

# Únik citlivých firemných údajov

M. Mateáš

<https://bestudent.fpvucm.sk/~mateasmarek/dfa/prezentacia.pdf>

## Prípado:

V poisťovni vzniklo podozrenie na hromadné sťahovanie databázových súborov, ktoré obsahovali citlivé osobné údaje klientov, ako sú mená, adresy a rodné čísla. Podľa analýzy sieťových záznamov bolo zistené, že neobvyklý objem prenesených dát súvisí s konkrétnym zamestnancom a jeho počítačom. Zatiaľ však nie je jasné, či je tento zamestnanec priamo zodpovedný za tento incident. Je možné, že niekto z IT tímu mohol neoprávnene získať prístup k jeho zariadeniu a vykonať túto činnosť.

## Predmet vyšetrovania:

Cieľom vyšetrovania je identifikovať a usvedčiť osobu zodpovednú za únik citlivých údajov prostredníctvom digitálnej forenznej analýzy a sieťového auditu.

## Ciele vyšetrovania:

- **Identifikácia páchatela** - Určenie osoby zodpovednej za neoprávnený prístup k citlivým údajom.
- **Stanovenie časovej osi udalostí** - Presné určenie času a spôsobu sťahovania údajov, ako aj určenie možných komunikačných spojení medzi podozrivým a tretou stranou.
- **Zisťovanie motivácie a úmyslu** - Vyhodnotenie, či išlo o individuálny čin, kybernetický útok alebo spoluprácu viacerých osôb.

## 5WH:

### Who? (Kto?)

- **Podozrivý zamestnanec** - Osoba, ktorej firemný notebook bol použitý na stiahnutie citlivých údajov klientov.
- **IT oddelenie** - Skupina zamestnancov, ktorí majú prístup k sieťovým nastaveniam a mohli manipulovať s prenosom dát.
- **Externý útok** - Notebook bol kompromitovaný, pravdepodobne prostredníctvom škodlivého softvéru (malvéru alebo vírusu), ktorým útočník získal neoprávnený prístup.

### What? (Čo sa stalo?)

- Bolo zaznamenané hromadné sťahovanie databázových súborov obsahujúcich citlivé údaje klientov (mená, adresy, rodné čísla).
- Sieťová analýza odhalila neobvyklý objem prenesených dát spojený s firemným notebookom konkrétného zamestnanca.

- Nie je jasné, či bol tento zamestnanec priamo zodpovedný alebo či bol jeho počítač kompromitovaný.
- Existuje podozrenie, že údaje mohli byť odoslané tretej strane výmenou za finančnú odmenu.

### **When? (Kedy sa to stalo?)**

- Incident sa stal v roku 2018.
- Vyšetrovanie sa začalo až po nastúpení nového IT tímu kde po detekcii neobvyklého dátového prenosu a internom audite bezpečnostných záznamov zistili že došlo k sťahovaniu veľkého objemu citlivých údajov.

### **Where? (Kde sa to stalo?)**

- **Fyzicky:** Incident súvisí s firemným notebookom podozrivého zamestnanca, ktorý bol používaný v rámci kancelárskych priestorov firmy.
- **Digitálne:** Únik sa udial cez internú sieť spoločnosti, pričom dáta mohli byť odoslané na externý server alebo úložisko.

### **Why? (Prečo sa to stalo?)**

- Motivácia páchatela môže byť finančný zisk predajom citlivých údajov tretím stranám.
- Možnosť vnútorného podvodu alebo spolupráce s osobami mimo spoločnosti.
- Podozrenie na kompromitáciu zariadenia zamestnanca vírusom/malwarom.

### **How? (Ako?)**

- Prepokladá sa že išlo o interný útok alebo externý útok.

### **Hypotézy:**

**Hypotéza 1:** Tento zamestnanec mohol sám neoprávnene stiahnuť citlivé údaje z firemného systému s úmyslom ich získať a následne ich predať tretej strane. Tento krok by mohol byť motivovaný finančným ziskom. Na mobilnom telefóne podozrivého zamestnanca sa môžu nachádzať správy alebo iné dôkazy, ktoré by potvrdili dohodu s nelegálnym partnerom.

**Hypotéza 2:** Zamestnanci IT oddelenia majú prístup k technickým nástrojom na manipuláciu s prenosom dát a sieťovými nastaveniami. Je možné, že jeden z týchto zamestnancov zneužil svoj prístup na to, aby umožnil prenos citlivých údajov zo zamestnaneckého notebooku alebo pomohol zamestnancovi skryť stopy po úniku.

Tento zamestnanec mohol mať motiváciu získať osobné údaje na predaj alebo iné nelegálne účely.

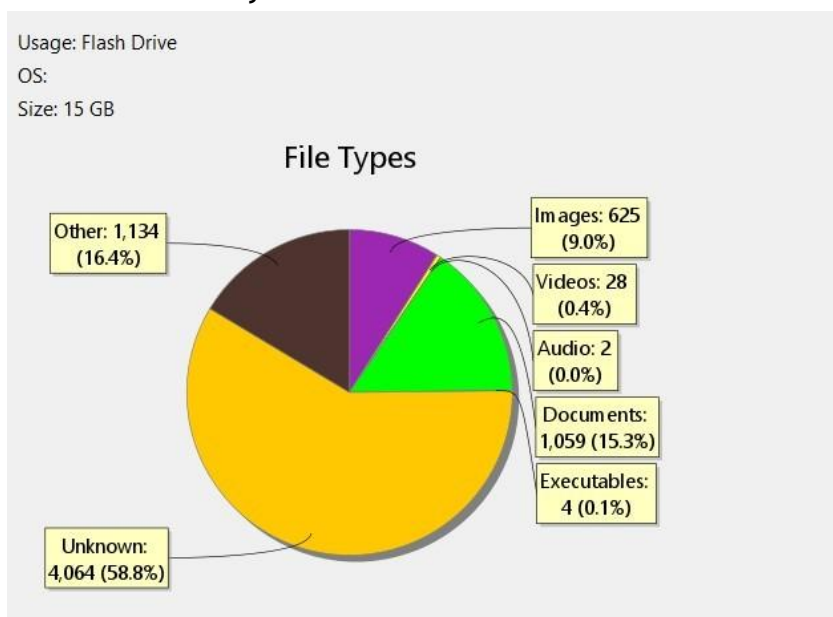
**Hypotéza 3:** Zamestnanec mohol byť obeťou škodlivého softvéru, ako je malware alebo vírus, ktorý infikoval jeho počítač. Tento škodlivý kód mohol útočníkovi umožniť získať

neoprávnený prístup k systému a vykonať prenos citlivých dát bez vedomia zamestnanca. V takomto prípade je potrebné podrobiť počítač dôkladnej analýze, aby sa zistilo, či existujú dôkazy o prítomnosti škodlivého softvéru alebo známkach infekcie.

### Príprava dát:

Pri vyšetrovaní budem pracovať s **datasetom**, obsahuje okolo 6000 súborov. Medzi hlavné analyzované údaje patria:

- **Metadáta súborov** - Dátum, čas, zariadenie použité na prístup k databáze a IP adresy.
- **Komunikačné záznamy** - Obsah správ alebo e-mailov medzi podozrivým zamestnancom a možnými tretími stranami.



### Odkazy na datasety

- <https://www.digitalforensicsworkbook.com/data-sets>
- <https://cfreds.nist.gov/all/TariqueAnwar%2FMuhammedAbulais/ChatLogs>
- <https://web.archive.org/web/20160402173454/http://dfrws.org/2009/rodeo.shtml>
- <https://corp.digitalcorpora.org/corpora/scenarios/2012-ngdc/email/>
- <https://fau1-files.cs.fau.de/public/sqlite-forensic-corpus/>
- <https://web.archive.org/web/20160403140908/http://www.dfrws.org/2006/challenge/submission.shtml>

- <https://web.archive.org/web/20160402191131/http://www.dfrws.org/2007/challenge/submission.shtml>

#### Digitálne zariadenia:

- **Firemný notebook podozrivého zamestnanca** - Detailná analýza dátových prenosov, histórie sťahovania a možných neoprávnených prístupov. Model - Lenovo IdeaPad 330-15ICH (81FK00JACK)



| Parameter       | Hodnota                            |
|-----------------|------------------------------------|
| Produkt         | Lenovo IdeaPad 330-15              |
| Kód produktu    | 81FK00JACK                         |
| Procesor        | Intel® Core™ i7-8750H (2.20 GHz)   |
| Pamäť (RAM)     | 16GB                               |
| Úložisko        | 128GB SSD                          |
| Grafická karta  | NVIDIA GeForce GTX 1050, 4GB GDDR5 |
| Rozmery         | 378mm × 260mm × 22.9mm             |
| Operačný systém | Windows 11                         |

#### Ram pamäť:

- **Memory dump** - Po vykonaní pamäťového výpisu bol v pamäti nájdený záznam o stiahnutí súboru s názvom InsuranceDB.sql, čím sa potvrdilo, že databázové údaje boli stiahnuté

[illegible]

- **Notebook** - Pri zaist'ovaní notebooku sme postupovali nasledovne: Notebook bol zapnutý počas zaist'ovania, odpojili sme ho zo siete, aby sme zabezpečili, že údaje nemôžu byť upravené alebo vymazané pomocou externých online programov. Následne sme vytvorili RAM obraz, aby sme získali jeho obsah. Po získaní údajov z RAM sme notebook vypli a vložili do Faradayovho vrečka, aby sme zablokovali všetky bezdrôtové signály. Potom sme ho umiestnili do pevného kufríka, aby sme zabránili jeho poškodeniu počas prepravy.

- **Kópie** - Boli vytvorené 3 kópie na 3 HDD disky, z toho 2 sme uložili do stráženého trezoru a 1 na ktorej sa robila analýza
- **Chain of custody** - Po zaistení údajov sme vytvorili chain of custody -

|                                         |      |                                                                                 |                      |          |       |
|-----------------------------------------|------|---------------------------------------------------------------------------------|----------------------|----------|-------|
| Číslo:                                  | 01   | Typ :                                                                           | Digitálne zariadenie | Veľkosť: | 250GB |
| Popis prípadu:                          |      | Únik citlivých firemných údajov                                                 |                      |          |       |
| Zariadenie:                             |      | Lenovo IdeaPad 330-15 - 81FK00JACK                                              |                      |          |       |
| Miesto získania digitálneho zariadenia: |      | V zamestnancovej kancelárii vo firme                                            |                      |          |       |
| Poznámky:                               |      | Pri zabavovaní boli prítomní IT technik firmy a právnik firmy                   |                      |          |       |
|                                         |      |                                                                                 |                      |          |       |
| Digitálny odtlačok (heš)                | MD5  | 6d369fc8e1fe0f688c8f6886e2eca5f1                                                |                      |          |       |
|                                         | SHA1 | dabbebc8c3398a58d229e06f5b3aa32b21b55cbe                                        |                      |          |       |
|                                         |      |                                                                                 |                      |          |       |
| Časová pečiatka                         |      |                                                                                 |                      |          |       |
| Pia Mar 7<br>18:23:20 2025              |      | Vypojenie notebooku od siete                                                    |                      |          |       |
| Pia Mar 7<br>18:24:20 2025              |      | Vytvorenie RAM-obrazu                                                           |                      |          |       |
| Pia Mar 7<br>18:30:15 2025              |      | Vypnutie notebooku                                                              |                      |          |       |
| Pia Mar 7<br>18:35:46 2025              |      | Zabalenie notebooku do Faradayovho vrečka a následne vložený do pevného kufríka |                      |          |       |

#### Použité nástroje digitálnej forenznnej analýzy

- **AutoPsy** - nástroj na otvorenie obrazu disku, analýza súborov
- **FTK Imager** - vytvorenie RAM-obrazu a kópie disku (vytvorené dve kópie, jedna na USB a druhá na disku)
- **HxD editor** - nástroj na preskúmanie obrazu RAM

## Dátová analýza:

Analyzovali sme notebook zamestnankyne z ktorého bolo zaznamenané sťahovanie. Podrobnejšie sme skúmali či sa nachádzali na notebooku databázové súbory, emailovú komunikáciu a logy.

| Name                                                                                          | S | C | O | ⚡ Modified Time               | Change Time         | Access Time                   |
|-----------------------------------------------------------------------------------------------|---|---|---|-------------------------------|---------------------|-------------------------------|
|  01-18.db    |   |   | 2 | 2017-10-07 21:00:50 GMT+01:00 | 0000-00-00 00:00:00 | 2025-03-28 00:00:00 GMT+01:00 |
|  01-02.sql   | ▼ |   | 2 | 2018-07-14 10:03:24 GMT+01:00 | 0000-00-00 00:00:00 | 2025-03-28 00:00:00 GMT+01:00 |
|  01-03.sql   | ▼ |   | 2 | 2018-07-14 10:03:24 GMT+01:00 | 0000-00-00 00:00:00 | 2025-03-28 00:00:00 GMT+01:00 |
|  01-04.sql   | ▼ |   | 2 | 2018-07-14 10:03:24 GMT+01:00 | 0000-00-00 00:00:00 | 2025-03-28 00:00:00 GMT+01:00 |
|  01-05.sql   | ▼ |   | 2 | 2018-07-14 10:03:24 GMT+01:00 | 0000-00-00 00:00:00 | 2025-03-28 00:00:00 GMT+01:00 |
|  01-06.sql   | ▼ |   | 2 | 2018-07-14 10:03:24 GMT+01:00 | 0000-00-00 00:00:00 | 2025-03-28 00:00:00 GMT+01:00 |
|  01-07.sql   | ▼ |   | 2 | 2018-07-14 10:03:24 GMT+01:00 | 0000-00-00 00:00:00 | 2025-03-28 00:00:00 GMT+01:00 |
|  01-08.sql   | ▼ |   | 2 | 2018-07-14 10:03:24 GMT+01:00 | 0000-00-00 00:00:00 | 2025-03-28 00:00:00 GMT+01:00 |
|  01-09.sql   | ▼ |   | 2 | 2018-07-14 10:03:24 GMT+01:00 | 0000-00-00 00:00:00 | 2025-03-28 00:00:00 GMT+01:00 |
|  01-10.sql   | ▼ |   | 2 | 2018-07-14 10:03:24 GMT+01:00 | 0000-00-00 00:00:00 | 2025-03-28 00:00:00 GMT+01:00 |
|  01-11.sql   | ▼ |   | 2 | 2018-07-14 10:03:24 GMT+01:00 | 0000-00-00 00:00:00 | 2025-03-28 00:00:00 GMT+01:00 |
|  01-12.sql   | ▼ |   | 2 | 2018-07-14 10:03:24 GMT+01:00 | 0000-00-00 00:00:00 | 2025-03-28 00:00:00 GMT+01:00 |
|  01-13.sql   | ▼ |   | 2 | 2018-07-14 10:03:24 GMT+01:00 | 0000-00-00 00:00:00 | 2025-03-28 00:00:00 GMT+01:00 |
|  01-14.sql  | ▼ |   | 2 | 2018-07-14 10:03:24 GMT+01:00 | 0000-00-00 00:00:00 | 2025-03-28 00:00:00 GMT+01:00 |
|  01-15.sql | ▼ |   | 2 | 2018-07-14 10:03:24 GMT+01:00 | 0000-00-00 00:00:00 | 2025-03-28 00:00:00 GMT+01:00 |
|  01-16.sql | ▼ |   | 2 | 2018-07-14 10:03:24 GMT+01:00 | 0000-00-00 00:00:00 | 2025-03-28 00:00:00 GMT+01:00 |
|  01-17.sql | ▼ |   | 2 | 2018-07-14 10:03:24 GMT+01:00 | 0000-00-00 00:00:00 | 2025-03-28 00:00:00 GMT+01:00 |
|  01-18.sql | ▼ |   | 2 | 2018-07-14 10:03:24 GMT+01:00 | 0000-00-00 00:00:00 | 2025-03-28 00:00:00 GMT+01:00 |
|  01-01.sql | ▼ |   | 2 | 2018-07-20 10:02:58 GMT+01:00 | 0000-00-00 00:00:00 | 2025-03-28 00:00:00 GMT+01:00 |
|  01-01.xml | ▼ |   | 2 | 2018-07-22 11:17:22 GMT+01:00 | 0000-00-00 00:00:00 | 2025-03-28 00:00:00 GMT+01:00 |

Našli sa stiahnuté súbory z daného roka kedy došlo k incidentu. Dané SQL súbory obsahovali údaje mená a priezviská klientov s ktorými firma spolupracovala.

```

PRAGMA page_size=4096;
PRAGMA page_size;
PRAGMA encoding="UTF-8";
PRAGMA encoding;
PRAGMA secure_delete=1;
PRAGMA secure_delete;
CREATE TABLE ")" (
    'id' INT UNSIGNED NOT NULL,
    'name' TEXT NOT NULL,
    'surname' TEXT NULL,
    'zip' INT UNSIGNED NULL
INSERT INTO ")"
    (id, name, surname, zip)
VALUES
    (20001, 'Isabella', 'Fischer', '84543'),
    (20002, 'Heinrich', 'Schulz', '88317'),
    (20003, 'Linus', 'Pohl', '73642'),
    (20004, 'Walter', 'Hofmann', '24891'),
    (20005, 'Claudia', 'Engel', '83339'),
    (20006, 'Leon', 'Hoffmann', '86447'),
    (20007, 'Werner', 'Bergmann', '6642'),
    (20008, 'Fritz', 'Engel', '38465'),
    (20009, 'Hanna', 'Frank', '65396'),
    (20010, 'Amelie', 'Schmidt', '54636');

```

```

PRAGMA page_size=4096;
PRAGMA page_size;
PRAGMA encoding="UTF-8";
PRAGMA encoding;
PRAGMA secure_delete=1;
PRAGMA secure_delete;
CREATE TABLE "
    'id' INT UNSIGNED NOT NULL,
    'name' TEXT NOT NULL,
    'surname' TEXT NULL,
    'zip' INT UNSIGNED NULL
INSERT INTO "
    (id, name, surname, zip)
VALUES
    (20001, 'Marie', 'Meier', '66871'),
    (20002, 'Matthias', 'Stein', '97727'),
    (20003, 'Tobias', 'Kuhn', '40470'),
    (20004, 'Timo', 'Mayer', '98693'),
    (20005, 'Marlene', 'K
hn', '83544'),
    (20006, 'Andrea', 'Vogt', '16562'),
    (20007, 'Thomas', 'Ludwig', '67468'),
    (20008, 'Maximilian', 'Schmitt', '48151'),
    (20009, 'Florian', 'Roth', '56112'),
    (20010, 'Alexandra', 'Roth', '32683');

```

## Ďalej sa našli rozhovory v mailovej komunikácii zamestnankyne a bývalého IT technika.

![User 'tracysumtwelve' has logged in : Mon Jun 2 16:02:42 2012]  
joe.sum.twelve@gmail.com<tab><tab>Regarding Terry<tab>Joe,

Sory<del>ry to bothre <del><del><del>er you, but I have a serious question about Terry and her school. Her tut<del>ition is getting a bit too much for me right now and I coud<del>ld use a little help. I hate to impose on you for this, but is there any way you would be hillin<del><del><del><del><del><del>willing to help me a<del>out with her ut<del><del>tuition for <del><del><del>this s<del>year?

Please get back to me,  
TracyHi Engy<del>od!

That sounds great, I'll gie<del>be<del><del>ve you a all s<del><del><del><del><del>call soe<del>me time and we can figure out some plans

![LogKext Daemon created new logfile : Mon Jun 2 12:00:04 2012]

ing interesting. everyb<del><del><del><del><del>Er<del><del>verybody around the office seems to be buzzed about a foreign exhibit thats supposed to<del><del><del><del><del><del><del><del><del><del> is supposed to be coming over. There hasn't been any official release in writing but we have been going through a q<del><del><del>quite an ordeal with all this paperwo rk. From what I can tell, this exhibit<del><del><del>bit has to be a big deal. I'll let you know if I found out anything else.

Coral,<del>private school financial aid  
legalBee

Z týchto rozhovorov vyplýva že zamestnankyňa bola v zlej finančnej situácii a opýtala sa IT technika či by jej s tým vedel nejako pomôcť. IT technik jej na toto odpovedal s tým že sa vo firme bude konať niečo veľké a že jej dá vedieť bližšie informácie.

hun<del>Coral<tab>coralbluetwo@hotmail.com<tab>legalBeePerr<del><del><del><del>pe<del><del><del><del>Perry, <del>

know what you meanj<del>. If anything comes up around the office that we can maybe... get in on... <del>, <del><del><del><del>, please lets try to do so. Kiddo is getting really bent out of shape ab ou <del>t possibly having to switch schools. I have been paying some more attention to the mmo<del><del><del>memos and papers that come across my desk. We get a bunch of insurance type documents hat plac val<del><del><del>e values on a certain objects. If anything stands out, I  
[LogKext Daemon starting up : Fri Jun 29 09:04:12 2018]

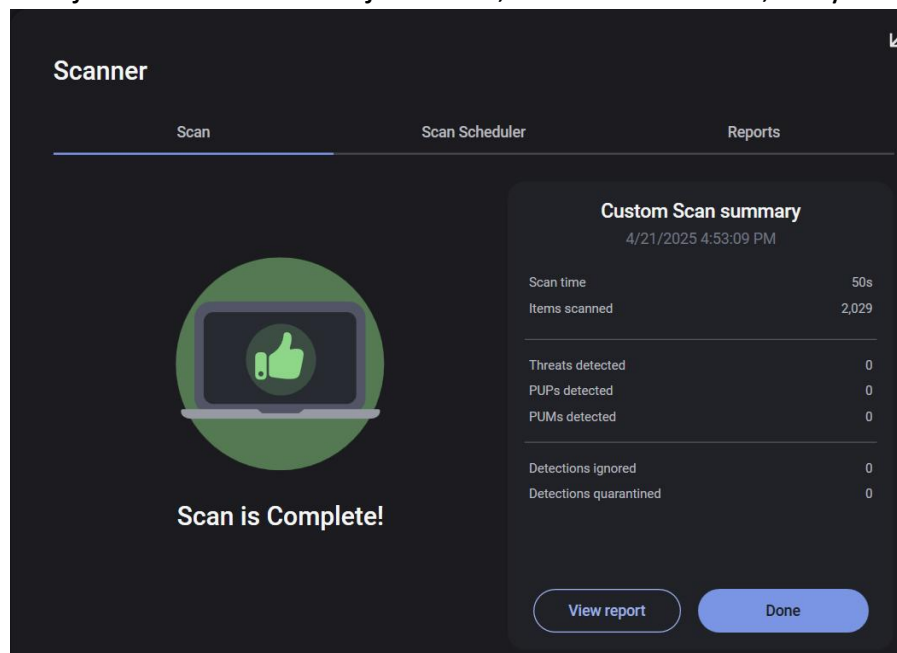
[User 'tracysumtwelve' has logged in : Fri Jun 29 09:14:10 2018]

V ďalšej konverzácii sa dostávame ku zmienke dokumentov ktoré sa týkali poistenia a že by tieto dokumenty mohli mať finančnú hodnotu.

![User 'tracysumtwelve' has logged in : Fri Jun 29 10:33:25 2018]  
9<del>legalBee  
<del><del><del><del>

Be careful! We have enough problems as it is, we can't get <del><del><del><del>be getting in trouble or losing our jobs. Nothing special has turned up here, but I am still keeping an eye out. We usually sot<del><del><del>start to host some interesting events this time of the year, I'm sure som

Ďalej bolo z komunikácie je zistené, že si uvedomovali, že tým riskujú svoje pracovné miesta.



Ďalej sa skúmalo či počítač bol kompromitovaný vírusom alebo malwarom. Výsledkom bolo že zariadenie nič takéto neobsahovalo.

## Záver / Overenie hypotéz:

### Hypotéza 1 a Hypotéza 2:

Potvrdili sme pomocou analýzou emailov a zariadenia, že sa jednalo o interný únik dát. Nevieme ale potvrdiť, či dané osoby mali nakoniec finančnú odmenu alebo nie z predaju informácií. Takže táto hypotéza je **nekonkluzívna**.

### Hypotéza 3:

Táto hypotéza je **vyvrátená** – V analýze sme nenašli žiadne vírusy alebo malware.

### Výsledok:

Výsledkom analýzy bolo zistenie, že firma má nedostatočné bezpečnostné opatrenia. Odporúča sa zvýšiť úroveň zabezpečenia a zaviesť dôslednejšiu kontrolu činností zamestnancov s cieľom posilniť celkovú bezpečnosť.

### Odporúčané kroky:

Odporúčaným krokom je zlepšenie úrovne kybernetickej bezpečnosti a zavedenie pravidelných bezpečnostných auditov. Ďalej sa odporúča vypočítať zamestnanca s cieľom potvrdiť alebo vyvrátiť hypotézy č. 1 a č. 2.

## Literatúra:

### "Live Memory Forensics of Mobile Phones"

[https://dfrws.org/sites/default/files/session-files/2010\\_USA\\_paper-live\\_memory\\_forensics\\_of\\_mobile\\_phones.pdf](https://dfrws.org/sites/default/files/session-files/2010_USA_paper-live_memory_forensics_of_mobile_phones.pdf)

Táto štúdia skúma forenznú analýzu živej pamäte mobilných telefónov, ktorá uchováva dočasné dáta, bežiacie procesy a neuložené správy. Výskum ukazuje, že odchádzajúce správy sa dajú získať na 100 %, zatiaľ čo prichádzajúce majú nižšiu mieru zotavenia (75,6 – 100 %). Analýza RAM pomáha získať dôkazy z komunikácií, ktoré by inak mohli byť stratené.

### "Database memory forensics: Identifying cache patterns for log verification"

<https://dfrws.org/wp-content/uploads/2023/07/wagner-databasememoryforensics.pdf>

Táto štúdia sa zaoberá analýzou pamäte databázových systémov s cieľom overiť správnosť logovacích mechanizmov. Autori skúmajú vzory v cache pamäti, ktoré vznikajú pri spracovaní databázových dotazov, a navrhujú metódy na identifikáciu týchto vzorov za účelom verifikácie logov. Tento prístup je obzvlášť užitočný v prípadoch, keď sú logy neúplné alebo nedôveryhodné, pretože umožňuje rekonštruovať nedávnu aktivitu v databáze priamo z pamäťových artefaktov. Výsledky výskumu prispievajú k zlepšeniu forennej analýzy databáz tým, že poskytujú nástroje na detekciu neoprávnených alebo skrytých operácií, ktoré by inak mohli zostať neodhalené.