

UNIVERZITA SV. CYRILA A METODA V TRNAVE
FAKULTA PRIRODNÝCH VIED

Podozrenie z manipulácie databázy prijímacieho konania

PREZENTACIA

Semestrálna práca

2025/2026

Ľubomír Zubák

1. Obsah

1.Prípád	3
1.1.Zaistené digitálne zariadenia	3
1.2.Digitálne stopy	4
1.3.Hypotézy	4
1.3.1.Hypotéza 1	4
1.3.2.Hypotéza 2	5
1.3.3.Hypotéza 3	6
1.4.5 WH	8
1.5.Ciele vyšetrovania	8
1.6.Postup vyšetrovania	9
1.7.Literatúra	9
2.Zaistovanie a zber	10
2.1.Pracovný notebook referenta	10
2.2.USB zariadenie	12
3.Dáta	14
3.1.Typy analyzovaných súborov	14
3.2.Vlastné simulované dáta	14
3.3.Verejne dostupné dataset-y	15
4.RAM image	16
5.Image zariadení	18
5.1.Parametre vytvoreného obrazu	18
5.2.Identifikované súbory na obraze	19
5.3.Nálezy podporujúce hypotézy	20
5.3.1.Databázový súbor prijimacky_case_ascii.db	20
5.3.2.Tabuľka system_logy	21
5.3.3.Vymazaný SQL skript modify_scores.sql.txt	22
5.3.4.Vymazané pomocné poznámky	23
5.3.5.Súbor komunikacia.txt	24
5.3.6.Súbor uchadzaci_export_ascii.csv	25
5.4.Zhrnutie nálezov	26
6.SW nástroje a ich účel	27
6.1.FTK Imager	27
6.2.HxD	27
6.3.DB Browser for SQLite	27
6.4.Autopsy	27
7.Bezpečnostné opatrenia	28

7.1.Bitove kopie	28
------------------------	----

1. Prípád

Na univerzite vzniklo podozrenie na manipuláciu výsledkov prijímacieho konania po sťažnosti uchádzača, ktorý si po teste odfotil svoje odpovede a po zverejnení výsledkov zistil nesúlad v bodovom hodnotení. Interná kontrola preukázala, že databázový záznam bol upravený tri dni pred zverejnením výsledkov z interného administrátorského účtu. V kancelárii študijného oddelenia bol zaistený pracovný notebook referenta a USB zariadenie. Predmetom vyšetrovania je analýza notebooku, USB, databázových logov a RAM s cieľom určiť, či išlo o úmyselné interné konanie, kompromitáciu účtu alebo neoprávnený externý prístup.

1.1. Zaistené digitálne zariadenia

V rámci vyšetrovania budú analyzované tieto zariadenia:

- Pracovný notebook referenta študijného oddelenia (OS Windows 10)
- USB kľúč nájdený v kancelárii
- Serverový systém univerzity (analýza logov – export)
- Záloha databázy prijímacieho konania (.sql dump)

Tieto zariadenia môžu obsahovať dôkazy o manipulácii údajov alebo neoprávnenom prístupe.

1.2. Digitálne stopy

Vyšetovanie sa zameriava na nasledujúce digitálne stopy:

- Logy prihlásení do informačného systému
- Záznamy o úpravách databázy (SQL logy)
- Časové pečiatky modifikovaných záznamov
- História pripojených USB zariadení
- Systémové logy operačného systému
- Možné exporty databázových súborov (.sql, .csv)

Dôležitou súčasťou bude rekonštrukcia časovej osi udalostí.

1.3. Hypotézy

1.3.1. Hypotéza 1

Referent študijného oddelenia úmyselne manipuloval výsledky prijímacieho konania výmenou za finančnú odmenu.

Súvisiace digitálne stopy

- logy prihlásení do systému
- záznamy o úprave databázy
- časové pečiatky zmenených záznamov
- história pripojenia USB zariadenia
- databázový export .csv
- komunikácia medzi referentom a ďalšou osobou
- textové poznámky alebo pomocné súbory

Súvisiace zariadenia

- pracovný notebook referenta
- USB kľúč nájdený v kancelárii
- databázový export zo servera
- RAM image notebooku

Nástroje

- FTK Imager
- DB Browser for SQLite
- HxD

Postup overenia:

Najprv bude vykonaná analýza obrazu USB zariadenia nástrojom Autopsy, ktorý umožní prehľadanie súborovej štruktúry, identifikáciu alokovaných aj dealokovaných súborov a obnovu vymazaných dát z unallocated space. Následne sa overí, či sa na USB zariadení nachádzajú súbory preukazujúce otvorenie databázy, prítomnosť databázového exportu, SQL skriptov alebo komunikácie súvisiacej s úpravou výsledkov. Súčasne bude v nástroji HxD analyzovaná RAM image, v ktorej sa budú vyhľadávať textové reťazce súvisiace s názvom databázy, exportovaných súborov a SQL skriptov. Dôležitá bude aj časová korelácia medzi pripojením USB zariadenia, otvorením databázy a vykonaním zmeny záznamu, ktorú umožnia systémové logy uložené v databáze.

Výsledok: POTVRDENA

Hypotéza, podľa ktorej referent študijného oddelenia úmyselne manipuloval výsledky prijímacieho konania výmenou za finančnú odmenu, bola potvrdená. V databáze prijimacky_case_ascii.db bol identifikovaný záznam uchádzača Daniel Farkas (id=11), v ktorom sa pôvodné bodové hodnotenie (45 bodov) líši od aktuálneho hodnotenia (95 bodov), s časom úpravy 29.08.2025 22:14:33 a uvedeným používateľským účtom admin_referent. Vo vymazaných poznámkach bola nájdená priama zmienka o finančnej odmene 1500 EUR a plán zahľadania stôp. V súbore komunikacia.txt bola obnovená komunikácia, v ktorej sa páchatel' explicitne dohaduje na úprave bodov a finančnej odmene.

Kombinácia týchto nálezov preukazuje úmysel, finančný motív aj konkrétny postup manipulácie.

1.3.2. Hypotéza 2

Administrátorský účet bol kompromitovaný škodlivým softvérom alebo neoprávneným prístupom a manipuláciu vykonal externý útočník.

Súvisiace digitálne stopy

- logy prihlásenia do systému
- neštandardné časy prístupu
- prípadné spustenie neznámych procesov
- podozrivá sieťová aktivita
- systémové logy operačného systému
- artefakty v RAM

Súvisiace zariadenia

- pracovný notebook referenta
- RAM image notebooku
- databázový server a jeho logy
- USB zariadenie (ako možný nosič škodlivého kódu)

Nástroje

- FTK Imager
- HxD
- nástroje na analýzu Windows logov

Postup overenia

Bude vykonaná analýza systémových logov uložených v databázovom súbore s cieľom zistiť, či sa vyskytli neobvyklé prihlásenia, aktivita mimo bežného pracovného času alebo správanie nezodpovedajúce štandardnému používaniu účtu referenta. Pomocou nástroja FTK Imager bude overená integrita obrazov zariadení a vykonaná funkcia Hash Lookup na identifikáciu prípadného škodlivého softvéru. V nástroji Autopsy bude prehľadaná súborová štruktúra obrazu USB zariadenia s cieľom odhaliť prípadné podozrivé spustiteľné súbory alebo skripty, ktoré by mohli naznačovať kompromitáciu. V RAM image budú pomocou HxD vyhľadávané reťazce súvisiace s databázou a prípadné stopy neštandardných procesov alebo sieťovej aktivity. Ak sa nepreukáže priamy zásah legitímneho používateľa a objavia sa stopy neštandardnej aktivity, hypotéza kompromitácie účtu ostáva relevantná.

Výsledok: NEPOTVRDENA

Hypotéza o kompromitácii administrátorského účtu škodlivým softvérom alebo neoprávneným externým prístupom nebola potvrdená. Na obraze zariadenia neboli identifikované žiadne známky škodlivého softvéru, modul Hash Lookup nevrátil zhodu so známymi škodlivými súbormi a v systémových logoch sa nevyskytujú prihlásenia mimo bežnej IP adresy referenta (192.168.1.45) ani prístupy mimo štandardného pracovného režimu. Všetky zaznamenané udalosti zodpovedajú činnosti legitímneho používateľského účtu z dôveryhodnej lokality.

Z analýzy je preto možné konštatovať, že manipulácia nebola spôsobená kompromitáciou účtu externým útočníkom.

1.3.3. Hypotéza 3

USB zariadenie bolo použité ako pomocný nosič na prenos SQL skriptu, databázového exportu alebo iných súborov súvisiacich s manipuláciou výsledkov.

Súvisiace digitálne stopy

- história pripojenia USB zariadení
- názvy súborov na USB zariadení
- databázové exporty .csv
- SQL súbory
- časová korelácia medzi pripojením USB a otvorením databázy
- artefakty v RAM

Súvisiace zariadenia

- USB kľúč nájdený v kancelárii
- pracovný notebook referenta
- RAM image notebooku
- databázový export

Nástroje

- FTK Imager
- HxD
- DB Browser for SQLite

Postup overenia

Bude analyzovaný obraz USB zariadenia nástrojom Autopsy, ktorý umožní prehľadanie celej súborovej štruktúry vrátane vymazaných súborov obnovených z unallocated space. Overí sa, či sa na USB nachádzali súbory typu .sql, .csv, .db alebo textové poznámky súvisiace s incidentom. Časové pečiatky súborov (created, modified, accessed) zobrazené v Autopsy budú porovnané so systémovými logmi uloženými v databáze. V RAM image a obraze USB zariadenia budú pomocou HxD vyhľadávané textové reťazce ako modify_scores.sql, uchadzaci_export_ascii.csv a názov databázového súboru prijimacky_case_ascii.db. Kľúčové bude porovnanie času pripojenia USB zariadenia s časom otvorenia databázy a vykonania zmeny záznamu, čím sa overí časová korelácia medzi použitím USB nosiča a manipuláciou databázy.

Výsledok: POTVRDENA

Hypotéza, podľa ktorej bolo USB zariadenie použité ako pomocný nosič pri manipulácii databázy, bola potvrdená. Na obraze USB boli nájdené všetky relevantné typy súborov – databázový súbor, SQL skript (vymazaný a obnovený z unallocated space), exportovaný CSV súbor aj pomocné poznámky. Časová korelácia medzi pripojením USB zariadenia (21:47:33), otvorením databázy (21:52:18), vykonaním UPDATE príkazu (22:14:33), exportom (22:18:45) a odpojením USB (22:25:10) jasne preukazuje, že USB zariadenie bolo použité ako pracovný nosič počas celej operácie manipulácie.

1.4. 5 WH

WHO (Kto)

Referent študijného oddelenia, IT administrátor alebo externý útočník.

WHAT (Čo)

Neoprávnená úprava databázy prijímacieho konania.

WHEN (Kedy)

Tri dni pred zverejnením oficiálnych výsledkov.

WHERE (Kde)

Interný server univerzity a pracovná stanica referenta.

WHY (Prečo)

Možný finančný prospech, osobný záujem alebo kompromitácia používateľského účtu.

HOW (Ako)

Prihlásenie do systému a manuálna SQL úprava databázy, prípadne export/import údajov pomocou USB zariadenia alebo vzdialeného prístupu.

1.5. Ciele vyšetrovania

- ☐ Identifikovať účet alebo osobu zodpovednú za neoprávnené úpravy.
- ☐ Rekonštruovať presnú časovú os manipulácie.
- ☐ Overiť, či bol použitý externý USB nosič.
- ☐ Zistiť, či došlo k exportu alebo úniku citlivých údajov.
- ☐ Vypracovať forenznú správu použiteľnú v disciplinárnom alebo trestnom konaní.

1.6. Postup vyšetrovania

- ☐ Bezpečné zaistenie digitálnych zariadení.
- ☐ Vytvorenie bitových kópií úložných zariadení.
- ☐ Overenie integrity dôkazov pomocou hashovacích algoritmov.
- ☐ Analýza systémových a databázových logov.
- ☐ Analýza histórie pripojených externých zariadení.
- ☐ Rekonštrukcia časovej osi udalostí.
- ☐ Vyhodnotenie hypotéz a vypracovanie záverečnej správy.

1.7. Literatúra

https://dfrws.org/sites/default/files/session-files/2007_USA_paper-automated_windows_event_log_forensics.pdf

Tento odborný príspevok sa zameriava na analýzu Windows Event Logov, ktoré slúžia ako dôležitý zdroj digitálnych dôkazov. Autori vysvetľujú, ako je možné z týchto logov získať informácie o aktivitách používateľa, ako ich medzi sebou prepojiť a správne interpretovať. Pomocou tejto metodiky je možné spätne zrekonštruovať, čo sa v systéme dialo, a zistiť, či došlo k neoprávnenému zásahu alebo manipulácii so systémom.

https://dfrws.org/wp-content/uploads/2021/09/2021-usa-paper-20-duck_hunt_memory_forensics_of_usb_attack_platforms.pdf

Odborný príspevok rieši artefakty po USB zariadeniach vo Windows 10 (identifikátory zariadení, diagnostické eventy) a odporúča aj nástroje/plugins na extrakciu týchto artefaktov.

2. Zaist'ovanie a zber

Vyšetrované zariadenia :

- Notebook
- USB

2.1. Pracovný notebook referenta

Pracovný notebook referenta študijného oddelenia predstavuje hlavné zariadenie, na ktorom mohlo dôjsť k otvoreniu databázy, úprave záznamov a vytvoreniu exportu výsledkov.

Typ zariadenia: notebook

Model: Lenovo ThinkPad E14 Gen 4

Operačný systém: Windows 10 Pro

Processor: Intel Core i5-1235U

Operačná pamäť: 16 GB DDR4

Úložisko: 512 GB SSD NVMe

Rozhrania: USB 3.0, USB-C, HDMI, Ethernet

Rýchlosť čítania úložiska: približne 3000 MB/s

Rýchlosť zápisu úložiska: približne 1800 MB/s

Prístupová doba SSD: menej ako 0,1 ms



Obrázok 1: notebook referenta študijného oddelenia

Číslo:	01	Typ súboru:	Disk Image	Obnovený súbor:	Nie	Veľkosť:	512GB
Popis prípadu:	Manipulácia výsledkov prijímacieho konania						
Názov súboru:	notebook_referent.E01						
Miesto získania digitálnej stopy:	Pracovný notebook referenta študijného oddelenia – kancelária študijného oddelenia univerzity						
Poznámky:	Diskový obraz zariadenia bol vytvorený pomocou nástroja FTK Imager. Pred vytvorením obrazu bol notebook odpojený od siete, aby sa zabránilo zmene dát. Originálne zariadenie bolo následne zabezpečené a uložené v zabezpečenom priestore pre digitálne dôkazy.						
Časové pečiatky							
Access:	03.09.2025 09:12:45	Modify:	03.09.2025 09:38:20	Change:	03.09.2025 09:44:11		
Digitálny odtlačok (heš)	MD5	d41d8cd98f00b204e9800998ecf8427e					
	SHA1	da39a3ee5e6b4b0d3255bfe95601890afd80709					
Časová pečiatka							
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
03.09.2025 09:12		Zaistenie pracovného notebooku referenta študijného oddelenia					
03.09.2025 09:20		Dokumentovanie zariadenia a evidovanie dôkazu					
03.09.2025 09:30		Vytvorenie bitovej kópie disku pomocou FTK Imager					
03.09.2025 09:38		Dokončenie vytvárania diskového obrazu					
03.09.2025 09:44		Overenie hash hodnôt a uloženie dôkazu do zabezpečeného úložiska					

2.2. USB zariadenie

USB zariadenie nájdené v kancelárii študijného oddelenia mohlo slúžiť ako pomocný nosič na prenos SQL skriptu, databázového exportu alebo iných súborov súvisiacich s incidentom.

Typ zariadenia: USB flash disk

Model: Kingston DataTraveler 8GB

Kapacita: 8 GB

Rozhranie: USB 2.0 / USB 3.0

Súborový systém: FAT32

Rýchlosť čítania: približne 20–80 MB/s

Rýchlosť zápisu: približne 5–20 MB/s

Prístupová doba: menej ako 1 ms

Typ pamäte: NAND Flash

Hmotnosť: približne 10 g

Farba: čierna / čierno-biela

Sériové číslo: 0B8E6B0166E7

Pri vyšetrovaní bude skúmané, či sa na USB zariadení nachádzali súbory typu .sql, .csv, .txt alebo iné pomocné dáta, ktoré mohli byť použité pri manipulácii databázy. Dôležitá bude aj analýza časových pečiatok súborov, histórie pripojenia zariadenia a prípadnej súvislosti medzi použitím USB a úpravou databázového záznamu.



Obrázok 2: USB kľúč nájdený v kancelárii študijného oddelenia

Číslo:	02	Typ súboru:	Disk Image (.E01)	Obnovený súbor:	Nie	Veľkosť:	8 GB
Popis prípadu:	Manipulácia výsledkov prijímacieho konania						
Názov súboru:	usb_device.E01						
Miesto získania digitálnej stopy:	USB kľúč nájdený v kancelárii študijného oddelenia na pracovisku referenta						
Poznámky:	USB zariadenie bolo zaistené na mieste pracoviska referenta študijného oddelenia. Pred analýzou bol vytvorený forenzný obraz zariadenia pomocou nástroja FTK Imager. Originálne zariadenie bolo následne zabezpečené a uložené v prostredí určenom na uchovávanie digitálnych dôkazov.						
Časové pečiatky							
Access:	03.09.2025 10:10:15		Modify:	03.09.2025 10:25:47		Change:	03.09.2025 10:30:12
Digitálny odtlačok (heš)	MD5	b2706fbc7c02170b62b098fc26f57be1					
	SHA1	7cc5624e53c370be2dc43e6144fc87442471a7a2					
Časová pečiatka	Akcia vykonaná s digitálnou stopou						
03.09.2025 10:10	Zaistenie USB zariadenia v kancelárii študijného oddelenia						
03.09.2025 10:20	Dokumentovanie zariadenia (fotografia a označenie dôkazu)						
03.09.2025 10:25	Vytvorenie bitovej kópie USB zariadenia pomocou FTK Imager						
03.09.2025 10:35	Overenie hash hodnôt a uloženie dôkazu do zabezpečeného úložiska						

3. Dáta

V rámci vyšetrovania budú analyzované vlastné simulované dáta vytvorené pre potreby prípadu a doplnkové verejne dostupné forenzné datasety použité ako metodický podklad. Cieľom je vytvoriť realistické prostredie, v ktorom je možné skúmať manipuláciu databázových záznamov, používateľskú aktivitu na pracovnej stanici, pripojenie externého USB zariadenia a komunikáciu súvisiacu s incidentom.

3.1. Typy analyzovaných súborov

- V prípade budú analyzované najmä tieto typy súborov:
- databázové súbory .db
- databázové exporty .sql
- exportované tabuľky .csv
- textové poznámky .txt
- systémové a databázové logy .log, .txt, .csv
- obraz operačnej pamäte .mem alebo .raw
- obrazy zariadení .E01

3.2. Vlastné simulované dáta

Použité súbory:

- prijimacky_case_ascii.db
- prijimacky_case_ascii.sql
- uchadzaci_export_ascii.csv
- textové poznámky k bodovému hodnoteniu
- simulovaná komunikácia vo forme správ

Obsah simulovaných dát:

- tabuľka uchádzačov s pôvodným a aktuálnym bodovým hodnotením
- záznam o podozrivej zmene bodov jedného uchádzača
- systémové logy o prihlásení, otvorení databázy a exporte údajov
- USB artefakty
- komunikácia medzi podozrivými osobami

3.3. Verejne dostupné dataset-y

- ☐ NIST CFReDS – Forensics Image Test Image
- ☐ Digital Forensics Workbook datasets
- ☐ SQLite Forensic Corpus
 - **Odkazy:**
 - https://cfreds.nist.gov/all/DFIR_AB/ForensicsImageTestimage
 - <https://www.digitalforensicsworkbook.com/data-sets>
 - <https://digitalcorpora.org/corpora/sql/sqlite-forensic-corpus/>

4. RAM image

Analýza RAM image preukázala prítomnosť textových reťazcov súvisiacich s databázovou a používateľskou aktivitou. V operačnej pamäti bol identifikovaný názov databázového súboru `prijimacky_case_ascii.db`, názov exportovaného súboru `uchadzaci_export_ascii.csv` a reťazce súvisiace s použitím nástroja na úpravu databázy. Zároveň boli v RAM image zistené aj artefakty webovej aktivity, ktoré poukazujú na vyhľadávanie informácií súvisiacich s históriou súborov a USB zariadení vo Windows. Tieto nálezy podporujú hypotézu, že databáza bola v čase incidentu na zariadení aktívne otvorená a spracovávaná.

```
6D1D59390 61 64 73 2F 70 72 69 6A 69 6D 61 63 6B 79 5F 63 ads/prijimacky c
6D1D593A0 61 73 65 5F 61 73 63 69 69 2E 64 62 04 03 00 06 ase_ascii.db....
```

Obrázok 4: V obraze operačnej pamäte bol identifikovaný názov databázového súboru, čo podporuje predpoklad, že databáza bola v čase incidentu na zariadení otvorená alebo spracovávaná.

```
0014767B0 31 65 30 66 63 38 64 62 62 38 35 37 37 34 34 35 1e0fc8dbb8577445
0014767C0 35 37 35 64 39 36 26 76 3D 30 75 63 68 61 64 7A 575d96&v=0uchadz
0014767D0 61 63 69 5F 65 78 70 6F 72 74 5F 61 73 63 69 69 aci_export_ascii
0014767E0 2E 63 73 76 6D 6F 63 2E 74 70 67 74 61 68 63 2E .csvmoc.tpgtahc.
```

Obrázok 5: V operačnej pamäti bol identifikovaný názov exportovaného CSV súboru, čo naznačuje, že po uprave databázy bol vytvorený alebo otvorený export výsledkov.

```
80BAC7D90 4A 11 00 36 15 01 23 02 43 15 01 37 02 02 00 00 J..6...#.C../....
80BAC7DA0 1C 00 00 05 00 00 09 01 00 00 00 03 00 02 67 6D .....gm
80BAC7DB0 6F 64 69 66 79 5F 73 63 6F 72 65 73 2E 73 71 6C odify_scores.sql
80BAC7DC0 2E 74 78 74 1F F0 00 97 AA 9D AE 33 5C C0 DC 01 .txt.d.-$t03\ŘŮ.
```

Obrázok 6: V RAM image bol nájdený názov SQL súboru, ktorý mohol slúžiť na vykonanie alebo prípravu zmeny bodového hodnotenia v databáze prijímacieho konania.

```
56DA12290 73 74 75 64 65 6E 74 5C 44 65 73 6B 74 6F 70 5C student\Desktop\
56DA122A0 70 72 69 6A ED 6D 61 E8 6B 79 2E 74 78 74 00 00 prijimacky.txt..
56DA122B0 25 00 2E 00 2E 00 5C 00 2E 00 2E 00 5C 00 2E 00 %.....\.....\...
```

Obrázok 7: Otvorenie textového súboru s názvom prijímačky

Webová aktivita:

001476C40	75 01 05 25 05 00 00 02 00 20 00 00 03 15 01 0D	y.1/.....s.....
001476C50	00 02 08 00 09 68 74 74 70 73 3A 2F 2F 73 75 70	https://sup
001476C60	65 72 75 73 65 72 2E 63 6F 6D 2F 71 75 65 73 74	eruser.com/quest
001476C70	69 6F 6E 73 2F 31 35 30 38 34 35 37 2F 77 68 65	ions/1508457/whe
001476C80	72 65 2D 64 6F 65 73 2D 77 69 6E 64 6F 77 73 2D	re-does-windows-
001476C90	31 30 2D 73 74 6F 72 65 2D 74 68 65 2D 6C 61 73	10-store-the-las
001476CA0	74 2D 76 69 73 69 74 65 64 2D 66 69 6C 65 73 2D	t-visited-files-
001476CB0	72 65 63 65 6E 74 2D 66 6F 6C 64 65 72 73 2D 61	recent-folders-a
001476CC0	6E 64 2D 66 72 65 71 75 65 6E 74 57 68 65 72 65	nd-frequentWhere
001476CD0	20 64 6F 65 73 20 57 69 6E 64 6F 77 73 20 31 30	does Windows 10

Obrázok 8: snaha páchatela nájsť možnosti ako zahadiť stopy

85AF8EF00	30 31 2E 70 64 66 1B 04 02 02 33 1F A6 01 0C 0E	01.pdf....3.1..
85AF8EF10	61 63 65 62 6F 6F 6B 20 6C 6F 67 69 6E 20 2E 70	acebook login .p
85AF8EF20	5F 67 12 04 02 02 31 1F 3E 01 0C 64 72 68 75 65	... 1.2 drive

Obrázok 9: Prihlásenie na Facebook krátko po incidente

5. Image zariadení

V rámci forenznej analýzy bol vytvorený bitový obraz USB zariadenia zaisteného v kancelárii študijného oddelenia. Obraz bol vyhotovený nástrojom FTK Imager v režime Physical Drive, ktorý zachytáva celý fyzický obsah zariadenia vrátane neobsadeného priestoru (unallocated space) a zvyškov vymazaných súborov. Tento postup je nevyhnutný pre úspešnú obnovu vymazaných dát počas analýzy.

5.1. Parametre vytvoreného obrazu

Vytvorený obraz obsahuje úplnú kópiu zariadenia vrátane systémovej oblasti FAT32 a všetkých dátových sektorov.

Súbor obrazu: dfazubak.001

Formát: Raw image (DD)

Zdrojové zariadenie: Generic Flash Disk USB Device

Veľkosť zdroja: 7800 MB

Počet sektorov: 15 974 400

Veľkosť sektora: 512 bajtov

Súborový systém: FAT32

Čas vytvorenia obrazu: 30.03.2026 11:56:09

Čas dokončenia obrazu: 30.03.2026 12:06:45

Čas overenia integrity: 30.03.2026 12:07:02

Hash hodnoty obrazu:

MD5: b2706fbc7c02170b62b098fc26f57be1

SHA1: 7cc5624e53c370be2dc43e6144fc87442471a7a2

Overenie integrity bolo úspešné – vypočítané hash hodnoty po vytvorení obrazu a po jeho verifikácii sa zhodujú, čím je preukázané, že obraz je identický so zaisteným zariadením a počas spracovania nedošlo k jeho modifikácii.

5.2. Identifikované súbory na obraze

Analýza obrazu odhalila prítomnosť alokovaných (existujúcich) aj dealokovaných (vymazaných) súborov:

Alokované súbory:

- prijimacky_case_ascii.db (12 288 B) – databáza prijímacieho konania
- uchadzaci_export_ascii.csv (881 B) – exportované výsledky
- komunikacia.txt (572 B) – textové poznámky

Dealokované (vymazané) súbory obnovené z unallocated space:

- modify_scores.sql.txt (173 B) – SQL skript úpravy
- prijimacky.txt (326 B) – pomocné poznámky

komunikacia.txt	0	2026-04-28 20:25:36 SELČ	0000-00-00 00:00:00	2026-04-28 01:00:00 SELČ
modify_scores.sql	0	2026-04-28 20:20:24 SELČ	0000-00-00 00:00:00	2026-04-28 01:00:00 SELČ
modify_scores.sql.txt	0	2026-03-30 18:46:38 SELČ	0000-00-00 00:00:00	2026-04-28 01:00:00 SELČ
Navstivena stranka pachatelom .png	0	2026-03-18 10:54:12 SELČ	0000-00-00 00:00:00	2026-03-30 01:00:00 SELČ
otvorenie databazy .png	0	2026-03-25 10:26:02 SELČ	0000-00-00 00:00:00	2026-03-30 01:00:00 SELČ
prijimacky.txt .png	0	2026-03-18 10:58:32 SELČ	0000-00-00 00:00:00	2026-03-30 01:00:00 SELČ
prijimacky_case_ascii(1).db	0	2026-03-25 09:24:44 SELČ	0000-00-00 00:00:00	2026-03-30 01:00:00 SELČ
prijimacky_case_ascii(1).sql	0	2026-03-25 09:24:50 SELČ	0000-00-00 00:00:00	2026-03-30 01:00:00 SELČ
prijimacky_case_ascii.db	0	2026-04-28 20:17:22 SELČ	0000-00-00 00:00:00	2026-04-28 01:00:00 SELČ
prijimacky.txt	0	2026-03-18 09:36:16 SELČ	0000-00-00 00:00:00	2026-03-30 01:00:00 SELČ
PRIME-B365M-A-ASUS-2208.CAP	0	2021-07-09 17:24:16 SELČ	0000-00-00 00:00:00	2026-03-12 00:00:00 SELČ
PRIME-B365M-A-ASUS-2208.ZIP	0	2022-03-14 15:55:34 SELČ	0000-00-00 00:00:00	2022-03-14 00:00:00 SELČ
pripojenie-jednotky-hist%C3%B3rie-s%C3%BAborc	0	2026-03-18 11:01:14 SELČ	0000-00-00 00:00:00	2026-03-30 01:00:00 SELČ
prijimacky.txt	0	2026-04-28 20:24:38 SELČ	0000-00-00 00:00:00	2026-04-28 01:00:00 SELČ
Screenshot 2026-03-18 100515.png	0	2026-03-18 10:05:20 SELČ	0000-00-00 00:00:00	2026-03-30 01:00:00 SELČ
uchadzaci export .png	0	2026-03-18 10:59:38 SELČ	0000-00-00 00:00:00	2026-03-30 01:00:00 SELČ
uchadzaci_export_ascii.csv	0	2026-04-28 20:23:26 SELČ	0000-00-00 00:00:00	2026-04-28 01:00:00 SELČ
prijimacky.txt	0	2026-04-28 20:24:38 SELČ	0000-00-00 00:00:00	2026-04-28 01:00:00 SELČ
modify_scores.sql.txt	0	2026-03-30 18:46:38 SELČ	0000-00-00 00:00:00	2026-04-28 01:00:00 SELČ

5.3.Nálezy podporujúce hypotézy

Z obrazu USB zariadenia bolo získaných niekoľko zásadných digitálnych dôkazov, ktoré priamo súvisia s vyšetrovaným incidentom.

5.3.1. Databázový súbor prijimacky_case_ascii.db

Súbor obsahuje tabuľku uchadzaci s 15 záznamami uchádzačov o štúdium a tabuľku system_logy so záznamami systémových udalostí. Pri detailnom prehliadnutí obsahu databázy bol identifikovaný záznam s id=11 (Daniel Farkas), pri ktorom sa pôvodné bodové hodnotenie 45 bodov líši od aktuálneho hodnotenia 95 bodov. Záznam zároveň obsahuje informáciu o čase úpravy (29.08.2025 22:14:33) a používateľskom účte, ktorý úpravu vykonal (admin_referent).

Tento nález priamo potvrdzuje, že došlo k manipulácii bodového hodnotenia, identifikuje konkrétneho uchádzača, ktorému bola úprava v prospech, a zároveň presne určuje čas úpravy aj použitý účet.

Data Content								
Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations
Other Occurrences								
Table		uchadzaci	15 entries		Page 1 of 1		Export to CSV	
id	meno	priezvisko	rodne_cislo	email	body_po...	body_ak...	datum_zmeny	upravil
1	Jan	Novak	0301015432	novak@email.sk	78	78		
2	Maria	Kovacova	0455126789	kovacova@email.sk	65	65		
3	Peter	Horvath	0312087654	horvath@email.sk	82	82		
4	Lucia	Toth	0501234567	toth@email.sk	71	71		
5	Tomas	Balog	0289765432	balog@email.sk	88	88		
6	Eva	Szabo	0398765431	szabo@email.sk	59	59		
7	Martin	Varga	0276543210	varga@email.sk	92	92		
8	Zuzana	Molnar	0445567890	molnar@email.sk	67	67		
9	Adam	Kiss	0367890123	kiss@email.sk	74	74		
10	Petra	Nagy	0512345678	nagy@email.sk	81	81		
11	Daniel	Farkas	0234567891	farkas@email.sk	45	95	2025-08-29 22:14:33	admin_referent
12	Simona	Olah	0489012345	olah@email.sk	70	70		
13	Filip	Lakatos	0301234567	lakatos@email.sk	85	85		
14	Veronika	Toth	0467890123	veronika.toth@email.sk	63	63		
15	Michal	Bartos	0312345678	bartos@email.sk	77	77		

5.3.2. Tabuľka system_logy

Systémové logy uložené v databáze poskytujú detailnú časovú os incidentu zo dňa 29.08.2025:

21:45:12 Login (admin_referent)

21:47:33 USB device connected: Kingston DataTraveler 8GB

SN:0B8E6B0166E7

21:52:18 Database file opened: prijimacky_case_ascii.db

22:14:33 UPDATE query executed on table uchadzaci WHERE id=11

22:18:45 Export to CSV: uchadzaci_export_ascii.csv

22:25:10 USB device disconnected: Kingston DataTraveler 8GB

22:31:55 Logout

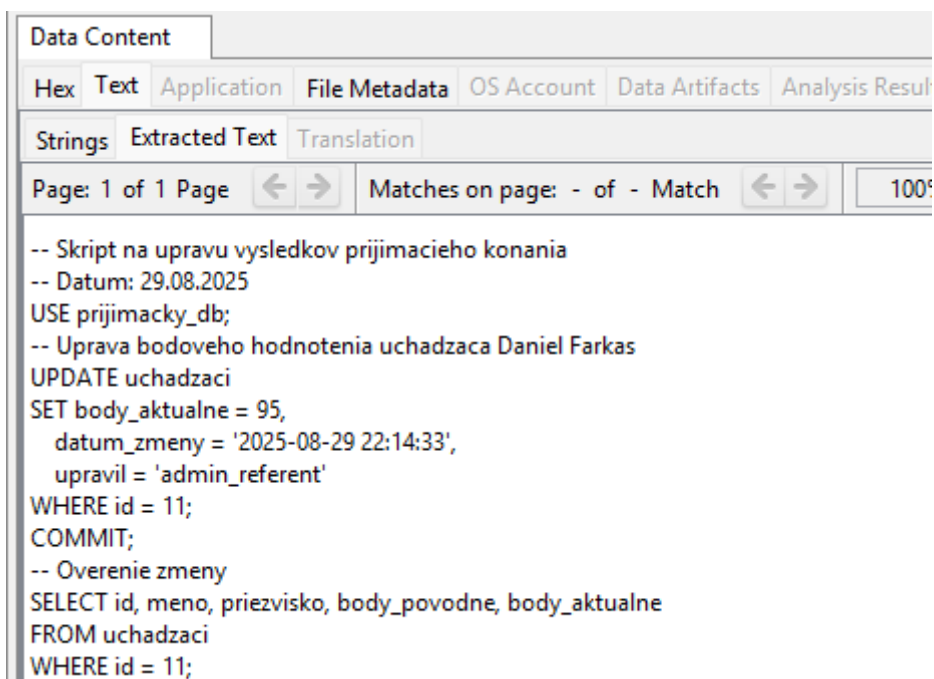
Časová korelácia medzi pripojením USB zariadenia, otvorením databázy, vykonaním UPDATE príkazu a následným odpojením USB jednoznačne preukazuje súvislosť medzi USB nosičom a úpravou bodového hodnotenia.

Data Content				
Hex	Text	Application	File Metadata	OS Account
Data Artifacts				
Analysis Results				
Context				
Annotations				
Other Occurrences				
Table: system_logy 7 entries Page 1 of 1				
Export to CSV				
id	cas	udalost	pouzivatel	ip_adresa
1	2025-08-29 21:45:12	Login	admin_referent	192.168.1.45
2	2025-08-29 21:47:33	USB device connected: Kingston DataTraveler 8GB SN:0B8E6B0166E7	admin_referent	192.168.1.45
3	2025-08-29 21:52:18	Database file opened: prijimacky_case_ascii.db	admin_referent	192.168.1.45
4	2025-08-29 22:14:33	UPDATE query executed on table uchadzaci WHERE id=11	admin_referent	192.168.1.45
5	2025-08-29 22:18:45	Export to CSV: uchadzaci_export_ascii.csv	admin_referent	192.168.1.45
6	2025-08-29 22:25:10	USB device disconnected: Kingston DataTraveler 8GB	admin_referent	192.168.1.45
7	2025-08-29 22:31:55	Logout	admin_referent	192.168.1.45

5.3.3. Vymazaný SQL skript modify_scores.sql.txt

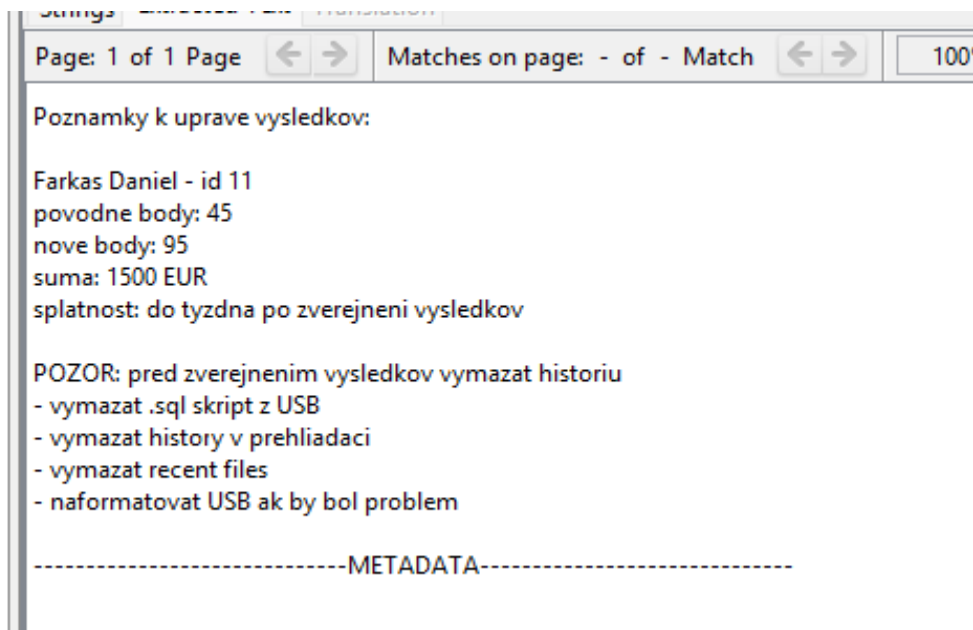
V neobsadenom priestore obrazu bol obnovený obsah vymazaného SQL skriptu, ktorý dokumentuje úpravu databázových záznamov:

Prítomnosť tohto skriptu v unallocated space dokazuje, že USB zariadenie bolo opakovane používané ako pomocný nosič pri manipulácii databázových záznamov a že sa páchatel pokúsil takéto stopy odstrániť zmazaním súboru. Pretože zmazanie v systéme FAT32 neznamená fyzické prepísanie dát, obsah skriptu zostal čitateľný.



5.3.4. Vymazané pomocné poznámky

V obnovenom textovom súbore boli nájdené poznámky obsahujúce meno uchádzača (Farkas Daniel), pôvodné aj nové bodové hodnotenie (45 → 95), sumu finančnej odmeny (1500 EUR) a explicitný plán zahľadania stôp (vymazanie SQL skriptu z USB, vymazanie histórie prehliadača, vymazanie recent files a v krajnom prípade naformátovanie USB). Obsah týchto poznámok preukazuje úmyselné konanie, finančný motív a vedomé úsilie o znemožnenie forenzej analýzy.



5.3.5. Súbor komunikacia.txt

Textový súbor obsahuje lokálne uložený záznam komunikácie medzi dvomi osobami, v ktorom sa dohadujú detaily úpravy bodového hodnotenia, výška odmeny (1500 EUR), požadovaný počet bodov (minimálne 90), čas vykonania zmeny aj forma platby. Posledná správa ("Hotovo. Body upravené.") z 29.08.2025 22:35 časovo nadväzuje na záznam UPDATE query v systémových logoch o 22:14:33.

Data Content						
Hex	Text	Application	File Metadata	OS Account	Data Artifacts	A
Strings		Extracted Text		Translation		
Page: 1 of 1 Page < > Matches on page: - of - Match < >						
[28.08.2025 14:23] - prijata sprava "Dobry den, dohodli sme sa na 1500 EUR za upravu bodov pre Farkasa. Body potrebujeme minimalne 90, aby sa dostal. Kedy to bude hotove?" [28.08.2025 14:45] - odoslana sprava "Spravim to zajtra vecer ked budem v kancelarii sam. Body upravim na 95 aby to nebolo podozrive ze je to presne 90. Plat sa az po zverejneni oficialnych vysledkov." [28.08.2025 14:47] - prijata sprava "OK, dakujem. Suma bude pripravena v hotovosti." [29.08.2025 22:35] - odoslana sprava "Hotovo. Body upravené. Vysledky sa zverejnuju v piatok." -----METADATA-----						

5.3.6. Súbor uchadzaci_export_ascii.csv

Exportovaný súbor obsahuje kópiu databázových záznamov vrátane upraveného bodového hodnotenia uchádzača Farkas (95 bodov). Existencia tohto súboru na USB zariadení preukazuje, že po vykonaní manipulácie bol vykonaný export upravených údajov.

The screenshot shows a file analysis tool interface. The 'Data Content' tab is selected, and the 'Text' sub-tab is active. The main area displays a CSV file with 15 rows of data. The first row is a header with fields: id, meno, priezvisko, rodne_cislo, email, body_povodne, body_aktualne, datum_zmeny, upravil. The subsequent rows contain data for 15 individuals, including names, IDs, emails, and phone numbers. The 11th row is for Daniel Farkas, with a timestamp '2025-08-29 22:14:33' and the role 'admin_referent'. Below the data, a 'METADATA' section is visible, showing details like 'Content-Encoding: windows-1252' and 'Content-Type: text/plain; charset=windows-1252'.

id	meno	priezvisko	rodne_cislo	email	body_povodne	body_aktualne	datum_zmeny	upravil
1	Jan	Novak	0301015432	novak@email.sk	78,78,,			
2	Maria	Kovacova	0455126789	kovacova@email.sk	65,65,,			
3	Peter	Horvath	0312087654	horvath@email.sk	82,82,,			
4	Lucia	Toth	0501234567	toth@email.sk	71,71,,			
5	Tomas	Balog	0289765432	balog@email.sk	88,88,,			
6	Eva	Szabo	0398765431	szabo@email.sk	59,59,,			
7	Martin	Varga	0276543210	varga@email.sk	92,92,,			
8	Zuzana	Molnar	0445567890	molnar@email.sk	67,67,,			
9	Adam	Kiss	0367890123	kiss@email.sk	74,74,,			
10	Petra	Nagy	0512345678	nagy@email.sk	81,81,,			
11	Daniel	Farkas	0234567891	farkas@email.sk	45,95,	2025-08-29 22:14:33		admin_referent
12	Simona	Olah	0489012345	olah@email.sk	70,70,,			
13	Filip	Lakatos	0301234567	lakatos@email.sk	85,85,,			
14	Veronika	Toth	0467890123	veronika.toth@email.sk	63,63,,			
15	Michal	Bartos	0312345678	bartos@email.sk	77,77,,			

-----METADATA-----

Content-Encoding: windows-1252
Content-Type: text/plain; charset=windows-1252
X-TIKA:Parsed-By: org.apache.tika.parser.DefaultParser
X-TIKA:Parsed-By-Full-Set: org.apache.tika.parser.DefaultParser
X-TIKA:detectedEncoding: windows-1252
X-TIKA:encodingDetector: UniversalEncodingDetector

5.4. Zhrnutie nálezov

Analýza obrazu USB zariadenia preukázala prítomnosť všetkých kľúčových typov digitálnych stôp predpokladaných v hypotézach – databázový súbor s upraveným záznamom, dôkaz o použití SQL skriptu, exportovaný CSV súbor, komunikáciu súvisiacu s incidentom, plánovanie zahľadania stôp a presnú časovú os manipulácie. Všetky tieto nálezy boli získané v rámci jedného obrazu, čo potvrdzuje význam USB zariadenia ako hlavného fyzického nosiča dôkazov v prípade.

6. SW nástroje a ich účel

V rámci simulácie incidentu a následnej digitálnej forenznej analýzy boli použité viaceré softvérové nástroje určené na vytváranie obrazov zariadení, analýzu digitálnych stôp, vyhľadávanie artefaktov v RAM image a skúmanie databázových súborov. Každý z nástrojov bol použitý na konkrétny účel, aby bolo možné overovať jednotlivé hypotézy a vytvoriť čo najpresnejšiu rekonštrukciu incidentu.

6.1. FTK Imager

Nástroj FTK Imager bol použitý na vytvorenie bitových kópií digitálnych zariadení a na vytvorenie obrazu operačnej pamäte RAM. Zároveň umožnil základnú prehliadku obsahu zaistených obrazov a overenie integrity dôkazov pomocou hash hodnôt.

6.2.HxD

Hex editor HxD bol použitý na analýzu RAM image a vyhľadávanie textových reťazcov súvisiacich s incidentom. Pomocou tohto nástroja boli vyhľadávané názvy databázových súborov, exportovaných CSV súborov, SQL súborov, webovej aktivity a ďalších artefaktov, ktoré mohli potvrdiť otvorenie databázy a prácu s podozrivými súbormi.

6.3.Autopsy

Autopsy je open-source platforma pre digitálnu foreznú analýzu, ktorá bola použitá na komplexné skúmanie obrazu USB zariadenia. Nástroj umožnil prehľadávanie súborovej štruktúry obrazu, identifikáciu alokovaných aj dealokovaných súborov a obnovu vymazaných dát z unallocated space – konkrétne SQL skriptu modify_scores.sql.txt a pomocných poznámok prijímačky.txt. Autopsy taktiež poskytlo prehľad časových pečiatok súborov (created, modified, accessed), čo umožnilo zostaviť presnú časovú os incidentu a korelovať ju s údajmi zo systémových logov uložených v databáze.

7. Bezpečnostné opatrenia

Pri zaistovaní a spracovaní digitálnych dôkazov je nevyhnutné zabezpečiť ich integritu, dohľadateľnosť a ochranu pred neoprávnenou manipuláciou. V tejto práci boli preto uplatnené základné princípy digitálnej forenznej analýzy, najmä vytvorenie bitových kópií, evidencia manipulácie s dôkazmi, použitie hashovacích algoritmov a fyzická ochrana zariadení.

7.1.Bitove kopie

Zo zaistených digitálnych zariadení boli vytvorené bitové kópie určené na ďalšiu analýzu. Minimálne jedna kópia slúži ako pracovná kópia, ďalšia ako archivovaná kópia a v prípade potreby bola vytvorená aj záložná kópia. Takýto postup znižuje riziko poškodenia originálnych dôkazov a umožňuje vykonávať analýzu bez zásahu do pôvodných zariadení.

Notebook referenta

- typ dôkazu: disk image pracovného notebooku
- počet kópií: 2
- uloženie:
 - 1 pracovná kópia na forenznom pracovnom disku
 - 1 archivná kópia v zabezpečenom úložisku
- čas vytvorenia: 03.09.2025
- účel: analýza používateľskej aktivity, databázy, logov a RAM artefaktov

USB zariadenie

- typ dôkazu: image USB zariadenia
- počet kópií: 2
- uloženie:
 - 1 pracovná kópia na forenznom pracovnom disku
 - 1 archivná kópia v zabezpečenom úložisku
- čas vytvorenia: 03.09.2025
- účel: analýza SQL súborov, textových poznámok, exportov a histórie práce s USB