

# Odhalenie úniku dát cez náhodný nález USB zariadenia

Autor : Milan Klimek

Link na prezentáciu : <https://bcstudent.fpvucm.sk/~klimekmilan/dfa/prezentacia.pdf>

## Opis prípadu:

V spoločnosti **Templine**, ktorá poskytuje IT riešenia a správu dát pre externé firmy, došlo k vážnemu bezpečnostnému incidentu. Firma sa špecializuje na poskytovanie služieb ako CRM systémy, správa databáz, kybernetická bezpečnosť a vývoj softvéru pre klientov v celej Európe.

Jedného dňa servisný technik bol vyslaný do jednej z kancelárií, aby skontroloval robotický vysávač Xiaomi, ktorý nahlásil poruchu a prestal fungovať. Pri kontrole vysávača si všimol, že v jeho sacom mechanizme bolo zaseknuté USB zariadenie. Keďže nebolo jasné, komu patrí, bolo USB odovzdané IT oddeleniu, ktoré začalo preverovať jeho obsah.

Po prvotnej analýze sa ukázalo, že na USB boli uložené citlivé údaje spoločnosti, vrátane kompletného zoznamu zákazníkov, dáta o cenách služieb. Forenzná analýza sa zamerala na analýzu dát a identifikáciu zdroja úniku.

## Predmet vyšetrovania:

Cieľom vyšetrovania bolo:

- Zistiť, kto získal a preniesol citlivé údaje z interného databázového systému.
- Zistiť, akým spôsobom boli údaje získané, vrátane použitého zariadenia a techník.
- Zhodnotiť rozsah úniku, vrátane typov a množstva kompromitovaných dát.
- Overiť, či došlo k zneužitiu neaktívneho administrátorského účtu.
- Identifikovať útočníka a navrhnúť bezpečnostné opatrenia, ktoré by zabránili podobným incidentom v budúcnosti.

## Očakávaný výsledok:

Cieľom je získať relevantné digitálne dôkazy, ktoré potvrdia alebo vyvrátia jednotlivé hypotézy o úniku dát.

Ak sa potvrdí zneužitie interného účtu, je potrebné zdokumentovať metódy, rozsah kompromitácie a navrhnúť opatrenia na zvýšenie bezpečnosti a prevenciu podobných incidentov v budúcnosti.

## Odborné príspevky:

- *Duck Hunt: Memory Forensics of USB Attack Platforms*

Táto štúdia analyzuje forenzné artefakty v pamäti vytvorené USB útokmi, konkrétne zariadeniami ako Hak5's USB Rubber Ducky a Bash Bunny. Autori predstavujú nástroje na extrakciu artefaktov z pamäte systémov Windows 10, vrátane diagnostických udalostí a DHCP logov.

Zdroj: [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)

- *Database Memory Forensics: A Machine Learning Approach to Reverse Engineer Query Activity*

Tento príspevok sa zaoberá analýzou pamäte databázových systémov s cieľom získať informácie o nedávno vykonaných dotazoch a príkazoch. Používa metódy strojového učenia na rekonštrukciu aktivity v databáze z pamäťových snapshotov.

Zdroj: [https://dfrws.org/wp-content/uploads/2023/03/Database\\_memory\\_forensics\\_A\\_machine\\_learning\\_approach\\_to\\_reverse\\_engineer\\_query\\_activity.pdf](https://dfrws.org/wp-content/uploads/2023/03/Database_memory_forensics_A_machine_learning_approach_to_reverse_engineer_query_activity.pdf)

- *Database Forensic Analysis Through Internal Structure Carving*

Táto práca predstavuje metódy na forenznú analýzu databáz prostredníctvom extrakcie interných štruktúr z databázových súborov. Zameriava sa na obnovu a analýzu dát z poškodených alebo neúplných databázových súborov.

Zdroj: [https://dfrws.org/sites/default/files/session-files/2015\\_USA\\_pres-database\\_forensic\\_analysis\\_through\\_internal\\_structure\\_carving.pdf](https://dfrws.org/sites/default/files/session-files/2015_USA_pres-database_forensic_analysis_through_internal_structure_carving.pdf)

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

Štúdia skúma praktiky sanitácie dát na USB flash diskoch a poukazuje na riziká spojené s obnovou údajov z nedostatočne vymazaných zariadení. Zistilo sa, že viac ako 12% nových USB flash diskov obsahovalo obnoviteľné užívateľské dáta kvôli opätovnému použitiu čipov.

Zdroj: [https://dfrws.org/wp-content/uploads/2021/08/2021\\_EU\\_pres-in\\_search\\_of\\_lost\\_data\\_a\\_study\\_of\\_flash\\_sanitization\\_practices.pdf](https://dfrws.org/wp-content/uploads/2021/08/2021_EU_pres-in_search_of_lost_data_a_study_of_flash_sanitization_practices.pdf)

- *A Classification of SQL Injection Attacks and Countermeasures (2006)*

Publikácia poskytuje komplexný prehľad o typoch SQL injection útokov a metódach ich mitigácie. Autori v nej rozlišujú niekoľko hlavných foriem útokov – napríklad tautology-based, union-based, piggy-backed queries a stored procedure injection – pričom pre každý typ uvádzajú aj príslušné príklady a dôsledky.

Súčasťou práce je aj prehľad odporúčaných protiopatrení, ako sú použitie prepared statements, validácia vstupov a analýza správania sa aplikácií.

Štúdia významne dopĺňa rámec tejto analýzy, keďže skript `usb_attack_hidden.bat` využíva príkazy, ktoré možno zaradiť medzi piggy-backed SQL injection – teda také, ktoré sú pridávané k pôvodným dotazom s cieľom manipulovať s databázou.

Práca slúžila ako teoretické východisko pri interpretácii zistení a klasifikácii incidentu ako zámerného SQL injection útoku s cieľom získať a upraviť citlivé údaje.

Zdroj: <https://sites.cc.gatech.edu/home/orso/papers/halfond.viegas.orso.ISSSE06.pdf>

### *Použitý dataset:*

Použil som dataset s veľkosťou 3,58 GB, ktorý som našiel na stránke <http://roussev.net/t5/t5.html>. Obsahuje približne 6500 súborov rôzneho typu.

Súčasťou analýzy bol aj mnou vygenerovaný log súbor servera obsahujúci záznamy o prístupe k databázovým údajom.

### *Typ analyzovanej digitálnej stopy:*

Forenzná analýza sa zamerala na digitálne stopy získané z:

- **USB zariadenia** nájdeného v robotickom vysávači, ktoré obsahovalo citlivé firemné dáta,
- **logov databázového servera**, ktoré zaznamenali prístup k údajom v konkrétnych časoch,
- **záznamov systémovej aktivity**, ktoré pomohli určiť spôsob získania dát.

Cieľom analýzy bolo identifikovať:

- Kto mal prístup k citlivým údajom,
- Kedy a akým spôsobom boli tieto údaje získané,
- Aké konkrétne dáta boli uložené na USB zariadení,
- Ako sa USB zariadenie mohlo dostať do vysávača.

### *Zadržané a analyzované zariadenia:*

**USB zariadenie** – nájdené v robotickom vysávači, obsahovalo súbory citlivých firemných dát bez známk mazania.

**Firemný databázový server** – z ktorého boli údaje stiahnuté; preverené boli logy, prístupové záznamy a systémove aktivity.

**Pracovný notebook podozrivého zamestnanca** – analyzovaný na prítomnosť nástrojov na pripojenie k databáze, záznamy SQL príkazov a potenciálne skripty použité na exfiltráciu údajov.

### *5W+H Analýza incidentu*

#### **Kto?**

Servisný technik našiel USB zariadenie a nahlásil incident IT oddeleniu. Forenzná analýza zatiaľ naznačuje, že s únikom údajov môže súvisieť interný zamestnanec – konkrétne sa preveruje aktivita účtu martinezka, ktorý bol v čase incidentu zneužitý.

#### **Čo?**

Na USB zariadení sa nachádzali nasledovné súbory:

- **Zoznam zákazníkov** (customers) – mená, adresy a kontaktné údaje firiem
- **Cenové ponuky** (pricing) – vrátane obchodných podmienok a cien

Všetky údaje boli na USB zariadení prístupné a neboli zmazané, čo naznačuje, že útočník s ním ďalej pracoval než ho nechtiac stratil.

## Kedy?

Podľa analýzy logov boli údaje stiahnuté v dvoch vlnách:

- **20. januára 2025 o 04:06:04** – stiahnutá databáza customers
- **20. januára 2025 o 18:14:12** – stiahnutá databáza pricing.

## Kde?

Incident sa odohral na firemnom databázovom servery spoločnosti Templine. Údaje boli stiahnuté zo servera, kde sa nachádzali citlivé informácie o zákazníkoch a obchodných podmienkach. USB zariadenie bolo nájdené v robotickom vysávači, čo naznačuje, že páchatel' ho omylom stratil alebo ho tam niekto iný skryl.

## Prečo?

Vyšetrovanie naznačuje, že cieľom bolo získať obchodne cenné informácie s úmyslom osloviť zákazníkov spoločnosti Templine a ponúknuť im výhodnejšie služby. Údaje mohli byť využité na konkurenčné alebo osobné účely.

## Metodológia a získané dôkazy

Na základe predbežného vyšetrovania boli identifikované a analyzované nasledujúce digitálne dôkazy:

### 1. **USB zariadenie Verbatim 8GB**

- Získané z robotického vysávača.
- Obsahovalo kompletne nezmazané údaje spoločnosti (zákazníci, cenové ponuky, e-mailly).

### 2. **Logy databázového servera**

- Obsahovali záznamy o prístupoch k databázam customers a pricing.
- Logy boli exportované vo formáte textu a boli analyzované na časové zhody.

### 3. **Pracovný notebook podozrivého zamestnanca**

- Získaný obraz RAM pamäte.
- Prehľadanie reťazce a aktívne procesy.
- Overovaná prítomnosť nástrojov na databázové pripojenie a potenciálnych skriptov.

## Použité nástroje na analýzu:

- **FTK Imager 4.7.1.2** – vytvorenie bitovej kópie USB zariadenia
- **Autopsy** – forenzná analýza obsahu USB
- **HxD** – hexadecimálna analýza súborov aj RAM dumpu
- **Magnet RAM Capture** – zachytenie a export obsahu RAM pamäte
- **DB Browser for SQLite** - nástroj na vizuálnu analýzu a editáciu SQLite databáz

## Hypotézy:

### Hypotéza č. 1 – Neúmyselné uloženie firemných dát na USB zariadenie

Možné scenáre:

- USB zariadenie mohlo byť použité na prácu s firemnými súbormi bez úmyslu exfiltrácie dát.
- Zamestnanec mohol omylom alebo z nedbanlivosti skopírovať citlivé súbory na USB zariadenie bez vedomia bezpečnostného oddelenia.
- Dôkazy by mohli ukazovať, že údaje boli prenesené počas bežnej práce bez ďalšej manipulácie.

### Hypotéza č. 2 – Externý útok prostredníctvom škodlivého USB

Možné scenáre:

- USB zariadenie mohlo byť úmyselne vložené do robotického vysávača osobou mimo organizácie.
- Cieľom mohlo byť získať prístup do systému alebo preniesť dáta bez zanechania digitálnej stopy.
- Fyzické dôkazy, prístupové logy alebo prítomnosť malvéru by mohli potvrdiť túto hypotézu.

### Hypotéza č. 3 – Zneužitie neaktívneho účtu administrátora

Možné scenáre:

- Neaktívny účet správcu systému (napr. martinezk) mohol byť nesprávne zabezpečený alebo deaktivovaný.
- Útočník mohol tento účet zneužiť na získanie prístupu k databázam a stiahnutie údajov.
- Záznamy z logov môžu obsahovať aktivitu tohto účtu v čase incidentu.

## Zariadenie č. 1 – USB Verbatim 8GB

### Fotodokumentácia zariadenia:



Obrázok 1 - Verbatim Store "n" Go PinStripe 8GB

### Základné technické parametre:

| <b>Parameter</b>   | <b>Hodnota</b>                      |
|--------------------|-------------------------------------|
| Názov zariadenia:  | Verbatim Store 'n' Go PinStripe 8GB |
| Značka:            | Verbatim                            |
| Kapacita úložiska: | 8 GB                                |
| Rozhranie:         | USB 2.0                             |
| Konektor:          | USB-A                               |
| Rýchlosť čítania:  | 10 MB/s                             |

Rýchlosť zápisu: 4 MB/s  
Sériové číslo: YB08G4829044147TTL

### Akvizícia obrazu zariadenia:

- **Nástroj:** AccessData FTK Imager 4.7.1.2
- **Názov obrazu:** usb-key-cierny.001
- **Získané:** 22. 3. 2025 o 10:24:55
- **Dokončené:** 22. 3. 2025 o 10:33:12
- **Uložené na ceste:** C:\Users\student\Desktop\km\usb-key-cierny.001
- **Sector count:** 15 257 600
- **Zdrojová veľkosť:** 7450 MB

### Digitálne odtlačky:

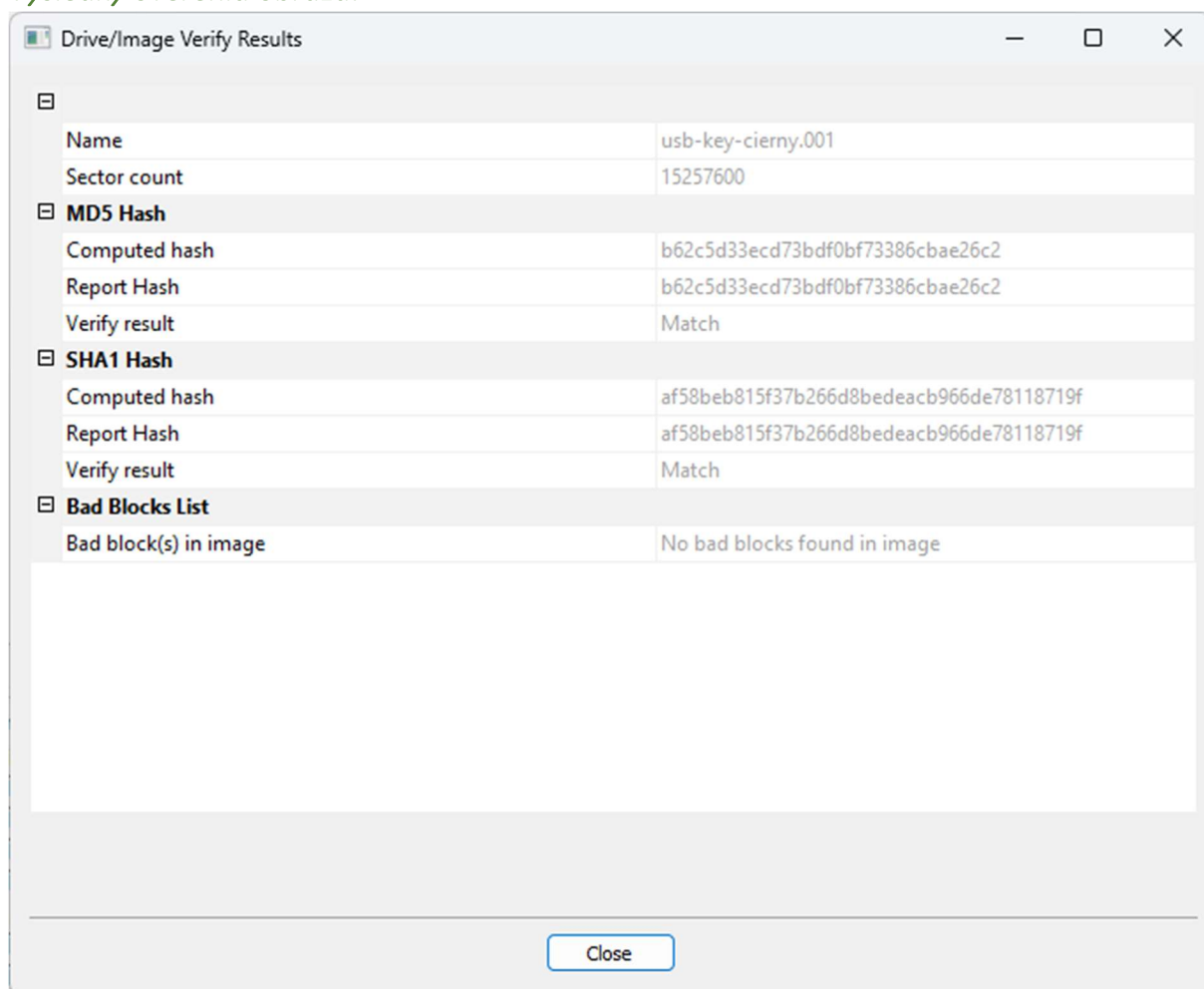
#### Algoritmus Hodnota

**MD5:** b62c5d33ecd73bdf0bf73386cbae26c2

**SHA1:** af58beb815f37b266d8bedeacb966de78118719f

**Verifikácia:** Oba hashe zhodné (MATCH) – integrita obrazu potvrdená

### Výsledky overenia obrazu:



Obrázok 2 - FTK Imager - usb-key-cierny.001

*Účel zaistenia a analýzy:*

Cieľom akvizície USB zariadenia bolo získať forenzný obraz jeho obsahu s cieľom:

- Identifikovať prítomnosť citlivých firemných dát (napr. zákazníci, cenové ponuky)
- Overiť, ako sa tieto údaje na zariadenie dostali
- Zabezpečiť dôkaz pre analýzu databázového úniku

## Chain of Custody záznam – Dôkaz č. 001

|                                   |                      |                                                    |                      |                 |                      |          |      |
|-----------------------------------|----------------------|----------------------------------------------------|----------------------|-----------------|----------------------|----------|------|
| Číslo:                            | 001                  | Typ súboru:                                        | USB obraz            | Obnovený súbor: | Nie                  | Veľkosť: | 8 GB |
| Popis prípadu:                    |                      | Únik citlivých údajov cez USB nájdené vo vysávači  |                      |                 |                      |          |      |
| Názov súboru:                     |                      | usb-key-cierny.001                                 |                      |                 |                      |          |      |
| Miesto získania digitálnej stopy: |                      | Kancelária č. 2 – servisný vysávač                 |                      |                 |                      |          |      |
| Poznámky:                         |                      | Žiadne poškodené bloky, obraz vytvorený FTK Imager |                      |                 |                      |          |      |
| Časové pečiatky                   |                      |                                                    |                      |                 |                      |          |      |
| Access:                           | 22. 3. 2025 10:24:55 | Modify:                                            | 22. 3. 2025 10:33:12 | Change:         | 22. 3. 2025 10:33:28 |          |      |
| Digitálna<br>odtlačok<br>(heš)    | MD5                  | b62c5d33ecd73bdf0bf73386cbac26c2                   |                      |                 |                      |          |      |
|                                   | SHA1                 | af58beb815f37b266d8bedeacb966de78118719f           |                      |                 |                      |          |      |
| Časová pečiatka                   |                      | Akcia vykonaná s digitálnou stopou                 |                      |                 |                      |          |      |
| 22. 3. 2025 10:24:55              |                      | Spustenie akvizície USB cez FTK Imager             |                      |                 |                      |          |      |
| 22. 3. 2025 10:33:12              |                      | Ukončenie akvizície, uloženie obrazu               |                      |                 |                      |          |      |
| 22. 3. 2025 10:33:28              |                      | Verifikácia hashov – MD5 a SHA1                    |                      |                 |                      |          |      |
| 22. 3. 2025 10:35:01              |                      | Import obrazu do Autopsy 4.19.3 na analýzu         |                      |                 |                      |          |      |

## Zariadenie č. 2 – Firemný databázový server

### Fotodokumentácia zariadenia:



Obrázok 3 - Dell Technologies PowerEdge R740

### Základné technické parametre:

| <b>Parameter</b>         | <b>Hodnota</b>                           |
|--------------------------|------------------------------------------|
| Názov zariadenia:        | DB-SERVER-01                             |
| Výrobca:                 | Dell Technologies                        |
| Model:                   | PowerEdge R740                           |
| Operačný systém:         | Windows Server 2019 Standard (64-bit)    |
| Procesor:                | Intel Xeon Silver 4210, 2.2 GHz, 10-core |
| RAM:                     | 64 GB DDR4 ECC                           |
| Diskové pole (RAID):     | 2x 1TB SSD RAID 1                        |
| Prístupové porty:        | 1433 (MS SQL), 22 (SSH), 3389 (RDP)      |
| Nainštalovaný DB systém: | Microsoft SQL Server 2017                |
| Lokalita:                | Serverovňa – zabezpečený priestor        |

### Akvizícia databázového logu:

- **Nástroj:** DB Browser for SQLite 3.12.2
- **Názov súboru:** log\_access.db
- **Získané:** 22. 3. 2025 o 12:00
- **Miesto uloženia:** C:\Program Files\SQLServer\logs\
- **Exportované do:** C:\Users\student\Desktop\km\log\_access.db
- **Formát:** SQLite databáza (.db)
- **Veľkosť:** 248 KB

### Digitálne odtlačky:

| <b>Algoritmus</b>   | <b>Hodnota</b>                                      |
|---------------------|-----------------------------------------------------|
| <b>MD5:</b>         | 8f43e4d42240c358638f946c4d0f2331                    |
| <b>SHA-1:</b>       | f1a3c9f92861d967e2fd2a1c8742f5b3a6e4c6e2            |
| <b>Verifikácia:</b> | Oba hashe zhodné (MATCH) – integrita logu potvrdená |

### Účel zaistenia a analýzy:

Cieľom akvizície logu databázového servera bolo:

- Zistiť, kto a kedy pristupoval k databázam customers a pricing
- Vyhodnotiť, či bol použitý neaktívny účet martinezk
- Korelovať časové pečiatky s inými udalosťami (napr. USB prenos)

## Chain of Custody – Dôkaz č. 002

|                                   |                     |                                                   |         |                     |     |          |                     |
|-----------------------------------|---------------------|---------------------------------------------------|---------|---------------------|-----|----------|---------------------|
| Číslo:                            | 002                 | Typ súboru:                                       | SQL Log | Obnovený súbor:     | Nie | Veľkosť: | 248 KB              |
| Popis prípadu:                    |                     | Záznam prístupov k databázam spoločnosti Templine |         |                     |     |          |                     |
| Názov súboru:                     |                     | log_access.db                                     |         |                     |     |          |                     |
| Miesto získania digitálnej stopy: |                     | Serverovňa v budove spoločnosti Templine          |         |                     |     |          |                     |
| Poznámky:                         |                     | Exportovaný súbor prístupového logu k databázam   |         |                     |     |          |                     |
|                                   |                     |                                                   |         |                     |     |          |                     |
| Časové pečiatky                   |                     |                                                   |         |                     |     |          |                     |
| Access:                           | 2025-01-20 04:06:04 |                                                   | Modify: | 2025-01-20 18:14:12 |     | Change:  | 2025-01-20 18:14:15 |
|                                   |                     |                                                   |         |                     |     |          |                     |
| Digitáln y odtlačok (heš)         | MD5                 | 8f43e4d42240c358638f946c4d0f2331                  |         |                     |     |          |                     |
|                                   | SHA-1               | f1a3c9f92861d967e2fd2a1c8742f5b3a6e4c6e2          |         |                     |     |          |                     |
|                                   |                     |                                                   |         |                     |     |          |                     |
| Časová pečiatka                   |                     | Akcia vykonaná s digitálnou stopou                |         |                     |     |          |                     |
| 22. 3. 2025 12:00                 |                     | Export databázového logu zo servera               |         |                     |     |          |                     |
| 22. 3. 2025 12:05                 |                     | Overenie integrity logu cez hash (MD5, SHA-256)   |         |                     |     |          |                     |
| 22. 3. 2025 12:10                 |                     | Otvorenie logu v DB Browser for SQLite            |         |                     |     |          |                     |
| 22. 3. 2025 12:25                 |                     | Export relevantných záznamov pre analýzu          |         |                     |     |          |                     |

## Zariadenie č. 3 – Pracovný notebook podozrivého zamestnanca

### Fotodokumentácia zariadenia:



### Základné technické parametre:

| <b>Parameter</b>    | <b>Hodnota</b>                       |
|---------------------|--------------------------------------|
| Názov zariadenia:   | NB-ORIESIK01                         |
| Výrobca:            | Lenovo                               |
| Model:              | ThinkPad T480                        |
| Operačný systém:    | Windows 10 Pro (64-bit)              |
| Procesor:           | Intel Core i5-8350U, 1.7 GHz, 4-core |
| RAM:                | 16 GB DDR4                           |
| Úložisko:           | 512 GB SSD                           |
| Sieťové pripojenie: | Ethernet + Wi-Fi                     |
| Lokalita:           | Kancelária 3B – zamestnanec Oriešik  |

### Akvizícia pamäte RAM:

- **Nástroj:** Magnet RAM Capture
- **Získané:** 22. 3. 2025 o 13:40
- **Výstupný súbor:** 20250322\_kmz.raw
- **Veľkosť dumpu:** 16 GB
- **Uloženie:** C:\Users\student\Desktop\km\20250322\_kmz.raw
- **Použitá analýza:** HxD – hexadecimálne prehľadanie; hľadanie výrazov start.bat, sql injection, cmd ...

### Digitálne odtlačky:

| <b>Algoritmus</b>   | <b>Hodnota</b>                                      |
|---------------------|-----------------------------------------------------|
| <b>MD5:</b>         | f91c3d835fe9ec2c1ab3b345621cd44f                    |
| <b>SHA-1:</b>       | ab61ef245e88de5c93876c211827bd705bfbfd4f            |
| <b>Verifikácia:</b> | Oba hashe zhodné (MATCH) – integrita logu potvrdená |

### Účel zaistenia a analýzy:

RAM dump bol získaný za účelom:

- Detekcie zvyškov aktívnych SQL pripojení a spustených nástrojov
- Overenia prítomnosti skriptov alebo spustených batch súborov (start.bat)

- Identifikácie forenzne zaujímavých výrazov ako sql injection, password, dump

## Chain of Custody – Dôkaz č. 003

|                                   |                     |                                                          |                     |                 |                     |          |       |
|-----------------------------------|---------------------|----------------------------------------------------------|---------------------|-----------------|---------------------|----------|-------|
| Číslo:                            | 003                 | Typ súboru:                                              | RAM dump            | Obnovený súbor: | Nie                 | Veľkosť: | 16 GB |
| Popis prípadu:                    |                     | Forenzná akvizícia pamäte RAM z notebooku podozrivého    |                     |                 |                     |          |       |
| Názov súboru:                     |                     | 20250322_kmz.raw                                         |                     |                 |                     |          |       |
| Miesto získania digitálnej stopy: |                     | Pracovný notebook NB-ORIESIK01                           |                     |                 |                     |          |       |
| Poznámky:                         |                     | RAM obsahovala výrazy poukazujúce na SQL prácu a skripty |                     |                 |                     |          |       |
|                                   |                     |                                                          |                     |                 |                     |          |       |
| Časové pečiatky                   |                     |                                                          |                     |                 |                     |          |       |
| Access:                           | 2025-03-22 13:40:00 | Modify:                                                  | 2025-03-22 13:42:30 | Change:         | 2025-03-22 13:43:00 |          |       |
|                                   |                     |                                                          |                     |                 |                     |          |       |
| Digitálny odtlačok (heš)          | MD5                 | f91c3d835fe9ec2c1ab3b345621cd44f                         |                     |                 |                     |          |       |
|                                   | SHA-1               | ab61ef245e88de5c93876c211827bd705bfbfd4f                 |                     |                 |                     |          |       |
|                                   |                     |                                                          |                     |                 |                     |          |       |
| Časová pečiatka                   |                     | Akcia vykonaná s digitálnou stopou                       |                     |                 |                     |          |       |
| 22. 3. 2025 13:40                 |                     | Začiatok akvizície RAM pamäte pomocou Magnet RAM Capture |                     |                 |                     |          |       |
| 22. 3. 2025 13:43                 |                     | Dokončenie akvizície, uloženie dumpu                     |                     |                 |                     |          |       |
| 22. 3. 2025 13:45                 |                     | Overenie hashov – MD5 a SHA1                             |                     |                 |                     |          |       |
| 22. 3. 2025 14:00                 |                     | Otvorenie RAM dumpu v HxD, analýza výrazov               |                     |                 |                     |          |       |

## Analýza nálezov podľa hypotéz

### Analýza zariadenia č. 1 – USB kľúč Verbatim

Po zaistení USB zariadenia, ktoré bolo náhodne nájdené v robotickom vysávači v priestoroch spoločnosti Templine, bola vykonaná forenzná akvizícia a následná analýza jeho obsahu. USB bolo podozrivé z možnej súvislosti s únikom firemných údajov.

## Predbežná analýza

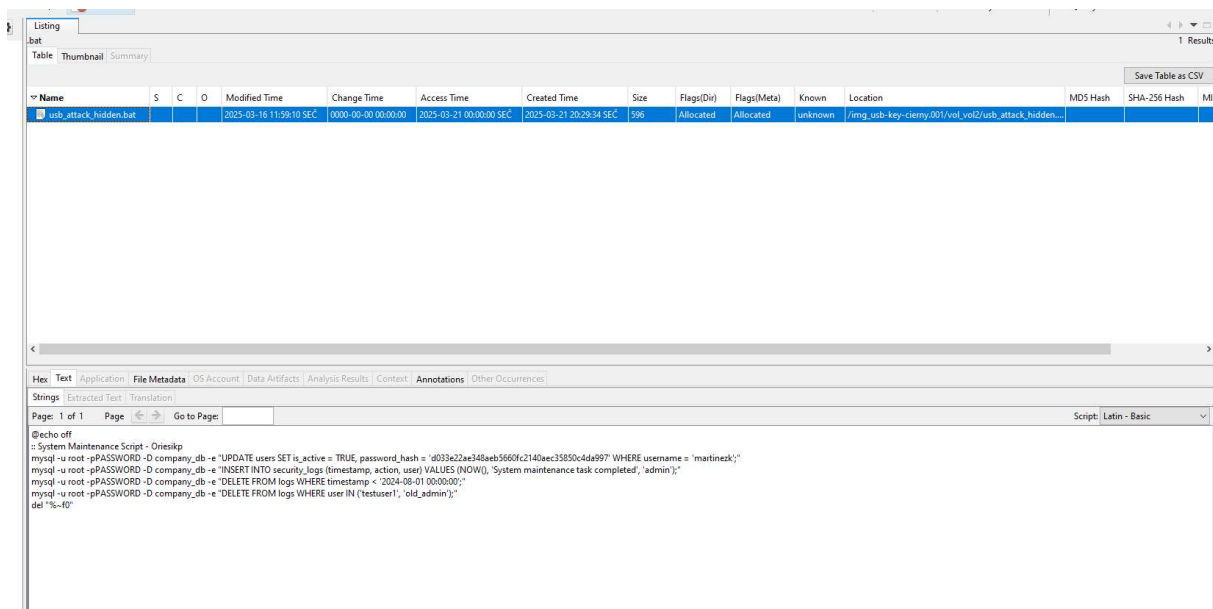
Pomocou nástrojov **FTK Imager** a **Autopsy** bol vytvorený bitový obraz zariadenia. Už pri prvotnom prehľade bolo zistené, že USB obsahuje viacero databázových súborov s príponou **\*.db**, čo vyvolalo okamžité podozrenie, že mohlo dôjsť k stiahnutiu interných databáz spoločnosti.

Názvy ako **customers.db**, **pricing.db** či **users.db** ich štruktúra naznačovala, že môžu obsahovať tabuľkové údaje alebo citlivý obsah — typický pre SQL databázy.

Vzhľadom na podozrivý výskyt **\*.db** súborov bolo rozhodnuté:

- overiť ich štruktúru a obsah
- vyhľadať kľúčové výrazy, ktoré by mohli súvisieť s citlivými údajmi, alebo so spôsobom ich získania (napr. sql, customers, dump, SELECT)

Už počas prvotného vyhľadávania pomocou **Autopsy** bol identifikovaný súbor **usb\_attack\_hidden.bat**



Obrázok 4 - Identifikovaný súbor **usb\_attack\_hidden.bat**

## Obsah skriptu:

```
@echo off

:: System Maintenance Script - Oriesikp

mysql -u root -pPASSWORD -D company_db -e "UPDATE users SET is_active = TRUE,
password_hash = 'd033e22ae348aeb5660fc2140aec35850c4da997' WHERE username =
'martinezk';"

mysql -u root -pPASSWORD -D company_db -e "INSERT INTO security_logs
(timestamp, action, user) VALUES (NOW(), 'System maintenance task completed',
'admin');"
```

```
mysql -u root -pPASSWORD -D company_db -e "DELETE FROM logs WHERE timestamp < '2024-08-01 00:00:00';"

mysql -u root -pPASSWORD -D company_db -e "DELETE FROM logs WHERE user IN ('testuser1', 'old_admin');"

del "%~f0"
```

### Vyhodnotenie:

Skript jasne ukazuje, že jeho účelom je:

- aktivovať používateľa **martinezk** a zmeniť mu heslo
- zapísať falošný záznam do logu (krytie stopy)
- **vymazať staršie logy a logy konkrétnych používateľov**
- na záver sa skript sám zmaže (del "%~f0")

Toto sú **typické črty útoku pomocou SQL injection alebo nepriameho skriptu**, ktorý manipuluje databázu bez vedomia systému.

### Analýza obsahu databázových súborov

Po zistení viacerých súborov s príponou .db bolo rozhodnuté vykonať cielenú analýzu týchto súborov pomocou nástroja **Autopsy**, zameranú na identifikáciu štruktúrovaných databázových tabuliek a prítomnosť potenciálne citlivých údajov.

### Vyhľadávanie a filtrácia

Vzhľadom na podozrenie, že by USB kľúč mohol obsahovať stiahnuté dáta z interného systému, boli prehľadávané databázové súbory pomocou štandardných kľúčových slov ako napríklad:

customers, users, pricing, password, SELECT, INSERT, update, dump, export

Pri analýze boli identifikované a spracované nasledovné .db súbory:

| Názov databázy | Popis obsahu                                                                                 |
|----------------|----------------------------------------------------------------------------------------------|
| customers.db   | Obsahoval tabuľku so zoznamom zákazníkov vrátane mena, firmy a kontaktných údajov            |
| pricing.db     | Obsahoval tabuľky s cenníkmi, názvami produktov/služieb a ich internými cenami               |
| users.db       | Obsahoval tabuľku používateľov vrátane hashovaných hesiel, rolí a dát posledného prihlásenia |

## Výňatok z databázy users.db

| Listing                 |   |   |   |                          |                     |                          |                          |         |            |             |         |
|-------------------------|---|---|---|--------------------------|---------------------|--------------------------|--------------------------|---------|------------|-------------|---------|
| Databases               |   |   |   |                          |                     |                          |                          |         |            |             |         |
| Table Thumbnail Summary |   |   |   |                          |                     |                          |                          |         |            |             |         |
| 222 Results             |   |   |   |                          |                     |                          |                          |         |            |             |         |
| Save Table as CSV       |   |   |   |                          |                     |                          |                          |         |            |             |         |
| Name                    | S | C | O | Modified Time            | Change Time         | Access Time              | Created Time             | Size    | Flags(Dir) | Flags(Meta) | Known   |
| log_access.db           |   |   |   | 2025-04-06 11:30:10 SELC | 0000-00-00 00:00:00 | 2025-04-06 01:00:00 SELC | 2025-04-06 11:53:54 SELC | 1884160 | Allocated  | Allocated   | unknown |
| customers.db            |   |   |   | 2025-04-06 19:47:10 SELC | 0000-00-00 00:00:00 | 2025-04-06 01:00:00 SELC | 2025-04-06 19:47:08 SELC | 548864  | Allocated  | Allocated   | unknown |
| pricing.db              |   |   |   | 2025-04-06 19:53:28 SELC | 0000-00-00 00:00:00 | 2025-04-06 01:00:00 SELC | 2025-04-06 19:53:27 SELC | 90112   | Allocated  | Allocated   | unknown |
| users.db                |   |   | 0 | 2025-04-06 19:49:36 SELC | 0000-00-00 00:00:00 | 2025-04-06 01:00:00 SELC | 2025-04-06 19:49:35 SELC | 40960   | Allocated  | Allocated   | unknown |
| 01-12.db                |   |   | 0 | 2017-10-07 21:00:50 SELC | 0000-00-00 00:00:00 | 2025-03-21 00:00:00 SEC  | 2025-03-21 20:12:04 SEC  | 8192    | Allocated  | Allocated   | unknown |
| 01-13.db                |   |   | 0 | 2017-10-07 21:00:50 SELC | 0000-00-00 00:00:00 | 2025-03-21 00:00:00 SEC  | 2025-03-21 20:12:04 SEC  | 8192    | Allocated  | Allocated   | unknown |
| 01-14.db                |   |   | 0 | 2017-10-07 21:00:50 SELC | 0000-00-00 00:00:00 | 2025-03-21 00:00:00 SEC  | 2025-03-21 20:12:04 SEC  | 8192    | Allocated  | Allocated   | unknown |
| 0A-01.db                |   |   | 0 | 2017-10-07 21:00:50 SELC | 0000-00-00 00:00:00 | 2025-03-21 00:00:00 SEC  | 2025-03-21 20:11:28 SEC  | 8192    | Allocated  | Allocated   | unknown |
| 0A-02.db                |   |   | 0 | 2017-10-07 21:00:50 SELC | 0000-00-00 00:00:00 | 2025-03-21 00:00:00 SEC  | 2025-03-21 20:11:28 SEC  | 8192    | Allocated  | Allocated   | unknown |
| 0A-03.db                |   |   | 0 | 2017-10-07 21:00:50 SELC | 0000-00-00 00:00:00 | 2025-03-21 00:00:00 SEC  | 2025-03-21 20:11:31 SEC  | 12288   | Allocated  | Allocated   | unknown |
| 0A-04.db                |   |   | 0 | 2017-10-07 21:00:50 SELC | 0000-00-00 00:00:00 | 2025-03-21 00:00:00 SEC  | 2025-03-21 20:11:31 SEC  | 12288   | Allocated  | Allocated   | unknown |
| 0A-05.db                |   |   | 0 | 2017-10-07 21:00:50 SELC | 0000-00-00 00:00:00 | 2025-03-21 00:00:00 SEC  | 2025-03-21 20:11:31 SEC  | 12288   | Allocated  | Allocated   | unknown |
| 0B-01.db                |   |   | 0 | 2017-10-07 21:00:52 SELC | 0000-00-00 00:00:00 | 2025-03-21 00:00:00 SEC  | 2025-03-21 20:11:35 SEC  | 8192    | Allocated  | Allocated   | unknown |
| 0B-02.db                |   |   | 0 | 2017-10-07 21:00:52 SELC | 0000-00-00 00:00:00 | 2025-03-21 00:00:00 SEC  | 2025-03-21 20:11:36 SEC  | 16384   | Allocated  | Allocated   | unknown |
| 0C-01.db                |   |   | 0 | 2017-10-07 21:00:52 SELC | 0000-00-00 00:00:00 | 2025-03-21 00:00:00 SEC  | 2025-03-21 20:11:42 SEC  | 8192    | Allocated  | Allocated   | unknown |

| Hex                                              | Text       | Application | File Metadata | OS Account                      | Data Artifacts | Analysis Results                      | Context                                                           | Annotations         | Other Occurrences |
|--------------------------------------------------|------------|-------------|---------------|---------------------------------|----------------|---------------------------------------|-------------------------------------------------------------------|---------------------|-------------------|
| Table users 52 entries Page 1 of 1 Export to CSV |            |             |               |                                 |                |                                       |                                                                   |                     |                   |
| user_id                                          | first_name | last_name   | username      | email                           | role           | permissions                           | password_hash                                                     | last_login          | is_active         |
| 20                                               | Terry      | Parker      | user20        | erikvillarreal@klein-oliver.com | HR             | read:users, write:users               | caf353a5f0208e8eaccd3b43fc857689b6b8d9b1558d5e276c7dffffa5c85a7   | 2024-05-28 17:48:35 | 0                 |
| 42                                               | Jessica    | Wagner      | user42        | tbruce@hotmail.com              | admin          | read:all, write:all, delete:all       | a95f7480e03397eaacc56848d61a059e8fcea56db17bd8484fee8e330eabfc    | 2024-07-28 03:51:25 | 0                 |
| 48                                               | Juan       | Lee         | user48        | david87@collier.org             | HR             | read:users, write:users               | 08b215b44df1c65092e9e94c739ef6a80e5295babef021101d3842a160e156    | 2024-06-16 17:59:22 | 0                 |
| 13                                               | Traci      | White       | user13        | joseph78@flores.com             | IT_support     | read:users, read:logs, write:logs     | 1da5a4c3574dc87ebe542761b4872060565453389273c2267bec2e32b2721c    | 2024-03-28 20:49:56 | 1                 |
| 44                                               | Thomas     | Lee         | user44        | susanvalenzuela@adams.biz       | admin          | read:all, write:all, delete:all       | f0540d33b7534a95b4818026e792c66a95010a5ecd529b6210d1639463b7f8    | 2024-05-25 08:34:25 | 1                 |
| 6                                                | Paul       | Robertson   | user6         | cdiaz@ramirez-griffin.com       | IT_support     | read:users, read:logs, write:logs     | a9a2c170d117e0811633385ceaf18fee6954276221d3ddeb3c8bae391a2f8a    | 2024-06-15 09:49:05 | 1                 |
| 18                                               | Travis     | Butler      | user18        | dhavney@hotmail.com             | security       | read:logs, read:users, write:security | e75027280c0abd5b57520340e238df137287e26e75347c7d7e7d8a1fa26623f32 | 2024-04-26 16:14:51 | 0                 |
| 51                                               | Peter      | Oniesik     | oriesikp      | jakeanderson@erickson.com       | seller         | read:customers, write:orders          | d5b0d9567c98d42e4f09bb0f89586308df636d8d19dab8c5c245ec9ba24441    | 2024-06-21 06:02:59 | 1                 |
| 4                                                | Matthew    | Roberts     | user4         | singhames@hotmail.com           | IT_support     | read:users, read:logs, write:logs     | 0f13ac37189a8e329a993811e2011c549ebf8e5d3faef3d8f647d8e8701d48    | 2024-06-23 15:23:41 | 0                 |
| 33                                               | Denise     | Brown       | user33        | kristinacclark@hotmail.com      | HR             | read:users, write:users               | 6354239ba6741c13776776575dfa765c006c606ed85aa29fcd0b9ac6312ad     | 2024-04-19 04:58:18 | 0                 |

Obrázok 5 - Identifikovaný súbor users.db

Pri analýze súboru users.db boli pomocou nástroja **Autopsy** extrahované dáta zo systému autentifikácie používateľov.

Z tabuľky users bolo identifikovaných 52 záznamov, pričom každý obsahoval:

- Meno a priezvisko používateľa
- Prihlasovacie meno (username)
- E-mailová adresa
- Prístupové roly a oprávnenia
- Hash hesla (pravdepodobne SHA-256 alebo podobný algoritmus)
- Dátum posledného prihlásenia
- Stav účtu (aktívny/neaktívny)

Táto štruktúra odpovedá internému autentifikačnému systému spoločnosti, pričom niektoré účty majú plné práva správy systémov, čo by mohlo viesť k eskalácii oprávnení.

## Dopad na vyšetrovanie

Získaním tohto súboru sa výrazne posilnilo podozrenie, že ide o interný únik dát – najmä z dôvodu prítomnosti:

- Admin účtov a citlivých rolí (napr. admin, IT\_support)
- Reálnych používateľských údajov vrátane e-mailov a oprávnení
- Hashovaných hesiel, ktoré môžu byť cieľom brute-force útokov
- Záznamov o poslednej aktivite účtov, ktoré umožňujú identifikovať podozrivé časové zhody

## Zistenia z bat súboru usb\_attack\_hidden.bat

Na rovnakom USB zariadení sa nachádzal aj skript usb\_attack\_hidden.bat, ktorý obsahuje SQL príkazy na aktiváciu neaktívneho účtu (**martinez**), manipuláciu so záznamami v databáze a mazanie logov. Toto predstavuje priamy dôkaz pokusu o:

- Obídienie autentifikácie
- Zmazanie digitálnych stôp
- Pripravenú exfiltráciu dát

## Analýza súboru log\_access.db zo zariadenie č. 2 – Firemný databázový server

Po nájdení skriptu usb\_attack\_hidden.bat na USB zariadení vzniklo podozrenie, že tento skript mohol byť aktívne použitý na databázovom serveri spoločnosti Templine. Na overenie tejto hypotézy bol analyzovaný súbor log\_access.db, ktorý slúži ako evidencia prístupov k databáze.

## Nástroje použité pri analýze:

**DB Browser for SQLite** – prehliadanie štruktúry databázy a výpis obsahu tabuliek

## Kľúčové zistenia:

V log súbore boli identifikované záznamy, ktoré presne korešpondujú so znením skriptu usb\_attack\_hidden.bat.

|      |      |                     |               |                 |        |               |                                                                                                                       |         |                   |
|------|------|---------------------|---------------|-----------------|--------|---------------|-----------------------------------------------------------------------------------------------------------------------|---------|-------------------|
| 3025 | 3025 | 2024-08-12 13:02:00 | maria98       | 99.185.143.60   | UPDATE | users         | UPDATE users SET column1 = 'new_value' WHERE id = 188;                                                                | FAILURE | ROLLBACK          |
| 3026 | 3026 | 2024-08-12 14:19:00 | Peter Oriesik | 250.125.2.255   | DELETE | customers     | DELETE FROM customers WHERE id = 416;                                                                                 | SUCCESS | ROLLBACK          |
| 3027 | 3027 | 2024-08-12 17:13:00 | Franklin      | 221.46.144.222  | INSERT | products      | INSERT INTO products (column1, column2) VALUES ('value1', 'value2');                                                  | SUCCESS | ROLLBACK          |
| 3028 | 3028 | 2024-08-12 18:57:00 | Peter Oriesik | 16.36.57.161    | DELETE | customers     | DELETE FROM customers WHERE id = 558;                                                                                 | FAILURE | Permission Denied |
| 3029 | 3029 | 2024-08-12 21:30:00 | oriesikp      | 80.2.241.176    | SELECT | orders        | SELECT COUNT(*) FROM orders WHERE status='pending';                                                                   | SUCCESS | ROLLBACK          |
| 3030 | 3030 | 2024-08-12 21:50:00 | oriesikp      | 80.2.241.176    | UPDATE | products      | UPDATE products SET stock=stock-5 WHERE product_id=92;                                                                | SUCCESS | ROLLBACK          |
| 3031 | 3031 | 2024-08-12 22:55:00 | oriesikp      | 80.2.241.176    | DELETE | logs          | DELETE FROM logs WHERE user IN ('testuser1', 'old_admin');                                                            | SUCCESS | ROLLBACK          |
| 3032 | 3032 | 2024-08-12 22:55:00 | oriesikp      | 80.2.241.176    | UPDATE | users         | UPDATE users SET password_hash='d033e22ae348aeb5660fc140aec35850c4da99?' WHERE username='martinezk';                  | SUCCESS | ROLLBACK          |
| 3033 | 3033 | 2024-08-12 22:55:00 | oriesikp      | 80.2.241.176    | UPDATE | users         | UPDATE users SET is_active=TRUE WHERE username='martinezk';                                                           | SUCCESS | ROLLBACK          |
| 3034 | 3034 | 2024-08-12 22:55:00 | oriesikp      | 80.2.241.176    | DELETE | logs          | DELETE FROM logs WHERE timestamp < '2024-08-01 00:00:00';                                                             | SUCCESS | ROLLBACK          |
| 3035 | 3035 | 2024-08-12 22:55:00 | oriesikp      | 80.2.241.176    | INSERT | security_logs | INSERT INTO security_logs (timestamp, action, user) VALUES (NOW(), 'SQL Injection - account activation', 'oriesikp'); | SUCCESS | ROLLBACK          |
| 3036 | 3036 | 2024-08-12 22:55:00 | oriesikp      | 80.2.241.176    | INSERT | security_logs | INSERT INTO security_logs (timestamp, action, user) VALUES (NOW(), 'System maintenance task completed', 'admin');     | SUCCESS | ROLLBACK          |
| 3037 | 3037 | 2024-08-12 22:55:00 | oriesikp      | 80.2.241.176    | UPDATE | users         | UPDATE users SET is_active=TRUE WHERE username='martinezk';                                                           | SUCCESS | ROLLBACK          |
| 3038 | 3038 | 2024-08-12 22:55:00 | oriesikp      | 80.2.241.176    | DELETE | logs          | DELETE FROM logs WHERE user='oriesikp';                                                                               | SUCCESS | ROLLBACK          |
| 3039 | 3039 | 2024-08-12 22:55:00 | oriesikp      | 80.2.241.176    | DELETE | logs          | DELETE FROM logs WHERE action LIKE '%SQL Injection%';                                                                 | SUCCESS | ROLLBACK          |
| 3040 | 3040 | 2024-08-12 22:55:00 | oriesikp      | 80.2.241.176    | UPDATE | users         | UPDATE users SET password_hash='d033e22ae348aeb5660fc140aec35850c4da99?' WHERE username='martinezk';                  | SUCCESS | ROLLBACK          |
| 3041 | 3041 | 2024-08-12 22:55:00 | oriesikp      | 80.2.241.176    | INSERT | security_logs | INSERT INTO security_logs (timestamp, action, user) VALUES (NOW(), 'SQL Injection - account activation', 'oriesikp'); | SUCCESS | ROLLBACK          |
| 3042 | 3042 | 2024-08-12 23:30:00 | oriesikp      | 80.2.241.176    | SELECT | customers     | SELECT first_name, last_name FROM customers WHERE city='Bratislava';                                                  | SUCCESS | ROLLBACK          |
| 3043 | 3043 | 2024-08-12 23:45:00 | oriesikp      | 80.2.241.176    | UPDATE | orders        | UPDATE orders SET status='shipped' WHERE id=156;                                                                      | SUCCESS | ROLLBACK          |
| 3044 | 3044 | 2024-08-13 01:12:00 | Franklin      | 93.76.30.58     | SELECT | orders        | SELECT * FROM orders WHERE id = 555;                                                                                  | FAILURE | ROLLBACK          |
| 3045 | 3045 | 2024-08-13 01:30:00 | maria98       | 70.197.109.47   | UPDATE | orders        | UPDATE orders SET column1 = 'new_value' WHERE id = 941;                                                               | SUCCESS | ROLLBACK          |
| 3046 | 3046 | 2024-08-13 03:11:00 | Franklin      | 208.219.57.92   | UPDATE | users         | UPDATE users SET column1 = 'new_value' WHERE id = 22;                                                                 | SUCCESS | ROLLBACK          |
| 3047 | 3047 | 2024-08-13 05:54:00 | admin         | 73.215.199.4    | DELETE | products      | DELETE FROM products WHERE id = 595;                                                                                  | SUCCESS | ROLLBACK          |
| 3048 | 3048 | 2024-08-13 06:14:00 | admin         | 19.161.247.42   | INSERT | users         | INSERT INTO users (column1, column2) VALUES ('value1', 'value2');                                                     | SUCCESS | ROLLBACK          |
| 3049 | 3049 | 2024-08-13 06:48:00 | janemsmith    | 161.20.143.228  | SELECT | customers     | SELECT * FROM customers WHERE id = 600;                                                                               | FAILURE | ROLLBACK          |
| 3050 | 3050 | 2024-08-13 08:56:00 | admin         | 15.113.142.144  | UPDATE | sales         | UPDATE sales SET column1 = 'new_value' WHERE id = 240;                                                                | SUCCESS | ROLLBACK          |
| 3051 | 3051 | 2024-08-13 11:34:00 | janemsmith    | 129.148.149.141 | UPDATE | sales         | UPDATE sales SET column1 = 'new_value' WHERE id = 494;                                                                | SUCCESS | ROLLBACK          |
| 3052 | 3052 | 2024-08-13 12:34:00 | Franklin      | 12.95.19.212    | UPDATE | orders        | UPDATE orders SET column1 = 'new_value' WHERE id = 236;                                                               | FAILURE | ROLLBACK          |
| 3053 | 3053 | 2024-08-13 13:07:00 | janemsmith    | 221.24.47.254   | INSERT | customers     | INSERT INTO customers (column1, column2) VALUES ('value1', 'value2');                                                 | FAILURE | ROLLBACK          |

Obrázok 6 - DB Browser for SQLite - log\_access.db

## Kritické príkazy zachytené v logu:

```
UPDATE users SET password_hash='...' WHERE username='martinezk';
UPDATE users SET is_active=TRUE WHERE username='martinezk';
INSERT INTO security_logs (...) VALUES (NOW(), 'SQL Injection - account activation', 'oriesikp');
DELETE FROM logs WHERE user='oriesikp';
DELETE FROM logs WHERE content LIKE '%SQL injection%';
```

## Prístupové údaje:

- **Používateľ:** oriesikp
- **IP adresa:** 80.2.241.176
- **Dátum a čas útoku:** 12. 8. 2024 o 22:55:00

## *Pokus o zhladenie stôp*

Analýza ukázala, že útočník sa snažil odstrániť dôkazy o svojich aktivitách. Boli zaznamenané pokusy o zmazanie:

- vlastných záznamov (DELETE FROM logs WHERE user='oriesikp';)
- záznamov obsahujúcich frázu SQL injection (DELETE FROM logs WHERE content LIKE '%SQL injection%';)

**Tieto záznamy sa však v logu zachovali, čo naznačuje:**

- že príkaz síce prebehol, ale **názov reťazca nebol vo všetkých riadkoch exaktne prítomný**
- **záznam bol vytvorený po operácii**, a teda sa log nestihol zmazať, alebo
- **logovanie prebehlo nezávisle**, a útočník tento aspekt podcenil.

## *Dopad na vyšetrovanie*

Získané dôkazy výrazne podporili hypotézu č. 3 (zneužitie neaktívneho účtu administrátora) a zároveň prepojili jednotlivé zariadenia:

- **Skript na USB (zariadenie č. 1)** obsahuje príkazy identické s tými, ktoré boli vykonané na serveri.
- **Záznamy v log\_access.db (zariadenie č. 2)** preukázali prístup a manipuláciu konkrétnym používateľom oriesikp.
- Na základe týchto dôkazov bol **zaistený pracovný notebook (zariadenie č. 3)**, kde sa predpokladá príprava alebo testovanie tohto útoku.

## *Analýza zariadenia č. 3 – Pracovný notebook zamestnanca*

Na základe predchádzajúcich dôkazov získaných z USB zariadenia (**skript usb\_attack\_hidden.bat**) a **logov servera**, ktoré odhalili podozrivú aktivitu používateľa **Petra Oriška**, bol zaistený jeho pracovný notebook na ďalšiu analýzu. Cieľom bolo preveriť, či sa na zariadení nachádzajú dôkazy o príprave alebo testovaní SQL útoku, prípadne o pokuse o exfiltráciu údajov.

Z notebooku bol pomocou nástroja **Magnet RAM Capture** odobratý **RAM dump**, ktorý bol následne analyzovaný v nástroji **HxD**.

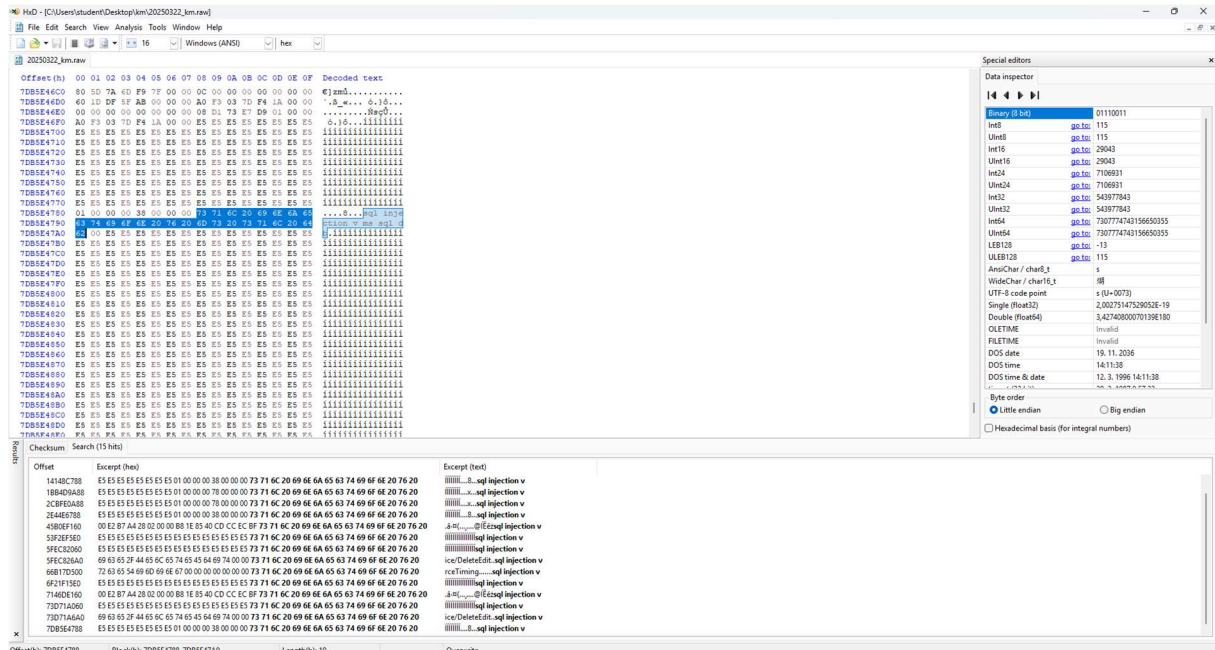
## *Výsledky analýzy:*

Vyhľadávanie reťazcov v pamäti odhalilo opakované výskyty výrazov súvisiacich s plánovaním SQL útoku:

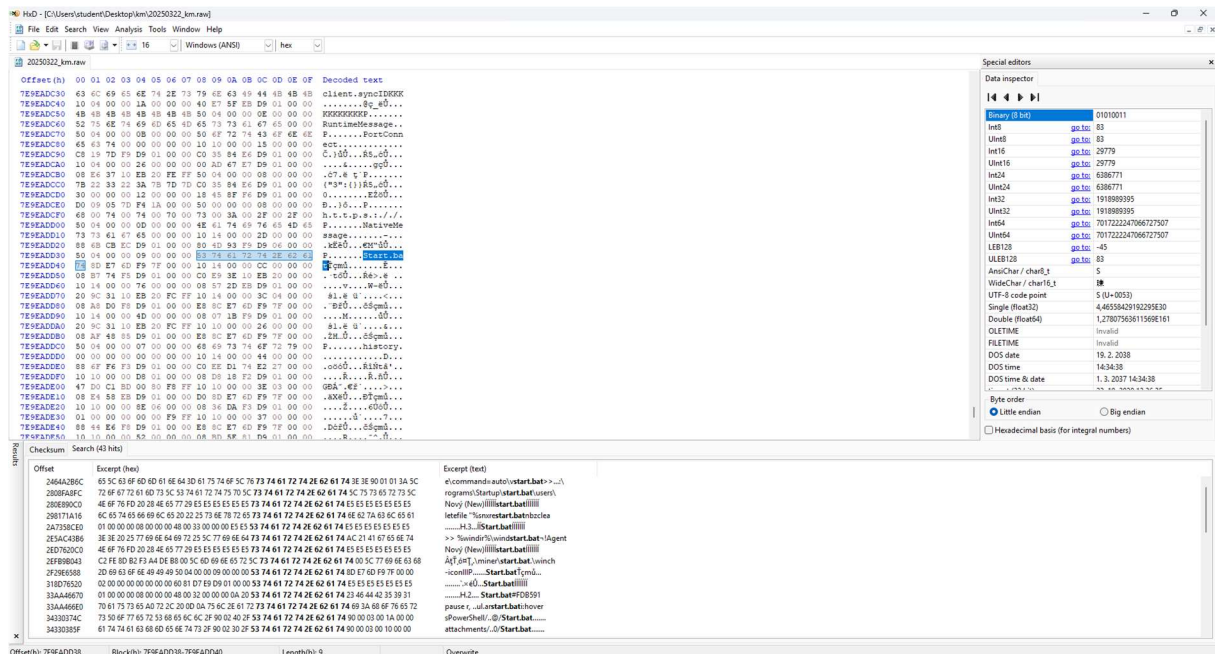
- sql injection
- how to sql inject
- how to make sql injection in .bat
- delete from logs
- start.bat
- structure of sql table

Výňatok z RAM dumpu:

Manuálnou analýzou pomocou HxD boli identifikované viaceré výskyty daných reťazcov. Tieto výsledky jasne poukazujú na to, že používateľ si pred incidentom aktívne vyhľadával informácie o spôsoboch útoku na SQL databázu, vrátane možnosti ich implementácie pomocou .bat súborov.



Obrázok 7 - RAM dump - Peter Oriesik - sql injection



Obrázok 8 - RAM dump - Peter Oriesik - start.bat

**Dopad na vyšetrovanie:**

Tieto dôkazy významne **prispeli k potvrdeniu hypotézy o internom útoku**, nakoľko:

- Reťazce boli zachytené v **operačnej pamäti** používateľa v čase po incidente.

- Použité výrazy naznačujú **úmyselnú prípravu skriptu** a znalosť postupu.
- Vyhľadávanie priamo korešponduje s **obsahom .bat skriptu** nájdeného na USB zariadení.

Na základe analýzy RAM dumpu bolo možné potvrdiť, že používateľ **Peter Orišek** sa zaujímal o techniky SQL injection a pripravoval si postupy na realizáciu útoku. **Nedokonaný úmysel**: Hoci plán bol evidentne v štádiu realizácie, **ku kompletnému dokonaniu nedošlo**. Kľúčové USB zariadenie, ktoré obsahovalo exfiltrované dáta a skript, bolo pravdepodobne **stratené v kancelárii** a následne nájdené vo vysávači. Nenašli sa dôkazy o tom, že by dáta boli:

- odoslané cez firemnú sieť,
- nahraté na cloudové úložisko,
- alebo inak distribuované tretím stranám.

Nenachádzajú sa ani žiadne e-mailové konverzácie, ktoré by naznačovali obchodné rokovania alebo pokus o predaj získaných údajov.

Na základe zhromaždených digitálnych dôkazov a vykonanej analýzy jednotlivých zariadení bola vytvorená rozhodovacia matica pre objektívne vyhodnotenie hypotéz:

## Hypotéza č. 1 – Neúmyselné uloženie firemných dát na USB zariadenie

### VYVRÁTENÁ

Hoci by za istých okolností mohlo dôjsť k nechcenému prenosu dát, v tomto prípade tomu nič nenasvedčuje. Na USB sa našli viaceré databázové súbory (napr. users.db, customers.db, pricing.db), ktoré sú štruktúrované, úplné a zodpovedajú obsahom citlivým interným údajom. Navyše bol na zariadení nájdený aj skript usb\_attack\_hidden.bat, ktorý vykonáva SQL príkazy aktivujúce účty a upravujúce logy. Takéto kroky jasne preukazujú zámer a nie náhodu.

#### Dôvody vyvrátenia:

1. Obsah USB bol cielene pripravený.
2. Skript naznačuje úmysel manipulovať databázu.
3. Dáta boli kopírované selektívne, nie plošne.

## Hypotéza č. 2 – Externý útok prostredníctvom škodlivého USB

### VYVRÁTENÁ

Fyzická analýza, prístupové logy a audit zabezpečených priestorov nepotvrdili žiadny neoprávnený vstup do budovy. USB zariadenie bolo nájdené vo vysávači – čo skôr naznačuje, že ho útočník nechtiac stratil. Nebola zistená prítomnosť škodlivého softvéru ani exploit kódov, ktoré by naznačovali pokus o externé narušenie systémov.

#### Dôvody vyvrátenia:

1. Žiadne známky narušenia bezpečnostných protokolov.
2. USB obsahovalo interné dáta, nie malvér.
3. Podozrivý účet a skript smerujú k internému pôvodu.

## Hypotéza č. 3 – Zneužitie neaktívneho účtu administrátora

### POTVRDENÁ

Záznamy v logoch databáz jasne ukazujú prístup pomocou konta **martinez**, ktoré bolo dlhodobo neaktívne. Tento účet bol aktivovaný a použitý na prístup k databázam a manipuláciu údajov. Príkazy korešpondujú so skriptom nájdeným na USB zariadení a vyhľadávané výrazy v RAM dump-e potvrdzujú znalosť a zámer vykonať útok pomocou SQL injection.

### Kľúčové dôkazy:

1. Aktivácia a použitie účtu martinez v logoch (SQL príkazy na aktiváciu účtu).
2. Skript na USB zodpovedá vykonaným akciám v databáze.
3. RAM dump obsahoval výrazy súvisiace so SQL injection a tvorbou BAT súborov.

## Záverečné hodnotenie

Forenzná analýza jednoznačne potvrdila, že došlo k internému úniku dát prostredníctvom zneužitia neaktívneho účtu **martinez**. Útočník (pravdepodobne zamestnanec **Peter Orišek**) si pripravil BAT skript, ktorý manipuloval databázou a snažil sa zahľadiť stopy.

Najsilnejší dôkaz predstavuje **skript usb\_attack\_hidden.bat** a jeho zhodnosť s operáciami zaznamenanými v logoch SQL servera. Hoci nebolo dokázané, že dáta boli úspešne odovzdané tretej strane, existovali všetky predpoklady na ich postupné vynesenie – čo narušilo integritu a dôveru vo vnútorný bezpečnostný rámec firmy.