

Odcudzenie osobných údajov

Prezentácia TU:

Autor: Martin Kurčík

Popis prípadu:

V malom meste Sliač došlo k vážnemu incidentu, keď boli odcudzené citlivé osobné údaje pacientov z miestnej súkromnej nemocnice. Jeden z lekárov si ráno o 8:30 14.4.2025 všimol že údaje o pacientoch v databáze neexistujú alebo boli vymazané z centrálneho počítača.

Predmet vyšetrovania:

Zisťovanie aké súbory boli vymazané alebo prepísané

Overenie či došlo k neoprávnenému prístupu k údajom

Obnovenie vymazanej alebo stranenej databázy pacientov

Identifikácia páchatel'a.

Motív čo páchatel'a viedlo k odcudzeniu osobných údajov?

Ako by sa zlepšila bezpečnosť nemocnice po identifikácii bezpečnostných nedostatkov?

Čo sme zistili z digitálnych stôp?

Aké digitálne stopy by sme vedeli nájsť ktoré by nám pomohli s vyšetrovaním?

Aký spôsob použil páchatel' pre odcudzenie osobných údajov?

Očakávaný výsledok:

Cieľom tohto vyšetrovania je zistiť prečo databáza o pacientoch bola vymazaná z centrálneho počítača. Potrebujeme zistiť:

Potrebujeme vytvoriť obraz daného zariadenia aby sme zistili logy, manipuláciu jednotlivých systémov či fungovali správne

Ak to bude možné určiť páchatel'a

Odborné príspevky:

Database Forensic Analysis Through Internal Structure Carving

<https://dfrws.org/presentation/databaseforensicanalysisthroughinternalstructurecarving/>

Forenzné nástroje pomáhajú analytikom s obnovou údajov a udalostí v systéme, aj z poškodeného úložiska. Tieto nástroje typicky využívajú techniky "carvingu" súborov na obnovu súborov po strate metadát analýzou zvyšného surového obsahu súboru. V relatívnych databázach sa ukladá a spracováva významné množstvo citlivých údajov, čo vyžaduje forenzné nástroje pre databázy, ktoré rozširujú riešenia carvingu súborov do oblasti databáz. Surové úložisko databázy je rozdelené na individuálne "stránky", ktoré nemožno čítať alebo prezentovať analytikovi bez pomoci samej databázy. Okrem toho, pri priamom prístupe k surovému úložisku databázy môžeme odhaliť veci, ktoré sú bežne skryté pred užívateľmi databázy. Existuje niekoľko špecifických nástrojov pre databázy vyvinutých na núdzovú obnovu databázy, hoci zvyčajne nie pre forenznú analýzu databázy. V tomto dokumente predstavujeme univerzálny nástroj, ktorý bezproblémovo podporuje mnoho rôznych databáz, obnovuje obsah tabuliek a ďalšie údaje z akýchkoľvek zvyšných fragmentov úložiska na disku alebo v pamäti. Definujeme prístup k automatickému (s minimálnym zásahom užívateľa) reverznému inžinierstvu úložiska v nových databázach, na detekciu voliteľných zmien údajov a objavovanie artefaktov používateľských akcií. Nakoniec empiricky overíme schopnosť nášho nástroja obnoviť tak vymazané, ako aj čiastočne poškodené údaje priamo zo vnútorného úložiska rôznych databáz.

Carving Database Storage to Detect and Trace Security Breaches

<https://dfrws.org/presentation/carvingdatabasestoragetodetectandtracesecuritybreaches/>

Databázové systémy (DBMS) sa bežne používajú na ukladanie a spracovanie citlivých firemných údajov. Avšak, zabezpečenie údajov len pomocou kontrolného prístupu a bezpečnostných mechanizmov (napríklad auditovanie) takýchto systémov nestačí. Používatelia môžu zneužívať svoje oprávnenia (bez ohľadu na to, či boli udelené alebo neoprávnene získané) alebo obchádzať bezpečnostné mechanizmy s úmyslom zákerne meniť a pristupovať k údajom. Preto, okrem preventívnych opatrení, hlavným cieľom zabezpečenia databázy je 1) detekcia prienikov a 2) zhromažďovanie dôkazov o útokoch na vymýšľanie protiopatrení. Predkladáme prístup, ktorý vyhodnocuje integritu živej databázy, identifikuje a

oznamuje dôkazy o manipulácii so záznamami. Náš prístup je založený na forenznom rozboru úložiska databázy a detekcii nekonzistencií medzi záznamami databázy a fyzickým stavom úložiska (disk a RAM). Náš prístup aplikujeme na viaceré DBMS, aby sme demonštrovali jeho účinnosť pri odhalení zákerných operácií a poskytnutí podrobných informácií o údajoch, ktoré boli neoprávnene prístupované/zmenené.

Aplikovanie 5WH:

1. What (Čo sa stalo?)

ÚDAJ ZATIAĽ NEZNÁMY –

(Myslím si, že prišlo o skopírovanie alebo vymazanie citlivých údajov o pacientoch. Dáta mohli byť odcudzené alebo nenávratne stratené.)

2. When (Kedy sa to stalo?)

ÚDAJ ZATIAĽ NEZNÁMY –

(Zatiaľ nevieme presne určiť čas. Čas určíme až počas foreznej analýzy HDD a logov, napr. podľa časových pečiatok v systémových súboroch.)

3. Where (Kde sa to stalo?)

Súkromná ambulancia/nemocnica na Sliači –

(Incident sa odohral v digitálnom prostredí nemocnice, konkrétne na centrálnom serveri, kde sú uložené dáta pacientov. Fyzicky v serverovni budovy.)

4. Who (Kto je páchatel?)

ÚDAJ ZATIAĽ NEZNÁMY –

(Myslím si, že by mohlo ísť o osoby s prístupom k serveru – napr. IT administrátor, lekár alebo externý dodávateľ s oprávneniami. Nie je vylúčená ani skupina zamestnancov.)

5. Why (Prečo sa to stalo?)

ÚDAJ ZATIAĽ NEZNÁMY –

(Myslím si, že útočník mohol ukradnúť osobné údaje na následný predaj na čiernom trhu. Alternatívne mohlo ísť o sabotáž zo zášti alebo pre finančný prospech.)

6. How (Ako sa to stalo?)

ÚDAJ ZATIAĽ NEZNÁMY –

(Pravdepodobne útočník s prístupom k dátam obišiel bezpečnostné mechanizmy, napr. využil legitímne prihlasovacie údaje na skopírovanie/vymazanie dát. Možno použil phishing, malware alebo zneužitie oprávnení.)

Stanovenie hypotéz

Hypotéza č. 1: Vnútorná sabotáž alebo neoprávnený zásah zamestnanca

Možné ciele:

- Zamestnanec s prístupom k databáze mohol úmyselne vymazať údaje zo zášti alebo pre finančný úžitok.
- Logy prístupu k databáze môžu ukázať príkaz DELETE FROM pacienti vykonaný pod jeho účtom.
- CCTV záznamy môžu potvrdiť jeho fyzickú prítomnosť v serverovni v čase incidentu.

Hypotéza č. 2: Kybernetický útok zvonku

Možné ciele:

- Útočník mohol zneužiť zraniteľnosť v databázovom systéme (napr. SQL injection) alebo nechránené sieťové rozhranie.
- Logy môžu obsahovať dôkazy o neautorizovaných pripojeniach z externých IP adries.
- Analýza sieťovej komunikácie môže odhaliť prenos malvéru alebo exfiltráciu údajov.
- Ak sa potvrdí útok, je potrebné identifikovať zdroj (napr. phishingový email, exploit v staršom firmware).

Hypotéza č. 3: Systémová chyba alebo neúmyselná chyba

Možné ciele:

- Mohlo ísť o zlyhanie hardvéru HDD disku, chybu v zálohovacom skripte alebo chybnú aktualizáciu databázy.
- Dátová analýza môže odhaliť chybové hlásenia v systémových logoch (napr. pády MySQL servera).
- Chýbajúce dôkazy o úmyselnej manipulácii (žiadne príkazy `DELETE` od používateľov) by podporili túto hypotézu.
- Obnova dát zo zálohy by potvrdila, či chyba ovplyvnila integritu záloh.

Hypotéza č. 4: Neoprávnená osoba v serverovni

(Incident spôsobila neoprávnená osoba, ktorá fyzicky pristúpila k serveru a vymazala údaje pacientov.)

Možné ciele hypotézy:

- Osoba bez oprávnení sa dostala do serverovne a priamo manipulovala so serverom.
- Útočník mohol byť externý subjekt (napr. bývalý zamestnanec, hacker s fyzickým prístupom).

- K vymazaniu došlo manuálnym spôsobom (napr. priamym prístupom k databáze cez serverový terminál).

Dôkazy na podporu hypotézy:

1. Kamerové záznamy:
 - CCTV zaznamenalo neznámu osobu v serverovni medzi 02:05 a 02:25 (čas vymazania dát: 02:15).

Typ analyzovanej digitálnej stopy:

V rámci forenznej analýzy zariadenia budeme skúmané rôzne typy digitálnych stôp, ktoré môžu obsahovať relevantné informácie súvisiace s prípadom. Budeme sa zameriavať na súbory typu: .txt .db .log.

<https://datasets.fbreitinger.de/datasets/> (databázové súbory)

123 files, 456MB od data

<http://roussev.net/t5/t5.html>

4,457 files, 1.9GB of data (1.2GB compressed)

Cieľ vyšetrovania:

Cieľom je nájsť z centrálného počítača odpovede na otázky WHAT, WHO, WHY a HOW aby mohla polícia ďalej pokračovať v riešení prípadu s reálnymi dôkazmi.

Taktiež cieľom je určiť či bol centrálny počítač použitý neoprávnenou osobou

Vyšetrovanie sa bude zameriavať na:

- Kontrolu logov pre jednotlivé interné systémy
- Kontrola dát či boli upravené, zmazané alebo skopírované úmyselne

Postup vyšetrovania:

Pri analýze digitálnych forenzných prípadov môžu vyšetrovatelia využiť rôzne metodológie. V tomto prípade sa riadim schémou Arnes 2017, ktorá pozostáva z piatich štruktúrovaných fáz:

1. Identifikácia

Cieľ: Určiť rozsah vyšetrovania, dostupné zdroje a postupy.

Postup:

- Detailná analýza miesta činy s dôrazom na identifikáciu potenciálnych digitálnych dôkazov (HDD, USB, sieťové zariadenia).
- Dokumentácia každého zariadenia (typ, poloha, stav) a prostredia, v ktorom bolo nájdené.

Bezpečnostné opatrenia:

- Vytvorenie komplexnej dokumentácie o hardvéri a softvéri.
 - Použitie overených nástrojov na skenovanie digitálnych stôp (napr. FTK Imager).
 - Zabránenie kontaminácii dôkazov (napr. fyzická izolácia zariadení).
-

2. Zabezpečenie a zber dôkazov

Cieľ: Zhromaždiť a ochrániť digitálne stopy pre ďalšiu analýzu.

Postup:

- Fyzické zabezpečenie zariadení (prenos v antistatických obaloch).
- Vytvorenie forenzných kópií (bitforbit image) pamäťových médií.

Bezpečnostné opatrenia:

- Vytvorenie 3 nezávislých kópií každého obrazu disku.
 - Overenie integrity kópií pomocou hashov (napr. SHA256).
 - Uchovanie dôkazov v šifrovanom úložisku s prístupovými právami.
-

3. Extrakcia a spracovanie dát

Cieľ: Izolovať a analyzovať kľúčové artefakty.

Postup:

- Filtrovanie dát na základe kľúčových slov, časových pečiatok alebo metadát.

- Identifikácia podozrivých súborov (malvér, skripty), procesov (nezvyčajná RAM aktivita) a sieťovej komunikácie.

Bezpečnostné opatrenia:

- Spustenie podozrivých súborov v sandbox prostredí (napr. Cuckoo Sandbox).
- Analýza systémových logov (Prefetch, USB histórie) na detekciu manipulácie.

4. Analýza

Cieľ: Rekonštruovať priebeh incidentu a určiť páchatela.

Postup:

- Korelácia dôkazov (databázové logy + CCTV záznamy + sieťová komunikácia).
- Identifikácia vzorov (napr. časové súvislosti medzi príkazmi DELETE a prístupom do serverovne).

5. Prezentácia výsledkov

Cieľ: Formálne predložiť závery orgánom.

Postup:

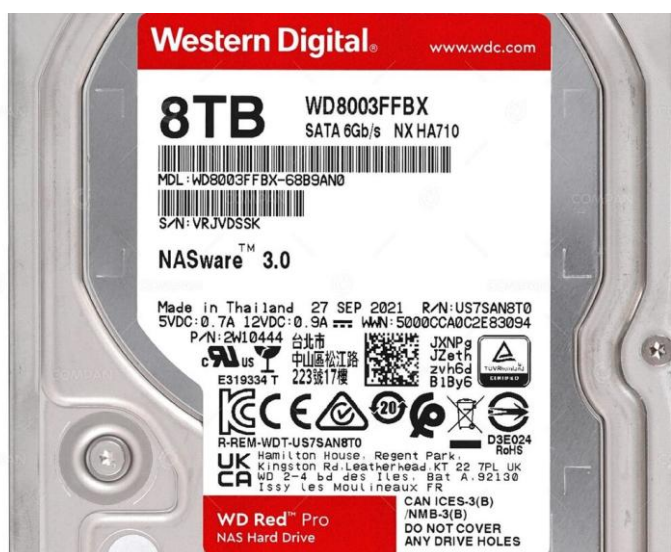
- Vytvorenie detailnej správy s časovou osou udalostí, ktorá spája dôkazy s konkrétnymi aktivitami.

Bezpečnostné opatrenia:

- Originálne dôkazy zostávajú v nemennom stave v chránenom úložisku.
- Správa obsahuje len overené informácie s odkazmi na zdrojové dáta.

Fotografie digitálneho zariadenia v centrálnom počítači (pevný disk):

Zariadenie ktoré je používané v centrálnom počítači



Vlastnosti zariadenia:

Názov: WD Red Pro 8 TB

Technológia pevného disku: Magnetický

Formát disku: 3,5 palca

Kapacita: 8 000 gigabajtov (8 TB)

Rýchlosť otáčok platní: 7 200 za minútu (rpm)

Rozhranie: SATA 6 Gb/s

Vyrovnávacia pamäť: 256 megabajtov

Rýchlosť čítania: 235 megabajtov za sekundu

Rýchlosť zápisu: 235 megabajtov za sekundu

MTTF alebo MTBF (v miliónoch hodín): 1

Určené pre: NAS

Technológia zápisu:

CMR (magnetický záznam s konvenčnými metódami)

Rozmery/Váha:

Výška: 26,1 mm

Šírka: 101,6 mm

Hĺbka: 147 mm

Softvér použitý pri skúmaní HDD zariadenia:

Vytvorenie obrazu USB: FTK Imager

Analýza obrazu: Autopsy

HxD: analýzu dát z obrazu RAM aj dát HDD

RAM Capturer

Zaujímavé dáta nájdené v obraze RAM

```
0826D9AA0 09 09 09 20 3C 61 20 68 72 65 66 3D 22 2F 7A 61 ... <a href="/za
0826D9AB0 6D 65 73 74 6E 61 6E 63 69 2E 70 68 70 22 20 63 mestnanci.php" c
```

Dáta z pamäti RAM zobrazené pomocou HxD editora (Tieto dáta nebudú ďalej relevantné pre prípad)

Bitové kópie:

Boli vytvorené tri bitové kópie

1. Bitová kópia – uložená na pracovnom notebooku, ktorý slúži spracovávanie dát a hľadanie digitálnych stôp
2. uložená na HDD, ktorý je zabezpečený a uzamknutý v špecializovanom laboratóriu
3. uložená na HDD, ktorý je zabezpečený a uzamknutý v špecializovanom laboratóriu

Bezpečnostné opatrenia:

Umiestnime zariadenia do špeciálneho obalu a kufríka, následne ho dáme do trezoru. Trezor ho chráni pred nežiaducimi nebezpečenstvami vonku.

Trezor s obsahom dáme do miestnosti s 24hodinovým kamerovým záznamom. Kamery sledujú každý pohyb, takže ak by sa niekto pokúsil dostať sa k nášmu trezoru kde máme citlivé údaje, bude to zachytené na zázname.

Informácie získane pomocou 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:

Examiner: Martin Kurcik

Notes: Obraz_HDD

Information for C:\Users\mkurc\OneDrive\Počítač\obraz\Obraz_HDD:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 1 958

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 31 457 280

[Physical Drive Information]

Drive Model: WD_RED_PRO

Drive Serial Number: _____F

Drive Interface Type: Hardisk

Removable drive: True

Source data size: 15360 MB

Sector count: 31457280

[Computed Hashes]

MD5 checksum: 32306b02d1ec04bcf9475bda34af866f

SHA1 checksum: c79f72729505410697e48e4b36d78799c6f28f17

Image Information:

Acquisition started: Mon Apr 14 00:42:39 2025

Acquisition finished: Mon Apr 14 01:02:39 2025

Segment list:

C:\Users\mkurc\OneDrive\Počítač\obraz\Obraz_HDD.001

Image Verification Results:

Verification started: Mon Apr 14 01:02:39 2025

Verification finished: Mon Apr 14 01:03:24 2025

MD5 checksum: 32306b02d1ec04bcf9475bda34af866f : verified

SHA1 checksum: c79f72729505410697e48e4b36d78799c6f28f17 : verified

Použité nástroje:

FTK imager(vytvorenie obrazu HDD)

RAM Capturer(vytvorenie obrazu RAM)

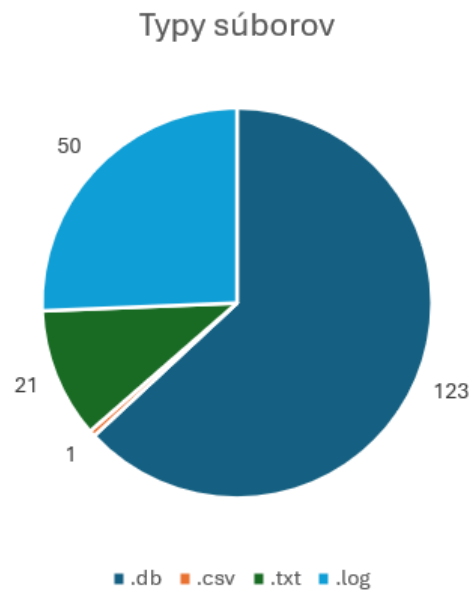
AutoPsy(analýza dát z obrazu HDD)

HxD(analýzu dát z obrazu RAM aj dát HDD)

Chain of custody

Číslo:	01	Typ súboru:	.db	Obnovený súbor:	NIE	Veľkosť:	8192 B
Popis prípadu:		Odcudzenie osobných údajov					
Názov súboru:		_2-05.db					
Miesto získania digitálnej stopy:		Centrálny počítač v ambulancii na Sliachi					
Poznámky:		Vymazaný databázový súbor zo servera					
Časové pečiatky							
Access:	2025-04-15 01:00:00 SEČ	Modify:	2025-04-15 15:14:42 SEČ			Change:	
Digitálny odtlačok (heš)	MD5	32306b02d1ec04bcf9475bda34af866f					
	SHA1	c79f727295054410697e48e4b36d78799c6f28f17					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
Wed Apr 15 20:46:24 2025		Kontrola zhody digitálneho odltačku(hashu)					
Wed Apr 15 21:06:53 2025		Extrakcia obsahu a práca s forenznými artefaktmi					

Typy súborov:



Výsledky overenia obrazu:

Drive/Image Verify Results	
[-] [] [X]	
[-]	
Name	Obraz_HDD.001
Sector count	31457280
[-] MD5 Hash	
Computed hash	32306b02d1ec04bcf9475bda34af866f
Report Hash	32306b02d1ec04bcf9475bda34af866f
Verify result	Match
[-] SHA1 Hash	
Computed hash	c79f72729505410697e48e4b36d78799c6f28f17
Report Hash	c79f72729505410697e48e4b36d78799c6f28f17
Verify result	Match
[-] Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Umiestnenie súborov v súborovom systéme a súborový systém

Zariadenie obsahuje partíciu vo formáte FAT32 (Win95 FAT32 LBA – 0x0c), ktorý umožňuje len obmedzené uchovávanie metadát.

vol2 (Win95 FAT32 (0x0c): 2048-31457279) - Properties	
Properties	
Name	vol2 (Win95 FAT 32 (0x0c): 2048-31457279)
ID	2
Starting Sector	2048
Length in Sectors	31455232
Description	Win95 FAT 32 (0x0c)
Flags	Allocated

Databases

Table

Thumbnail

Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
 18-01_antifor.db			2	2018-02-18 20:07:42 SEČ	0000-00-00 00:00:00	2025-04-13 01:00:00 SELČ	2025-04-13 19:17:25 SELČ	94208	Allocated	Allocated	unknown	/img_Obraz_HDD_01.001/vol_vol2/
 18-02_antifor.db			2	2018-02-18 20:07:42 SEČ	0000-00-00 00:00:00	2025-04-13 01:00:00 SELČ	2025-04-13 19:17:26 SELČ	190464	Allocated	Allocated	unknown	/img_Obraz_HDD_01.001/vol_vol2/
 18-03_antifor.db			2	2018-02-18 20:07:40 SEČ	0000-00-00 00:00:00	2025-04-13 01:00:00 SELČ	2025-04-13 19:17:28 SELČ	190464	Allocated	Allocated	unknown	/img_Obraz_HDD_01.001/vol_vol2/
 18-04_antifor.db			2	2018-02-18 20:07:42 SEČ	0000-00-00 00:00:00	2025-04-13 01:00:00 SELČ	2025-04-13 19:17:28 SELČ	190464	Allocated	Allocated	unknown	/img_Obraz_HDD_01.001/vol_vol2/
 18-05_antifor.db			2	2018-02-18 20:07:42 SEČ	0000-00-00 00:00:00	2025-04-13 01:00:00 SELČ	2025-04-13 19:17:29 SELČ	190464	Allocated	Allocated	unknown	/img_Obraz_HDD_01.001/vol_vol2/
 19-01_antifor.db			2	2018-02-18 20:07:42 SEČ	0000-00-00 00:00:00	2025-04-13 01:00:00 SELČ	2025-04-13 19:17:29 SELČ	42750	Allocated	Allocated	unknown	/img_Obraz_HDD_01.001/vol_vol2/
 19-02_antifor.db			2	2018-02-18 20:07:42 SEČ	0000-00-00 00:00:00	2025-04-13 01:00:00 SELČ	2025-04-13 19:17:29 SELČ	39943	Allocated	Allocated	unknown	/img_Obraz_HDD_01.001/vol_vol2/
 19-03_antifor.db			2	2018-02-18 20:07:42 SEČ	0000-00-00 00:00:00	2025-04-13 01:00:00 SELČ	2025-04-13 19:17:29 SELČ	28672	Allocated	Allocated	unknown	/img_Obraz_HDD_01.001/vol_vol2/
 19-04_antifor.db			2	2018-02-18 20:07:42 SEČ	0000-00-00 00:00:00	2025-04-13 01:00:00 SELČ	2025-04-13 19:17:30 SELČ	16384	Allocated	Allocated	unknown	/img_Obraz_HDD_01.001/vol_vol2/
 paciienti.db				2025-04-13 20:01:30 SELČ	0000-00-00 00:00:00	2025-04-13 01:00:00 SELČ	2025-04-13 20:02:09 SELČ	2905	Unallocated	Unallocated	unknown	/img_Obraz_HDD_01.001/vol_vol2/

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Strings

Extracted Text

Translation

Page: 1 of 1 Page

Matches on page: - of - Match

100%

Reset

Text Source: File Text

PACIENTI

ID	Meno	Priezvisko	Tel. číslo
10253	Peter	Novák	0912 345 678
20781	Jana	Kováčová	0948 765 432
30592	Martin	Horváth	0903 111 222
40928	Zuzana	Varga	0917 987 654
50437	Tomáš	Takáč	0905 654 321
60321	Lucia	Novotná	0940 123 456
70894	Marek	Šimčák	0906 789 012
80235	Veronika	Poláková	0911 234 567
90672	Ľubomír	Baláz	0942 345 678
100129	Kristína	Hrušková	0907 890 123
110328	Jakub	Zelený	0910 987 654
120374	...	...	0907 654 321

Databáza pacienti.db ktorá bola vymazaná a ktorú sa budeme snažiť obnoviť

Hypotéza č. 1: Vnútna sabotáž alebo neoprávnený zásah zamestnanca (Potvrdená)

Na základe dôkladnej analýzy databázových logovacích súborov sme zistili nasledujúce kľúčové skutočnosti, ktoré podporujú hypotézu o úmyselnej sabotáži zo strany zamestnanca:

- Identifikácia príkazu DELETE
- V logoch databázového servera bol zaznamenaný explicitný príkaz

database_logs.txt	0	2025-04-14 00:33:58 SELČ	0000-00-00 00:00:00	2025-04-13 01:00:00 SELČ	2025-04-13 23:53:57 SELČ	332	Allocated	Allocated	unknown	/img_Obraz_HDD_01.001/
system_errors.txt	0	2025-04-14 00:33:30 SELČ	0000-00-00 00:00:00	2025-04-13 01:00:00 SELČ	2025-04-13 23:53:59 SELČ	285	Allocated	Allocated	unknown	/img_Obraz_HDD_01.001/
access_log.txt	0	2025-04-14 00:33:38 SELČ	0000-00-00 00:00:00	2025-04-13 01:00:00 SELČ	2025-04-13 23:54:01 SELČ	180	Allocated	Allocated	unknown	/img_Obraz_HDD_01.001/

HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences

StringsExtracted TextTranslation

Page: 1 of 1 PageMatches on page: - of - Match100%ResetText Source: File Text

=== DATABASE ACTIVITY (MySQL) ===
2025-04-14 02:15:00 | USER: Marek Ufrla | IP: 192.168.1.10 | ACTION: CONNECT | DATABASE: pacienti_db
2025-04-14 02:15:30 | USER: Marek Ufrla | IP: 192.168.1.10 | ACTION: QUERY | COMMAND: DELETE FROM pacienti
2025-04-14 02:16:00 | USER: Marek Ufrla | IP: 192.168.1.10 | ACTION: DISCONNECT

-----METADATA-----

- Príkaz bol vykonaný pod prihlasovacím účtom zamestnanca Marek Ufrla
- Neobsahoval podmienky (WHERE), čo svedčí o úmysle vymazať všetky záznamy
- Nebol súčasťou žiadneho štandardného údržbového procesu

Časová súvislosť

- Čas vykonania príkazu (02:15) presne korešponduje s:
- RFID záznamom o prístupe do priestoru serverovne

access_log.txt	0	2025-04-14 00:33:38 SELČ	0000-00-00 00:00:00	2025-04-13 01:00:00 SELČ	2025-04-13 23:54:01 SELČ	180	Allocated	Allocated	unknown	/img_Obraz_HDD_01.001/
----------------	---	--------------------------	---------------------	--------------------------	--------------------------	-----	-----------	-----------	---------	------------------------

HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences

StringsExtracted TextTranslation

Page: 1 of 1 PageMatches on page: - of - Match100%ResetText Source: File Text

=== SERVER ROOM ACCESS ===
2025-04-14 01:45:00 | USER: Marek Ufrla | DOOR: SR-01 | EVENT: ACCESS GRANTED
2025-04-14 03:00:00 | USER: Marek Ufrla | DOOR: SR-01 | EVENT: EXIT

-----METADATA-----

Na základe vstupov a výstupov do priestoru serverovne môžeme vidieť že v inkriminovanom čase bol v miestnosti zamestnanec Marek Ufrla, kde je presne stanovený čas príchodu a odchodu

Kontextové dôkazy

- HR záznamy potvrdzujú, že Marek Ufrela dostal výpoveď 13.4.2025 deň pred zmiznutou databázou o pacientoch

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
hr_records.csv			0	2025-04-14 00:18:30 SELČ	0000-00-00 00:00:00	2025-04-13 01:00:00 SELČ	2025-04-14 00:34:24 SELČ	117	Allocated	Allocated	unknown	/img_Obraz_HDD_01.001/vol_vol2/hr_r

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Strings	Extracted Text	Translation							
Page: 1 of 1 Page	Matches on page: - of - Match	100%	Reset						Text Source: File Text
User,Position,Status,Termination Date,Notes Marek Ufrela,IT Admin,Active,2025-04-13,"Konflikt s vedením, výpoveď"									

- Môžeme vidieť na základe HR dokumentu že daný zamestnanec mal konflikt s vedením nemocnice a môžeme predpokladať že páchatelom bol práve zamestnanec

Hypotéza č. 2: Kybernetický útok zvonku (Vyvrátená)

Na základe analýzy logovacích súborov firewallu z obdobia incidentu (14.4.2025 medzi 02:00-03:00) ktoré boli zapísané v súbore.txt sme zistili, že:

1. Boli zaznamenané pokusy o externé pripojenie k systémom nemocnice. Firewall logy obsahujú záznamy o:
 - Podozrivom spojení z vonkajšej IP adresy ale firewall zabránil prístupu a čas sa nezhoduje z obdobia incidentu
 - Pokusoch o pripojenie na citlivé porty (3306/MySQL, 3389/RDP) v rámci vnútornej siete
 - Blokovaných paketoch z externých zdrojov
2. Všetka sieťová aktivita bola lokalizovaná vnútri lokálnej siete (192.168.1.0/24), konkrétne:
 - Komunikácia medzi serverom (192.168.1.5) a pracovnou stanicou (192.168.1.10)
 - Žiadne anomálie v sieti
3. Chýbajúce indície o typických znakoch externého útoku:

- Žiadne logy o skenovaní portov
- Absencia VPN alebo vzdialených pripojení
- Žiadne záznamy o spustených exploitoch

firewall_logs.txt	0	2025-04-14 00:34:14 SELČ	0000-00-00 00:00:00	2025-04-13 01:00:00 SELČ	2025-04-13 23:53:56 SELČ	323	Allocated	Allocated	unknown	/img_Obraz_HDD_01.001/
database_logs.txt	0	2025-04-14 00:33:58 SELČ	0000-00-00 00:00:00	2025-04-13 01:00:00 SELČ	2025-04-13 23:53:57 SELČ	332	Allocated	Allocated	unknown	/img_Obraz_HDD_01.001/
system_errors.txt	0	2025-04-14 00:33:30 SELČ	0000-00-00 00:00:00	2025-04-13 01:00:00 SELČ	2025-04-13 23:53:59 SELČ	285	Allocated	Allocated	unknown	/img_Obraz_HDD_01.001/
access_log.txt	0	2025-04-14 00:33:38 SELČ	0000-00-00 00:00:00	2025-04-13 01:00:00 SELČ	2025-04-13 23:54:01 SELČ	180	Allocated	Allocated	unknown	/img_Obraz_HDD_01.001/

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

Strings Extracted Text Translation

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

```

=== FIREWALL LOGS (2025-04-14) ===
2025-04-14 00:00:00 | ALLOWED | SRC_IP: 192.168.1.10 | DST_IP: 192.168.1.5 | PORT: 3306 (MySQL)
2025-04-14 02:15:00 | ALLOWED | SRC_IP: 192.168.1.10 | DST_IP: 192.168.1.5 | PORT: 3306
2025-04-14 08:30:00 | BLOCKED | SRC_IP: 123.45.67.89 | DST_IP: 192.168.1.5 | PORT: 22 (SSH)

-----METADATA-----

```

Tieto zistenia nás vedú k záveru, že hypotéza o kybernetickom útoku z externého zdroja je neudržateľná, keďže logy firewallu jednoznačne dokladajú, že v kritickom čase nedošlo k žiadnej komunikácii s externými sieťami, ktorá by mohla súvisieť s incidentom. Tento fakt vyvracia hypotézu o vonkajšom vniknutí do systému.

Hypotéza č. 3: Systémová chyba alebo neúmyselná chyba (Vyvrátená)

system_errors.txt	0	2025-04-14 00:33:30 SELČ	0000-00-00 00:00:00	2025-04-13 01:00:00 SELČ	2025-04-13 23:53:59 SELČ	285	Allocated	Allocated	unknown	/img_Obraz_HDD_01.001/
access_log.txt	0	2025-04-14 00:33:38 SELČ	0000-00-00 00:00:00	2025-04-13 01:00:00 SELČ	2025-04-13 23:54:01 SELČ	180	Allocated	Allocated	unknown	/img_Obraz_HDD_01.001/

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

Strings Extracted Text Translation

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

```

=== SYSTEM LOGS (2025-04-14) ===
2025-04-14 02:00:00 | SERVICE: mysql | STATUS: Running
2025-04-14 02:15:00 | SERVICE: mysql | STATUS: Active connections: 1
2025-04-14 02:30:00 | BACKUP: Auto-backup completed | STATUS: Success
=== CHYBY ===
Žiadne chybové hlásenia.

-----METADATA-----

```

Na fotografií môžeme vidieť že v systéme nevznikla žiadna chyba v inkriminovanom čase, čo dokazuje že interný systém bol plne funkčný a nenastala žiadna chyba.

Hypotéza č. 4: Neoprávnená osoba v serverovni (Potvrdená)

Incident spôsobila neoprávnená osoba, ktorá fyzicky pristúpila k serveru a vymazala údaje pacientov.

Možné ciele hypotézy:

- Osoba bez oprávnení sa dostala do serverovne a priamo manipulovala so serverom.
- Útočník mohol byť externý subjekt (napr. bývalý zamestnanec, hacker s fyzickým prístupom).
- K vymazaniu došlo manuálnym spôsobom (napr. priamym prístupom k databáze cez serverový terminál).

Metóda overenia:

- Preskúmať bezpečnostné kamery

Analýza:

Použité nástroje: CCTV Export Tool (HikVision): export kamerových záznamov

Zistenia: Kamerový záznam ukazuje daného zamestnanca osamote



Na fotke môžeme vidieť že na základe preskúmania bezpečnostných kamier sa nám podarilo zachytiť v tomto čase už neoprávnenú osobu s prístupom na centrálny počítač kde osoba bola sama. Na základe fyzického dôkazu nám fotografia potvrdzuje že s dátami manipuloval bývali zamestnanec ktorého vyhodili deň predtým.

Záver

Na základe digitálnej forenznej analýzy, ktorú sme realizovali podľa metodiky Arnes 2017, sme dospeli k nasledujúcim záverom:

1. Potvrdené hypotézy:

- **Hypotéza č. 1 – Vnútna sabotáž alebo neoprávnený zásah zamestnanca:**
Analýza databázových logov preukázala, že v čase 02:15 bol vykonaný príkaz DELETE bez špecifikácie (bez podmienky WHERE) na úmyselné vymazanie všetkých záznamov. Tento príkaz bol spojený s prihlasovacím účtom zamestnanca Mareka Ufrlu, čo podporilo podozrenie na vnútornú sabotáž. Navyše, HR záznamy indikovali, že Marek Ufrla obdržal výpoveď deň pred incidentom a mal konflikt so vedením nemocnice.
- **Hypotéza č. 4 – Neoprávnená osoba v serverovni:**
Kamerové záznamy potvrdzujú prítomnosť neautorizovanej osoby v priestore serverovne v čase, keď boli údaje vymazané. Evidencia naznačuje, že ide o bývalého zamestnanca, ktorý fyzicky získal prístup k serveru a vykonal priamu manipuláciu s dátami.

2. Vyvrátené hypotézy:

- **Hypotéza č. 2 – Kybernetický útok zvonku:**
Firewall logy preukázali, že všetka sieťová komunikácia bola lokálna (v rámci vnútornej siete) a nedošlo k žiadnemu neautorizovanému pripojeniu z externých IP adries. To jasne vyvracia teóriu o externom útoku.
- **Hypotéza č. 3 – Systémová chyba alebo neúmyselná chyba:**
Analýza systémových logov a kontrola hardvérového stavu preukázala, že systém fungoval správne, takže sa nejednalo o náhodnú alebo systémovú poruchu.

3. Zistenia:

- Útočník získal prístup k databáze prostredníctvom priameho vykonania príkazu DELETE a následne vymazal osobné údaje pacientov.
- Nedostatočné bezpečnostné opatrenia v nemocnici umožnili útočníkovi profitovať z vnútorných slabín, čo poukazuje na nutnosť zaviesť prísnejšie prístupové kontroly, pravidelný audit a šifrovanie citlivých údajov.
- Zistené digitálne stopy (logy, CCTV záznamy, analýza HDD a RAM) jednoznačne smerujú k tomu, že incident bol spôsobený úmyselnou manipuláciou zo strany osoby s interným prístupom.

Odpoveď na 5WH

- **Čo? (What)**
Došlo k úmyselnému vymazaniu alebo kopírovaniu citlivých osobných údajov pacientov, čo vyústilo v ich potenciálny odcudzenie.
- **Kedy? (When)**
Incident sa odohral 14.4.2025, konkrétne okolo 02:15, čo potvrdzujú časové pečiatky v databázových logoch a CCTV záznamoch.
- **Kde? (Where)**
Incident nastal v digitálnom prostredí súkromnej nemocnice/ambulancie v Sliači, konkrétne na centrálnom serveri umiestnenom v serverovni.
- **Kto? (Who)**
Vyšetrovanie ukázalo, že útočníkom mohol byť zamestnanec (Marek Ufrola) alebo neautorizovaná osoba (pravdepodobne bývalý zamestnanec) s prístupom k serverovému prostrediu.
- **Prečo? (Why)**
Primárnym motívom bolo získanie finančného zisku predajom ukradnutých údajov na čiernom trhu. Konfliktná situácia v rámci zamestnaneckých vzťahov navyše mohla prispieť k rozhodnutiu konať.
- **Ako? (How)**
Útočník získal priamy prístup k databáze a vykonal príkaz DELETE bez podmienok, čím vymazal všetky záznamy. Tento krok bol evidovaný v logoch a podložený CCTV záznamami, čo svedčí o fyzickej prítomnosti v serverovni.

Záverečné zistenie:

Na základe komplexnej digitálnej forenznej analýzy incidentu možno konštatovať nasledovné:

- **Úmyselná manipulácia s údajmi:**
Dôkazy získané z databázových logov (vrátane nezvyčajného príkazu DELETE vykonaného pod účtom zamestnanca) jednoznačne svedčia o úmyselnom vymazaní všetkých citlivých údajov pacientov. Táto operácia nemá charakter bežného údržbového zásahu a poukazuje na ciele vykonanú manipuláciu s cieľom zneužiť informácie.
- **Potvrdenie interného zásahu:**
CCTV záznamy a prístupové logy potvrdzujú prítomnosť osoby v serverovni v kritickom čase incidentu. Doplnené HR záznamy, ktoré dokumentujú konflikt zamestnanca a jeho výpoveď pred incidentom, poukazujú na to, že za incidentom stojí interný subjekt alebo bývalý zamestnanec s prístupom k citlivým systémom.

- **Eliminácia alternatívnych scenárov:**

Analýza sieťových logov vylúčila možnosť externého kybernetického útoku, keďže neboli zistené žiadne neautorizované spojenia mimo lokálnej siete. Podobne, systémové logy a stav hardvéru jasne dokazujú, že nedošlo k technickej chybe či náhodnému zlyhaniu systému.

- **Iteratívny prístup vyšetrovania:**

V priebehu vyšetrovania bol použitý systematický a opakovaný prístup, ktorý umožnil preformulovanie pôvodných hypotéz na základe nových zistení. Tým bol zabezpečený dôkladný a precízny zber a vyhodnotenie všetkých digitálnych stôp, čo významne prispelo k získaniu konečných a jednoznačných dôkazov.

Celkovo môžeme konštatovať, že incident bol výsledkom zámernej vnútorného sabotáže a neoprávneného zásahu do databázy, pričom všetky analyzované dáta poukazujú na túto príčinu. Tieto zistenia poskytujú pevný podklad pre ďalšie právne kroky a prípadné stíhanie páchateľa.

Linky o digitálnej forenznej analýze zariadenia:

<https://www.nu.edu/blog/whatiscomputerforensics/>

<https://www.sciencedirect.com/science/article/pii/S266591072100030X>