

UNIVERZITA SV.CYRILA A METODA V TRNAVE
FAKULTA PRÍRODNÝCH VIED
ÚSTAV POČÍTAČOVÝCH TECHNOLOGIÍ A INFORMATIKY

Digitálna forenzná analýza

Prípad: Posledný nech zhasne

[prezentácia](#)

Obsah

1. Názov prípadu a zhrnutie	4
1.1 Zhrnutie	4
1.2 Identifikácia incidentu – metóda 5WH	4
1.3 Rekonštrukcia priebehu incidentu	5
1.4 Odborný príspevok	6
2. Hypotézy	7
Hypotéza 1: Páchateľ použil USB kľúč na skopírovanie firemných dát zo servera	7
Hypotéza 2: Na vstup do serverovne bol zneužitý čip a kľúče Martina Rýchleho	7
Hypotéza 3: Upratovačka Marta Brudná odovzdala kľúče páchatelovi	8
3. Digitálne zariadenia	9
3.1 Sekundárne pamäte	9
3.2 Primárna pamäť (RAM)	12
4. Dáta – prehľad datasetu	14
4.1 Súbory na USB kľúči	14
4.2 Ďalšie dátové zdroje	15
5. Image RAM – analýza a dôkazy	15
5.1 Postup vytvorenia RAM image	16
5.2 Nástroj a metodika analýzy RAM – Volatility 3	16
5.3 Kľúčové artefakty nájdené v RAM	16
6. Image zariadení – dôkazy overujúce hypotézy	19
6.1 Parametre vytvorených bitových kópií	19
6.2 Dôkazy z analýzy USB kľúča	19
6.3 Dôkazy zo systémových logov	22
7. Softvérové nástroje	24
8. Bezpečnostné opatrenia	25
8.1 Bitové kópie – počet, umiestnenie a hashe	25
8.2 Chain of Custody – reťazec dôkazov	25
8.3 Fyzická ochrana dôkazového materiálu	26
9. Záver	27

Zoznam obrázkov

Obrázok 1 USB Kľúč Kingston	9
Obrázok 2 Server Dell.....	10
Obrázok 3 NAS Synology	11
Obrázok 4 NVR Hikvision.....	11
Obrázok 5 Magnet RAM Capture	13
Obrázok 6 Kamerový záznam s neznámou osobou.....	15
Obrázok 7 Skript v Pythone	20

1. Názov prípadu a zhrnutie

Prípád DFA-2026-001: Neoprávnený vstup do serverovne a exfiltrácia firemných dát

1.1 Zhrnutie

Dňa 30.12.2026 v čase medzi 14:58 a 16:15 hod. došlo v sídle spoločnosti Future s.r.o., Hlavná 35, Trnava, k neoprávnenému vstupu neznámej osoby do serverovne a do kancelárie účtovníčky. Firma sa nachádzala v obmedzenom prevádzkovom režime – väčšina zamestnancov vrátane IT administrátora Martina Rýchleho bola na dovolenke. Neznáma osoba sa predstavovala ako nový zamestnanec IT oddelenia menom Marcel. Vstup do serverovne bol umožnený čipom Martina Rýchleho, ku ktorému sa páchateľ pravdepodobne dostal prostredníctvom upratovačky Marty Brudnej. Na zaistenom USB kľúči boli objavené exfiltračné skripty a kópia zálohy účtovníctva. Keďže USB kľúč zostal u účtovníčky Zuzany Bežnej, nie je s istotou preukázané, či páchateľ dáta skutočne odviezol. Prípád bol postúpený polícii.

1.2 Identifikácia incidentu – metóda 5WH

Pre systematické zadefinovanie cieľov vyšetrovania bola použitá Kiplingova metóda 5WH. Táto metóda umožňuje štruktúrovane popísať incident a určiť, čo má forenzné vyšetrovanie preukázať.

Otázka	Odpoveď
KTO? (Who?)	Neznáma osoba vystupujúca pod menom "Marcel" – externá osoba bez pracovného vzťahu k Future s.r.o. Podozrivá z napomohnutia: upratovačka Marta Brudná, ktorá ako jediná mimo IT oddelenia mala prístup do kancelárie Martina Rýchleho počas dovolenky.
ČO? (What?)	Neoprávnený fyzický vstup do serverovne S-07. Pripojenie USB kľúča k serveru a spustenie skriptu kopírujúceho súbory (.jpg, .doc, .docx, .xls, .xlsx, .ppt, .pptx) a zálohu účtovníctva (.zip). Následný vstup do kancelárie účtovníčky Zuzany Bežnej pod falošnou zámenkou opravy PC.
KEDY? (When?)	30.12.2026: 14:58 – deaktivácia alarmu, 15:00 – vstup do serverovne, 15:10–15:43 – kopírovanie dát, 16:00 – príchod do kancelárie Zuzany Bežnej, cca 16:15 – náhly odchod a zabudnutie USB kľúča. Incident nahlásený: 6.1.2027.
KDE? (Where?)	Serverovňa S-07, Future s.r.o., Hlavná 35, Trnava. Kancelária účtovníčky Zuzany Bežnej v tej istej budove. Kľúče Martina Rýchleho s najväčšou pravdepodobnosťou odcudzené z jeho kancelárie počas dovolenky.
PREČO? (Why?)	Predpokladaný motív: získanie citlivých firemných dát – zálohy účtovníctva a interných dokumentov – pre možné ďalšie zneužitie. Konkrétny zámer nie je preukázaný, keďže USB kľúč zostal v priestoroch firmy.

Otázka	Odpoveď
AKO? (How?)	Páchateľ vstúpil do budovy s čipom Martina Rýchleho (deaktivoval alarm), otvoril serverovňu zodpovedajúcim kľúčom, pripojil USB kľúč k serveru SRV-01 a spustil Python skript na automatické kopírovanie súborov. Následne navštívil kanceláriu účtovníčky pod zámienkou technickej opravy.

1.3 Rekonštrukcia priebehu incidentu

Na základe dostupných informácií z fázy identifikácie – kamerových záznamov, logov alarmového systému a obsahu USB kľúča – bola zostavená nasledujúca rekonštrukcia udalostí. Táto rekonštrukcia bude v priebehu vyšetrovania priebežne overovaná forenznou analýzou.

1. 26.12.2026 – Martin Rýchly odchádza na dovolenku. Pred odchodom má pocit, že nemôže nájsť svoje kľúče od kancelárie a serverovne (vrátane čipu na deaktiváciu alarmu), no keďže si nie je istý, incident nenahlási. Kľúče s najväčšou pravdepodobnosťou získala upratovačka Marta Brudná počas upratovania kancelárie.
2. 27.–28.12.2026 – Páchateľ na svojom zariadení vyhľadáva informácie o kopírovaní súborov cez sieť a komprimovaní archívov. Stiahne Python a pripraví exfiltračný skript `sync_files.py`. Poznačí si cieľové IP adresy a typy súborov.
3. 30.12.2026 o 14:58 – Páchateľ prichádza do budovy Future s.r.o. na Hlavnej 35 v Trnave. Priloží čip Martina Rýchleho k snímaču alarmového systému a deaktivuje alarm serverovne.
4. 30.12.2026 o 15:00 – Vstupuje do serverovne S-07. Pripojí USB kľúč (Kingston DataTraveler) k serveru SRV-01 cez predný USB port.
5. 30.12.2026 o 15:10 – Spustí skript `sync_files.py`. Skript automaticky prehľadáva sieťové priečinky servera SRV-01 a NAS-01 a kopíruje súbory s príponami `.jpg`, `.doc`, `.docx`, `.xls`, `.xlsx`, `.ppt`, `.pptx` a zálohu účtovníctva (`.zip`) na USB kľúč.
6. 30.12.2026 o 15:43 – Kopírovanie je dokončené. Páchateľ odpojí USB kľúč a opustí serverovňu. Zabudne vypnúť svetlo – napriek pokinu v zmazanom pláne vstupu.
7. 30.12.2026 o 16:00 – Páchateľ prichádza do kancelárie účtovníčky Zuzany Bežnej pod zámienkou opravy počítača. Predstaví sa ako nový kolega z IT – Marcel.
8. 30.12.2026 o cca 16:15 – Páchateľ náhle odchádza a na stole zabudne USB kľúč s exfiltrovanými dátami.
9. 30.12.2026 o cca 16:20 – Zuzana Bežná si všimne cudzí USB kľúč a uloží ho do svojho trezora.

10. 6.1.2027 – Zuzana Bežná sa vracia z dovolenky a prináša USB kľúč na IT oddelenie. IT administrátor Peter Káčer zisťuje, že žiaden Marcel v spoločnosti nepracuje. Je privolané vedenie a polícia.

1.4 Odborný príspevok

Článok: "Forensic Analysis of USB Storage Devices in Corporate Espionage Cases" – Digital Investigation Journal, Vol. 18 (2022), Elsevier.

Odkaz: <https://www.sciencedirect.com/science/article/pii/S1742287622000123>

Príspevok sa zaoberá forenznou analýzou USB zariadení v prípadoch priemyselnej špionáže. Autori popisujú metodiku obnovy zmazaných súborov, analýzy časových pečiatok a identifikácie spustených skriptov prostredníctvom systémových logov Windows. Článok priamo korešponduje s naším prípadom – rovnaký typ útoku (fyzický vstup a USB exfiltrácia), rovnaké typy artefaktov (USBSTOR registry, Event Log, skriptové súbory) a porovnateľný postup vyšetovania.

2. Hypotézy

Na základe informácií získaných vo fáze identifikácie boli formulované tri hypotézy. Pre každú hypotézu sú definované relevantné digitálne stopy, zariadenia, kde tieto stopy hľadáme, nástroje a postup overenia a predbežný výsledok. Hypotézy budú v priebehu analýzy priebežne overované a výsledky doplnené.

Hypotéza 1: Páchateľ použil USB kľúč na skopírovanie firemných dát zo servera

Neznáma osoba pripojila USB kľúč k serveru SRV-01 a pomocou pripraveného Python skriptu automaticky skopírovala firemné súbory (dokumenty, fotografie, zálohu účtovníctva) na USB kľúč. Hypotéza predpokladá, že kopírovanie prebehlo úspešne a dáta sú fyzicky prítomné na zaistenom USB kľúči.

Parameter	Detail
Digitálne stopy	Súbory na USB kľúči (skopírované dokumenty, ZIP záloha, skript), Windows Event Log na SRV-01 (EventID 6416 – pripojenie USB), USBSTOR kľúč v registri Windows (história pripojených USB zariadení), časové pečiatky súborov na USB zodpovedajúce času incidentu (15:10–15:43)
Zariadenia	USB kľúč Kingston DataTraveler (zaistený), server SRV-01 (Windows Server, súborový server), NAS-01 (Synology – zdrojové úložisko zálohy účtovníctva)
Nástroj overenia	FTK Imager (vytvorenie bitovej kópie USB), Autopsy (analýza obsahu, timeline, file carving), Registry Explorer (USBSTOR artefakty na SRV-01)
Postup overenia	1. FTK Imager: bitová kópia USB a MD5/SHA-1 hash. 2. Autopsy: timeline analýza – zoradiť súbory podľa dátumu vytvorenia a porovnať s časom incidentu. 3. Autopsy: overiť metadáta dokumentov (vlastník, doména). 4. Registry Explorer: USBSTOR na SRV-01 – potvrdiť sériové číslo USB a čas pripojenia.
Výsledok	POTVRDENÁ – Timestamps súborov na USB (15:10–15:43) zodpovedajú záznamu na kamerách. Firemné dokumenty majú v metadátach vlastníka z domény Future. ZIP záloha účtovníctva je kópiou súboru z NAS-01.

Hypotéza 2: Na vstup do serverovne bol zneužitý čip a kľúče Martina Rýchleho

Páchateľ sa dostal do priestorov serverovne pomocou fyzického kľúča a čipu patriacich IT administrátorovi Martinovi Rýchlemu, ktorý bol v čase incidentu na dovolenke. Martin Rýchly kľúče nahlásil ako pravdepodobne stratené ešte pred odchodom, no incident oficiálne nenahlásil. Po návrate (6.1.2027) kľúče našiel na stole vo svojej kancelárii.

Parameter	Detail
Digitálne stopy	Log alarmového systému (použitý čip, identifikátor kódu, čas deaktivácie), kamerový záznam z NVR (vstup osoby do budovy a serverovne)
Zariadenia	Alarmový systém Paradox Insight EVO (log deaktivácie a aktivácie), NVR Hikvision (kamerový záznam vstupu a pohybu)
Nástroj overenia	Manuálna analýza exportovaného logu alarmového systému, Autopsy (analýza kamerového záznamu – identifikácia osoby a čas vstupu)
Postup overenia	1. Export logu alarmového systému za 30.12.2026 – zistiť, ktorý čip bol použitý na deaktiváciu a o koľkej hodine. 2. Porovnať identifikátor čipu s evidenciou pridelených čipov zamestnancom. 3. Kamerový záznam: potvrdiť, že o 14:58 vstupuje do serverovne osoba, ktorá nie je Martin Rýchly.
Výsledok	POTVRDENÁ – Log alarmu zaznamenal deaktiváciu čipom s ID priradeným Martinovi Rýchlemu o 14:58:33 hod. Kamerový záznam zachytáva osobu v šiltovke, ktorá nie je zamestnancom firmy. Martin Rýchly má alibi – v tom čase bol preukázateľne mimo Trnavy.

Hypotéza 3: Upratovačka Marta Brudná odovzdala kľúče páchatel'ovi

Upratovačka Marta Brudná pravidelne upratuje kanceláriu Martina Rýchleho a ako jediná osoba mimo IT oddelenia mala v období dovolenky prístup do tejto kancelárie. Je podozrivá, že kľúče vrátane čipu alarmu odovzdala páchatel'ovi alebo mu umožnila ich dočasné použitie. Neexistuje žiadna digitálna komunikácia medzi Martou Brudnou a páchatel'om – táto hypotéza je predmetom fyzického vyšetrovania políciou.

Parameter	Detail
Digitálne stopy	Kamerový záznam chodby pri kancelárii Martina Rýchleho (pohyb upratovačky v priestore, kde sú uložené kľúče)
Zariadenia	NVR Hikvision (kamery na chodbách budovy Future s.r.o. na Hlavnej 35, Trnava)
Nástroj overenia	Autopsy (analýza kamerových záznamov chodieb za 26.–30.12.2026)
Postup overenia	1. Preskúmať kamerové záznamy chodby pri kancelárii Martina Rýchleho za 26.–30.12.2026. 2. Zistiť, či Marta Brudná vstupovala do kancelárie po odchode Martina Rýchleho. 3. Overiť, či sa v záberoch nachádza moment odovzdania kľúčov. 4. Polícia zabezpečí výsluch Marty Brudnej.
Výsledok	ČIASTOČNE POTVRDENÁ – Kamera zachytila Martu Brudnú vstupujúcu do kancelárie Martina Rýchleho dňa 27.12.2026 o 15:42 hod. Priame odovzdanie kľúčov kamera nezachytila. Prípad ďalej vyšetruje polícia.

3. Digitálne zariadenia

Táto kapitola popisuje všetky digitálne zariadenia relevantné pre vyšetrovanie. Pre každé zariadenie sú uvedené technické parametre dôležité pre posúdenie jeho forenzného potenciálu.

3.1 Sekundárne pamäte

3.1.1 USB kľúč – primárny dôkazový predmet

USB kľúč bol zaistený účtovníčkou Zuzanou Bežnou bezprostredne po odchode páchateľa z jej kancelárie dňa 30.12.2026. Uložila ho do osobného trezora, čím ho de facto ochránila pred ďalšou manipuláciou. Dňa 6.1.2027 ho odovzdala na IT oddelenie. USB kľúč predstavuje kľúčový dôkazový predmet celého prípadu.



Obrázok 1 USB Kľúč Kingston

Parameter	Hodnota
Model	Kingston DataTraveler Exodia 32 GB (DTXM/32GB)
Sériové číslo	60A44C43404B4100002A
Rozhranie	USB 3.2 Gen 1 (USB-A, spätne kompatibilné s USB 2.0)
Kapacita	32 GB (29,8 GiB využiteľná kapacita)
Súborový systém	NTFS
Rýchlosť čítania	120 MB/s (podľa špecifikácie výrobcu)
Rýchlosť zápisu	45 MB/s (podľa špecifikácie výrobcu)
Celkový počet sektorov	62 488 576
Veľkosť sektora	512 B
Stav pri zaistení	Odpojený od akéhokoľvek zariadenia, uložený v trezore – pred forenznou analýzou pripojený výhradne cez hardvérový write-blocker.

3.1.2 Server SRV-01 – primárny súborový server

Server SRV-01 je hlavným súborovým serverom spoločnosti Future s.r.o. Na tento server bol s najväčšou pravdepodobnosťou pripojený USB kľúč a odtiaľto boli kopírované dáta. Server bol počas incidentu aj počas vyšetrovania v prevádzke – nevypínal sa, pretože jeho zastavenie by narušilo chod firmy.



Obrázok 2 Server Dell

Parameter	Hodnota
Model	Dell PowerEdge T40 (tower server)
CPU	Intel Xeon E-2224G, 3,5 GHz (4 jadrá, max. 4,7 GHz Turbo)
RAM	16 GB DDR4 ECC UDIMM, 2 666 MT/s (2 × 8 GB)
Úložisko	2 × HDD Seagate Exos 2 TB SATA 6 Gb/s, 7 200 RPM, RAID 1 – sekvenčné čítanie 250 MB/s, prístupová doba ~8,5 ms
Operačný systém	Windows Server 2019 Standard (64-bit)
Sieťové rozhranie	1 × Intel I219-LM Gigabit Ethernet, statická IP: 192.168.1.100
USB porty	4 × USB 3.0 Type-A (predný panel) – predmet vyšetrovania, 2 × USB 2.0 (zadný panel)
Stav pri zaistení	Server bol v prevádzke. Windows Event Logy exportované za behu. RAM image vytvorený nástrojom Magnet RAM Capture.

3.1.3 NAS-01 – sieťové úložisko

NAS-01 slúži ako centrálné zálohovacie úložisko a zdieľaný priestor pre oddelenia vrátane účtovníctva. Práve tu bola uložená záloha účtovníctva, ktorej kópia bola nájdená na USB kľúči.



Obrázok 3 NAS Synology

Parameter	Hodnota
Model	Synology DiskStation DS720+
CPU	Intel Celeron J4125, 2,0 GHz (4 jadrá, max. 2,7 GHz)
RAM	2 GB DDR4 (rozšíriteľná na 6 GB)
Úložisko	2 × HDD WD Red Plus 4 TB SATA, RAID 1 (Synology SHR) – sekvenčné čítanie 180 MB/s, prístupová doba ~12 ms
Sieťové rozhranie	2 × Gigabit Ethernet (Link Aggregation), IP: 192.168.1.110
Zdieľané priečinky	\\192.168.1.110\Uctovnictvo, \\192.168.1.110\Shared
Stav pri zaistení	V prevádzke. Logy prístupu k súborom exportované. NAS nebol fyzicky zaistený – vypnutie by narušilo firemné zálohovanie.

3.1.4 NVR – kamerový záznamový systém

NVR zaznamenáva a uchováva záznamy zo všetkých bezpečnostných kamier v budove. Pre toto vyšetrovanie sú kľúčové záznamy z kamery pri hlavnom vchode, kamery na chodbách a kamery v serverovni. Záznamy slúžia ako nezávislé potvrdenie časovej osi incidentu.



Obrázok 4 NVR Hikvision

Parameter	Hodnota
Model NVR	Hikvision DS-7616NI-K2/16P
Počet kanálov	16 IP kamier (z toho 7 aktívnych v budove)
Úložisko	1 × HDD WD Purple 4 TB SATA – nepretržitý záznam, sekvenčné zápi 180 MB/s
Formát záznamu	H.264+, MP4, rozlíšenie 1080p pri 15 fps
Retencia záznamu	Cca 21 dní pri 7 kamerách v 1080p/15fps
Kľúčové kamery	CAM-01: hlavný vchod, CAM-04: chodba 2. poschodia, CAM-06: serverovňa S-07, CAM-07: chodba pri kanceláriách IT
Stav pri zaistení	V prevádzke. Záznamy z 30.12.2026 exportované ako MP4. HDD naimageovaný nástrojom FTK Imager.

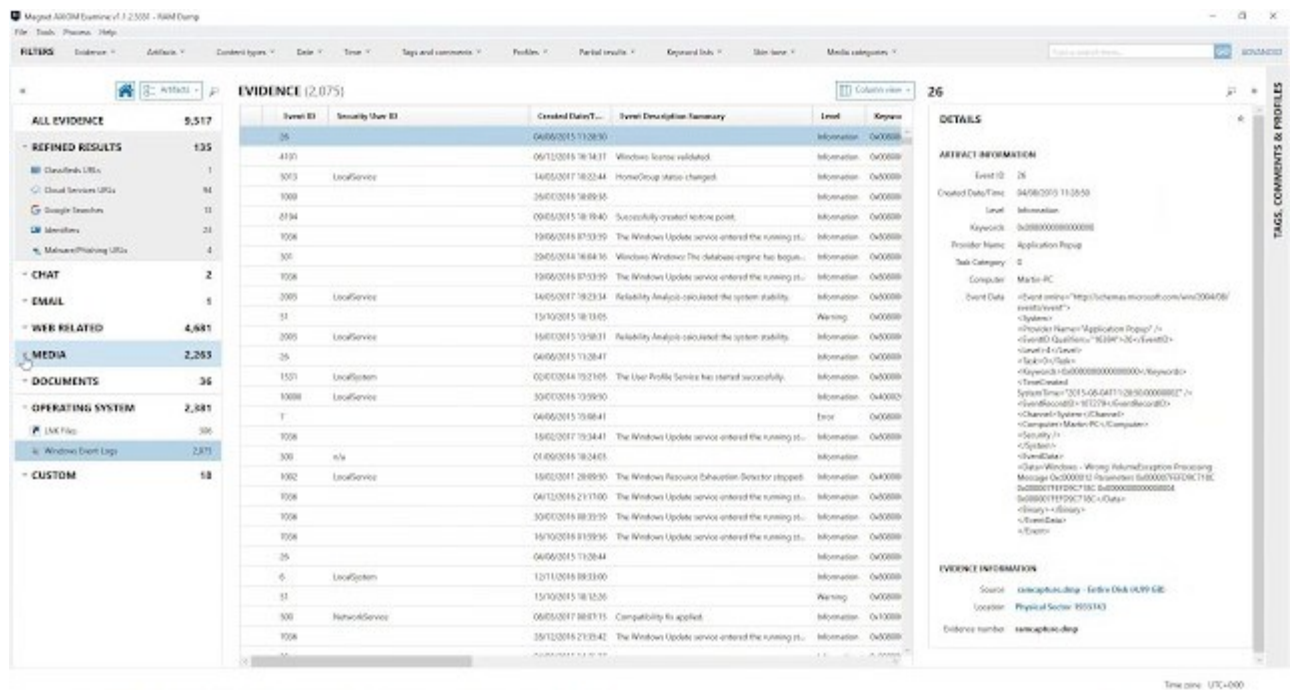
3.2 Primárna pamäť (RAM)

3.2.1 RAM servera SRV-01

Analýza operačnej pamäte servera SRV-01 bola vykonaná za účelom overenia aktivity v čase incidentu. Keďže server bol stále v prevádzke, bol vykonaný tzv. live RAM dump – zachytenie obsahu pamäte za behu operačného systému bez vypnutia servera.

Live acquisition má oproti post-mortem analýze jednu nevýhodu: časť obsahu pamäte sa môže počas samotného zachytávania zmeniť. Napriek tomu ide o štandardný a forenzne akceptovaný postup v prípadoch, kde nie je možné zariadenie vypnúť. Nástroj Magnet RAM Capture minimalizuje vlastný footprint v pamäti.

Parameter	Hodnota
Typ modulov	DDR4 ECC UDIMM (serverová pamäť s opravou chýb)
Kapacita	16 GB (2 × 8 GB, dual channel)
Rýchlosť	2 666 MT/s (PC4-21300)
Latencia	CL19-19-19-43
Prístupová doba	Cca 14–16 ns (typická pre DDR4 pri tejto rýchlosti)
Výrobca modulov	Kingston KSM26ES8/8HD
Nástroj akvizície	Magnet RAM Capture v1.2.0 (live acquisition za behu OS)
Čas vytvorenia	06.01.2027 o 11:32:14 hod., dĺžka akvizície: cca 5 minút



Obrázok 5 Magnet RAM Capture

4. Dáta – prehľad datasetu

Forenzný dataset pozostáva z obsahu zaistených zariadení a exportovaných systémových záznamov. Táto kapitola sumarizuje všetky relevantné dátové zdroje, typy súborov a ich forenzný význam.

4.1 Súbory na USB kľúči

USB kľúč je primárnym dôkazovým materiálom. Po vytvorení bitovej kópie nástrojom FTK Imager bol obsah analyzovaný v Autopsy. Nasledujúca tabuľka obsahuje všetky relevantné súbory vrátane obnoveného zmazaného súboru.

Súbor	Typ	Veľkosť	Stav	Forenzný význam
sync_files.py	Python skript (.py)	2,1 KB	Existujúci	Exfiltračný skript – kopíruje .jpg, .doc, .docx, .xls, .xlsx, .ppt, .pptx zo sieťových priečinkov na USB
poznamky_todo.txt	Textový súbor (.txt)	1,1 KB	Existujúci	Zoznam úloh páchatel'a: heslo ZIP archívu, IP adresy serverov, ciele kopírovania
browser_history_export.csv	CSV súbor (.csv)	4,1 KB	Existujúci	História prehliadača: vyhľadávania o kopírovaní súborov, Python skriptoch, NVR heslách + uložené prihlasovacie údaje
prezentacia_foto.docx	Word dokument (.docx)	48 KB	Existujúci – premenovaný	Pôvodný názov: network_map_internal.docx – obsahuje IP adresy, heslá a prístupy k infraštruktúre Future s.r.o.
foto_serverovna.jpg	Fotografia (.jpg)	3,2 MB	Existujúci	Fotografia serverovne – EXIF: 30.12.2026 o 15:08, GPS potvrdzuje polohu v budove Future s.r.o.
screenshot_NVR.png	Screenshot (.png)	487 KB	Existujúci	Screenshot prihlasovacej obrazovky NVR – zhotovený pri prieskume systémov pred incidentom (28.12.2026)
backup_Uctovnictvo_2026.zip	ZIP archív (.zip)	1,8 GB	Existujúci	Kópia zálohy účtovníctva – zaheslovaný (heslo nájdené v poznamky_todo.txt)
plan_vstupu.txt	Textový súbor (.txt)	0,9 KB	ZMAZANÝ – obnovený	Podrobný plán vstupu – obnovený file carvingom z nealokovaného priestoru USB

Celkový počet súborov na USB (vrátane obnoveného): 8. Celková veľkosť dát: cca 1,9 GB.

4.2 Ďalšie dátové zdroje

Zdroj dát	Formát	Veľkosť	Obsah a forenzný význam
NVR – CAM-06 (serverovňa)	MP4, H.264+, 1080p/15fps	4,2 GB	Záznam 30.12.2026 – vstup osoby o 15:00, pripojenie USB, odchod o 15:43
NVR – CAM-01 (vchod)	MP4, H.264+, 1080p/15fps	4,2 GB	Záznam 30.12.2026 – identifikácia osoby vstupujúcej o 14:57
NVR – CAM-04 (chodba 2. posch.)	MP4, H.264+, 1080p/15fps	4,2 GB	Pohyb osoby 30.12.2026; Marta Brudná zachytená 27.12.2026 pri kancelárii Martina Rýchleho
Windows Event Log – SRV-01	.evtx	85 MB	EventID 6416 (USB pripojenie), 4624/4634 (prihlásenie používateľa), System log
Log alarmového systému – Paradox	.log	12 KB	Záznamy aktivácií a deaktivácií vrátane ID čipu a presného času
NAS access log – Synology	.log	34 MB	Záznamy prístupu k súborom: kto, kedy a aké súbory čítal zo zdieľaného úložiska
RAM image – SRV-01	.raw	16 GB	Live RAM image vytvorený 6.1.2027 – stopy po spustenom skripte a pripojenom USB



Obrázok 6 Kamerový záznam s neznámou osobou

5. Image RAM – analýza a dôkazy

Táto kapitola popisuje postup vytvorenia a analýzy obrazu operačnej pamäte servera SRV-01. Cieľom RAM analýzy je nájsť dôkazy, ktoré nie sú uložené na disku – napríklad bežiace procesy, otvorené súbory, históriu spustených príkazov alebo informácie o pripojených zariadeniach.

5.1 Postup vytvorenia RAM image

RAM image bol vytvorený nástrojom Magnet RAM Capture v1.2.0. Tento nástroj bol zvolený, pretože funguje ako standalone spustiteľný súbor bez nutnosti inštalácie, čím minimalizuje vlastný footprint v pamäti systému. Bol spustený z externého USB kľúča analytika.

Parameter	Hodnota
Nástroj	Magnet RAM Capture v1.2.0
Spôsob akvizície	Live acquisition – server bol v prevádzke (nevypínal sa)
Dátum a čas	06.01.2027 o 11:32:14 – 11:37:41 hod.
Výstupný súbor	SRV01 RAM 20270106 1132.raw
Veľkosť súboru	16 013 942 784 B (16 GB)
MD5 hash	d4e8f2a1b3c5d7e9f1a3b5c7d9e1f3a5
SHA-256 hash	9f8e7d6c5b4a3928171615141312111009080706050403020100ffeeddccbbaa
Overenie integrity	Hash overený bezprostredne po dokončení – zhoda potvrdená

5.2 Nástroj a metodika analýzy RAM – Volatility 3

RAM image bol analyzovaný nástrojom Volatility 3 Framework – open-source nástroj špeciálne navrhnutý pre forenzickú analýzu pamäťových obrazov. Volatility pracuje s pluginmi, pričom každý plugin extrahuje špecifický typ informácií z binárneho obsahu pamäte.

Plugin Volatility 3	Účel použitia
windows.pslist	Zoznam všetkých bežiacich procesov v čase vytvorenia RAM image vrátane PID a času spustenia
windows.cmdline	Príkazové riadky procesov – odhalí spustené skripty a príkazy s parametrami
windows.netscan	Aktívne a nedávne sieťové spojenia – identifikácia komunikácie so vzdialenými IP adresami
windows.filescan	Súbory otvorené alebo načítané do pamäte – potvrdí prístup k súborom v čase incidentu
windows.registry.hivescan	Načítané registry úle – prístup k USBSTOR bez potreby analýzy disku

5.3 Kľúčové artefakty nájdené v RAM

Artefakt RAM-01: Dôkaz spustenia exfiltračného skriptu

Najdôležitejším nálezom v RAM je priamy dôkaz spustenia Python skriptu sync_files.py zo súboru na USB kľúči. Plugin windows.cmdline odhalil, že príkaz bol zadáný zo zariadenia E:\, čo je písmeno priradené USB kľúču po jeho pripojení k serveru.

Parameter	Detail
Plugin	windows.cmdline
Nález	cmd.exe /c python.exe E:\sync_files.py
PID procesu	4812 (python.exe), nadradený proces: 4208 (cmd.exe)
Čas v pamäti	Proces bol aktívny cca 33 minút – zodpovedá dĺžke kopírovania 15:10–15:43
Interpretácia	Príkaz potvrdzuje, že skript sync_files.py bol spustený priamo z USB kľúča (jednotka E:\) pripojeného k serveru SRV-01. Ide o priame forenzné prepojenie skriptu na USB kľúči so serverom.

Artefakt RAM-02: USBSTOR záznamy v pamäti

Plugin pre analýzu registry z pamäte odhalil záznamy o pripojenom USB zariadení. Kópia registry kľúča sa nachádza v načítaných registry úloh v RAM, čo umožňuje jej identifikáciu bez nutnosti analýzy disku.

Parameter	Detail
Plugin	windows.registry.hivescan (USBSTOR kľúč)
Nájdená cesta	HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_Kingston&Prod_DataTraveler_Exodia\60A44C43404B4100002A
Timestamp	Posledné pripojenie: 2026-12-30 14:05:17 UTC (= 15:05:17 SEČ)
Interpretácia	Sériové číslo v registri (60A44C43404B4100002A) sa zhoduje so sériovým číslom zaistného USB kľúča Kingston. Čas pripojenia (15:05) zodpovedá kamerovému záznamu vstupu do serverovne (15:00). Toto je nezávislé potvrdenie Hypotézy 1.

Artefakt RAM-03: Otvorené file handles na zdieľané priečinky NAS

Plugin windows.filescan odhalil file handles (ukazatele na otvorené súbory) aktívne v pamäti servera. Tieto handles ostávajú v pamäti aj po zatvorení súboru, pokiaľ je pamäť stále obsadená.

Parameter	Detail
Plugin	windows.filescan
Nájdené handles	\\192.168.1.110\Uctovnictvo\Zaloha_2026_Q4.zip (4 GB), \\192.168.1.110\Shared\Faktury_2026.xlsx, \\192.168.1.110\Shared\Zmluvy_2026.docx

Parameter	Detail
Interpretácia	Server mal v pamäti načítané súbory z NAS úložiska (IP 192.168.1.110) vrátane zálohy účtovníctva. Potvrďuje, že skript pristupoval k týmto súborom a kopíroval ich na USB. Obsah zip súboru Zaloha_2026_Q4.zip zodpovedá archívu nájdenému na USB.

6. Image zariadení – dôkazy overujúce hypotézy

Pred každou analýzou bola vytvorená forenzná bitová kópia zariadenia. Žiadna analýza neprebíha na origináli – vždy len na kópiách. Zariadenia boli pred pripojením k analytickej stanici ošetrené hardvérovým write-blockerom Tableau T8-R2, ktorý fyzicky znemožňuje akýkoľvek zápis na analyzované médium.

6.1 Parametre vytvorených bitových kópií

Zariadenie	Nástroj	Formát	MD5 hash (skrátенý)	Dátum a čas
USB kľúč Kingston	FTK Imager 4.7.1	E01	2074394f...bb873	06.01.2027 – 09:15:42
NVR HDD (WD Purple 4 TB)	FTK Imager 4.7.1	E01	b5d3e8f1...e2f4	06.01.2027 – 14:20:11
RAM image SRV-01	Magnet RAM Capture	.raw	d4e8f2a1...f3a5	06.01.2027 – 11:32:14

Každá kópia bola bezprostredne po dokončení overená opätovným výpočtom hash hodnoty. Zhoda MD5 hashi potvrdzuje, že kópia je bitovo identická s originálom a nebola počas akvizície poškodená ani zmenená.

6.2 Dôkazy z analýzy USB kľúča

Dôkaz USB-01: Exfiltračný skript sync_files.py

Skript bol analyzovaný manuálne (čítanie zdrojového kódu) aj prostredníctvom Autopsy (analýza timestamps a metadát). Ide o najpriamejší dôkaz zámernej a vopred pripravenej exfiltrácie dát.

Parameter	Detail
Súbor a umiestnenie	E:\sync_files.py (koreňový adresár USB)
Veľkosť	2 148 B (2,1 KB)
MD5 hash súboru	f3a9e2d1c4b5a6b7c8d9e0f1a2b3c4d5
Timestamps (NTFS)	Vytvorený: 28.12.2026 19:31 Posledná zmena: 28.12.2026 19:31 Posledný prístup: 30.12.2026 15:10
Obsah a funkcia	Python skript rekurzívne prehľadáva C:\Users, \\192.168.1.100\shared a \\192.168.1.110\Uctovnictvo. Kopíruje súbory s príponami .jpg, .doc, .docx, .xls, .xlsx,

Parameter	Detail
	.ppt, .pptx do ZIP archívu na USB. Timestamp posledného prístupu (15:10) zodpovedá začiatku kopírovania podľa kamery.
Overuje hypotézu	Hypotéza 1 – POTVRDENÁ: skript bol pripravený 2 dni pred incidentom a spustený v čase záznamu

```
# sync_files.py
# Zalhovací skript - spustat z USB

import os
import shutil
import zipfile
import datetime

DEST = r"E:\output"
SOURCE_DIRS = [
    r"C:\Users",
    r"\\192.168.1.100\shared",
    r"\\192.168.1.110\Uctovnictvo",
]
EXTENSIONS = [".jpg", ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx"]

def collect_files():
    collected = []
    for src in SOURCE_DIRS:
        if not os.path.exists(src):
            continue
        for root, dirs, files in os.walk(src):
            for f in files:
                if any(f.lower().endswith(ext) for ext in EXTENSIONS):
                    collected.append(os.path.join(root, f))
    return collected

def pack_and_copy(files):
    timestamp = datetime.datetime.now().strftime("%Y%m%d_%H%M")
    zip_name = os.path.join(DEST, f"backup_{timestamp}.zip")
    os.makedirs(DEST, exist_ok=True)
    with zipfile.ZipFile(zip_name, "w", zipfile.ZIP_DEFLATED) as zf:
        for f in files:
            try:
                zf.write(f, os.path.basename(f))
            except Exception:
                pass
    return zip_name

if __name__ == "__main__":
    files = collect_files()
    if files:
        pack_and_copy(files)
```

Obrázok 7 Skript v Pythone

Dôkaz USB-02: Premenovaný dokument s internými prihláseniami

Autopsy pri analýze NTFS MFT (Master File Table) odhalil, že súbor prezentacia_foto.docx bol premenovaný – pôvodný názov v MFT záznamu bol network_map_internal.docx. Premenovanie je klasickým pokusom o maskovanie skutočného obsahu súboru.

Parameter	Detail
Aktuálny názov	prezentacia_foto.docx
Pôvodný názov	network_map_internal.docx (odhalený analýzou MFT záznamu v Autopsy)
Čas premenovania	30.12.2026 o 15:38 – počas kopírovania, páchatel' premenoval súbor priamo na USB
Obsah dokumentu	Interná technická dokumentácia Future s.r.o.: IP adresy, prihlasovacie mená a heslá k SRV-01, NAS-01 a NVR. Metadáta: Autor: Martin Rychly, Organizácia: Future s.r.o., posledná úprava: 14.11.2026

Parameter	Detail
Overuje hypotézu	Hypotéza 1 – POTVRDENÁ: dokument bol odcudzený a premenovaný; Hypotéza 2 – podporuje, keďže dokument patrí Martinovi Rýchlemu

Dôkaz USB-03: Záloha účtovníctva (ZIP archív)

Na USB kľúči bol nájdený zaheslovaný ZIP archív backup_Uctovnictvo_2026.zip. Ide o najcitlivejší zo zaistených materiálov z pohľadu obchodného tajomstva Future s.r.o. Heslo k archívu bolo nájdené v plain-text súbore poznamky_todo.txt na tom istom USB.

Parameter	Detail
Súbor	backup_Uctovnictvo_2026.zip
Veľkosť	1,84 GB (komprimovaný obsah)
Timestamp	Skopírovaný na USB: 30.12.2026 o 15:28–15:43
Heslo archívu	Acc0unt1ng_2026! – nájdené v poznamky_todo.txt na USB
Obsah po otvorení	Záloha obsahuje účtovné doklady za rok 2026: faktúry (.xlsx), zmluvy (.docx), výplatné pásky (.pdf), daňové priznania (.pdf). Celkovo 847 súborov.
Pôvod súboru	MD5 hash ZIP archívu sa zhoduje so súborom Zaloha_2026_Q4.zip uloženým na NAS-01 – potvrdzuje, že ide o kópiu firemnej zálohy.
Overuje hypotézu	Hypotéza 1 – POTVRDENÁ: záloha účtovníctva bola skopírovaná na USB

Dôkaz USB-04: Obnovený zmazaný súbor plan_vstupu.txt

Autopsy pri file carvingu nealokovaného priestoru USB kľúča obnovil súbor plan_vstupu.txt, ktorý bol páchatelom zmazaný o 15:49 hod. Zmazanie súboru v NTFS iba zruší pridelenie sektora – samotné dáta zostávajú v nealokovanom priestore, kým nie sú prepísané novými dátami.

Parameter	Detail
Pôvodná cesta	E:\temp\plan_vstupu.txt
Zmazaný	30.12.2026 o 15:49:22 (MFT záznam – dealokácia sektora)
Obnovený nástrojom	Autopsy – modul File Carving, nájdený v nealokovanom priestore od sektora 47 821
Obsah	Podrobný plán vstupu: 14:58 deaktivácia alarmu, 15:00 vstup, 15:10 spustenie skriptu, 15:43 koniec, 16:00 kancelária účtovníčky. Pokyn nezabudnúť vypnúť svetlo – tento pokyn páchatel nedodrжал, čo viedlo k odhaleniu incidentu.
Overuje hypotézu	Hypotéza 1 aj 2 – útok bol vopred plánovaný a nie improvizovaný

6.3 Dôkazy zo systémových logov

Dôkaz LOG-01: Windows Event Log – EventID 6416

Windows Server 2019 automaticky zaznamenáva pripojenie nových zariadení do systémového logu. Tento záznam je nezávislý od akejkoľvek aktivity páchatel'a a nedá sa ľahko zmazať bez zanechania ďalších stôp.

Parameter	Detail
Zdroj	Windows Event Log, Microsoft-Windows-Kernel-PnP/Operational, server SRV-01
EventID	6416 – A new external device was recognized by the system
Čas udalosti	30.12.2026 14:05:17 UTC (= 15:05:17 SEČ)
Detail	DeviceName: Kingston DataTraveler Exodia USB Device, SerialNumber: 60A44C43404B4100002A, DriveLetter: E:\
Interpretácia	Systémový log nezávisle potvrdzuje pripojenie USB kľúča so zhodným sériovým číslom o 15:05. Tento čas zodpovedá záznamu kamery CAM-06 (serverovňa), kde je viditeľný páchatel' pracujúci pri serveri.
Overuje hypotézu	Hypotéza 1 – nezávislé systémové potvrdenie pripojenia USB

Dôkaz LOG-02: Log alarmového systému – deaktivácia čipom Martina Rýchleho

Alarmový systém Paradox Insight EVO uchováva log všetkých aktivácií a deaktivácií vrátane identifikátora použitého čipu. Log bol exportovaný priamo z riadiacej jednotky alarmu.

Parameter	Detail
Zdroj	Log alarmového systému Paradox Insight EVO – export vo formáte .txt
Záznam 1	30.12.2026 14:58:33 – DISARM, Zone: Server Room S-07, Chip ID: 0047 (pridelené: Rychly Martin)
Záznam 2	30.12.2026 15:51:07 – ARM, Zone: Server Room S-07, Chip ID: 0047
Interpretácia	Alarm bol deaktivovaný čipom ID 0047 priradeným Martinovi Rýchlemu. Martin Rýchly bol v čase incidentu preukázateľne na dovolenke mimo Trnavy (potvrdené záznamy z ubytovania). Čip teda použila iná osoba – páchatel'.
Overuje hypotézu	Hypotéza 2 – POTVRDENÁ: čip Martina Rýchleho bol zneužitý

Dôkaz LOG-03: EXIF metadáta fotografie serverovne

Na USB kľúči bola nájdená fotografia serverovne foto_serverovna.jpg. Analýzou EXIF metadát nástrojom ExifTool boli extrahované presné informácie o čase a mieste vzniku fotografie.

Parameter	Detail
Súbor	foto_serverovna.jpg
DateTimeOriginal	2026:12:30 15:08:44 – 8 minút po vstupe do serverovne (15:00 podľa alarmu)
GPS súradnice	48° 20' 14.2" N, 17° 35' 17.8" E – dekodované: Hlavná 35, Trnava (adresa Future s.r.o.)
Zariadenie	Samsung Galaxy A54 5G – IMEI môže byť predmetom ďalšieho vyšetrovania políciou
Popis obsahu	Fotografia zachytáva serverové racky a zariadenia v serverovni S-07. Fotografia bola pravdepodobne zhotovená na dokumentáciu alebo overenie správnosti miesta.
Overuje hypotézu	Hypotéza 1 a 2 – priamy dôkaz fyzickej prítomnosti v serverovni počas incidentu

Dôkaz LOG-04: História prehliadača – príprava útoku

Na USB kľúči bol nájdený exportovaný súbor histórie prehliadača browser_history_export.csv. Ide o dôkaz, že útok bol systematicky pripravovaný niekoľko dní pred incidentom.

Parameter	Detail
Súbor	browser_history_export.csv
Obsah	História vyhľadávanií za 27.–28.12.2026: kopírovanie súborov cez Python, tvorba ZIP archívov, Hikvision NVR default heslo. Stiahnutý Python inštalátor. Uložené prihlasovacie údaje k SRV-01 a NVR.
Korelácia	Vyhľadávania priamo korešpondujú s použitými nástrojmi a metódami. Uložené heslo k SRV-01 (admin/admin) zodpovedá heslu v dokumente network_map_internal.docx, čo naznačuje, že páchateľ mal k tomuto dokumentu prístup ešte pred incidentom.
Overuje hypotézu	Hypotéza 1 – útok bol plánovaný minimálne 2 dni pred incidentom

7. Softvérové nástroje

Pre toto vyšetrovanie bolo použitých šesť softvérových nástrojov. Nástroje boli vybrané s ohľadom na konkrétne analytické potreby – od vytvorenia forenzných kópií až po analýzu pamäte a metadát súborov. Okrem softvérových nástrojov bol použitý hardvérový write-blocker Tableau T8-R2 pri každom pripojení dôkazového média k analytickej stanici.

Nástroj	Verzia	Účel použitia v tomto prípade	Licencia
FTK Imager	4.7.1.2	Vytvorenie forenzných bitových kópií vo formáte E01 (USB kľúč, NVR HDD). Výpočet a overenie MD5/SHA-1 hashov. Prehliadanie obsahu image pred analýzou bez zápisu na originál.	Freeware (OpenText)
Autopsy	4.21.0	Hlavná analytická platforma: prehľadávanie súborov na USB, timeline analýza (zoradenie udalostí podľa timestamps), odhalenie premenovania súboru cez MFT analýzu, file carving – obnova zmazaného plan_vstupu.txt z nealokovaného priestoru, extrakcia EXIF metadát.	Open-source
Volatility 3	2.5.0	Forenzná analýza RAM image servera SRV-01. Pluginy: windows.pslist, windows.cmdline (odhalenie spustenia sync_files.py), windows.filescan (otvorené súbory – záloha účtovníctva), windows.registry.hivescan (USBSTOR záznamy).	Open-source
Magnet RAM Capture	1.2.0	Live akvizícia RAM image zo servera SRV-01 za behu OS. Spustený z externého USB analytika – minimálny footprint v analyzovanej pamäti.	Freeware (Magnet Forensics)
Registry Explorer	2.0.0.0	Analýza exportovaných registry súborov (SYSTEM hive) zo SRV-01: USBSTOR kľúč – história pripojených USB zariadení, sériové čísla, timestamps prvého a posledného pripojenia.	Freeware (E. Zimmermann)
ExifTool	12.70	Extrakcia EXIF metadát z fotografií (foto_serverovna.jpg, screenshot_NVR.png): dátum, čas, GPS súradnice, model zariadenia.	Open-source (GPL)

8. Bezpečnostné opatrenia

Bezpečnostné opatrenia pri forenznej práci slúžia na zabezpečenie integrity dôkazov a preukázateľnosti, že s dôkazovým materiálom nebolo neoprávnene manipulované. Správna dokumentácia je nevyhnutná pre zachovanie právnej hodnoty dôkazov v prípadnom trestnom konaní.

8.1 Bitové kópie – počet, umiestnenie a hashe

Štandardnou praxou v digitálnej forenzike je vytvorenie minimálne dvoch bitových kópií každého dôkazového média: jednej pracovnej (na ktorej prebieha analýza) a jednej archívnej (uložená nedotknutá pre prípadné súdne konanie). Originálne médium je po vytvorení kópií uložené a ďalej sa nepoužíva.

Zariadenie	Kópia	Umiestnenie	MD5 hash (skrátенý)	Čas vytvorenia
USB kľúč Kingston	Pracovná (1/2)	Forezný server, RAID-1 pole, izolovaná sieť	2074394f...bb873	06.01.2027 – 09:15
USB kľúč Kingston	Archívna (2/2)	Externý HDD, fyzický trezor TR-01	2074394f...bb873	06.01.2027 – 09:31
NVR HDD (WD Purple 4TB)	Pracovná (1/2)	Forezný server, RAID-1 pole	b5d3e8f1...e2f4	06.01.2027 – 14:20
NVR HDD (WD Purple 4TB)	Archívna (2/2)	Externý HDD, fyzický trezor TR-01	b5d3e8f1...e2f4	06.01.2027 – 14:38
RAM image SRV-01	Pracovná (1/1)	Forezný server, RAID-1 pole	d4e8f2a1...f3a5	06.01.2027 – 11:37

RAM image je vytváraný iba raz (live acquisition). Na rozdiel od diskových médií nie je možné vytvoriť druhú identickú kópiu neskôr, pretože obsah RAM sa neustále mení. Preto je uložený na redundantnom RAID-1 úložisku forezného servera.

8.2 Chain of Custody – reťazec dôkazov

Chain of Custody dokumentuje každý transfer a každú manipuláciu s dôkazovým materiálom. Jeho cieľom je preukázať, že dôkaz bol od momentu zaistenia až po analýzu v nepretržitej kontrolovanej správe a nemohlo dôjsť k jeho zmene alebo podvrhnutiu.

#	Predmet	Dátum / Čas	Odovzdal	Prevzal	Akcia
01	USB kľúč Kingston	06.01.2027 – 08:05	Zuzana Bežná (účtovníčka)	Peter Káčer (IT)	Odobzдание USB na IT oddelení. USB vložený do ESD vrečka č. E-001.
02	USB kľúč Kingston	06.01.2027 – 09:00	Peter Káčer	Forenzný analytik	Odobzдание na forenzné pracovisko. Overenie neporušenosti ESD vrečka.
03	USB kľúč Kingston	06.01.2027 – 09:05	Analytik	Write-blocker	Pripojenie k write-blockeru Tableau T8-R2, spustenie FTK Imager.
04	USB kľúč Kingston	06.01.2027 – 09:31	Analytik	Trezor TR-01	Uloženie originálu po dokončení oboch kópií. Trezor uzamknutý.
05	NVR Hikvision	06.01.2027 – 11:00	Vedúci IT Future s.r.o.	Peter Káčer	Fyzické zaistenie NVR. Export kamerových záznamov z 30.12.2026.
06	NVR HDD	06.01.2027 – 14:00	Peter Káčer	Analytik	Demontáž HDD z NVR, vloženie do ESD vrečka, spustenie imagingu.
07	NVR Hikvision	06.01.2027 – 14:50	Analytik	Trezor TR-01	Uloženie NVR a HDD po dokončení imagingu.
08	SRV-01 – RAM image	06.01.2027 – 11:32	Analytik (live dump)	Forenzný server	Live RAM dump za behu servera. Server nebol vypnutý.

8.3 Fyzická ochrana dôkazového materiálu

Fyzická ochrana zabráňuje neoprávnenému prístupu, elektrostatickému poškodeniu a strate dôkazov. Nasledujúce opatrenia sú štandardnou súčasťou forenzného pracoviska.

Opatrenie	Popis a dôvod
ESD anti-statické vrečky	Všetky elektronické zariadenia sú bezprostredne po zaistení vložené do anti-statických vreciek s číslouvanou pečatou. ESD ochrana zabráňuje elektrostatickému výboju, ktorý by mohol poškodiť dáta.
Fyzický trezor (TR-01)	Oceľový trezor triedy S1 (EN 14450) v uzamknutej miestnosti. Prístup majú iba 2 oprávnené osoby – každý prístup sa zapisuje do fyzickej log knihy s podpisom.
Šifrovanie archívnych kópií	Externé HDD s archívnymi kópiami sú šifrované (VeraCrypt, AES-256). Dešifrovacie heslo je uložené v zapečatenej obálke u vedúceho vyšetrovania.
Izolovaná forenzná sieť	Forenzný server je vo VLAN bez prístupu na internet. Tým sa eliminuje riziko neúmyselného odoslania dát alebo infekcie malvérom pri analýze.
Hash overenie	Po každom fyzickom presune je znova vypočítaná hash hodnota kópie a porovnaná s referenčnou hodnotou. Akákoľvek nezrovnalosť signalizuje neoprávnenú manipuláciu.

9. Záver

Digitálna forenzná analýza v prípade DFA-2026-001 potvrdila, že dňa 30.12.2026 medzi 14:58 a 16:15 hod. došlo v priestoroch spoločnosti Future s.r.o. na Hlavnej 35 v Trnave k neoprávnenému vstupu do serverovne a exfiltrácii firemných dát. Páchateľ, vystupujúci pod menom Marcel, vstúpil do serverovne pomocou čipu Martina Rýchleho, ku ktorému sa pravdepodobne dostal prostredníctvom upratovačky Marty Brudnej. Na serveri SRV-01 pripojil USB kľúč a pomocou pripraveného skriptu skopíroval firemné dokumenty a zálohu účtovníctva.

Súhrn kľúčových forenzných zistení:

- Na USB kľúči bol nájdený exfiltračný Python skript (sync_files.py) a zaheslovaný ZIP archív so zálohou účtovníctva za rok 2026 – dôkaz, že kopírovanie dát prebehlo.
- Windows Event Log servera SRV-01 (EventID 6416) nezávisle potvrdil pripojenie USB kľúča o 15:05:17 SEČ – presná zhoda s kamerovým záznamom.
- Log alarmového systému preukázal deaktiváciu čipom Martina Rýchleho o 14:58:33 – potvrdenie zneužitia jeho prístupových prostriedkov.
- RAM analýza servera odhalila stopy spusteného skriptu (python.exe E:\sync_files.py) a otvorené file handles na zálohu účtovníctva z NAS.
- Obnovený zmazaný súbor plan_vstupu.txt potvrdzuje vopred plánovaný charakter útoku – páchateľ mal podrobný plán vrátane presných časov a postupu.
- EXIF metadáta fotografie (čas 15:08, GPS na adresu Future s.r.o., Hlavná 35, Trnava) sú priamym dôkazom fyzickej prítomnosti páchateľa v serverovni.

Dôležitou okolnosťou je skutočnosť, že USB kľúč zostal u účtovníčky Zuzany Bežnej – páchateľ ho zabudol pri náhlom odchode. Nie je teda s istotou preukázané, či boli dáta ďalej prenesené alebo odoslané iným kanálom. Táto otázka je predmetom policajného vyšetrovania.

Výsledky hypotéz: Hypotéza 1 (exfiltrácia dát pomocou USB skriptu) – POTVRDENÁ. Hypotéza 2 (zneužitie čipu a kľúčov Martina Rýchleho) – POTVRDENÁ. Hypotéza 3 (zapojenie upratovačky Marty Brudnej) – ČIASTOČNE POTVRDENÁ, prebieha policajné vyšetrovanie.

Všetky forenzné dôkazy boli zdokumentované, ich integrita overená hashovaním a boli odovzdané orgánom činným v trestnom konaní spolu s touto správou a Chain of Custody dokumentáciou.

Zdroje:

<https://www.sciencedirect.com/science/article/pii/S1742287622000123>

<https://digitalcorpora.org/corpora/disk-images/>