1 checksum: c02cc442639c414a58cb6a617bd6ea4a176de8f8

Image Information:

Acquisition started: Sun Mar 23 15:38:48 2025

Acquisition finished: Sun Mar 23 15:40:57 2025

Segment list:

C:\Users\Alex Wolfie\Documents\2\_rocnik\letny\Digitalna Forenzna Analyza\captured disk\usb\_kingstone\_dt50\_16\_GB.001

Image Verification Results:

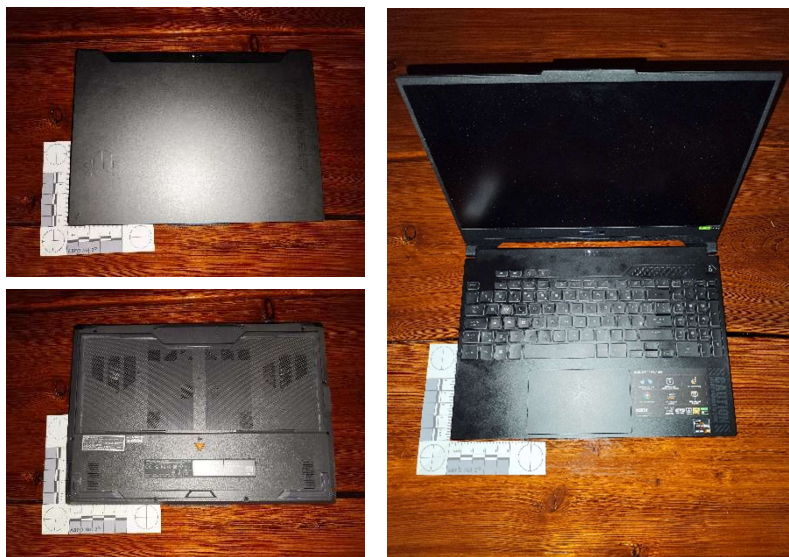
Verification started: Sun Mar 23 15:40:57 2025

Verification finished: Sun Mar 23 15:41:31 2025

MD5 checksum: dccebbe84c46f00353e75531a31498c0 : verified

SHA1 checksum: c02cc442639c414a58cb6a617bd6ea4a176de8f8 : verified

## 2. Notebook manažéra projektu



Obrázok 2-4 : Notebook manažéra projektu

- Notebook manažéra projektu – spoločnosťou zabezpečený notebook so zvýšenou bezpečnosťou
- Medzi projektami sa notebooky menia medzi manažérmi a vydávajú ich technici v spoločnosti
- Parametre zaradenia:

|                         |                                                  |
|-------------------------|--------------------------------------------------|
| <b>Značka</b>           | Asus                                             |
| <b>Model</b>            | ASUS TUF Gaming A15 FA507NV                      |
| <b>Serial Number</b>    | S4NRCX0DW116148                                  |
| <b>Rozmery</b>          | 35.4 x 25.1 x 2.24 ~ 2.49 cm                     |
| <b>Hmotnosť</b>         | 2,20 kg                                          |
| <b>Kapacita</b>         | 1 TB                                             |
| <b>Rozhranie</b>        | Windows 10                                       |
| <b>Názov zariadenia</b> | DESKTOP-A6QMBAJ                                  |
| <b>Procesor</b>         | AMD Ryzen 5 7535HS with Radeon Graphics 3.30 GHz |
| <b>Inštalovaná RAM</b>  | 16.0 GB (15.2 GB použiteľná)                     |
| <b>ID zariadenia</b>    | 51021C38-41A5-4ED2-B831-31AC8C86B881             |
| <b>ID produktu</b>      | 00329-10330-65365-AA375                          |
| <b>Systémový typ</b>    | 64-bit operačný systém, x64 procesor             |
| <b>Pero a dotyk</b>     | Podpora pera                                     |

- **Informácie o hard-disku získané z FTK Imager:**

Created By AccessData® FTK® Imager 4.7.1.2

Case Information:

Acquired using: ADI4.7.1.2

Case Number: 01

Evidence Number: 04

Unique description: asus\_gaming\_tuf\_a15\_notebook

Examiner: Alex Budinsky

Notes: notebook manazera

-----  
Information for C:\Users\Alex Wolfie\Documents\2\_rocnik\letny\Digitalna Forenzna Analyza\captured disk\laptop\_manazera:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Logical

[Drive Geometry]

Bytes per Sector: 512

Sector Count: 18.429.952

[Physical Drive Information]

Removable drive: False

Source data size: 8999 MB

Sector count: 18429952

[Computed Hashes]

MD5 checksum: be975e9cac4662983d64626d49843084

SHA1 checksum: 4235ac77ce925f5e7ff5b835fa5ab2d5d1c992a8

Image Information:

Acquisition started: Tue Mar 25 14:35:06 2025

Acquisition finished: Tue Mar 25 14:35:20 2025

Segment list:

C:\Users\Alex Wolfie\Documents\2\_rocnik\letny\Digitalna Forenzna Analyza\captured disk\laptop\_manazera.001

Image Verification Results:

Verification started: Tue Mar 25 14:35:21 2025

Verification finished: Tue Mar 25 14:35:41 2025

MD5 checksum: be975e9cac4662983d64626d49843084 : verified

SHA1 checksum: 4235ac77ce925f5e7ff5b835fa5ab2d5d1c992a8 : verified

## Vytvorenie kópií a zabezpečenie

Bitové kópie RAM z notebooku boli vytvorené pomocou nástroja FTK Imager (verzia: 4.7.1.2) a Magnet RAM Capture (verzia: 1.2.0). Bitovú kópiu úložného zariadenia sme vytvorili vďaka FTK Imagera.

Tieto kópie boli nasledovne uložené na externý pracovný disk, ktorý slúži na zachovanie a prácu s obrazmi diskov – originál a kópie máme bezpečnostne uložené v anti-statickej skrinke v plastových obaloch (na zabránenie vlhkosti), túto krabičku máme následne uloženú v trezore. Trezor sa nachádza v areáli na digitálnu forenznú analýzu – monitorované priestory a aj s bezpečnostnými opatreniami aj s ťažkou ochranou.

## Chain of Custody

|                                   |                     |                                                             |         |                     |     |          |      |
|-----------------------------------|---------------------|-------------------------------------------------------------|---------|---------------------|-----|----------|------|
| Číslo:                            | 01                  | Typ súboru:                                                 | WinRAR  | Obnovený súbor:     | Nie | Veľkosť: | 16GB |
| Popis prípadu:                    |                     | Únik tajných fotiek z exkluzívneho photoshoot pre magazín   |         |                     |     |          |      |
| Názov súboru:                     |                     | usb_kingstone_dt50_16_GB.001                                |         |                     |     |          |      |
| Miesto získania digitálnej stopy: |                     | Nájdenný USB kľúč                                           |         |                     |     |          |      |
| Poznámky:                         |                     | USB kľúč DT50 16GB, obraz bol robený cez FTK Imager 4.7.1.2 |         |                     |     |          |      |
|                                   |                     |                                                             |         |                     |     |          |      |
| Časové pečiatky                   |                     |                                                             |         |                     |     |          |      |
| Access:                           | 23.03.2025 15:40:16 |                                                             | Modify: | 23.03.2025 15:40:16 |     | Change:  | -    |
|                                   |                     |                                                             |         |                     |     |          |      |
| Digitálny odtlačok (heš)          | MD5                 | dccebce84c46f00353e75531a31498c0                            |         |                     |     |          |      |
|                                   | SHA1                | c02cc442639c414a58cb6a617bd6ea4a176de8f8                    |         |                     |     |          |      |
|                                   |                     |                                                             |         |                     |     |          |      |
| Časová pečiatka                   |                     | Akcia vykonaná s digitálnou stopou                          |         |                     |     |          |      |
| Ned Mar 23 15:38:48 2025          |                     | Zber informácií/dát z USB disku                             |         |                     |     |          |      |
| Ned Mar 23 15:40:57 2025          |                     | Dokončenie zberu informácií/dát z USB disku                 |         |                     |     |          |      |
| Ned Mar 23 15:40:57 2025          |                     | Overovanie hashov spustenie                                 |         |                     |     |          |      |
| Ned Mar 23 15:41:31 2025          |                     | Dokončenie overenia hashov – prebehlo úspešne               |         |                     |     |          |      |

|                                   |                     |                                                           |         |                     |     |          |        |
|-----------------------------------|---------------------|-----------------------------------------------------------|---------|---------------------|-----|----------|--------|
| Číslo:                            | 02                  | Typ súboru:                                               | mem     | Obnovený súbor:     | Nie | Veľkosť: | 17,4GB |
| Popis prípadu:                    |                     | Únik tajných fotiek z exkluzívneho photoshoot pre magazín |         |                     |     |          |        |
| Názov súboru:                     |                     | memdump.mem                                               |         |                     |     |          |        |
| Miesto získania digitálnej stopy: |                     | Manažérov notebook - RAM                                  |         |                     |     |          |        |
| Poznámky:                         |                     | Súbor bol vytvorený cez FTK Imager 4.7.1.2 .              |         |                     |     |          |        |
|                                   |                     |                                                           |         |                     |     |          |        |
| Časové pečiatky                   |                     |                                                           |         |                     |     |          |        |
| Access:                           | 02.03.2025 18:32:16 |                                                           | Modify: | 02.03.2025 18:32:16 |     | Change:  | -      |
|                                   |                     |                                                           |         |                     |     |          |        |
| Digitálny odtlačok (heš)          | MD5                 | 9b84685398b9c068d073990acaf21575                          |         |                     |     |          |        |
|                                   | SHA1                | 6eeda606c6787778e7d7f8245fdf92c054c431aa                  |         |                     |     |          |        |
|                                   |                     |                                                           |         |                     |     |          |        |
| Časová pečiatka                   |                     | Akcia vykonaná s digitálnou stopou                        |         |                     |     |          |        |
| Str Mar 5<br>23:23:26 2025        |                     | Zistenie MD5 hash – úspešné vykonané                      |         |                     |     |          |        |
| Str Mar 5<br>23:26:20 2025        |                     | Zistenie SHA1 hash – úspešne vykonané                     |         |                     |     |          |        |
|                                   |                     |                                                           |         |                     |     |          |        |
|                                   |                     |                                                           |         |                     |     |          |        |

|                                   |                     |                                                           |         |                     |     |          |        |
|-----------------------------------|---------------------|-----------------------------------------------------------|---------|---------------------|-----|----------|--------|
| Číslo:                            | 03                  | Typ súboru:                                               | raw     | Obnovený súbor:     | Nie | Veľkosť: | 17,4GB |
| Popis prípadu:                    |                     | Únik tajných fotiek z exkluzívneho photoshoot pre magazín |         |                     |     |          |        |
| Názov súboru:                     |                     | RAM_capture.raw                                           |         |                     |     |          |        |
| Miesto získania digitálnej stopy: |                     | Manažérov notebook - RAM                                  |         |                     |     |          |        |
| Poznámky:                         |                     | Súbor bol vytvorený pomocou Magnet RAM Capture 1.2.0 .    |         |                     |     |          |        |
|                                   |                     |                                                           |         |                     |     |          |        |
| Časové pečiatky                   |                     |                                                           |         |                     |     |          |        |
| Access:                           | 02.03.2025 18:32:16 |                                                           | Modify: | 02.03.2025 18:32:16 |     | Change:  | -      |
|                                   |                     |                                                           |         |                     |     |          |        |
| Digitálny odtlačok (heš)          | MD5                 | 776521e448a0f8184731b2ed9f73ad09                          |         |                     |     |          |        |
|                                   | SHA1                | b734cf396d128956232d9f035cbdf754cc9fc902                  |         |                     |     |          |        |
|                                   |                     |                                                           |         |                     |     |          |        |
| Časová pečiatka                   |                     | Akcia vykonaná s digitálnou stopou                        |         |                     |     |          |        |
| Str Mar 5<br>23:31:07 2025        |                     | Zistenie MD5 hash – úspešné vykonané                      |         |                     |     |          |        |
| Str Mar 5<br>23:32:14 2025        |                     | Zistenie SHA1 hash – úspešne vykonané                     |         |                     |     |          |        |
|                                   |                     |                                                           |         |                     |     |          |        |
|                                   |                     |                                                           |         |                     |     |          |        |

|                                   |                     |                                                           |                     |                 |     |          |         |
|-----------------------------------|---------------------|-----------------------------------------------------------|---------------------|-----------------|-----|----------|---------|
| Číslo:                            | 04                  | Typ súboru:                                               | raw                 | Obnovený súbor: | Nie | Veľkosť: | 8,78 GB |
| Popis prípadu:                    |                     | Únik tajných fotiek z exkluzívneho photoshoot pre magazín |                     |                 |     |          |         |
| Názov súboru:                     |                     | laptop_manazera.raw                                       |                     |                 |     |          |         |
| Miesto získania digitálnej stopy: |                     | Manažérov notebook – Hard-Disk                            |                     |                 |     |          |         |
| Poznámky:                         |                     | Súbor bol vytvorený cez FTK Imager 4.7.1.2 .              |                     |                 |     |          |         |
|                                   |                     |                                                           |                     |                 |     |          |         |
| Časové pečiatky                   |                     |                                                           |                     |                 |     |          |         |
| Access:                           | 25.03.2025 14:35:06 | Modify:                                                   | 25.03.2025 14:35:06 | Change:         | -   |          |         |
|                                   |                     |                                                           |                     |                 |     |          |         |
| Digitálny odtlačok (heš)          | MD5                 | be975e9cac4662983d64626d49843084                          |                     |                 |     |          |         |
|                                   | SHA1                | 4235ac77ce925f5e7ff5b835fa5ab2d5d1c992a8                  |                     |                 |     |          |         |
|                                   |                     |                                                           |                     |                 |     |          |         |
| Časová pečiatka                   |                     | Akcia vykonaná s digitálnou stopou                        |                     |                 |     |          |         |
| Uto Mar 25 14:35:06 2025          |                     | Zber informácií/dát z USB disku                           |                     |                 |     |          |         |
| Uto Mar 25 14:35:20 2025          |                     | Dokončenie zberu informácií/dát z USB disku               |                     |                 |     |          |         |
| Uto Mar 25 14:35:21 2025          |                     | Overovanie hashov spustenie                               |                     |                 |     |          |         |
| Uto Mar 25 14:35:41 2025          |                     | Dokončenie overenia hashov – prebehlo úspešne             |                     |                 |     |          |         |

## Analýza dát

### Čo vieme zatiaľ ešte mimo analýzy?

- Fotky unikli na internet týždeň pred vydaním magazínu. Miesto zverejnenia je známa stránka na celebrityné klebety – TMZ
- Únik fotiek sa uskutočnil **3.3.2025**
- Takéto stránky a iné podobné sociálne siete/stránky sú zablokované firemným internetom
- Od TMZ boli rozšírené fotky na iné stránky ako plameň (zdroj úniku dát)
  - Ako sa dostali ku dátam?
  - Prehľadáme dáta pre nejaké výskyty TMZ kontaktov alebo niečomu podobné ako „gossip“, „celebrity“ a podobné kľúčové slová
  - TMZ kontakty
    - Mobil – (888) 847-9869
    - Email – [meno].[priezvisko]@tmz.com alebo [tips@tmz.com](mailto:tips@tmz.com)

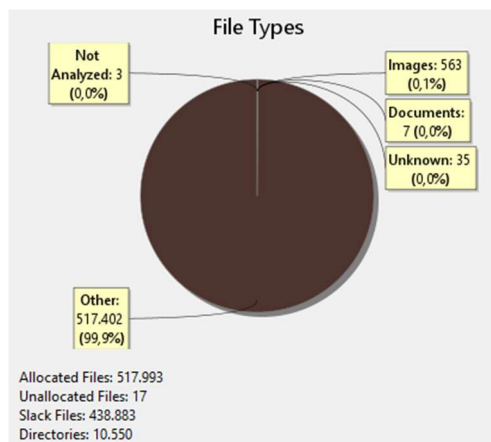
Budeme analyzovať súbory obrázkové a ich metadáta, ktoré som si dal extrahovať (pomocou Exiftool) zo súboru fotiek - ktoré nám boli poskytnuté od firmy na ich analýzu a porovnanie s uniknutými fotkami. Budeme na to potrebovať asi minimálne 5 súborov.

Súbory sú uložené na záložnom disku, cez ktorý nám poskytla firma fotky - čo sa mali vydať, čo vznikli fotky a čo uniklo na internet. Súborový systém sa používa FAT32.

Ďalej máme aj stiahnutú históriu prehľadávania v počítači (internetovú aj súborovú) a takisto aj históriu USB použitia na zariadení – USBDeview.

Z fotiek budeme získavať aj GPS adresu zverejnenia na internet, keďže nám spoločnosť poskytla zoznam zamestnancov pracujúcich v spoločnosti. Takže budeme ľahko vedieť - kto to zverejnil na internet.

## Autopsy dátová analýza



Náš image disku notebooku manažéra sa skladá z nejakých iných súborov 99,9% (517 402), potom z obrázkov 0,1% (563), dokumentov 0,0% (7), neznámych súborov 0,0% (35) a potom 3 neanalyzované súbory.

Keby by sme mali ignorovať tie ostatné súbory tak by sme mali čistejší diagram:

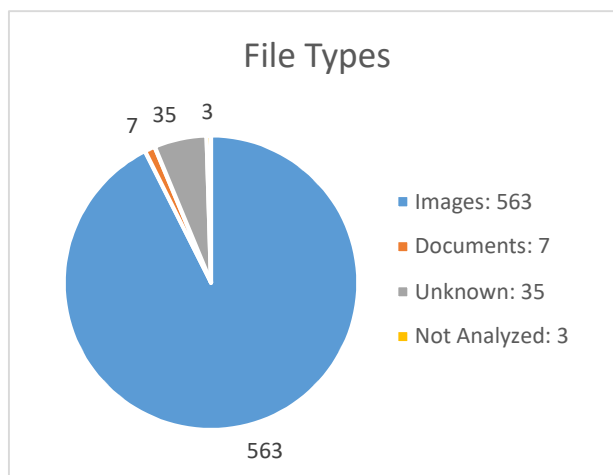
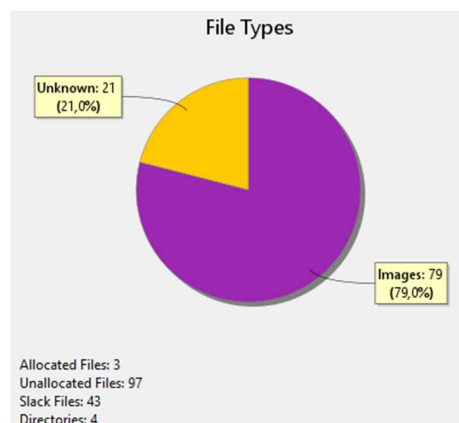


Image USB kľúča odhaľuje to, že sa na USB zariadení nachádza 79,0% fotiek (79) a 21 neznámych súborov (21%)



## RAM analýza

| Checksum | Search (512 hits)                                                                                      |                                  |
|----------|--------------------------------------------------------------------------------------------------------|----------------------------------|
| Offset   | Excerpt (hex)                                                                                          | Excerpt (text)                   |
| B48F270  | 31 2F 30 2F 5F 64 6B 5F 68 74 74 70 73 3A 2F 2F <b>74 6D 7A 2E 63 6F 6D</b> 20 68 74 74 70 73 3A 2F 2F | 1/0/_dk_https://tmz.com https:// |
| B48F280  | 74 6D 7A 2E 63 6F 6D 20 68 74 74 70 73 3A 2F 2F <b>74 6D 7A 2E 63 6F 6D</b> 20 68 74 74 70 73 3A 2F 2F | tmz.com https://tmz.com https:// |
| B48F297  | 20 68 74 74 70 73 3A 2F 2F 69 6D 61 67 65 7A 2E <b>74 6D 7A 2E 63 6F 6D</b> 2F 69 6D 61 67 65 2F 30 63 | https://imagez.tnz.com/image/0c  |
| B48F370  | 31 2F 30 2F 5F 64 6B 5F 68 74 74 70 73 3A 2F 2F <b>74 6D 7A 2E 63 6F 6D</b> 20 68 74 74 70 73 3A 2F 2F | 1/0/_dk_https://tmz.com https:// |
| B48F380  | 74 6D 7A 2E 63 6F 6D 20 68 74 74 70 73 3A 2F 2F <b>74 6D 7A 2E 63 6F 6D</b> 20 68 74 74 70 73 3A 2F 2F | tmz.com https://tmz.com https:// |
| B48F397  | 20 68 74 74 70 73 3A 2F 2F 69 6D 61 67 65 7A 2E <b>74 6D 7A 2E 63 6F 6D</b> 2F 69 6D 61 67 65 2F 36 32 | https://imagez.tnz.com/image/62  |
| D20F370  | 31 2F 30 2F 5F 64 6B 5F 68 74 74 70 73 3A 2F 2F <b>74 6D 7A 2E 63 6F 6D</b> 20 68 74 74 70 73 3A 2F 2F | 1/0/_dk_https://tmz.com https:// |
| D20F380  | 74 6D 7A 2E 63 6F 6D 20 68 74 74 70 73 3A 2F 2F <b>74 6D 7A 2E 63 6F 6D</b> 20 68 74 74 70 73 3A 2F 2F | tmz.com https://tmz.com https:// |
| F025C84  | 00 AD DB BA 00 AD DB BA 00 AD DB BA 77 77 77 7E <b>74 6D 7A 2E 63 6F 6D</b> 00 FC 7F 00 00 D0 EA DF 75 | „Ű“.Ű“.Ű“www.tnz.com.ű...DéBu    |
| F025CD0  | F6 91 86 C0 FC 7F 00 00 D0 EA DF 75 9A 00 00 05 <b>74 6D 7A 2E 63 6F 6D</b> 00 00 00 00 00 00 00 00    | ő+Äü...DéBuš...tmz.com.....      |
| F025D20  | F6 91 86 C0 FC 7F 00 00 D0 EA DF 75 9A 00 00 05 <b>74 6D 7A 2E 63 6F 6D</b> 00 00 00 00 00 00 00 00    | ő+Äü...DéBuš...tmz.com.....      |
| 13C38570 | 31 2F 30 2F 5F 64 6B 5F 68 74 74 70 73 3A 2F 2F <b>74 6D 7A 2E 63 6F 6D</b> 20 68 74 74 70 73 3A 2F 2F | 1/0/_dk_https://tmz.com https:// |
| 13C38580 | 74 6D 7A 2E 63 6F 6D 20 68 74 74 70 73 3A 2F 2F <b>74 6D 7A 2E 63 6F 6D</b> 20 68 74 74 70 73 3A 2F 2F | tmz.com https://tmz.com https:// |
| 13C38594 | 63 6F 6D 20 68 74 74 70 73 3A 2F 2F 77 77 77 7E <b>74 6D 7A 2E 63 6F 6D</b> 2F 5F 2F 70 72 6F 6D 6F 74 | com https://www.tnz.com/_/promot |
| 13C38770 | 31 2F 30 2F 5F 64 6B 5F 68 74 74 70 73 3A 2F 2F <b>74 6D 7A 2E 63 6F 6D</b> 20 68 74 74 70 73 3A 2F 2F | 1/0/_dk_https://tmz.com https:// |
| 13C38780 | 74 6D 7A 2E 63 6F 6D 20 68 74 74 70 73 3A 2F 2F <b>74 6D 7A 2E 63 6F 6D</b> 20 68 74 74 70 73 3A 2F 2F | tmz.com https://tmz.com https:// |
| 13C38797 | 20 68 74 74 70 73 3A 2F 2F 69 6D 61 67 65 7A 2E <b>74 6D 7A 2E 63 6F 6D</b> 2F 69 6D 61 67 65 2F 65 64 | https://imagez.tnz.com/image/ed  |
| 1618E070 | 31 2F 30 2F 5F 64 6B 5F 68 74 74 70 73 3A 2F 2F <b>74 6D 7A 2E 63 6F 6D</b> 20 68 74 74 70 73 3A 2F 2F | 1/0/_dk_https://tmz.com https:// |
| 1618E080 | 74 6D 7A 2E 63 6F 6D 20 68 74 74 70 73 3A 2F 2F <b>74 6D 7A 2E 63 6F 6D</b> 20 68 74 74 70 73 3A 2F 2F | tmz.com https://tmz.com https:// |
| 1618E097 | 20 68 74 74 70 73 3A 2F 2F 73 74 61 74 69 63 2E <b>74 6D 7A 2E 63 6F 6D</b> 2F 74 6D 7A 2D 77 65 62 2F | https://static.tnz.com/tmz-web/  |
| 1618E170 | 31 2F 30 2F 5F 64 6B 5F 68 74 74 70 73 3A 2F 2F <b>74 6D 7A 2E 63 6F 6D</b> 20 68 74 74 70 73 3A 2F 2F | 1/0/_dk_https://tmz.com https:// |
| 1618E180 | 74 6D 7A 2E 63 6F 6D 20 68 74 74 70 73 3A 2F 2F <b>74 6D 7A 2E 63 6F 6D</b> 20 68 74 74 70 73 3A 2F 2F | tmz.com https://tmz.com https:// |
| 1618E197 | 20 68 74 74 70 73 3A 2F 2F 73 74 61 74 69 63 2E <b>74 6D 7A 2E 63 6F 6D</b> 2F 74 6D 7A 2D 77 65 62 2F | https://static.tnz.com/tmz-web/  |
| 1618E270 | 31 2F 30 2F 5F 64 6B 5F 68 74 74 70 73 3A 2F 2F <b>74 6D 7A 2E 63 6F 6D</b> 20 68 74 74 70 73 3A 2F 2F | 1/0/_dk_https://tmz.com https:// |
| 1618E280 | 74 6D 7A 2E 63 6F 6D 20 68 74 74 70 73 3A 2F 2F <b>74 6D 7A 2E 63 6F 6D</b> 20 68 74 74 70 73 3A 2F 2F | tmz.com https://tmz.com https:// |
| 1618E297 | 20 68 74 74 70 73 3A 2F 2F 73 74 61 74 69 63 2E <b>74 6D 7A 2E 63 6F 6D</b> 2F 74 6D 7A 2D 77 65 62 2F | https://static.tnz.com/tmz-web/  |
| 1618E370 | 31 2F 30 2F 5F 64 6B 5F 68 74 74 70 73 3A 2F 2F <b>74 6D 7A 2E 63 6F 6D</b> 20 68 74 74 70 73 3A 2F 2F | 1/0/_dk_https://tmz.com https:// |
| 1618F380 | 74 6D 7A 2E 63 6F 6D 20 68 74 74 70 73 3A 2F 2F <b>74 6D 7A 2E 63 6F 6D</b> 20 68 74 74 70 73 3A 2F 2F | tmz.com https://tmz.com https:// |

Pomocou predtým spomenutých kľúčových slov sme našli výskyty TMZ stránky (tmz.com),bolo ich 512 úderov – vinník musel nejako získať prístup na internet mimo firemnej a našiel tmz.com stránku na únik fotiek.

| Checksum | Search (4308 hits)                                                                                     |                                     |
|----------|--------------------------------------------------------------------------------------------------------|-------------------------------------|
| Offset   | Excerpt (hex)                                                                                          | Excerpt (text)                      |
| B56C5C   | C5 61 55 C1 13 09 A7 EA 26 B9 91 22 52 D0 94 0E <b>74 6D 7A 98 8D 7B DE CD C3 A2 C2 49 1A C8 51 D2</b> | ÄaÜÄ..šě““RD“. tmz“.(bÄcÄ.ËQÖ       |
| F526ED   | 35 8E DB 95 B0 91 75 13 EA 5F EB A1 3F A0 3F AA <b>74 4D 5A 3C 08 75 2E 6F E0 BD F9 DE 7C 7D 7F 7C</b> | SŽÜ.*“u.ě_? ?“tmz<.u.o.ä“zúb ].     |
| 2106BFF  | 62 E5 05 3C 9D 7F D0 CD A4 E4 1C FA CC 7F 25 3E <b>74 6D 5A AC C8 D6 A1 1B 6A 7F 00 01 4F 9E 91 66</b> | bä.<.,Dl=ä.ül.%>tmz<.Öj...ÖzF       |
| 21C788D  | 43 BD B5 C3 92 76 3E FA 73 7E CF D8 6F 2B 35 38 <b>54 6D 5A CC 87 07 7B CE 5E F2 D1 F3 46 37 CA 75</b> | C½µÄ“v>ús- 0o+58TmZl{.i^oN6F7Ëu     |
| 25F6E68  | EA B1 DD CD AE 5D 45 47 90 55 C0 68 19 6A D0 E9 <b>74 4D 5A 6F EF 03 C6 48 96 E4 FC 7D 7C AD 0C 36</b> | ězYl® EG.UÄhJ.DétMZOi.EH-äü .. 6    |
| 28B790A  | 54 55 35 4E 62 68 32 61 54 61 35 4E 79 45 33 73 <b>54 6D 5A 4F 33 45 39 59 54 34 35 50 73 6B 2F 55</b> | TU5Nbk2aTs5NyE3sTmZO3E9YT45Psk/U    |
| 55CE888  | 2D B8 58 62 F3 C5 86 70 AC 9E 92 D3 58 87 C1 08 <b>74 6D 7A 54 0E B3 83 E3 A0 74 3A DA B4 1D 54 9C</b> | ->[b6Ä+p-z“ÖX+Ä.tmzT.“j8 tÜ“.Tœ     |
| 75E3D5F  | 00 B8 2D 97 81 FD CB 68 92 12 FC A7 D2 CB 7F 17 <b>54 4D 7A E9 EF 76 C8 8C 45 2F FB 3D 5D B4 46 2F</b> | „-y.Ëk“.üÖË..TmZëvËEE/ü= “F/        |
| 787A3FC  | 1A 72 69 D8 39 7D 2E 67 67 6C 55 6A 69 6B 54 42 <b>74 4D 7A 43 5A 46 67 1F 03 FC 03 53 6D 70 53 7B</b> | .ri09 .gg UjikTbTmZCZfg..u.SmpS{    |
| 78BB7A7  | DF 1B E1 C4 44 CB 1A 45 D8 7E 08 96 1A 44 43 2A <b>54 6D 5A E2 9F 78 25 64 01 36 77 3D 41 46 26 41</b> | B.äADE.ËÖ-.-.DC“TmZäYx%d.6w=AFÄ     |
| 78E098F  | 1C 70 4F 68 40 DF 74 16 E7 9C 5A 18 FF 76 54 EE <b>74 4D 7A CA 09 BA 7E 03 64 98 78 50 EE 29 02 F2</b> | ü Q_@Bt.çœZ.jvTtTmZë“-..d“xPj .ö    |
| 7DACB4D  | 3B 36 9D 77 4C 85 3F E8 93 04 EA 64 38 5D A1 25 <b>54 4D 5A 0F D1 FD 6C 5A 4F D0 34 B9 0D C2 01 18</b> | :6.wL...?e“.ëd8 ].%TmZ.Nj ZOD4“.Ä.. |
| 8136C41  | B2 77 D5 5B 2E B1 75 F5 58 2E B1 74 4D 59 2E 71 <b>74 6D 5A 4A DD E8 3A B6 94 62 ED C2 B4 92 62 EE</b> | “wÖ[.z.üX.z.tMY.qtmZJ“ÿeT“biÄ“bi    |
| 81402C7  | 2F 4D 54 49 36 4E 44 41 36 4D 44 46 55 4D 7A 45 <b>74 4D 7A 41 74 4E 51 3D 3D 22 66 B9 58 04 0F 44</b> | /MTI6NDA6MDFUMzEtTmZAtNQ==“f“X...D  |
| 81F0DF8  | 75 7A 91 97 B1 BF 8C 35 26 AD C4 51 9F 55 DB 25 <b>74 4D 7A 5F 5D C4 63 F3 6D 3D 66 3F B7 60 48 CD</b> | uz“—z.ÇE5.ÄQYÜÜ% tmZ.]Äcöme=f?“Hl   |
| 8597A8A  | 15 91 D4 2E BC 6F 85 28 C3 19 D1 C8 0B C3 88 79 <b>74 4D 5A BA 41 0D A2 09 46 DD 7C 0A 06 8D 94 B4</b> | “Ö.“%o...(.Ä.NË.Ä.“ytmZ“Ä.ç.FY ...“ |
| 85B0DCB  | E7 A8 68 51 61 17 A6 77 59 96 A1 40 17 FB E5 12 <b>74 4D 7A D9 78 6F 94 C6 16 BA AA 17 44 18 60 8A</b> | ç“hQa.¿wY- @.ü.ä.tmZÜxo““E.“D.Š     |
| 88DD36E  | 4A 73 61 47 39 77 62 32 46 71 5A 57 39 75 63 47 <b>74 6D 5A 32 6C 72 62 79 49 73 49 43 4A 6F 62 6D</b> | JsaG9wb2FqZW9ucGtmZ2lrbYslCJobm     |
| 902DB0C  | 6C 6A 00 0D 0F 20 00 66 B8 00 72 68 10 00 00 40 <b>54 4D 7A 11 72 68 00 73 18 00 66 00 74 79 0F 82</b> | lj... .f,rh...@TMZ.rh.s.f.ty,       |
| 91AF495  | 00 00 00 6A 37 70 6A 73 69 62 68 64 39 64 7A <b>74 6D 7A 6B 37 64 64 67 64 6F 68 78 75 78 35 6C</b>    | ...j7pjsibhd9dztmzk7ddgdohxux5l     |
| 95A508A  | 4C C8 DB 53 A3 39 89 BE 04 5E 2D 72 75 69 B8 ED <b>54 4D 7A 3C 8D 1A 7B 6E C7 3F C4 D9 34 2A BB 90</b> | LËÜ5E9%ç%Ä.“-rujJTMZ<..{nÇ?ÄÜ4*„    |
| 9938D81  | C1 7F DC 99 84 2E E1 13 FF 9F 77 85 56 08 FA 83 <b>74 4D 7A B9 40 30 B6 58 59 7A BD B8 F8 7A B1 8A</b> | Ä.Ü““..ä.yYw...V.üfTmZ“@0fXYz½.øzzŠ |
| A71DB0E  | A5 F0 80 6A 86 51 FE CD E7 9F B3 BB 7E C2 A3 12 <b>74 6D 7A CE 0F 95 9E 25 ED CF E9 A4 03 CA F4 09</b> | ¥ðej+QblçYš“--Ä.E.tmzi..z%ñëÄ.Ëö.   |
| B2F9AB7  | 32 89 89 E0 07 30 14 EC 02 7F 00 DF 83 EF C0 F1 <b>54 4D 7A 2D 41 90 1C 0D 44 E3 A3 22 5A 1D A9 8A</b> | ?.%ä.0.i...BfiÄñTmZ-A...DäE“Z.©Š    |
| B48F270  | 31 2F 30 2F 5F 64 6B 5F 68 74 74 70 73 3A 2F 2F <b>74 6D 7A 2E 63 6F 6D</b> 20 68 74 74 70 73 3A 2F 2F | 1/0/_dk_https://tmz.com https://    |
| B48F280  | 74 6D 7A 2E 63 6F 6D 20 68 74 74 70 73 3A 2F 2F <b>74 6D 7A 2E 63 6F 6D</b> 20 68 74 74 70 73 3A 2F 2F | tmz.com https://tmz.com https://    |
| B48F297  | 20 68 74 74 70 73 3A 2F 2F 69 6D 61 67 65 7A 2E <b>74 6D 7A 2E 63 6F 6D</b> 2F 69 6D 61 67 65 2F 30 63 | https://imagez.tnz.com/image/0c     |
| B48F370  | 31 2F 30 2F 5F 64 6B 5F 68 74 74 70 73 3A 2F 2F <b>74 6D 7A 2E 63 6F 6D</b> 20 68 74 74 70 73 3A 2F 2F | 1/0/_dk_https://tmz.com https://    |

Špecifikoval som to na „tmz.com“, keďže „tmz“ vyhodilo 4308 hitov a väčšina z nich mala náhodný text okolo seba a samotné slovo malo variácie čo sa týka jej veľkosti (veľké/malé písmeno). Predpokladám, že tieto texty sú iba prepísané fragmenty pamäti alebo sú pozostatky predošlých dát – pričom variabilita veľkosti znakov skôr naznačuje prepísanie dát ako ich uloženie.

| Checksum  | Search (124 hits)                                                                                      |                                     |
|-----------|--------------------------------------------------------------------------------------------------------|-------------------------------------|
| Offset    | Excerpt (hex)                                                                                          | Excerpt (text)                      |
| 1B88A307  | 73 73 5C 66 6C 6F 6F 7A 79 53 6F 66 74 31 40 5C <b>47 6F 73 73 69 70</b> 6D 6F 6E 67 65 72 30 41 5C 4E | ss\floozySoft1@\Gossipmonger0A\N    |
| 1F6DD054  | 63 6F 6D 6D 61 6E 64 65 78 65 3C 23 00 80 00 0A <b>67 6F 73 73 69 70</b> 65 72 2E 70 3D 23 00 80 00 05 | commandexe<#€.gossip.p=#€.          |
| 29F81EE5  | 6D 2F 73 65 61 72 63 68 3F 71 3D 62 65 73 74 2B <b>67 6F 73 73 69 70</b> 2B 77 65 62 73 69 74 65 73 26 | m/search?q=best+gossip+websites     |
| 2BA5F8B6  | 6E 0E 5E 94 C1 A4 72 4F 01 15 31 24 79 70 74 6F <b>67 6F 73 73 69 70</b> 76 88 26 91 BE 0E A4 0D 0E 65 | n.^^ÂrO..l\$yptogossipv'¼¼¼¼e       |
| 2D753AFD  | EB 2B AB FF 2D B8 46 CA 93 83 3E FD C2 A3 FF F1 <b>47 6F 73 73 69 70</b> 65 72 4D 6F 64 65 6C 67 65 74 | ë+«j-FÊ³>ýÄËñGossipModelget         |
| 2FC20DAB  | 20 01 00 AC F9 07 EA 0B 00 00 00 00 00 00 78 <b>67 6F 73 73 69 70</b> 2E 65 78 65 00 00 00 00 00 00    | ..r.ü.ë.....xgossip.exe.....        |
| 33D2010E  | 72 00 65 00 72 00 73 00 2E 00 7A 00 61 00 6E 00 <b>67 6F 73 73 69 70</b> 70 65 64 2E 61 6E 6C 67 00 6F | r.e.r.s...z.a.n.gossipped.anlg.o    |
| 3626C63E  | 4D 61 72 67 69 6E 20 46 72 6F 6E 74 69 65 72 20 <b>47 6F 73 73 69 70</b> AF 01 41 73 79 6E 63 52 61 74 | Margin Frontier Gossip".AsyncRat    |
| 36273EA2  | AC 14 FF 67 0A BA 44 1C CA F2 59 6E 7F DF A0 37 <b>67 6F 73 73 69 70</b> 65 72 2E 70 68 70 2F 72 61 74 | ~.yg.°D.êöYn.B 7gossip.php/rat      |
| 52E83061  | 6E 73 22 3A 20 5B 0A 20 20 20 20 20 20 22 <b>67 6F 73 73 69 70</b> 2D 74 76 2E 67 72 22 0A 20 20       | ns": [ "gossip-tv.gr".              |
| 55C6FA69  | 6C 2F 4D 53 0A 67 6F 73 73 61 6D 65 72 2F 4D 0A <b>67 6F 73 73 69 70</b> 2F 4D 44 52 5A 47 53 0A 67 6F | I/MS.gossamer/M.gossip/MDRZGS.go    |
| 55C6FA77  | 4D 0A 67 6F 73 73 69 70 2F 4D 44 52 5A 47 53 0A <b>67 6F 73 73 69 70</b> 65 72 2F 4D 0A 67 6F 73 73 69 | M.gossip/MDRZGS.gossip/M.gossi      |
| 55C6FA82  | 52 5A 47 53 0A 67 6F 73 73 69 70 65 72 2F 4D 0A <b>67 6F 73 73 69 70</b> 79 0A 67 6F 74 0A 67 6F 74 63 | RZGS.gossip/M.gossipy.got.gotc      |
| 56F68534  | 73 65 6C 69 6E 89 71 67 6F 73 73 65 74 74 8A C1 <b>67 6F 73 73 69 70</b> A2 D7 67 6F 73 73 69 70 69 6E | selin%«qgossett\$Agossip«x.gossipin |
| 56F6853C  | 6F 73 73 65 74 74 8A C1 67 6F 73 73 69 70 A2 D7 <b>67 6F 73 73 69 70</b> 69 6E 67 6F 03 67 6F 73 73 69 | ossett\$Agossip«x.gossiping¿gossi   |
| 56F68547  | 73 69 70 A2 D7 67 6F 73 73 69 70 69 6E 67 6F 03 <b>67 6F 73 73 69 70</b> 73 E1 B8 67 6F 73 74 61 D5 C1 | sip«x.gossiping¿gossips\$gostaÖÄ    |
| 59E0E528  | 00 00 07 00 FF 05 20 10 03 00 FF FF 0C 0D 40 2C <b>67 6F 73 73 69 70</b> 2D 74 76 2E 67 72 01 3C 01 01 | ....y...yÿ...@.gossip-tv.gr.<..     |
| 62E2719F  | 6E 10 0C 6A 61 76 63 A1 A0 15 87 5E 7C 01 28 0F <b>67 6F 73 73 69 70</b> 66 75 6E 64 B9 38 1C 0C 63 6C | ...javc; *~J.([gossipfund'8..cl     |
| 643834E5  | 6E 6C 69 6E 65 2E 62 65 F3 D6 DD EC 02 8F 6C 79 <b>67 6F 73 73 69 70</b> 73 2E 6E 65 F4 D7 D9 65 77 65 | nline.beöÖÿ..lygossips.neö«Üewe     |
| 1045DED9B | 72 65 6D 6F 74 65 6D 65 73 73 18 25 00 80 00 0A <b>67 6F 73 73 69 70</b> 65 72 6D 6F 19 25 00 80 00 0A | remotemess.%€.gossipermo.%€..       |
| 11357F305 | 6D 2F 73 65 61 72 63 68 3F 71 3D 62 65 73 74 2B <b>67 6F 73 73 69 70</b> 2B 77 65 62 73 69 74 65 73 26 | m/search?q=best+gossip+websites     |
| 120CB21E5 | 6D 2F 73 65 61 72 63 68 3F 71 3D 62 65 73 74 2B <b>67 6F 73 73 69 70</b> 2B 77 65 62 73 69 74 65 73 26 | m/search?q=best+gossip+websites     |
| 129643BCA | 5C 66 6C 6F 6F 7A 79 53 6F 66 74 77 61 72 65 5C <b>47 6F 73 73 69 70</b> 6D 6F 6E 67 65 72 69 6E 67 5C | \floozySoftware\Gossipmongering\    |
| 13037FD5E | 00 67 6F 72 69 6C 6C 61 00 67 6F 73 70 65 6C 00 <b>67 6F 73 73 69 70</b> 00 67 6F 76 65 72 6E 00 67 6F | .gorilla.gospel.gossip.govern.go    |
| 14CD74AC7 | 6F 76 65 0E 22 20 72 3C 02 11 30 24 79 70 74 6F <b>67 6F 73 73 69 70</b> 76 06 03 2D 28 14 73 2E 73 61 | ove." r<..öSyptogossipv..-(s.sa     |
| 18A9639A5 | 12 AC 33 0E BD 11 8A A0 12 15 69 28 79 70 74 6F <b>67 6F 73 73 69 70</b> 2E 0E DB 13 62 D0 04 1E D1 12 | ..~3.½:Š...llyptogossip..Ü.bö..N.   |
| 1B740ACE1 | 61 62 6C 65 20 45 6D 61 69 6C 0A 6F 66 66 69 73 <b>67 6F 73 73 69 70</b> 2E 63 6F 6D 2C 44 69 73 70 6F | able.Email.offisaoissio.com.Dispo   |

Pri vyhľadávani „gossip“ sme našli až 124 hitov. Predpokladáme, že útočník prehľadával viaceré stránky predtým ako si vybral TMZ ako svoj cieľ na únik dát.

HxD nevedel nájsť nejaký výskyt telefónneho čísla či emailu TMZ stránky – predpokladáme, že útočník iba vyhľadával informácie a nepoužil notebook na kontaktovanie.

| Checksum  | Search (45 hits)                                                                                       |                                   |
|-----------|--------------------------------------------------------------------------------------------------------|-----------------------------------|
| Offset    | Excerpt (hex)                                                                                          | Excerpt (text)                    |
| 1914D80B  | EE C5 65 55 8E 43 DD 93 FD 68 74 74 70 3A 2F 2F <b>63 65 6C 65 62 72 69 74 79 2D</b> 6E 75 64 65 2D 66 | iÄeUÛZÇÝ~ÿhttp://celebrity-nude-f |
| 30361C9E  | 2E 06 14 63 63 70 67 61 6D 7A 80 01 32 A1 08 34 <b>63 65 6C 65 62 72 69 74 79</b> 63 72 75 69 73 7A 3A | ...ccpgamz€¿¿4celebritycruis:z    |
| 40C3D9C4  | FC B0 A5 96 F9 BA B4 02 AA 68 74 74 70 3A 2F 2F <b>63 65 6C 65 62 72 69 74 79</b> 62 65 65 66 63 61 6B | ü*#-ü°.*http://celebritybeefcak   |
| 58573F50  | 2F 53 4D 0A 63 65 6C 65 62 72 61 74 6F 72 79 0A <b>63 65 6C 65 62 72 69 74 79</b> 2F 53 4D 0A 63 65 6C | /SM.celebratory.celebrity/SM.cel  |
| 122579CD6 | 9F 05 69 6E 76 65 6E 74 6F 72 79 54 02 30 00 2F <b>63 65 6C 65 62 72 69 74 79</b> 2A 01 3F 04 F1 DF FF | ü.inventoryT.0./celebrity".¿.ñBy  |
| 15C055856 | A1 5A EE B7 01 2A 9E 15 41 68 74 74 70 3A 2F 2F <b>63 65 6C 65 62 72 69 74 79</b> 68 6F 6C 6C 79 77 6F | ¿Zi-."¿Ahttp://celebrityhollywo   |
| 17605D8C6 | 63 6F 6D 7C 28 2E 2A 5B 2E 5D 29 2A 6D 61 74 68 <b>63 65 6C 65 62 72 69 74 79</b> 5B 2E 5D 63 6F 6D 7C | com ([".])"mathcelebrity[.].com   |
| 182E309DC | 52 59 03 5A 8E 03 00 0E 32 3B 00 52 43 07 34 16 <b>63 65 6C 65 62 72 69 74 79</b> 6D 6F 76 69 12 6F 27 | RY.ZZ...¿.RC.4.celebritymovi.o'   |
| 1B7172BBF | 20 45 6D 61 69 6C 0A 61 75 74 68 6F 72 69 74 79 <b>63 65 6C 65 62 72 69 74 79</b> 2E 63 6F 6D 2C 44 69 | Email.authoritycelebrity.com,Di   |
| 1B76B14C4 | 69 73 70 6F 73 61 62 6C 65 20 45 6D 61 69 6C 0A <b>63 65 6C 65 62 72 69 74 79</b> 2D 77 68 69 7A 2E 63 | isposable Email.celebrity-whiz.c  |
| 1B76B14E8 | 69 73 70 6F 73 61 62 6C 65 20 45 6D 61 69 6C 0A <b>63 65 6C 65 62 72 69 74 79</b> 61 64 7A 2E 63 6F 6D | isposable Email.celebrityadz.com  |
| 1B76B150A | 69 73 70 6F 73 61 62 6C 65 20 45 6D 61 69 6C 0A <b>63 65 6C 65 62 72 69 74 79</b> 64 69 73 63 6F 75 6E | isposable Email.celebritydiscoun  |
| 1B76B1533 | 69 73 70 6F 73 61 62 6C 65 20 45 6D 61 69 6C 0A <b>63 65 6C 65 62 72 69 74 79</b> 77 65 69 67 68 74 68 | isposable Email.celebrityweighth  |
| 1B78B289A | 73 61 62 6C 65 20 45 6D 61 69 6C 0A 74 68 65 2D <b>63 65 6C 65 62 72 69 74 79</b> 2D 63 6F 6E 66 65 73 | sable Email.the-celebrity-confes  |
| 1B7904B03 | 6C 65 20 45 6D 61 69 6C 0A 77 6F 72 6E 62 79 61 <b>63 65 6C 65 62 72 69 74 79</b> 2E 63 6F 6D 2C 44 69 | le Email.wornbyacelebrity.com,Di  |
| 1C38758ED | 74 20 74 68 65 20 69 6E 76 65 6E 74 6F 72 79 2F <b>63 65 6C 65 62 72 69 74 79</b> 70 6F 68 65 72 2E 65 | t the inventory/celebritypoker.e  |
| 1DA7C13F2 | 20 2D 20 54 68 65 20 43 72 61 7A 69 65 73 74 20 <b>43 65 6C 65 62 72 69 74 79</b> 20 52 69 64 65 72 73 | - The Craziest Celebrity Riders   |
| 224E1D115 | 6F 74 61 79 23 01 DC 5E FE 00 4E 2F 00 80 12 1F <b>43 65 6C 65 62 72 69 74 79</b> 20 2D 20 42 6C 6F 6F | otay#.Ü^þ.N/./€.Celebrity - Bloo  |
| 22F5E00CC | 65 00 00 00 AD 01 00 00 F6 E5 78 CC 15 00 00 00 <b>43 45 4C 45 42 52 49 54 59</b> 42 4C 45 4E 44 5F 45 | e.....öäxl....CELEBRITYBLEND_E    |
| 22F5E00F0 | 59 00 00 00 AD 01 00 00 CE 77 37 89 15 00 00 00 <b>63 65 6C 65 62 72 69 74 79</b> 62 6C 65 6E 64 2F 65 | Y.....Iw7%.....celebrityblend/e   |
| 2343B8612 | 65 20 69 6E 74 65 72 6E 61 74 69 6F 6E 61 6C 20 <b>63 65 6C 65 62 72 69 74 79</b> 20 66 65 6D 61 6C 65 | e international celebrity female  |
| 2362891CF | 20 44 4D 69 6E 67 20 41 20 46 61 6D 6F 75 73 20 <b>43 65 6C 65 62 72 69 74 79</b> 38 96 E3 83 04 62 18 | DMing A Famous Celebrity8-äf.b.   |
| 23700340F | 51 44 71 38 30 4D 4B 32 63 46 6F 74 61 79 12 1F <b>43 65 6C 65 62 72 69 74 79</b> 20 42 6C 6F 6F       | QDq80MK2cFotay..Celebrity - Bloo  |
| 23A960BDA | 65 20 69 6E 74 65 72 6E 61 74 69 6F 6E 61 6C 20 <b>63 65 6C 65 62 72 69 74 79</b> 20 66 65 6D 61 6C 65 | e international celebrity female  |
| 23C7AF2DA | CB A3 E6 52 40 43 8B 88 92 6E EF A7 C8 0C 12 0E <b>43 65 6C 65 62 72 69 74 79</b> 20 53 68 69 6E 1A DB | ÊÆeR@C<¿ni\$£...Celebrity Skin.Ü  |
| 23C7AF2F2 | 3C 56 73 2E 45 9D AD 97 0C FA CD D0 44 7D 12 0E <b>43 65 6C 65 62 72 69 74 79</b> 20 53 68 69 6E 1A 18 | <Vs.E.....üfDD)..Celebrity Skin.. |
| 23C7AF529 | 4D 41 F2 A1 30 68 2A E0 79 36 EC 10 01 DA 01 0E <b>43 65 6C 65 62 72 69 74 79</b> 20 53 68 69 6E 82 02 | MAö¿0h*äyöü..Ü..Celebrity Skin..  |
| ¿NDR8A9A3 | CB A3 E6 52 40 43 8B 88 92 6E EF A7 C8 0C 12 0E <b>43 65 6C 65 62 72 69 74 79</b> 20 53 68 69 6E 1A DB | ÊÆeR@C<¿ni\$£...Celebritv Skin.Ü  |

Pri vyhľadani „celebrity“ nám vyskočilo 45 výsledkov a všetky sú spojené s nejakými stránkami či emailovými adresami.

Takže vieme s istotou povedať, že došlo ku vyhľadávaniu neprístupných stránok a informácií na rozšírenie dát. Ale nevieme posúdiť akou formou boli odoslané fotky ďalej od firmy do TMZ – pomocou USB, E-mailom alebo inou formou.

### Analýza pripojených zariadení

Pomocou USBDeview sme si pozreli, aké zariadenia boli naposledy pripojené na notebooku. Skúsime nájsť či sa bude nachádzať naše USB zariadenie v zozname naposledy pripojených zariadení. USB názov ktorý hľadáme je „Kingston DataTraveler 3.0“

|                      |                                                        |
|----------------------|--------------------------------------------------------|
| Device Name          | : Port_#0004.Hub_#0002                                 |
| Description          | : Kingston DataTraveler 3.0 USB Device                 |
| Device Type          | : Mass Storage                                         |
| Connected            | : No                                                   |
| Safe To Unplug       | : Yes                                                  |
| Disabled             | : No                                                   |
| USB Hub              | : No                                                   |
| Drive Letter         | : D:                                                   |
| Serial Number        | : F46D0461E255F241C94C2F0C                             |
| Registry Time 1      | : 02/03/2025 22:05:20                                  |
| Registry Time 2      | : 02/03/2025 17:30:18                                  |
| VendorID             | : 0951                                                 |
| ProductID            | : 1666                                                 |
| Firmware Revision    | : 0.01                                                 |
| WCID                 | :                                                      |
| USB Class            | : 08                                                   |
| USB SubClass         | : 06                                                   |
| USB Protocol         | : 50                                                   |
| Hub / Port           | :                                                      |
| Computer Name        | : DESKTOP-A6QMBAJ                                      |
| Vendor Name          | :                                                      |
| Product Name         | :                                                      |
| ParentId Prefix      | :                                                      |
| Service Name         | : USBSTOR                                              |
| Service Description: | @usbstor.inf,%USBSTOR.SvcDesc%;USB Mass Storage Driver |
| Driver Filename      | : USBSTOR.SYS                                          |
| Device Class         | :                                                      |
| Device Mfg           | : Compatible USB storage device                        |
| Friendly Name        | :                                                      |
| Power                | :                                                      |
| USB Version          | :                                                      |
| Driver Description:  | USB Mass Storage Device                                |
| Driver Version       | : 10.0.19041.4355                                      |
| Driver InfSection    | : USBSTOR_BULK.NT                                      |
| Driver InfPath       | : usbstor.inf                                          |
| Instance ID          | : USB\VID_0951&PID_1666\F46D0461E255F241C94C2F0C       |
| Capabilities         | : Removable, UniqueID, SurpriseRemovalOK               |
| Install Time         | : 02/03/2025 17:30:18                                  |
| First Install Time:  | 02/03/2025 17:30:18                                    |
| Connect Time         | : 01/03/2025 22:05:20                                  |
| Disconnect Time      | : 01/03/2025 22:06:17                                  |

Z tejto správy vidíme, že naše zariadenie bolo pripojené na manažérov notebook a bolo to zrovna deň či dva predtým ako unikli fotky na internet (zvýraznené). Takže vieme povedať, že USB je spojené s únikom fotiek.

## Analýza prehľadávaných stránok

Z RAM sme zistili, že sa pristupovali nejaké stránky ohľadom klebiet a TMZ ale nevieme kedy presne – preto si pre kontrolu extrahujeme históriu prehľadávania z tohto notebooku a upresníme si dátum sprístupnenia týchto stránok. Pomocou BrowsingHistoryView som si extrahoval históriu vyhľadávania a našiel tieto zaujímavé výsledky:

```
=====
URL      :
https://www.google.com/search?q=tmz&oq=tmz&gs_lcrp=EgZjaHJvbWUqBggAEEUYOzIGCAAQRRg7MgcIARAAGIAEMgcIAhAA
GIAEMgcIAxAuGIAEMgYIBBBFGDwyBggFEUYPDIGCAYQRRg8MgYIBxAuGEDSAQgXNTc5ajBqMagCALACAA&sourceid=chrome&ie=U
TF-8
Title    : tmz - Google Search
Visit Time : 02/03/2025 20:38:06
Visit Count : 1
Visited From :
Visit Type :
Visit Duration : 00:00:02.245
Web Browser : Brave
User Profile : Alex Wolfie
Browser Profile : Default
URL Length : 210
Typed Count :
History File : C:\Users\Alex Wolfie\AppData\Local\BraveSoftware\Brave-Browser\User
Data\Default\History
Record ID : 19047
=====
=====
URL      : https://www.tnz.com/pages/contact-us/
Title    : Contact Us
Visit Time : 02/03/2025 20:29:38
Visit Count : 1
Visited From : https://www.tnz.com/
Visit Type :
Visit Duration : 00:00:15.259
Web Browser : Brave
User Profile : Alex Wolfie
Browser Profile : Default
URL Length : 37
Typed Count :
History File : C:\Users\Alex Wolfie\AppData\Local\BraveSoftware\Brave-Browser\User
Data\Default\History
Record ID : 19027
=====
=====
URL      : https://www.tnz.com/
Title    : Celebrity News | Entertainment News | TMZ.com
Visit Time : 02/03/2025 20:29:38
Visit Count : 5
Visited From : https://www.tnz.com/
Visit Type :
Visit Duration : 00:00:00.373
Web Browser : Brave
User Profile : Alex Wolfie
Browser Profile : Default
URL Length : 20
Typed Count :
History File : C:\Users\Alex Wolfie\AppData\Local\BraveSoftware\Brave-Browser\User
Data\Default\History
Record ID : 19026
=====
```

Z vyznačených častí vidíme, že osoba sprístupnila stránku **tmz.com** 2.3.2025 a dokonca aj 5x. Potom aj sprístupnili stránku kontaktovania TMZ. Vyzerá to, že akákoľvek komunikácia sa vyskytla – vyskytla sa na manažérovom notebooku ale ešte nevieme upresniť či sa odoslali fotky e-mailom alebo USB kľúčom.

```

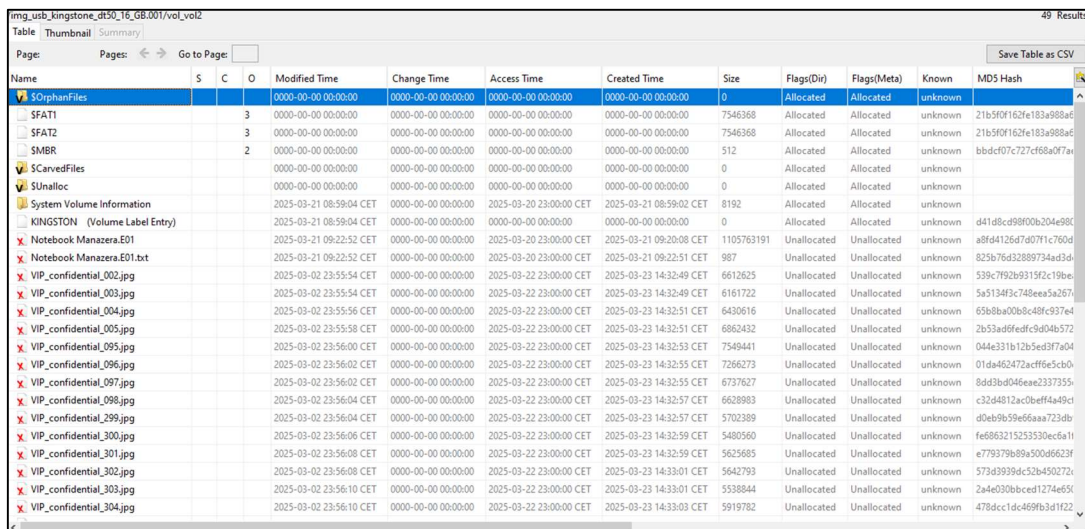
=====
URL      : https://www.diskpart.com/articles/how-to-delete-everything-on-a-usb-flash-drive-0310.html#:~:text=If%20you%20want%20to%20delete,rid%20of%20all%20files%20completely.
Title    : How to Delete Everything on a USB Flash Drive [Completely]?
Visit Time      : 02/03/2025 20:30:17
Visit Count     : 1
Visited From    :
URL      : https://www.google.com/search?q=how+to+delete+usb+content&oq=how+to+delete+usb+content&gs_lcrp=EgZjaHJvbnUyBggAEEUYOTIICAQABgWGB4yCAgCEAAYFhgeMg0IAxAAGIYDGIAGIoFMg0IBBAAGIYDGIAGIoFMg0IBRAAGIYDGIAGIoFMg0IBhAAGIYDGIAGIoFMg0IBxAAGIAEGKIEMgoICBAAGIAEGKIEMgYICRAuGEDSAQg1MTY5ajBqMagCALACAA&sourceid=chrome&ie=UTF-8
Visit Type      :
Visit Duration   : 00:00:08.063
Web Browser     : Brave
User Profile     : Alex Wolfie
Browser Profile  : Default
URL Length      : 164
Typed Count     :
History File     : C:\Users\Alex Wolfie\AppData\Local\BraveSoftware\Brave-Browser\User
Data\Default\History
Record ID       : 19030
=====
=====
URL      :
https://www.google.com/search?q=how+to+delete+usb+content&oq=how+to+delete+usb+content&gs_lcrp=EgZjaHJvbnUyBggAEEUYOTIICAQABgWGB4yCAgCEAAYFhgeMg0IAxAAGIYDGIAGIoFMg0IBBAAGIYDGIAGIoFMg0IBRAAGIYDGIAGIoFMg0IBhAAGIYDGIAGIoFMg0IBxAAGIAEGKIEMgoICBAAGIAEGKIEMgYICRAuGEDSAQg1MTY5ajBqMagCALACAA&sourceid=chrome&ie=UTF-8
Title          : how to delete usb content - Google Search
Visit Time     : 02/03/2025 20:30:13
Visit Count    : 1
Visited From   :
Visit Type     :
Visit Duration : 00:00:03.762
Web Browser    : Brave
User Profile   : Alex Wolfie
Browser Profile : Default
URL Length     : 314
Typed Count    :
History File   : C:\Users\Alex Wolfie\AppData\Local\BraveSoftware\Brave-Browser\User
Data\Default\History
Record ID      : 19029
=====

```

No s nasledujúcich vyhľadávaní vieme posúdiť, že sa daná osoba snažila naučiť/vykonať vymazanie celého USB disku – takže už je viacej potvrdené, že USB je spojené s prípadom. A pravdepodobne sa fotky preniesli a zverejnili pomocou USB zariadenia „Kingstone“.

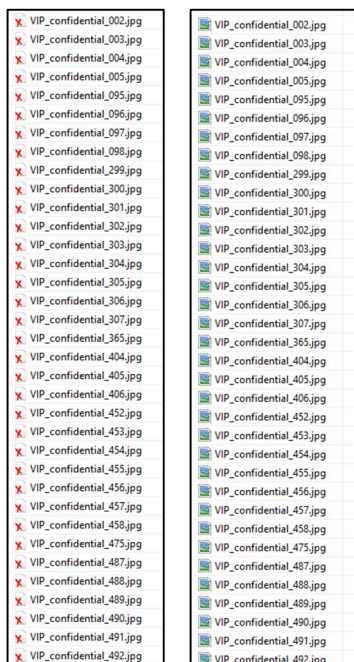
## Analýza USB zariadenia

Všetky predošlé stopy smerujú ku tomu, že naše USB zariadenie sa využívalo tak sa pozrieme na to USB a zistíme – čo sa s ním dialo...



| Name                          | S | C | O | Modified Time           | Change Time         | Access Time             | Created Time            | Size       | Flags(Dir)  | Flags(Meta) | Known   | MD5 Hash             |
|-------------------------------|---|---|---|-------------------------|---------------------|-------------------------|-------------------------|------------|-------------|-------------|---------|----------------------|
| OrphanFiles                   |   |   |   | 0000-00-00 00:00:00     | 0000-00-00 00:00:00 | 0000-00-00 00:00:00     | 0000-00-00 00:00:00     | 0          | Allocated   | Allocated   | unknown |                      |
| SFAT1                         |   |   | 3 | 0000-00-00 00:00:00     | 0000-00-00 00:00:00 | 0000-00-00 00:00:00     | 0000-00-00 00:00:00     | 7546368    | Allocated   | Allocated   | unknown | 21b5f0f162fe183a988a |
| SFAT2                         |   |   | 3 | 0000-00-00 00:00:00     | 0000-00-00 00:00:00 | 0000-00-00 00:00:00     | 0000-00-00 00:00:00     | 7546368    | Allocated   | Allocated   | unknown | 21b5f0f162fe183a988a |
| SMBR                          |   |   | 2 | 0000-00-00 00:00:00     | 0000-00-00 00:00:00 | 0000-00-00 00:00:00     | 0000-00-00 00:00:00     | 512        | Allocated   | Allocated   | unknown | bbdcf07c727cf68a977a |
| SCarvedFiles                  |   |   |   | 0000-00-00 00:00:00     | 0000-00-00 00:00:00 | 0000-00-00 00:00:00     | 0000-00-00 00:00:00     | 0          | Allocated   | Allocated   | unknown |                      |
| SUnalloc                      |   |   |   | 0000-00-00 00:00:00     | 0000-00-00 00:00:00 | 0000-00-00 00:00:00     | 0000-00-00 00:00:00     | 0          | Allocated   | Allocated   | unknown |                      |
| System Volume Information     |   |   |   | 2025-03-21 08:59:04 CET | 0000-00-00 00:00:00 | 2025-03-20 23:00:00 CET | 2025-03-21 08:59:02 CET | 8192       | Allocated   | Allocated   | unknown |                      |
| KINGSTON (Volume Label Entry) |   |   |   | 2025-03-21 08:59:04 CET | 0000-00-00 00:00:00 | 0000-00-00 00:00:00     | 0000-00-00 00:00:00     | 0          | Allocated   | Allocated   | unknown | d41d8cd98f00b204e980 |
| Notebook Manazera.E01         |   |   |   | 2025-03-21 09:22:52 CET | 0000-00-00 00:00:00 | 2025-03-20 23:00:00 CET | 2025-03-21 09:20:08 CET | 1105763191 | Unallocated | Unallocated | unknown | a8fd4126d7d0771c760d |
| Notebook Manazera.E01.txt     |   |   |   | 2025-03-21 09:22:52 CET | 0000-00-00 00:00:00 | 2025-03-20 23:00:00 CET | 2025-03-21 09:22:51 CET | 987        | Unallocated | Unallocated | unknown | 825b76d32889734d3d   |
| VIP_confidential_002.jpg      |   |   |   | 2025-03-02 23:55:54 CET | 0000-00-00 00:00:00 | 2025-03-22 23:00:00 CET | 2025-03-23 14:32:49 CET | 6612625    | Unallocated | Unallocated | unknown | 539c7992b9315f2c19be |
| VIP_confidential_003.jpg      |   |   |   | 2025-03-02 23:55:54 CET | 0000-00-00 00:00:00 | 2025-03-22 23:00:00 CET | 2025-03-23 14:32:49 CET | 6161722    | Unallocated | Unallocated | unknown | 5a5134f3c748ee5a267f |
| VIP_confidential_004.jpg      |   |   |   | 2025-03-02 23:55:56 CET | 0000-00-00 00:00:00 | 2025-03-22 23:00:00 CET | 2025-03-23 14:32:51 CET | 6430616    | Unallocated | Unallocated | unknown | 65b8ba00b8c48fc937e4 |
| VIP_confidential_005.jpg      |   |   |   | 2025-03-02 23:55:58 CET | 0000-00-00 00:00:00 | 2025-03-22 23:00:00 CET | 2025-03-23 14:32:51 CET | 6862432    | Unallocated | Unallocated | unknown | 2b53ad9fe0fc9d04b572 |
| VIP_confidential_095.jpg      |   |   |   | 2025-03-02 23:56:00 CET | 0000-00-00 00:00:00 | 2025-03-22 23:00:00 CET | 2025-03-23 14:32:53 CET | 7549441    | Unallocated | Unallocated | unknown | 044e331b12b5ed377a04 |
| VIP_confidential_096.jpg      |   |   |   | 2025-03-02 23:56:02 CET | 0000-00-00 00:00:00 | 2025-03-22 23:00:00 CET | 2025-03-23 14:32:55 CET | 7266273    | Unallocated | Unallocated | unknown | 01da462472ae0ff5c0b0 |
| VIP_confidential_097.jpg      |   |   |   | 2025-03-02 23:56:02 CET | 0000-00-00 00:00:00 | 2025-03-22 23:00:00 CET | 2025-03-23 14:32:55 CET | 6737627    | Unallocated | Unallocated | unknown | 8dd3bd046eae2337355f |
| VIP_confidential_098.jpg      |   |   |   | 2025-03-02 23:56:04 CET | 0000-00-00 00:00:00 | 2025-03-22 23:00:00 CET | 2025-03-23 14:32:57 CET | 6628983    | Unallocated | Unallocated | unknown | c32d4812ac0beff4a9c1 |
| VIP_confidential_299.jpg      |   |   |   | 2025-03-02 23:56:04 CET | 0000-00-00 00:00:00 | 2025-03-22 23:00:00 CET | 2025-03-23 14:32:57 CET | 5702389    | Unallocated | Unallocated | unknown | d0eb659e66aaa723db   |
| VIP_confidential_300.jpg      |   |   |   | 2025-03-02 23:56:06 CET | 0000-00-00 00:00:00 | 2025-03-22 23:00:00 CET | 2025-03-23 14:32:59 CET | 5480560    | Unallocated | Unallocated | unknown | fe686321525350ec5a1f |
| VIP_confidential_301.jpg      |   |   |   | 2025-03-02 23:56:08 CET | 0000-00-00 00:00:00 | 2025-03-22 23:00:00 CET | 2025-03-23 14:32:59 CET | 5625685    | Unallocated | Unallocated | unknown | e779379b89a500a6623f |
| VIP_confidential_302.jpg      |   |   |   | 2025-03-02 23:56:08 CET | 0000-00-00 00:00:00 | 2025-03-22 23:00:00 CET | 2025-03-23 14:33:01 CET | 5642793    | Unallocated | Unallocated | unknown | 573d9939dc52b450272f |
| VIP_confidential_303.jpg      |   |   |   | 2025-03-02 23:56:10 CET | 0000-00-00 00:00:00 | 2025-03-22 23:00:00 CET | 2025-03-23 14:33:01 CET | 5338844    | Unallocated | Unallocated | unknown | 2a4e030bced1274e65f  |
| VIP_confidential_304.jpg      |   |   |   | 2025-03-02 23:56:10 CET | 0000-00-00 00:00:00 | 2025-03-22 23:00:00 CET | 2025-03-23 14:33:03 CET | 5919782    | Unallocated | Unallocated | unknown | 478dccc1dc469b3d1f22 |

Takže podľa fotky vidíme, že sa na USB odohralo nejaké nahratie fotiek a následne aj ich vymazanie – došlo ku nesprávnej sanitácii zariadenia. Ale nevieme či zo strany IT oddelenia alebo vinníka, ktorý rozniesol tieto fotky ďalej. Skontrolujeme si, či sa všetky tieto fotky zhodujú s tými ktoré unikli na internet – overíme si tým, že či boli prenášané tie isté fotky na tomto zariadení alebo to bolo zariadenie, ktoré sa používalo na prácu v projekte.



|                          |                          |
|--------------------------|--------------------------|
| VIP_confidential_002.jpg | VIP_confidential_002.jpg |
| VIP_confidential_003.jpg | VIP_confidential_003.jpg |
| VIP_confidential_004.jpg | VIP_confidential_004.jpg |
| VIP_confidential_005.jpg | VIP_confidential_005.jpg |
| VIP_confidential_095.jpg | VIP_confidential_095.jpg |
| VIP_confidential_096.jpg | VIP_confidential_096.jpg |
| VIP_confidential_097.jpg | VIP_confidential_097.jpg |
| VIP_confidential_098.jpg | VIP_confidential_098.jpg |
| VIP_confidential_299.jpg | VIP_confidential_299.jpg |
| VIP_confidential_300.jpg | VIP_confidential_300.jpg |
| VIP_confidential_301.jpg | VIP_confidential_301.jpg |
| VIP_confidential_302.jpg | VIP_confidential_302.jpg |
| VIP_confidential_303.jpg | VIP_confidential_303.jpg |
| VIP_confidential_304.jpg | VIP_confidential_304.jpg |
| VIP_confidential_305.jpg | VIP_confidential_305.jpg |
| VIP_confidential_306.jpg | VIP_confidential_306.jpg |
| VIP_confidential_307.jpg | VIP_confidential_307.jpg |
| VIP_confidential_365.jpg | VIP_confidential_365.jpg |
| VIP_confidential_404.jpg | VIP_confidential_404.jpg |
| VIP_confidential_405.jpg | VIP_confidential_405.jpg |
| VIP_confidential_406.jpg | VIP_confidential_406.jpg |
| VIP_confidential_452.jpg | VIP_confidential_452.jpg |
| VIP_confidential_453.jpg | VIP_confidential_453.jpg |
| VIP_confidential_454.jpg | VIP_confidential_454.jpg |
| VIP_confidential_455.jpg | VIP_confidential_455.jpg |
| VIP_confidential_456.jpg | VIP_confidential_456.jpg |
| VIP_confidential_457.jpg | VIP_confidential_457.jpg |
| VIP_confidential_458.jpg | VIP_confidential_458.jpg |
| VIP_confidential_475.jpg | VIP_confidential_475.jpg |
| VIP_confidential_487.jpg | VIP_confidential_487.jpg |
| VIP_confidential_488.jpg | VIP_confidential_488.jpg |
| VIP_confidential_489.jpg | VIP_confidential_489.jpg |
| VIP_confidential_490.jpg | VIP_confidential_490.jpg |
| VIP_confidential_491.jpg | VIP_confidential_491.jpg |
| VIP_confidential_492.jpg | VIP_confidential_492.jpg |

Obrázky, ktoré boli vymazané na USB

Obrázky, ktoré unikli na internet

Tak ako môžeme vidieť, jedná sa o tie isté fotky ktoré unikli na internet – pravdepodobne vinník použil toto USB zariadenie na prenos týchto fotiek. Ale stále nevieme - kto presne ich odniesol kam?

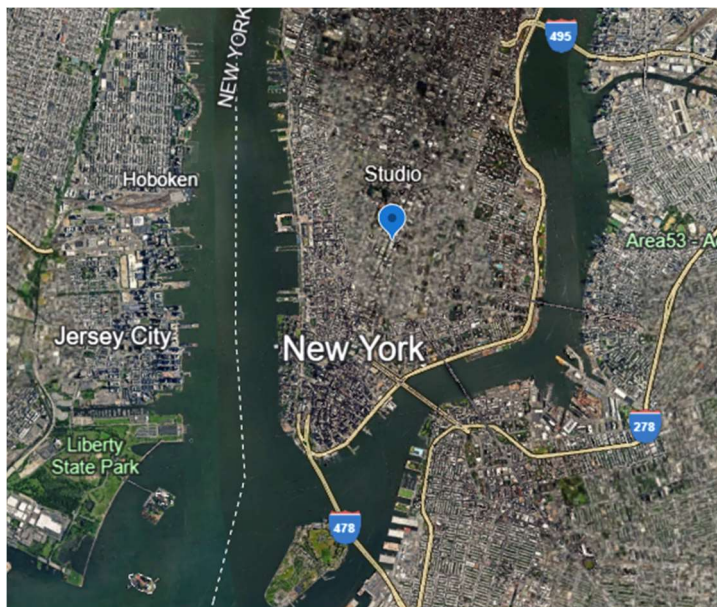
## Analýza fotiek a ich metadát

Keď sa pozrieme na metadáta originálnych fotiek – vieme vidieť kde boli vytvorené a akým foťákom boli vytvorené a iné metadáta. Tieto metadáta vieme porovnať s tými fotkami - ktoré sa mali vydať, originálmi a uniknutými fotkami – podľa toho vieme posúdiť ďalej čo sa dialo pravdepodobne.

Extrahoval som si metadáta pomocou exif tool do CVS formátu a môžeme tak vyhľadávať a porovnávať metadáta rovnakých fotiek (jedna z úniku a druhá originál od štúdia). Vieme posúdiť z tohto porovnávania, že niektoré informácie sú rozdielne a môžu poskytovať ďalšie stopy ku nášmu vinníkovi.

[illegible]

Pri metadátoch originálnych fotiek máme takéto údaje - ktoré budeme hľadať v tabuľke metadát uniknutých fotiek. Hľadáme hlavne šírku a výšku GPS pozície našich fotiek. V originálnych fotkách nás to smeruje na 40° 43' 29" N a 73° 59' 48" W – čo je v centre New York, čo je očakávané keďže štúdio je založené v New Yorku.



Ale tieto isté údaje budeme hľadať v metadátach uniknutých fotiek.

|                   |                   |                   |                   |                   |
|-------------------|-------------------|-------------------|-------------------|-------------------|
| 37 deg 32' 54.00" | 87 deg 52' 19.00" | 2.3.0.0           | Off               | Disable           |
| 2.3.0.0           | Off               | Disable           | 8.41 m            |                   |
| Not Known         | 38.3 deg          | 37 deg 32' 54.00" | 87 deg 52' 19.00" | 37 deg 32' 54.00" |
| 37 deg 32' 54.00" | 87 deg 52' 19.00" | 2.3.0.0           | Off               | Disable           |
| 37 deg 32' 54.00" | 87 deg 52' 19.00" | 37 deg 32' 54.00" | 87 deg 52' 19.00" | 2.3.0.0           |
| 51.0 deg          | 37 deg 32' 54.00" | 87 deg 52' 19.00" | 37 deg 32' 54.00" | 87 deg 52' 19.00" |
| 37 deg 32' 54.00" | 87 deg 52' 19.00" | 37 deg 32' 54.00" | 87 deg 52' 19.00" | 2.3.0.0           |
| 37 deg 32' 54.00" | 87 deg 52' 19.00" | 37 deg 32' 54.00" | 87 deg 52' 19.00" | 2.3.0.0           |
| 37 deg 32' 54.00" | 87 deg 52' 19.00" | 37 deg 32' 54.00" | 87 deg 52' 19.00" | 2.3.0.0           |
| 37 deg 32' 54.00" | 87 deg 52' 19.00" | 37 deg 32' 54.00" | 87 deg 52' 19.00" | 2.3.0.0           |
| 41.8 deg          | 37 deg 32' 54.00" | 87 deg 52' 19.00" | 37 deg 32' 54.00" | 87 deg 52' 19.00" |
| 2.3.0.0           | Off               | Disable           | 9.78 m            |                   |
| 87 deg 52' 19.00" | 37 deg 32' 54.00" | 87 deg 52' 19.00" | 2.3.0.0           | Off               |
| 87 deg 52' 19.00" | 37 deg 32' 54.00" | 87 deg 52' 19.00" | 2.3.0.0           | Off               |
| One-shot AF       | Not Known         | 45.9 deg          | 37 deg 32' 54.00" | 87 deg 52' 19.00" |
| 87 deg 52' 19.00" | 2.3.0.0           | Off               | Disable           | 5.98 m            |
| 37 deg 32' 54.00" | 87 deg 52' 19.00" | 2.3.0.0           | Off               | Disable           |
| 37 deg 32' 54.00" | 87 deg 52' 19.00" | 2.3.0.0           | Off               | Disable           |
| 87 deg 52' 19.00" | 37 deg 32' 54.00" | 87 deg 52' 19.00" | 2.3.0.0           | Off               |
| 87 deg 52' 19.00" | 2.3.0.0           | Off               | Disable           | 3.03 m            |
| 87 deg 52' 19.00" | 37 deg 32' 54.00" | 87 deg 52' 19.00" | 2.3.0.0           | Off               |

Ako je vidieť vyššie uvedené – dáta sa nejako poprehadzovali. Neviem či to je chyba poškodenia dát cez kompresiu alebo chyba extrakcie dát. Napriek tomu, našiel som si tie rovnaké fotky čo som porovnával z uniknutých s originálnymi a hneď sme videli rozdiel v súradniciach fotky. Tento krát nás smernice 37° 32’ 54’’ N a 87° 52’ 19’’ W umiestňujú na miesto v Kentucky, USA – špecificky, blízko Pride Rd.



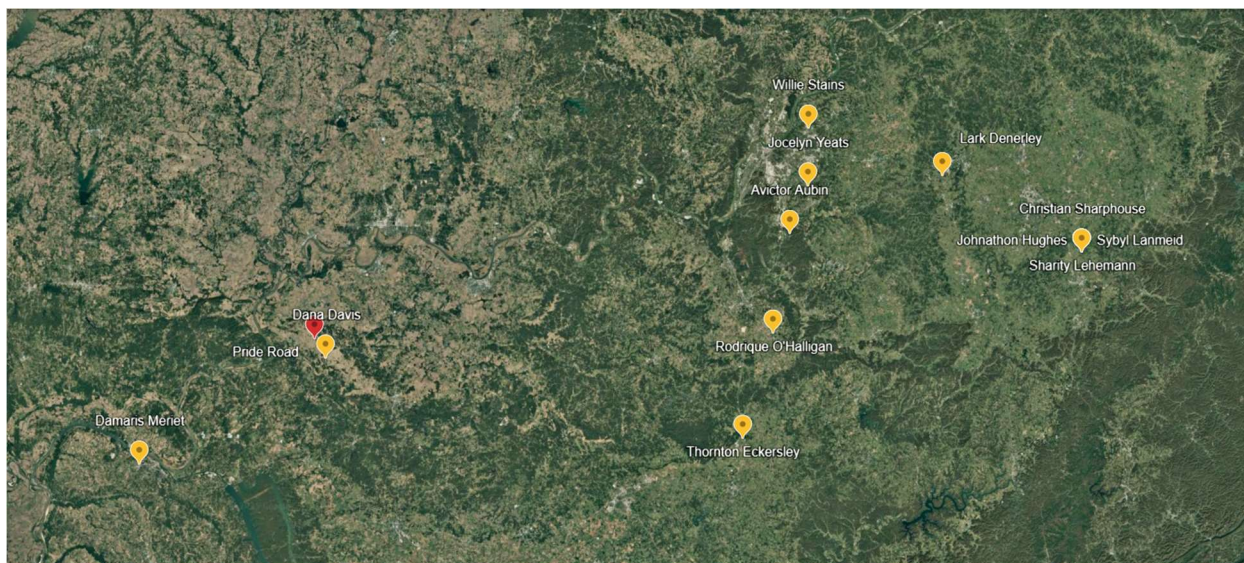
Takže náš vinník bude pochádzať z Kentucky, USA – najlepšie nejaký z okolia Pride Rd.

## Analýza databázy zamestnancov

Z poskytnutej databázy zamestnancov sme si upresnili zamestnancov, ktorý pochádzajú z Kentucky. Vyšlo nám 12 výsledkov z 1 000 zamestnancov – odľahčilo sa nám množstvo e-mailovej komunikácie na skúmanie.

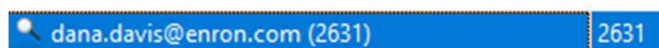
| employee | full_name            | job_title                     | department         | email                       | phone_num    | hire_date  | salary    | gender     | address                 | state    |
|----------|----------------------|-------------------------------|--------------------|-----------------------------|--------------|------------|-----------|------------|-------------------------|----------|
| 142      | Sybyl Lanmeid        | VP Sales                      | Human Resources    | slanmeid3x@phoca.cz         | 859-436-7502 | 06/04/2018 | 47464.98  | Bigender   | 0188 Debra Circle       | Kentucky |
| 164      | Sharity Lehemann     | Registered Nurse              | Accounting         | slehemann4j@posteros.com    | 859-681-9537 | 26/06/2024 | 93909.28  | Female     | 1175 Swallow Park       | Kentucky |
| 171      | Willie Stains        | Community Outreach Specialist | Human Resources    | wstains4q@cbslocal.com      | 502-800-3485 | 07/09/2020 | 107013.52 | Female     | 584 Summer Ridge Way    | Kentucky |
| 180      | Avictor Aubin        | Food Chemist                  | Product Management | aaubin4z@nyu.edu            | 502-811-4555 | 22/05/2015 | 87909.88  | Male       | 7 Claremont Lane        | Kentucky |
| 281      | Lark Denerley        | Design Engineer               | Training           | ldenerley7s@usnews.com      | 502-644-8200 | 30/03/2015 | 47325.64  | Female     | 18 Evergreen Parkway    | Kentucky |
| 313      | Damaris Meriet       | Financial Advisor             | Human Resources    | dmeriet8o@marketwatch.com   | 502-333-2529 | 24/09/2023 | 35308.38  | Female     | 1 McBride Terrace       | Kentucky |
| 440      | Christian Sharphouse | Pharmacist                    | Legal              | csharpousec7@deviantart.com | 502-907-6174 | 09/02/2024 | 40588.78  | Non-binary | 1 Mifflin Alley         | Kentucky |
| 578      | Johnathon Hughes     | Account Representative I      | Engineering        | jhughes1@vk.com             | 859-799-8770 | 14/01/2014 | 49398.8   | Male       | 9807 Melrose Point      | Kentucky |
| 602      | Thornton Eckersley   | Senior Financial Analyst      | Sales              | teckersleyg@pbs.org         | 502-900-8875 | 02/07/2010 | 104912.03 | Male       | 7 Harper Drive          | Kentucky |
| 607      | Jocelyn Yeats        | Computer Systems Analyst I    | Legal              | jyeatsg@unc.edu             | 502-331-6036 | 28/04/2015 | 49123.86  | Female     | 7 Meadow Valley Terrace | Kentucky |
| 786      | Rodrique O'Halligan  | Assistant Manager             | Accounting         | rohalligan@unesco.org       | 502-849-6638 | 13/02/2018 | 107628.4  | Male       | 2854 Rieder Alley       | Kentucky |
| 814      | Dana Davis           | Financial Analyst             | Marketing          | dshoardm1@hubpages.com      | 813-203-9263 | 26/06/2024 | 54075.68  | Female     | 4611 Michigan Way       | Kentucky |

Skúsil som spraviť to, že som si zobral adresy týchto zamestnancov a označil si ich bývania na mape v s tým, že pozeráme ako ďaleko sa nachádzajú od označenej cesty Pride Rd.



Z tohto obrázka vidíme, že zamestnanec Dana Davis je najbližšia ku Road Rd – takže ďalej môžeme analyzovať jej maily.

## Analýza e-mailovej komunikácie



Naša podozrivá osoba má e-mail [dana.davis@enron.com](mailto:dana.davis@enron.com) a pomocou Autopsy vieme, že sa vyskutuje 2631 v mailovej komunikácii – pre nás bude teraz dôležité prehľadať jej maily a nájsť nejaký, ktorý bude

|                           |                         |                   |
|---------------------------|-------------------------|-------------------|
| [current folder]          | 2025-03-24 10:37:38 CET | 2025-03-24 10:37: |
| [parent folder]           | 2025-03-24 10:51:00 CET | 2025-03-24 10:51: |
| _trash                    | 2025-03-24 10:37:32 CET | 2025-03-24 10:37: |
| _sent_mail                | 2025-03-24 10:37:39 CET | 2025-03-24 10:37: |
| accting                   | 2025-03-24 10:37:32 CET | 2025-03-24 10:37: |
| all_documents             | 2025-03-24 10:37:33 CET | 2025-03-24 10:37: |
| church                    | 2025-03-24 10:37:33 CET | 2025-03-24 10:37: |
| dana_s_extras             | 2025-03-24 10:37:33 CET | 2025-03-24 10:37: |
| deleted_items             | 2025-03-24 10:37:34 CET | 2025-03-24 10:37: |
| discussion_threads        | 2025-03-24 10:37:35 CET | 2025-03-24 10:37: |
| finanial_operations       | 2025-03-24 10:37:35 CET | 2025-03-24 10:37: |
| friends                   | 2025-03-24 10:37:35 CET | 2025-03-24 10:37: |
| fun                       | 2025-03-24 10:37:35 CET | 2025-03-24 10:37: |
| fyi                       | 2025-03-24 10:37:35 CET | 2025-03-24 10:37: |
| inbox                     | 2025-03-24 10:37:37 CET | 2025-03-24 10:37: |
| notes_inbox               | 2025-03-24 10:37:37 CET | 2025-03-24 10:37: |
| performance_review        | 2025-03-24 10:37:37 CET | 2025-03-24 10:37: |
| personal                  | 2025-03-24 10:37:37 CET | 2025-03-24 10:37: |
| sap                       | 2025-03-24 10:37:37 CET | 2025-03-24 10:37: |
| save_the_date             | 2025-03-24 10:37:38 CET | 2025-03-24 10:37: |
| sent                      | 2025-03-24 10:37:38 CET | 2025-03-24 10:37: |
| sent_items                | 2025-03-24 10:37:38 CET | 2025-03-24 10:37: |
| vacation                  | 2025-03-24 10:37:38 CET | 2025-03-24 10:37: |
| vargas_becton_lamb        | 2025-03-24 10:37:38 CET | 2025-03-24 10:37: |
| vargas_becton_lamb_galvan | 2025-03-24 10:37:38 CET | 2025-03-24 10:37: |

v súvislosti s našim prípadom.

Keď si otvoríme jej emailovú komunikáciu vidíme tieto priečinky e-mailov. Naším sústredením bude odoslané maily a vymazané maily.

Pomocou vyhľadávania kľúčovými slovami sme našli nasledovnú emailovú komunikáciu.

| Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences |
|-----|------|-------------|---------------|------------|----------------|------------------|---------|-------------|-------------------|
| 96  |      |             |               |            |                |                  |         |             |                   |
| 97  |      |             |               |            |                |                  |         |             |                   |
| 98  |      |             |               |            |                |                  |         |             |                   |
| 99  |      |             |               |            |                |                  |         |             |                   |

Strings

Extracted Text

Translation

Page: 1 of 1 Page

Matches on page: - of - Match

100%

Reset

Text Source: File Text

Forwarded by Dana Davis/HOU/ECT on 02/15/2001 10:11 AM

Rebecca Sanchez  
02/15/2001 09:33 AM  
To: tips@tmz.com  
cc: (bcc: Dana Davis/HOU/ECT)  
Subject: exclusive photos

I have some exclusive photos for you to see. It's from a secret photoshoot with a high-profile person. Send me a mail post and I will be able to give you a drive with the stuff.

DONT CONTACT ME BACK THROUGH HERE

adress:  
Kentucky, Pride, House near Pride RD  
Better if you send someone to fetch it.

Takže sa nám potvrdilo, že osoba ktorá kontaktovala TMZ je Dana Davis.

A tým že už nemáme ďalšie stopy na vypátranie – môžeme ukončiť analýzu, pátranie a prejsť na hypotézy.

# Overenie hypotéz

## Hypotéza 1:

*Podľa opísanej situácie vieme, že sa jedná o nejakú celebritu alebo osobnosť – dedukujem, že sa jedná o interný únik dát. Domnievam sa, že manažér, ktorý sa staral o celý tento projekt, bol v skutočnosti veľký fanúšik alebo nenávidel túto osobnosť a chceli zverejniť ich fotky buď na osvedčenie že sú fenomenálny alebo hrozný v realite.*

Potvrdil som pomocou analýzou emailov a USB zariadenia, že sa jedná o interný únik dát. Neviem ale zistiť, či daná osoba to robila z finančnej alebo osobnej motivácie – bolo by treba spraviť výsluch podozrivého. Takže táto hypotéza je **nekonkluzívna**.

## Hypotéza 2:

*Naša osoba sa napojila do notebooku a cez USB vložila skript na odomknutie prístupu na všetky stránky internetu – za normálnych okolností majú vo firemnej sieti zablokovaný prístup na všetky stránky okrem firmou povolených. Toto USB sa po použití zničilo a zahodilo v snahe sa zbaviť dôkazov.*

Táto hypotéza je **vyvrátená** – jedná sa o normálny transport súborov z notebooku na USB, ktoré sa ďalej dostalo mimo kancelárie štúdia. V analýze sme nenašli žiadne súbory, ktoré by naznačovali, že sa spustil nejaký skript na odomknutie prístupu na internet.

## Hypotéza 3:

*Notebook nebol správne nakonfigurovaný a odišli odtiaľ fotky cez externý útok – cez internet.*

Hypotéza je **vyvrátená** – nevyskytli sa v analýze podozrivé súbory, ktoré by sa týkali vírusov alebo iných externých útokov.

## Hypotéza 4:

*Jedná sa o externý únik dát – pozvaný fotograf, dizajnér setu a iní ľudia, ktorý nepatrili pod spoločnosť a mali prístup ku akýmkoľvek dátam s ktorými pracovali.*

Hypotéza je **vyvrátená** – konkretizovalo sa to na interný únik – presnejšie ide o zamestnancov pod spoločnosťou. Externý únik sa nemohol odohrať zároveň.

## Literatúra:

### **"Duck Hunt: Memory Forensics of USB Attack Platforms"**

[https://dfrws.org/wp-content/uploads/2021/09/2021-usa-paper-20-duck\\_hunt\\_memory\\_forensics\\_of\\_usb\\_attack\\_platforms.pdf](https://dfrws.org/wp-content/uploads/2021/09/2021-usa-paper-20-duck_hunt_memory_forensics_of_usb_attack_platforms.pdf)

Táto štúdia sa zaoberá analýzou pamäťových forenzných artefaktov generovaných USB zariadeniami, ako sú USB Rubber Ducky a Bash Bunny. Autori predstavujú open-source plugíny pre Volatility, ktoré dokážu extrahovať diagnostické udalosti a identifikátory zariadení z pamäťových obrazov systému Windows 10. Tieto nástroje môžu byť užitočné pri identifikácii neoprávneného použitia USB zariadení.

### **"In Search of Lost Data: A Study of Flash Sanitization Practices"**

<https://dfrws.org/wp-content/uploads/2021/03/In-Search-of-Lost-Data-A-Study-of-Flash-Sanitization-Practices.pdf>

Táto štúdia sa zameriava na analýzu USB diskov a odhaľuje, že viac ako 12% testovaných zariadení obsahovalo obnoviteľné používateľské dáta z dôvodu nedostatočných praktík sanitácie. Zistenia zdôrazňujú potrebu dôkladnej analýzy USB zariadení počas forenzného vyšetrovania.

## Pripravené dáta a použité datasety:

- Väčšina súborov sú vytvorené mnou (3,89 GB)
- [Enron Email Database](#)
  - nepoužil som celý dataset ale iba časť – presne 2,23 GB
- Celý dataset má 6,12 GB

## **Záver**

Na základe vykonanej digitálnej forenzej analýzy bolo jednoznačne potvrdené, že únik tajných fotiek z exkluzívneho photoshootu pre magazín bol spôsobený interným únikom dát. Dôkazy získané z analýzy USB zariadenia „Kingston DataTraveler“, prehľadávania histórie na notebooku manažéra projektu a e-mailovej komunikácie jasne ukazujú na konkrétneho zamestnanca, Dana Davis, ktorý s najväčšou pravdepodobnosťou kontaktoval TMZ a poskytol im uniknuté fotky.

Hypotézy o externom útoku, nesprávnej konfigurácii notebooku či o zásahu externých osôb boli jednoznačne vyvrátené. Potvrdilo sa, že únik bol realizovaný cez interné prenosové zariadenie, pričom nebolo možné určiť presnú motiváciu páchatel'a bez ďalšieho vypočúvania.

Na základe týchto zistení je odporúčané vykonať výsluch podozrivého zamestnanca a zabezpečiť implementáciu prísnejších kontrolných a bezpečnostných opatrení v oblasti digitálnej správy citlivých dát, aby sa predišlo podobným incidentom v budúcnosti.