



Univerzita sv. Cyrila a Metoda v Trnave
Fakulta prírodných vied
Námestie Jozefa Herdu 2
917 01 Trnava

Ústav počítačových technológií a informatiky

Ukradnuté USB

[PREZENTÁCIA](#)

Meno a priezvisko: Tomáš Zajac
Študijný program: aplikovaná informatika
Predmet: digitálna forenzná analýza
Akademický rok: 2025/2026
Semester: letný

Obsah

1. Úvod	4
• 1.2 Popis prípadu (5WH analýza).....	4
2. Hypotézy.....	4
2.3 Hypotéza č. 1	4
2.4 Hypotéza č. 2.....	6
2.5 Hypotéza č. 3.....	6
2.6 Hypotéza č. 4.....	7
3. Digitálne zariadenia.....	8
3.3 Pracovná stanica.....	8
3.4 USB zariadenie.....	8
3.5 Operačná pamäť (RAM).....	8
4. Metodika.....	8
5. Popis dôkazov	9
5.3 Časová os zaist'ovania dôkazov (Chain of Custody)	9
Analyzované zdroje.....	9
6. Analýza dôkazov	11
6.3 Identifikácia citlivých dát	11
6.4 Dôkaz o príprave exfiltrácie	11
6.5 Vytvorenie archívu	11
6.6 Prenos na USB.....	11
6.7 Pokus o zakrytie stop.....	11
6.8 Analýza časovej osi	12
7. Rekonštrukcia incidentu (časová os)	12
8. Záver.....	12
9. Prílohy:	13

Zoznam obrázkov:

Obrázok 1 Ukážka súborov a originalita pomocou SHA-256	9
Obrázok 2 Subory nachádzajúce sa na workstation m_Sabola	10
Obrázok 3 Záznam v Recycle Bin obsahujúci zmazaný dokument security_exception_request.pdf spolu s jeho obsahom – dôkaz pokusu o zakrytie stopy (Dôkaz č. 1).	13
Obrázok 4,6 Obsah archívu archive_final.zip na USB zariadení vrátane súboru server_access_snapshot.docx a jeho metadát – dôkaz prítomnosti citlivých serverových informácií (Dôkaz č. 2). Porovnanie obsahu archívu archive_final.zip v zariadení USB (USB_FOUND) a v pracovnej stanici (workstation) – identické súbory server_access_snapshot.docx, server_room_schedule.xlsx a badge_inventory.csv potvrdzujú prenos dát (Dôkaz č. 4).	14
Obrázok 5 Časová os udalostí v nástroji Autopsy zobrazujúca vytvorenie archívu, jeho kopírovanie na USB zariadenie a následnú emailovú komunikáciu – dôkaz koordinovanej exfiltrácie dát (Dôkaz č. 3).	15

Obrázok 6 Porovnanie obsahu archívu archive_final.zip v zariadení USB (USB_FOUND) a v pracovnej stanici (workstation) – identické súbory server_access_snapshot.docx, server_room_schedule.xlsx a badge_inventory.csv potvrdzujú prenos dát (Dôkaz č. 4).....	15
Obrázok 7 Obrázok 4: Porovnanie obsahu archívu archive_final.zip v zariadení USB (USB_FOUND) a v pracovnej stanici (workstation) – identické súbory server_access_snapshot.docx, server_room_schedule.xlsx a badge_inventory.csv potvrdzujú prenos dát (Dôkaz č. 4).....	16
Obrázok 8 Obsah priečinka Documents na pracovnej stanici (workstation) v nástroji Autopsy – prítomnosť archívu archive_final.zip spolu s ďalšími súbormi (server_access_snapshot.docx, server_room_schedule.xlsx, badge_inventory.csv) potvrdzuje manipuláciu	16
Obrázok 9HASH USB image	17
Obrázok 10kopia obrazu workstation	18
Obrázok 11kopia obrazu USB_FOUND	19

1. Úvod

Počas bezpečnostného incidentu bol nájdený USB kľúč obsahujúci citlivé firemné dáta. Predmetom vyšetrovania bolo zistiť, akým spôsobom sa tieto dáta dostali zo zabezpečeného servera na miesto nálezu.

Cieľom analýzy bolo:

- identifikovať pôvod dát,
- rekonštruovať postup ich prenosu,
- identifikovať zodpovednú osobu,
- overiť pokus o zakrytie stôp.

• 1.2 Popis prípadu (5WH analýza)

Kto (Who):

Neznámy páchateľ – predpokladá sa zamestnanec organizácie s prístupom k internému serveru.

Čo (What):

Neoprávnené kopírovanie a prenos citlivých dát zo zabezpečeného servera na externé USB zariadenie.

Kde (Where):

Administratívna budova organizácie – konkrétne pracovná stanica pripojená do internej siete.

Kedy (When):

Presný čas incidentu nie je známy – bude predmetom forenzej analýzy na základe časových pečiatok súborov a systémových logov.

Prečo (Why):

Možná snaha o únik dát, ich zneužitie alebo ďalšie šírenie mimo organizácie.

Ako (How):

Predpokladá sa použitie externého USB zariadenia na prenos dát zo servera prostredníctvom pracovnej stanice s oprávneným prístupom.

2. Hypotézy

V rámci vyšetrovania boli stanovené nasledujúce hypotézy, ktoré budú overované pomocou digitálnej forenzej analýzy získaných dát.

2.3 Hypotéza č. 1

Citlivé dáta boli skopírované zo zabezpečeného servera na pracovnú stanicu a následne prenesené na USB zariadenie.

Digitálne stopy:

- súbory nachádzajúce sa na USB zariadení
- rovnaké alebo podobné súbory na lokálnom disku (cache, temp)
- časové pečiatky (creation, modification)
- záznamy o pripojení USB zariadenia

Zariadenia:

- pracovná stanica (HDD/SSD)
- USB zariadenie

Obrázok 10 kopia obrazu workstationObrázok 10

Obrázok 11 kopia obrazu USB_FOUND
Obrázok 11

Nástroje:

- **Autopsy** – analýza súborového systému
- **FTK Imager** – vytvorenie image
- **OSForensics** – doplnková analýza

Postup overenia:

1. Vytvorenie forenzného obrazu disku pomocou FTK Imager
2. Analýza súborového systému v Autopsy
3. Vyhľadanie súborov s rovnakým názvom alebo obsahom ako na USB
4. Kontrola časových pečiatok a ich porovnanie
5. Identifikácia USB artefaktov (pripojenia zariadenia)

Výsledok:

potvrdená

2.4 Hypotéza č. 2

Páchateľ sa pokúsil zakryť svoju činnosť odstránením alebo premenovaním súborov.

Digitálne stopy:

- zmazané súbory (unallocated space)
- záznamy v koši (Recycle Bin)
- premenované súbory
- fragmenty súborov

Zariadenia:

- pracovná stanica (disk)

Nástroje:

- **Autopsy** – obnova zmazaných súborov
 - **OSForensics** – vyhľadávanie artefaktov
1. Postup overenia:
 2. Analýza nealokovaného priestoru
 3. Obnova zmazaných súborov
 4. Identifikácia premenovaných súborov (porovnanie obsahu)
 5. Analýza koša a systémových záznamov

Výsledok:

potvrdená – identifikované zmazané súbory v Recycle Bin

2.5 Hypotéza č. 3

Páchateľ využil webový prehliadač alebo internetové služby na získanie alebo odoslanie dát.

Digitálne stopy:

- história prehliadania
- stiahnuté súbory
- cookies a cache
- uložené prihlasovacie údaje

Zariadenia:

- pracovná stanica

Nástroje:

- **Autopsy** – analýza webových artefaktov
- **OSForensics** – analýza histórie a cache

Postup overenia:

1. Extrakcia histórie prehliadača
2. Identifikácia navštívených stránok
3. Analýza stiahnutých súborov
4. Vyhľadanie prihlasovacích údajov

Výsledok:

čiastočne potvrdená – neboli nájdené web artefakty, ale email komunikácia potvrdzuje prenos

2.6 Hypotéza č. 4

Páchateľ komunikoval s treťou stranou a poskytol jej citlivé údaje.

Digitálne stopy:

- e-maily
- chat komunikácia
- prílohy
- kontakty

Zariadenia:

- pracovná stanica
- (prípadne USB zariadenie – uložené súbory)

Nástroje:

- **Autopsy** – analýza komunikácie
- **OSForensics** – vyhľadávanie textových artefaktov

Postup overenia:

- 1 Vyhľadanie komunikačných súborov (email, chat)
- 2 Analýza obsahu komunikácie
- 3 Identifikácia príloh
- 4 Prepojenie komunikácie s časovou osou udalostí

Výsledok:

potvrdená – identifikovaná email komunikácia s pokynmi na prenos dát

3. Digitálne zariadenia

V rámci vyšetrovania boli identifikované nasledovné digitálne zariadenia, ktoré môžu obsahovať relevantné digitálne stopy.

3.3 Pracovná stanica

Typ zariadenia: Stolný počítač (workstation)

Operačný systém: Windows 10 Pro 64-bit

Procesor: Intel Core i5 (alebo ekvivalent)

RAM: 16 GB DDR4

Úložisko: SSD disk

Kapacita: 512 GB

Súborový systém: NTFS

Význam pre vyšetrovanie:

Pracovná stanica predstavuje hlavný zdroj digitálnych dôkazov. Predpokladá sa, že práve na tomto zariadení došlo k manipulácii so súbormi, ich kopírovaníu zo servera a následnému prenosu na USB zariadenie.

3.4 USB zariadenie

Typ zariadenia: USB flash disk

Kapacita: 32 GB

Súborový systém: exFAT / FAT32

Rozhranie: USB 3.0

Význam pre vyšetrovanie:

USB zariadenie bolo nájdené ako primárny dôkaz. Obsahuje citlivé dáta, ktoré sú predmetom vyšetrovania. Analýza tohto zariadenia umožní identifikovať prenesené súbory a ich časové pečiatky.

3.5 Operačná pamäť (RAM)

Typ pamäte: DDR4

Kapacita: 16 GB

Význam pre vyšetrovanie:

otvorené dokumenty

bežiace procesy

fragmenty komunikácie

prihlasovacie údaje

4. Metodika

- 1 Vytvorenie forenzného obrazu USB zariadenia pomocou FTK Imager. Analýza pracovnej stanice ako logical data source v Autopsy
- 2 Overenie integrity pomocou hash funkcií
- 3 Import dát do Autopsy (logical files)
- 4 Korelácia dôkazov a tvorba časovej osi
- 5 Analýza:
 - súborov
 - metadát
 - emailovej komunikácie
 - artefaktov zmazaných dát

5. Popis dôkazov

5.3 Časová os zaist'ovania dôkazov (Chain of Custody)

ID dôkazu	Popis dôkazu	Dátum	Osoba	Miesto	Hash	Uloženie	Manipulácia
USB-001	USB zariadenie (USB_FOUND)	2026-03-04	Vyšetrovateľ	pracovná stanica		evidencia	zaistenie
PC-001	Pracovná stanica (workstation)	2026-03-04	Vyšetrovateľ	kancelária		evidencia	zaistenie
IMG-001	Image USB (FTK Imager)	2026-03-06	Vyšetrovateľ	laboratórium	9123e04edffd75f6bff89e22ce10f97df44dcbf9	disk	vytvorenie obrazu
IMG-002	Image disku workstation (FTK Imager)	2026-03-06	Vyšetrovateľ	laboratórium	(nedostupné – analyzované ako logical data source v Autopsy)	disk	vytvorenie obrazu

1. **04.03.2026** – Vyšetrovateľ preberá prípad
2. **04.03.2026** – Zaistenie USB zariadenia
3. **04.03.2026** – Zaistenie pracovnej stanice
4. **06.03.2026** – Vytvorenie image USB (FTK Imager)
5. **(06.03.2026)** – Vytvorenie image disku (podozrivého) názov : workstation
6. **(06.03.2026)** – Analýza v Autopsy

Analyzované zdroje

USB zariadenie (USB_FOUND)

Obsahovalo:

- archive_final.zip
 - server_access_snapshot.docx
 - server_room_schedule.xlsx
 - badge_inventory.csv

Name	S	C	O	Modified Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash	SHA-256 Hash
badge_inventory.csv			0	2026-03-20 08:37:00 SEČ	210	Allocated	Allocated	unknown	/LogicalFileSet2/workstation/C/Users/m.sabol/Docum...	402a0de394e6cb3de59dbb1fb123037c	6c8ac6ed9f73a30a267294dfda8f162609a96e5d2642d3a728339a9e10736d4
server_access_snapshot.docx			0	2026-03-20 08:18:00 SEČ	2005	Allocated	Allocated	unknown	/LogicalFileSet2/workstation/C/Users/m.sabol/Docum...	24e2a30c5696f40170ea890b1ff90e24	9e2f3a9684204bde749af2a48cf296ba20c8ea0bc371ab1a77c2cf332d0ba5cf
server_room_schedule.xlsx			0	2026-03-20 08:24:00 SEČ	2675	Allocated	Allocated	unknown	/LogicalFileSet2/workstation/C/Users/m.sabol/Docum...	9397d6d35a14d01165cce579801a107e	b4e7bf65ed72ac5cfbabff6a7f1ccc55dd6b7c1247b16b8c679998227440e

Obrázok 1 Ukážka súborov a originalita pomocou SHA-256

Tieto súbory obsahovali citlivé informácie o prístupoch a infraštruktúre.

Znázornené na obrázku 2 v prílohách.

Pracovná stanica (workstation)

Používateľ:

- m_sabol (Martin Sabol)

Nájdené artefakty:

- archive_final.zip (identický súbor ako na USB)
- handoff_message.eml
- súbory v Recycle Bin
- dokumenty s citlivým obsahom




Name	S	C	O	Modified Time	Size	Flags(Div)	Flags(Meta)	Known	Location	MD5 Hash	SHA-256 Hash
badge_inventory.csv	0			2026-03-20 08:37:00 SEČ	210	Allocated	Allocated	unknown	/LogicalFileSet1/USB_FOUND/CONFIDENTIAL/archive.../K2a5de3948c8c3de5d8b1b123037c	8c8acde8b9f73a3a287294d8da876209a8b5c4d542d3a728519a810738d4	
server_access_mapshot.docx	0			2026-03-20 08:18:00 SEČ	2003	Allocated	Allocated	unknown	/LogicalFileSet1/USB_FOUND/CONFIDENTIAL/archive.../24c2a30c3699f40170ea90b1f99a2d4	9a33a98042d4bde788a2a8b4f098ba2b3c9ea8c37ab1a77c2df332af8a3cf	
server_room_schedule.xlsx	0			2026-03-20 08:04:00 SEČ	2675	Allocated	Allocated	unknown	/LogicalFileSet1/USB_FOUND/CONFIDENTIAL/archive.../93f7d6d35a14d01185cc579801a107e	b4a7e8f5ed72acdfab8ff8a7f1ccc55d88b7c1247b18c8c79988227848e	

Obrázok 2 Subory nachádzajúce sa na workstation m_Sabola

Znázornené na obrázku 4 v prílohách.

6. Analýza dôkazov

6.3 Identifikácia citlivých dát

Dokument: server_access_snapshot.docx

Obsahoval:

- prístupové informácie
- interné referencie

poznámku: „*This document should never leave the controlled workstation environment.*“

Znázornená na obrázku 4, v prílohách.

6.4 Dôkaz o príprave exfiltrácie

Email: handoff_message.eml

Obsah:

- zoznam súborov na prenos
- explicitné pokyny:
 - pripraviť balík
 - použiť maskovanie názvu

Kľúčová veta: „*Use the budget filename before any handoff.*“

6.5 Vytvorenie archívu

Súbor: archive_final.zip

Obsah:

- viaceré citlivé súbory
- konsolidácia dát do jedného balíka

Dôkaz č. 2 preukazuje, že archív archive_final.zip obsahoval dokument server_access_snapshot.docx, ktorý zahŕňal citlivé informácie o serverovej infraštruktúre.

6.6 Prenos na USB

Identický súbor:

- na workstation
- na USB zariadení

Dôkaz č. 4 potvrdzuje, že identický archív archive_final.zip sa nachádzal na USB zariadení aj na pracovnej stanici, čo jednoznačne preukazuje kopírovanie citlivých dát medzi týmito úložiskami.

6.7 Pokus o zakrytie stop

Recycle Bin obsahoval: \$|6A91F2C1.pdf, \$|6A91F2C1.pdf

Zistené:

- Súbor bol zmazaný
- Pôvodná cesta:

C:\Users\m_sabol\Documents\security_exception_request.pdf

Dôkaz č. 1 predstavuje zmazaný dokument security_exception_request.pdf identifikovaný v Recycle Bin, ktorý obsahuje informácie o výnimke na prenos dát mimo kontrolovaného prostredia.

Obsah dokumentu:

- žiadosť o výnimku na prenos dát
- schválenie nevyplnené

6.8 Analýza časovej osi

Analýza časovej osi v nástroji Autopsy potvrdila chronologickú postupnosť udalostí. Bolo možné sledovať vznik archívu, jeho prítomnosť na pracovnej stanici a následný výskyt na USB zariadení. Súčasne bola identifikovaná emailová komunikácia časovo korelujúca s týmito udalosťami, čo potvrdzuje úmyselný charakter konania.

Dôkaz č. 3 predstavuje časovú os udalostí, ktorá potvrdzuje postupnosť krokov – vytvorenie archívu, jeho prítomnosť na pracovnej stanici aj USB zariadení a následnú emailovú komunikáciu súvisiacu s prenosom dát.

7. Rekonštrukcia incidentu (časová os)

1. Používateľ pristupuje k citlivým dátam na serveri
2. Dáta sú uložené na pracovnej stanici
3. Vytvorenie archívu archive_final.zip
4. Emailová komunikácia potvrdzuje plán prenosu
5. Archív je skopírovaný na USB zariadenie
6. Pokus o zakrytie:
 - a. Zmazanie PDF dokumentu
 - b. Maskovanie názvov súborov

8. Záver

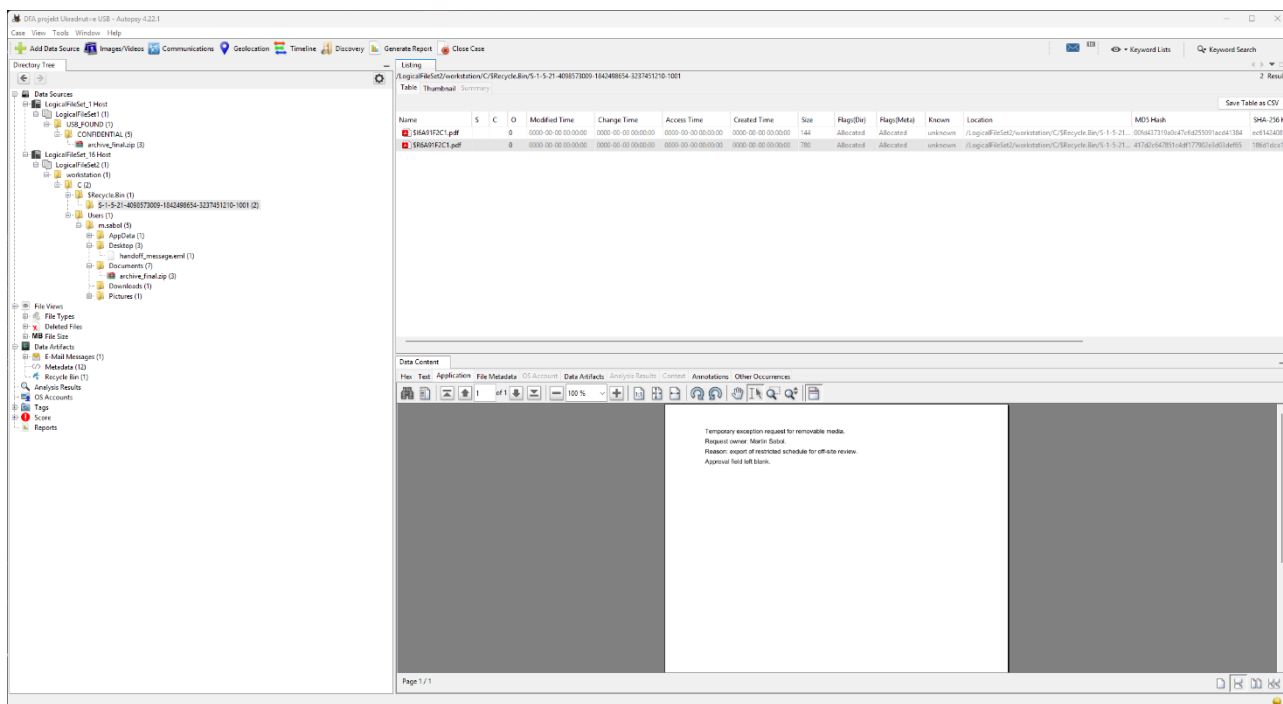
Na základe vykonanej analýzy bolo preukázané, že:

- citlivé dáta boli neoprávnene exportované zo zabezpečeného prostredia,
- prenos prebehol cez pracovnú stanicu používateľa m_sabol,
- dáta boli zabalené do archívu a následne prenesené na USB zariadenie,
- existuje dôkaz plánovania (email),
- existuje dôkaz pokusu o zakrytie stôp (Recycle Bin).

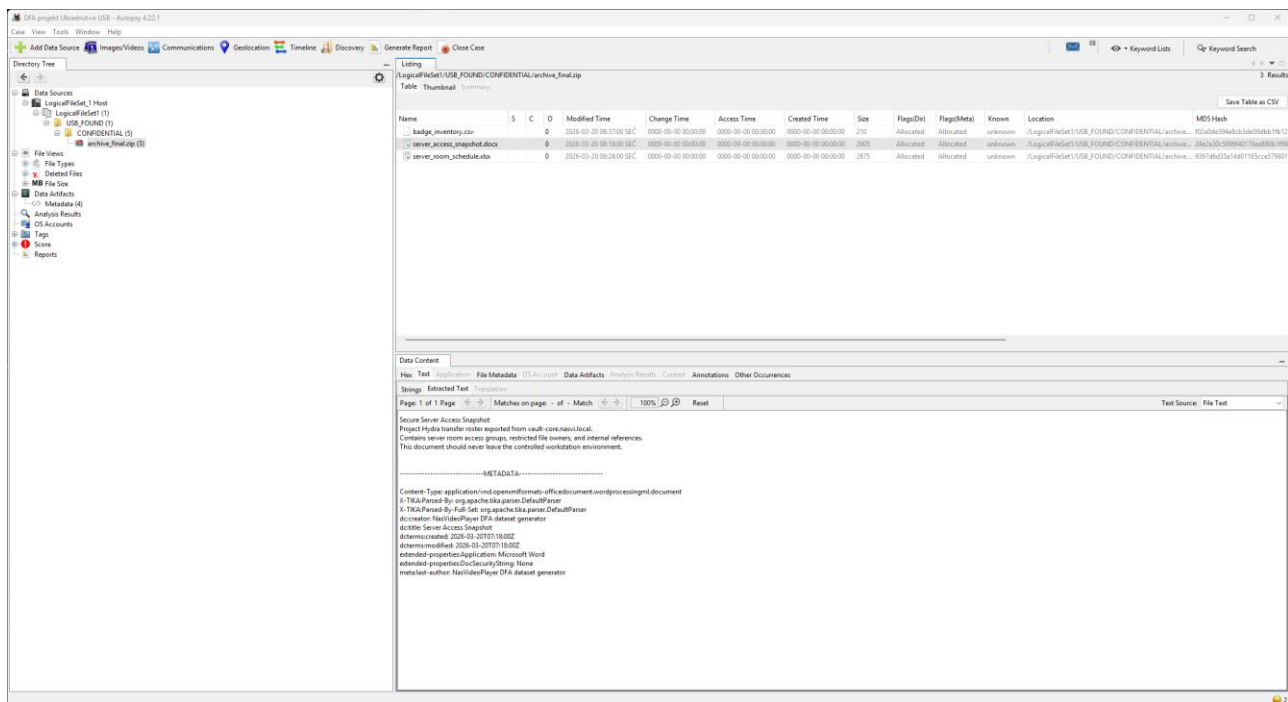
Finálny záver :

Na základe všetkých analyzovaných dôkazov je možné jednoznačne konštatovať, že došlo k úmyselnej exfiltrácii citlivých dát prostredníctvom USB zariadenia.

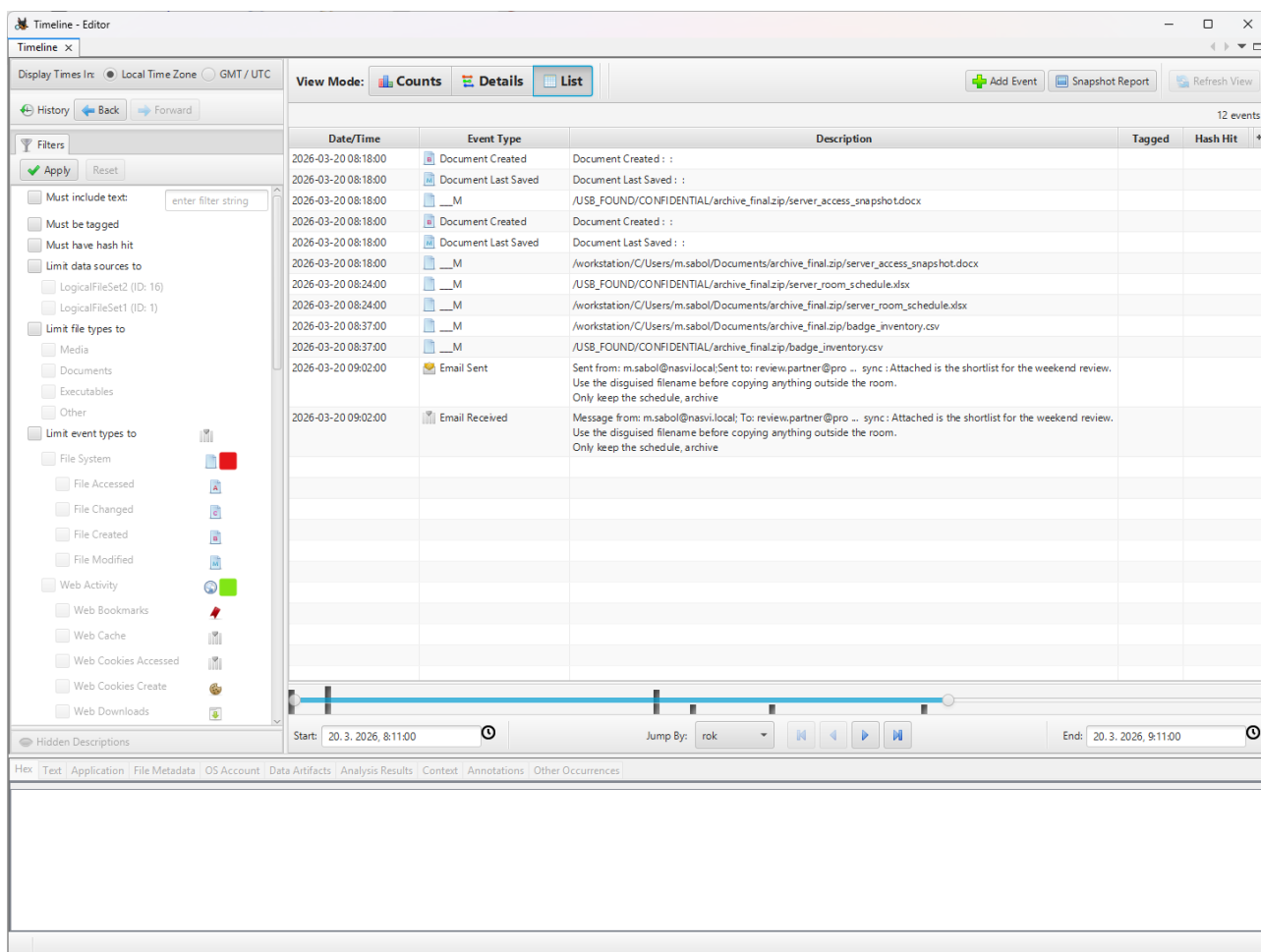
9. Prílohy:



Obrázok 3 Záznam v Recycle Bin obsahujúci zmazaný dokument `security_exception_request.pdf` spolu s jeho obsahom – dôkaz pokusu o zakrytie stopy (Dôkaz č. 1).

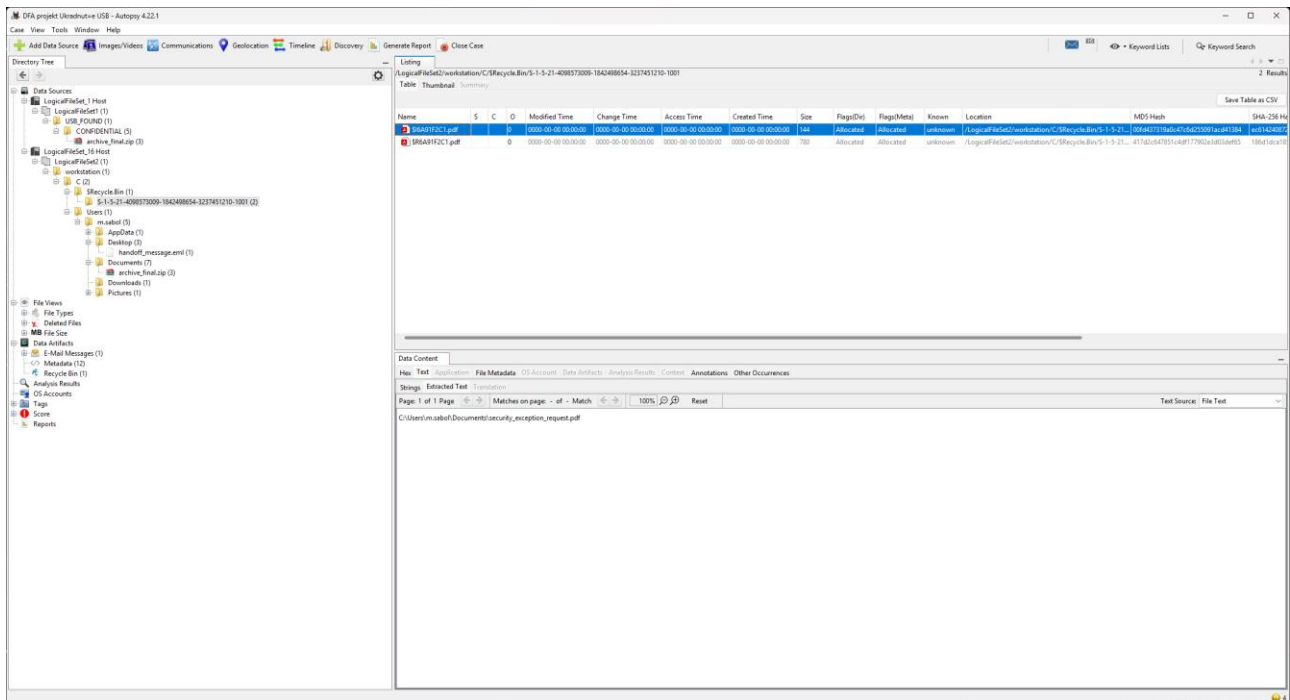


Obrázok 4,6 Obsah archívu archive_final.zip na USB zariadení vrátane súboru server_access_snapshot.docx a jeho metadát – dôkaz prítomnosti citlivých serverových informácií (Dôkaz č. 2). Porovnanie obsahu archívu archive_final.zip v zariadení USB (USB_FOUND) a v pracovnej stanici (workstation) – identické súbory server_access_snapshot.docx, server_room_schedule.xlsx a badge_inventory.csv potvrdzujú prenos dát (Dôkaz č. 4).

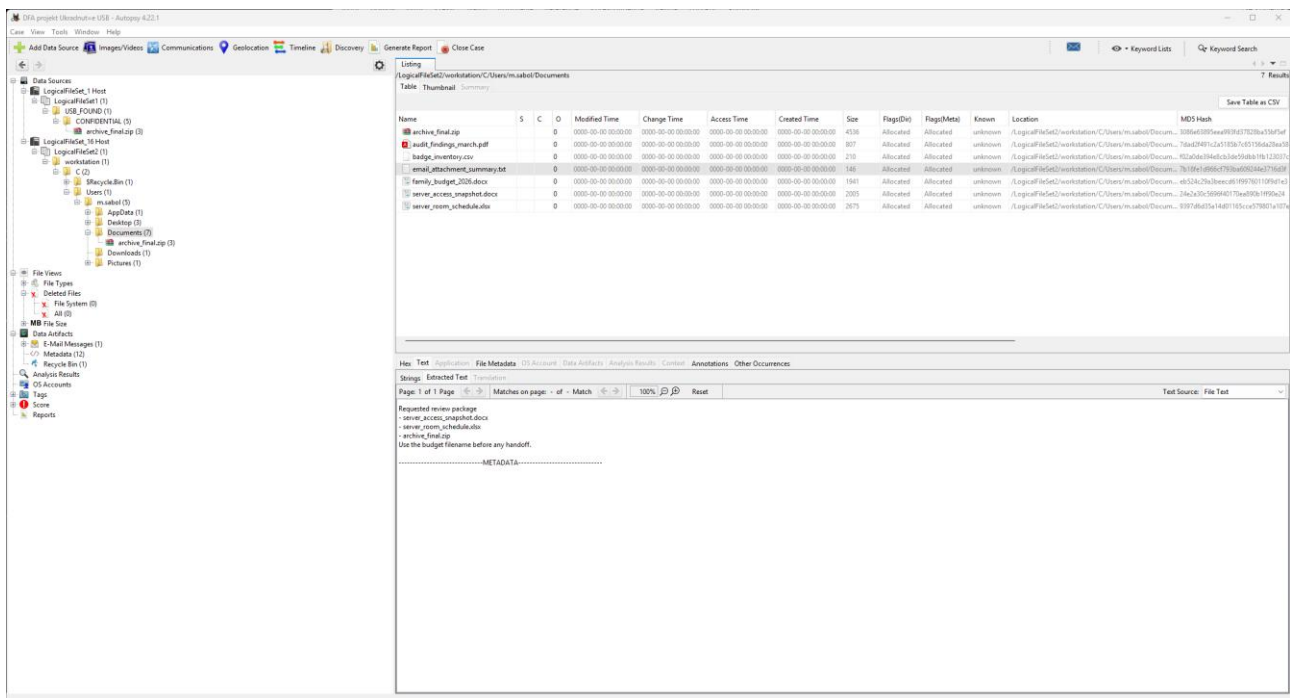


Obrázok 5 Časová os udalostí v nástroji Autopsy zobrazujúca vytvorenie archívu, jeho kopírovanie na USB zariadenie a následnú emailovú komunikáciu – dôkaz koordinovanej exfiltrácie dát (Dôkaz č. 3).

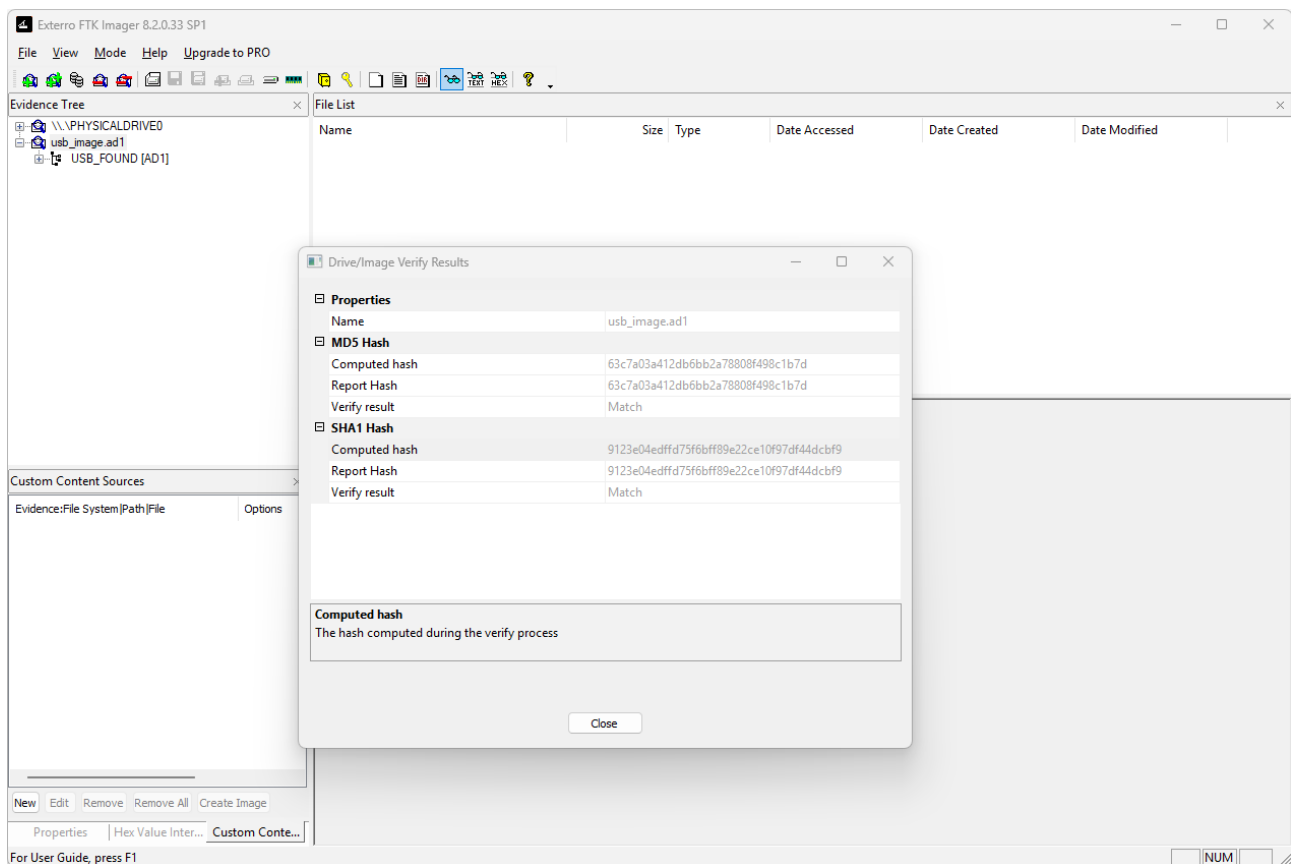
Obrázok 6 Porovnanie obsahu archívu `archive_final.zip` v zariadení USB (`USB_FOUND`) a v pracovnej stanici (`workstation`) – identické súbory `server_access_snapshot.docx`, `server_room_schedule.xlsx` a `badge_inventory.csv` potvrdzujú prenos dát (Dôkaz č. 4).



Obrázok 7 Obrázok 4: Porovnanie obsahu archívu archive_final.zip v zariadení USB (USB_FOUND) a v pracovnej stanici (workstation) – identické súbory server_access_snapshot.docx, server_room_schedule.xlsx a badge_inventory.csv potvrdzujú prenos dát (Dôkaz č. 4).



Obrázok 8 Obsah priečinka Documents na pracovnej stanici (workstation) v nástroji Autopsy – prítomnosť archívu archive_final.zip spolu s ďalšími súbormi (server_access_snapshot.docx, server_room_schedule.xlsx, badge_inventory.csv) potvrdzuje manipuláciu



Obrázok 9HASH USB image

Created By Exterro® FTK® Imager 8.2.0.33

Case Information:

Acquired using: ADI8.2.0.33

Case Number: 001

Evidence Number: USB1

Unique Description: USB evidence from dataset

Examiner: Tomáš Zajac

Notes:

Encrypted Password :

Information for D:\Forensics\Images\usb_image.ad1:

[Computed Hashes]

MD5 checksum: 63c7a03a412db6bb2a78808f498c1b7d

SHA1 checksum: 9123e04edffd75f6bff89e22ce10f97df44dcbf9

Image information:

Acquisition started: Wed Mar 25 11:47:49 2026

Acquisition finished: Wed Mar 25 11:47:49 2026

Segment list:

D:\Forensics\Images\usb_image.ad1

COMPUTED HASH : 63c7a03a412db6bb2a78808f498c1b7d

COMPUTED HASH : 9123e04edffd75f6bff89e22ce10f97df44dcbf9

Image Verification Results:

Verification started: Wed Mar 25 11:47:49 2026

Verification finished: Wed Mar 25 11:47:49 2026

MD5 checksum: 63c7a03a412db6bb2a78808f498c1b7d : verified

SHA1 checksum: 9123e04edffd75f6bff89e22ce10f97df44dcbf9 : verified

COMPUTED HASH : 63c7a03a412db6bb2a78808f498c1b7d

COMPUTED HASH : 9123e04edffd75f6bff89e22ce10f97df44dcbf9

Image Verification Results:

Verification started: Wed Apr 1 16:45:03 2026

Verification finished: Wed Apr 1 16:45:03 2026

MD5 checksum: 63c7a03a412db6bb2a78808f498c1b7d : verified

SHA1 checksum: 9123e04edffd75f6bff89e22ce10f97df44dcbf9 : verified

Obrázok 10kopia obrazu workstation

Created By Exterro® FTK® Imager 8.2.0.33

Case Information:

Acquired using: ADI8.2.0.33

Case Number: 001

Evidence Number: USB1

Unique Description: USB evidence from dataset

Examiner: Tomáš Zajac

Notes:

Encrypted Password :

Information for D:\Forensics\Images\usb_image.ad1:

[Computed Hashes]

MD5 checksum: 63c7a03a412db6bb2a78808f498c1b7d

SHA1 checksum: 9123e04edffd75f6bff89e22ce10f97df44dcbf9

Image information:

Acquisition started: Wed Mar 25 11:47:49 2026

Acquisition finished: Wed Mar 25 11:47:49 2026

Segment list:

D:\Forensics\Images\usb_image.ad1

COMPUTED HASH : 63c7a03a412db6bb2a78808f498c1b7d

COMPUTED HASH : 9123e04edffd75f6bff89e22ce10f97df44dcbf9

Image Verification Results:

Verification started: Wed Mar 25 11:47:49 2026

Verification finished: Wed Mar 25 11:47:49 2026

MD5 checksum: 63c7a03a412db6bb2a78808f498c1b7d : verified

SHA1 checksum: 9123e04edffd75f6bff89e22ce10f97df44dcbf9 :

verified

COMPUTED HASH : 63c7a03a412db6bb2a78808f498c1b7d

COMPUTED HASH : 9123e04edffd75f6bff89e22ce10f97df44dcbf9

Image Verification Results:

Verification started: Wed Apr 1 16:45:03 2026

Verification finished: Wed Apr 1 16:45:03 2026

MD5 checksum: 63c7a03a412db6bb2a78808f498c1b7d : verified

SHA1 checksum: 9123e04edffd75f6bff89e22ce10f97df44dcbf9 :

verified

Obrázok 11kopia obrazu USB_FOUND