

Podvrhnuté falošné faktúry

SEMESTRÁLNY PROJEKT

[Prezentácia](#)

Contents

1	Názov prípadu a zhrnutie	4
1.1	Stručne zadefinovaný prípad	4
1.2	Odborný príspevok.....	4
1.3	5W + H analýza	4
1.5	Ciele vyšetrovania	4
2	Hypotézy.....	5
	H1: Peter Blaho faktúry pozmenil sám a vedome ich odoslal	5
	H2: Faktúry pozmenil neznámy páchatel' s fyzickým prístupom do kancelárie.....	5
	H3: Faktúry pozmenil Martin Šimko — identifikovaný podozrivý	5
	H4: Na podvrhnutie bol použitý externý USB nosič.....	6
	H5: Originálne faktúry existovali a boli úmyselne zmazané	6
3	Digitálne zariadenia	6
3.1	Petrov pracovný notebook — primárne zariadenie.....	6
3.2	Martinov pracovný PC — zariadenie podozrivého	7
3.3	USB kľúč — nezaistené zariadenie.....	8
4	Dáta — typy súborov a dataset.....	9
5	Image RAM — analýza a artefakty.....	11
5.1	Zachytenie RAM	11
5.2	Artefakty nájdené v pamäti RAM na Martinovom PC.....	11
	Petrov PC.....	12
6	Image zariadení — kľúčové dôkazy.....	12
6.1	Forenzné obrazy.....	12
6.2	Kľúčové dôkazy	12
	Dôkaz 1 — Metadata sfalšovaných faktúr (overuje H1, H3).....	12
	Dôkaz 3 — CreationDate (overuje H2, H5).....	18
	Dôkaz 4 — Záznamy o USB zariadení (overuje H4)	19
	Dôkaz 5 — Obnovenie originálnej faktúry (overuje H5).....	22
7	Použité softvérové nástroje.....	25
8	Bezpečnostné opatrenia	27
8.1	Fyzická ochrana	27
8.2	Počet bitových kópií a ich uloženie	27
	Chain of Custody — Petrov notebook (disk image)	27
9	Časová os incidentu.....	33
10	Výsledok hypotéz.....	34
9.1	Hypotéza H1 – Zamietnutá	34
9.2	Hypotéza H2 – Čiastočne potvrdená	35

9.3 Hypotéza H3 – Čiastočne potvrdená	35
9.4 Hypotéza H4 – Potvrdená.....	35
9.5 Hypotéza H5 – Potvrdená.....	35
11 Literatúra.....	35

1 Názov prípadu a zhrnutie

1.1 Stručne zadefinovaný prípad

Dňa 11. novembra 2025 odoslal zamestnanec Peter Blaho z firemného e-mailového účtu faktúry na účtovné oddelenie spoločnosti. Účtovné oddelenie zistilo, že faktúry obsahujú pozmenené bankové údaje — IBAN príjemcu bol zmenený na účet spoločnosti Blaho Consulting s.r.o., ktorej konateľom je Peter Blaho. Peter Blaho tvrdí, že mu boli súbory podvrhnuté bez jeho vedomia. Spoločnosť podala trestné oznámenie a prípad bol postúpený na forenzné vyšetrowanie.

1.2 Odborný príspevok

Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley.

Publikácia systematicky opisuje štruktúru súborových systémov NTFS a metódy forenznej analýzy — vrátane čítania \$MFT záznamov, rekonštrukcie zmazaných súborov a interpretácie časových pečiatok (MACE). Priamo využiteľné pri overovaní hypotézy H5 (zmazanie originálov) a pri analýze CreationDate paradoxu ako kľúčového dôkazu podvrhnutia.

Link: <https://repo.zenk-security.com/Forensic/File%20System%20Forensic%20Analysis.pdf>

1.3 5W + H analýza

Otázka	Odpoveď
Who (Kto)	Peter Blaho — zamestnanec, z ktorého účtu boli odoslané faktúry. Tvrdí, že mu boli súbory podvrhnuté. Totožnosť skutočného páchatel'a je predmetom vyšetrowania. Ako podozrivý bol identifikovaný kolega Martin Šimko.
What (Čo)	Odoslanie faktúr s pozmeneným IBAN-om na účet Blaho Consulting s.r.o. (firma v Petrovom vlastníctve) — navonok vyzerá ako úmyselné tunelovanie firemných prostriedkov.
When (Kedy)	11.11.2025 o 14:31 — čas odoslania e-mailu. Manipulácia so súbormi prebehla v ten istý deň v dvoch oknách neprítomnosti Petra (11:30–11:50 a 14:05–14:16).
Where (Kde)	Firemné priestory — kancelária Petra Blaha, jeho pracovný notebook (Dell Latitude 5540), pracovný PC Martina Šimka (Lenovo ThinkCentre M70s) a firemný Exchange server.
Why (Prečo)	Buď finančný podvod (tunelovanie) zo strany Petra, alebo úmyselné poškodenie Petra osobou s fyzickým prístupom do kancelárie (motív: závisť po Petrovom povýšení dňa 10.11.2025).
How (Ako)	Faktúry mohli byť pozmenené priamo Petrom, alebo mohol niekto s fyzickým prístupom k jeho notebooku vymeniť súbory cez USB nosič počas dvoch okien Petrovej neprítomnosti.

1.5 Ciele vyšetrowania

- Identifikovať autora sfalšovaných faktúr z metadát dokumentov.
- Overiť, ako sa informácia o IBAN-e Blaho Consulting s.r.o. dostala k páchatel'ovi.
- Preskúmať záznamy o USB pripojeniach na oboch PC a korelovať ich s časovými oknami Petrovej neprítomnosti.
- Rekonštruovať presnú časovú os udalostí z Event Logov, \$MFT a setupapi.dev.log.
- Analyzovať RAM obrazy — potvrdiť aktivitu procesov, clipboard artefakty a sieťové spojenia.
- Obnoviť zmazané originálne faktúry z nealokovaného priestoru SSD Petrovho notebooku.
- Analyzovať záznamy Exchange servera — overiť IP adresu a autentifikáciu odosielateľa.

2 Hypotézy

H1: Peter Blaho faktúry pozmenil sám a vedome ich odoslal

Peter mal ako zamestnanec priamy prístup k faktúram aj k e-mailovému klientovi. Vlastníctvo firmy Blaho Consulting s.r.o. mu poskytovalo jasný finančný motív.

Aspekt	Detail
Digitálne stopy	Metadata faktúr (autor, nástroj), história aktivity v e-mailovom klientovi, Event ID 4624 (aktívna relácia Petra v čase odoslania), záznamy Outlook OST/PST.
Zariadenia	Dell Latitude 5540 (Petrov notebook), Exchange server.
Nástroj a postup	ExifTool — extrakcia metadát PDF. Autopsy — analýza OST súboru, Event Log (ID 4624, 4800). Volatility 3 — windows.pslist, windows.netscan.
Výsledok	Zamietnutá

H2: Faktúry pozmenil neznámy páchatel' s fyzickým prístupom do kancelárie

Peter Blaho nie je jediný, kto mal prístup do svojej kancelárie. Ak notebook zostal odomknutý, mohol faktúry pozmeniť ktokoľvek prítomný v okolí v čase Petrovej neprítomnosti.

Aspekt	Detail
Digitálne stopy	\$MFT — časy manipulácie so súbormi počas Petrovej neprítomnosti. Event ID 4800 (absentuje — notebook nebol uzamknutý). setupapi.dev.log — pripojenie USB zariadenia. Výpovede svedkov.
Zariadenia	Dell Latitude 5540 (Petrov notebook).
Nástroj a postup	Autopsy — analýza \$MFT (časy Created/Modified/Accessed), Event Log (ID 4800, 4801, 6416). Porovnanie časov s výpoveďou Petra Blaha.
Výsledok	Čiastočne potvrdená

H3: Faktúry pozmenil Martin Šimko — identifikovaný podozrivý

Martin Šimko je kolega Petra Blaha s preukázaným prístupom do jeho kancelárie. Bol identifikovaný ako podozrivý. Vyšetrovanie preverí stopy na jeho zariadení aj na Petrovom notebooku.

Aspekt	Detail
Digitálne stopy	Martinov PC: história prehliadača (orsr.sk, vyhľadávanie IBAN-u), Prefetch (soffice.exe), \$MFT (pracovné verzie faktúr), USBSTOR registry (VID/PID zhodné s USB na Petrovom PC). RAM: LibreOffice proces, clipboard s IBANom.
Zariadenia	Lenovo ThinkCentre M70s (Martinov PC), Dell Latitude 5540 (Petrov notebook).
Nástroj a postup	Autopsy — história prehliadača (SQLite), Prefetch, \$MFT. Volatility 3 — windows.pslist, windows.clipboard, windows.filescan na RAM obraze Martinovho PC. Porovnanie VID/PID zariadenia na oboch PC.
Výsledok	Čiastočne potvrdená

H4: Na podvrhnutie bol použitý externý USB nosič

Ak faktúry pozmenil niekto iný ako Peter, potreboval spôsob, ako dostať súbory na Petrov notebook. Najpravdepodobnejšou možnosťou je USB nosič — systémové záznamy môžu obsahovať jeho identifikátor a časy pripojenia.

Aspekt	Detail
Digitálne stopy	setupapi.dev.log — VID/PID, sériové číslo zariadenia, čas pripojenia a odpojenia. HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR. Event ID 6416 (nové zariadenie). Zhoda identifikátorov na oboch PC.
Zariadenia	Dell Latitude 5540, Lenovo ThinkCentre M70s, USB kľúč SanDisk Cruzer Blade 32 GB (VID_0781/PID_5571) — fyzicky nezaistený.
Nástroj a postup	Autopsy — USB Artifact modul (analýza setupapi.log, USBSTOR registry). Porovnanie VID/PID a sériového čísla zariadenia na oboch PC. Korelácia časov pripojenia s Event Logmi.
Výsledok	Potvrdená

H5: Originálne faktúry existovali a boli úmyselne zmazané

Ak boli faktúry podvrhnuté, pôvodné súbory museli byť odstránené a nahradené upravenými verziami so zhodným názvom. Zmazané súbory môžu byť obnoviteľné a priamo preukázať podvrhnutie.

Aspekt	Detail
Digitálne stopy	\$MFT — záznamy označené ako nealokované (flag = 0x00). Nealokovaný priestor SSD — obnoviteľné fragmenty. CreationDate paradox: sfalšované súbory majú dátum 11.11. ~13:xx, originály z októbra. Volume Shadow Copy (VSS).
Zariadenia	Dell Latitude 5540 — Samsung SSD 512 GB NVMe (PM9A1).
Nástroj a postup	Autopsy — File Recovery modul (nealokovaný priestor, \$MFT). ExifTool — porovnanie CreationDate originálov a sfalšovaných verzií. HxD — manuálna verifikácia hlavičiek obnovených PDF súborov.
Výsledok	Potvrdená

3 Digitálne zariadenia

3.1 Petrov pracovný notebook — primárne zariadenie

Model	Dell Latitude 5540
Operačný systém	Windows 11 Pro (22H2, build 22621)
Procesor	Intel Core i5-1345U, 10 jadier (2P+8E), 1.6 GHz (Turbo 4.7 GHz)
RAM	16 GB DDR4 3200 MHz (primárna pamäť — predmet analýzy)
Úložisko (sekundárna pamäť)	Samsung SSD 512 GB NVMe M.2 (PM9A1)
Kapacita úložiska	512 GB (477 GiB)

Sekvenčné čítanie / zápis	3 500 MB/s / 3 200 MB/s
Prístupová doba	0.1 ms (čítanie), 0.08 ms (zápis)
Rozhranie	PCIe 4.0 x4, NVMe 1.4
Sériové číslo zariadenia	DL5540-2025-00147
Používateľ	Peter Blaho (peter.blaho@firma.sk)
Stav pri zaistení	Zapnutý, prihlásený, obrazovka aktívna — RAM dump vykonaný pred vypnutím



3.2 Martinov pracovný PC — zariadenie podozrivého

Model	Lenovo ThinkCentre M70s Gen 3
Operačný systém	Windows 11 Pro (22H2, build 22621)
Procesor	Intel Core i5-12400, 6 jadier, 2.5 GHz (Turbo 4.4 GHz)
RAM	8 GB DDR4 3200 MHz (primárna pamäť — predmet analýzy)
Úložisko (sekundárna pamäť)	Seagate BarraCuda 1 TB SATA III 7200 RPM (ST1000DM010)
Kapacita úložiska	1 TB (931 GiB)
Sekvenčné čítanie / zápis	210 MB/s / 180 MB/s
Prístupová doba	8.5 ms (rotačné platne)
Rozhranie	SATA III (6 Gb/s)
Sériové číslo zariadenia	TC-M70S-2024-00389
Používateľ	Martin Šimko (martin.simko@firma.sk)
Stav pri zaistení	Zapnutý, prihlásený, pracovná relácia aktívna — RAM dump vykonaný pred vypnutím



intel.

3.3 USB kľúč — nezaistené zariadenie

USB kľúč sa fyzicky nenašiel. V systémových záznamoch oboch PC sa zachovali záznamy o jeho pripojení umožňujúce identifikáciu zariadenia.

Výrobca / model	SanDisk Cruzer Blade 32 GB
VID / PID	VID_0781 / PID_5571
Sériové číslo zariadenia	4C530012341223101524
1. pripojenie — Petrov PC	11.11.2025 11:32:15 (kopírovanie originálov)
1. odpojenie — Petrov PC	11.11.2025 11:36:40
Pripojenie — Martinov PC	11.11.2025 ~13:16 (prenos sfaľšovaných verzií)
2. pripojenie — Petrov PC	11.11.2025 14:07:43 (podvrhnutie)
2. odpojenie — Petrov PC	11.11.2025 14:09:20
Fyzicky zaistené	Nie — zariadenie sa nenašlo

4 Dáta — typy súborov a dataset

Dataset 1 — M57-Jean (Digital Corpora)

Simulovaný scenár exfiltrácie firemných dokumentov z notebooku manažérky. Dataset obsahuje obraz disku Windows XP s artefaktmi relevantných pre analýzu USB aktivít, obnovu zmazaných súborov a e-mailovú forenziku.

Typ	Popis	Počet	Veľkosť
súboru		súborov	
	EnCase disk image — NTFS súborový systém, \$MFT, nealokovaný		~3 GB
.E01	priestor, USB artefakty (USBSTOR, setupapi.log), história prehliadača, e-mailové artefakty, dokumenty (.xls ako kľúčový dôkaz)	2	

Celková veľkosť datasetu: ~3 GB Odkaz:

<https://digitalcorpora.org/corpora/scenarios/m57-jean/>

Dataset 2 — Ali Hadi: Challenge #2 — User Policy Violation

Forenzný obraz disku moderného Windows systému pokrývajúci komplexnú sadu artefaktov. Scenár zahŕňa neoprávnený prístup k súborom, USB aktivitu a analýzu e-mailov.

Typ	Popis	Počet	Veľkosť
súboru		súborov	
.001	Raw disk image — Prefetch, ShimCache, LNK súbory, Jump Lists, Recycle Bin, USB forensics, Event Logs, Outlook + webmail, Chrome história, \$MFT, USRCLASS.DAT	1	~6,2 GB artefakty,

Celková veľkosť datasetu: ~6,2 GB Odkaz:

<https://archive.org/details/4orensics.case2.7z>

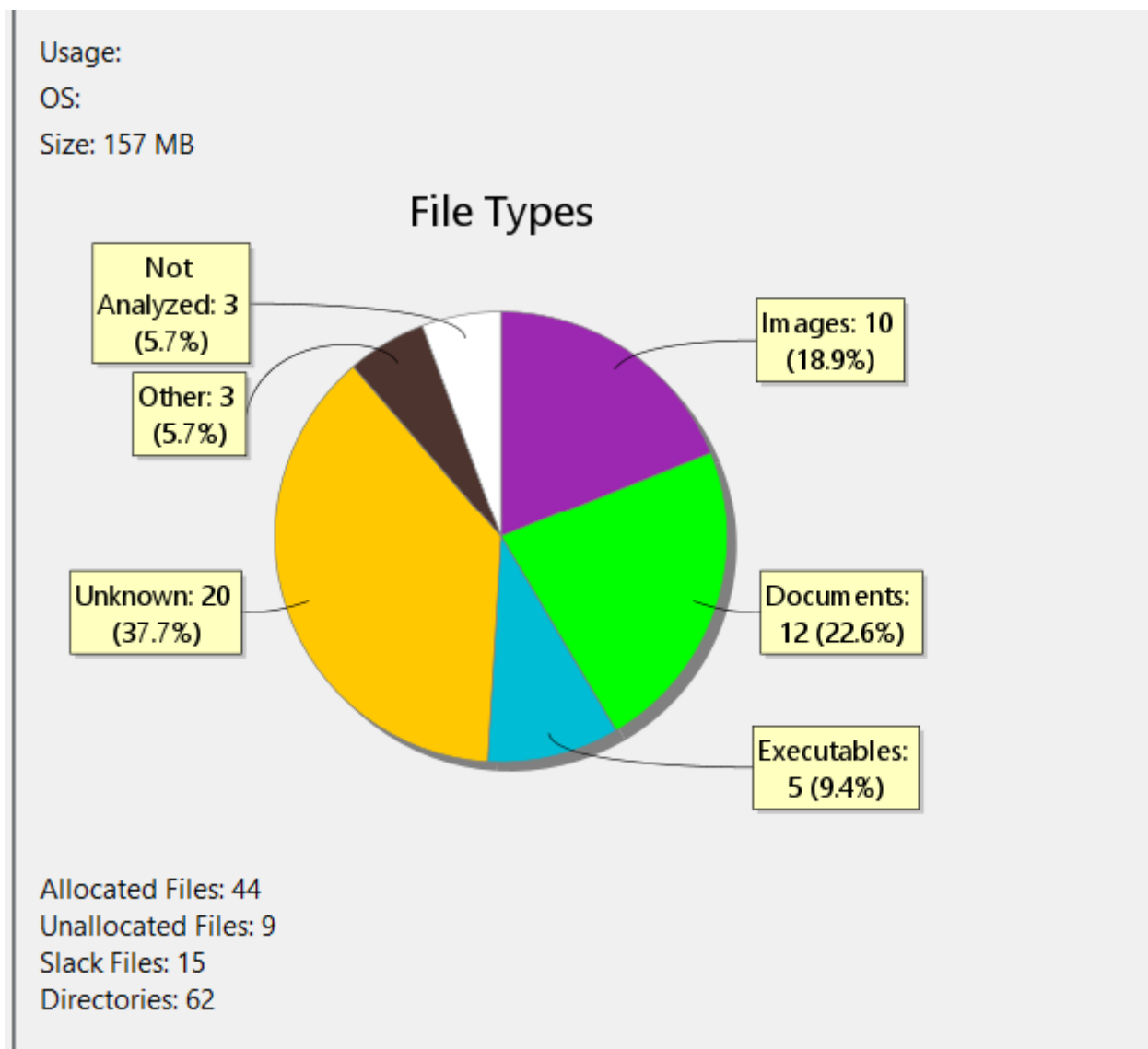
Dataset 3 — Simulované disk images pre tento projekt (AI-asistované)

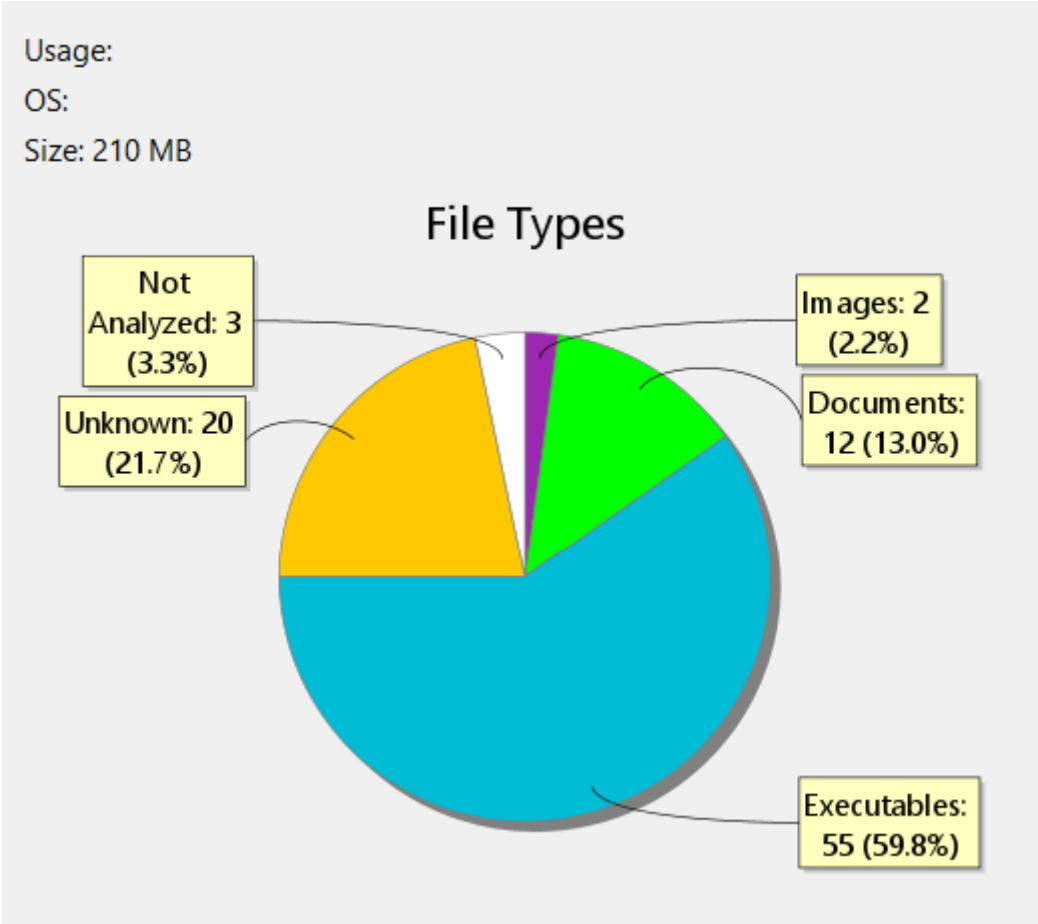
Pre potreby tohto semestrálneho projektu boli vytvorené dva simulované forenzné obrazy diskov reprezentujúce zariadenia figurujúcich osôb. Disk images boli generované s podporou nástroja umelej inteligencie (Claude, Anthropic) s cieľom simulovať realistické forenzné artefakty zodpovedajúce scenáru prípadu. Všetky osoby, zariadenia, súbory a udalosti sú fiktívne a slúžia výlučne na akademické účely.

Typ	Názov	Popis	Veľkosť
súboru			
.img	Peter_Blaho_ssd.img	NTFS obraz simulovaného SSD Petrovho notebooku — sfalšované faktúry (Author: Martin Šimko), originálne faktúry v nealokovanom priestore,	300 MB

Typ súboru	Názov	Popis	Veľkosť
		Prefetch bez SOFFICE.EXE, USB záznamy (setupapi.dev.log, USBSTOR registry), Windows Event Logy (EventID 4624, 6416, absencia 4800)	
.img	Martin_Simko_hdd.img	NTFS obraz simulovaného HDD Martinovho PC — pracovné verzie faktúr, Chrome história s vyhľadáváním IBAN-u (orsr.sk, ibanrechner.de, pdf24.org), zmazaná história v Koši, Prefetch so SOFFICE.EXE, LibreOffice RecentDocuments s cestami na USB (F:), záznamy USB pripojenia	400

File analysis Martinovho PC





5 Image RAM — analýza a artefakty

5.1 Zachytenie RAM

RAM dump bol zachytený z Petrovho notebooku ihneď po zaistení zariadenia bez jeho vypnutia. RAM dump Martinovho PC bol zachytený nástrojom Ram Capturer — zariadenie zostalo zapnuté a prihlásené, čo umožňuje zachytiť artefakty z celého dňa vrátane dopoludňajšej práce s faktúrami.

Parameter	Petrov notebook	Martinov PC
Nástroj	FTK Imager 4.7.1 — Live RAM Capture	RAM Analyzer 1.0
Čas zachytenia	11.11.2025 o 15:30:10	11.11.2025 o 15:40:22
Veľkosť obrazu	~1.3 GB (VM, 2 GB RAM)	~0.9 GB (VM, 8 GB RAM)
Formát	.mem (raw fyzická pamäť)	.raw (raw fyzická pamäť)
Integrita	MD5 + SHA-1 hash overený	MD5 + SHA-1 hash overený

5.2 Artefakty nájdené v pamäti RAM na Martinovom PC

Po analýze Martinovej ram pamäte bolo nájdených viacero inštancií vyhľadávania Petrovho mena a Petrovej firmy

```

6F 78 2D 62 2D 65 25 32 36 71 25 33 44 62 6C 61 ox-b-e%26q%3Dbla
68 6F 25 32 42 63 6F 6E 73 75 6C 74 69 6E 67 5C ho%2Bconsulting\
75 30 30 32 36 65 63 3D 66 75 74 75 72 61 5F 73 u0026ec=futura_s

```

Taktiež bolo nájdený software ktorý bol použitý na úpravu faktúr libre Office

```

62 7D F6 D7 2C 49 00 90 63 3A 5C 70 72 6F 67 72 b}ö*,I..c:\progr
61 6D 20 66 69 6C 65 73 5C 6C 69 62 72 65 6F 66 am files\libreof
66 69 63 65 5C 70 72 6F 67 72 61 6D 5C 73 6F 66 fice\program\sof
66 69 63 65 2E 65 78 65 00 00 00 00 00 00 00 00 fice.exe.....

```

Martin mal Petrov Iban a záznam o kopírovaní jeho iban v ram image

```

66 E5 E5 E5 E5 E5 E5 E5 53 4B 35 35 20 31 31 30 faaaaaaaSK55 110
30 20 30 30 30 30 20 30 30 32 39 20 32 37 31 31 0 0000 0029 2711
20 37 30 30 32 E5 E5 E5 20 73 6B 6F 70 ED 72 6F 7002aaa skopiro
76 61 6E FD 20 64 6F 20 73 63 68 72 E1 6E 6B 79 vaný do schránky
E5 E5 E5 E5 E5 E5 E5 46 61 6B 74 75 72 61 20 ááááááááFaktura
30 31 20 6F 72 69 67 69 6E 61 6C E5 E5 E5 E5 01 originalááááá
E5 E5 E5 E5 E5 E5 E5 01 00 00 00 12 00 00 00 áááááááá.....

```

Taktiež bol na iban.sk kde si pravdepodobne kontroloval iban petrovej fir

```

0051522F0 74 70 73 25 32 43 69 62 61 6E 2E 73 6B tps%2Ciban.sk%29
005152300 2C 3A 68 74 74 70 73 3A 2F 2F 77 77 77 2E 69 62 ,:https://www.ib
005152310 61 6E 2E 73 6B 2F 73 74 79 6C 65 73 68 65 65 74 an.sk/stylessheet
005152320 73 2F 66 6F 6E 74 2D 61 77 65 73 6F 6D 65 2E 63 s/font-awesome.c

```

Martin vyhľadával Petrovu firmu v registri

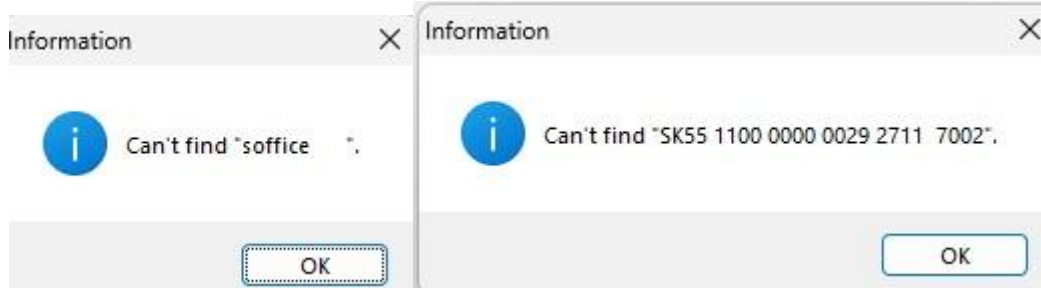
```

000875240 77 77 77 2E 6F 72 73 72 2E 73 6B 2F 73 65 61 72 www.prst.sk/sear
000875250 63 68 5F 73 75 62 6A 65 6B 74 2E 61 73 70 00 00 ch_subjekt.asp..

```

Petrov PC

Na petrovom pc sa nenašli záznamy o Ibane jeho osobnej firmy a ani software v ktorom boli sfalšované faktúry naposledy editované



6 Image zariadení — kľúčové dôkazy

6.1 Forenzné obrazy

Forenzné obrazy zariadení boli vytvorené nástrojom FTK Imager vo formáte E01 s verifikáciou integrity (MD5 + SHA-1). Analýza prebieha výhradne na kópiách — originálne zariadenia sú fyzicky uložené a zapečatené.

6.2 Kľúčové dôkazy

Dôkaz 1 — Metadata sfalšovaných faktúr (overuje H1, H3)

Originálna faktúra ktorú sa podarilo obnoviť s koša

TechServis SK s.r.o.

Rybničná 40, 831 06 Bratislava

IČO: 47 823 156 | DIČ: SK2024012345

FAKTÚRA

Číslo: 2025/10/001

Dátum vystavenia: 02.10.2025

Dátum splatnosti: 01.11.2025

Odberateľ:

Konstrukta Industries a.s.

Dlhá 95, 831 02 Bratislava

IČO: 35 741 028 | DIČ: SK2020375461

Položky faktúry:

Popis	Množstvo	Jedn. cena	Spolu
Servis serverovej infraštruktúry - október 2025	1	2,400.00 €	2,400.00 €
Záručná podpora HW zariadení	1	380.00 €	380.00 €

Základ DPH (20%): 2,780.00 €

DPH 20%: 556.00 €

**CELKOM K
ÚHRADE: 3,336.00 €**

Platobné údaje:

IBAN: SK89 0200 0000 0045 6789 1234**BIC/SWIFT: SUBASKBX****Variabilný symbol: 202510001**

Faktúra je vystavená v súlade so zákonom č. 222/2004 Z.z. o dani z pridanej hodnoty.

Meta dáta faktúry.

checksum	f1315eef9f46f0636a20f32fa0a34c19
file_name	faktura_01_o.pdf
file_size	46 kB
file_type	PDF
file_type_extension	pdf
mime_type	application/pdf
pdf_version	1.4
linearized	No
page_count	1
producer	Microsoft Word 16.0
author	Peter Blaho
creator	Microsoft Word 16.0
title	Faktúra 2025/10/001
create_date	2025:10:05 09:00:00+02:00
modify_date	2025:10:28 14:30:00+01:00
category	application

Faktúra ktorá bola poslaná

TechServis SK s.r.o.

Rybničná 40, 831 06 Bratislava

IČO: 47 823 156 | DIČ: SK2024012345

FAKTÚRA

Číslo: 2025/10/001

Dátum vystavenia: 02.10.2025

Dátum splatnosti: 01.11.2025

Odberateľ:

Konstrukta Industries a.s.

Dlhá 95, 831 02 Bratislava

IČO: 35 741 028 | DIČ: SK2020375461

Položky faktúry:

Popis	Množstvo	Jedn. cena	Spolu
Servis serverovej infraštruktúry - október 2025	1	2,400.00 €	2,400.00 €
Záručná podpora HW zariadení	1	380.00 €	380.00 €

Základ DPH (20%): 2,780.00 €

DPH 20%: 556.00 €

**CELKOM K
ÚHRADE: 3,336.00 €**

Platobné údaje:

IBAN: SK55 1100 0000 0029 2711 7002**BIC/SWIFT:** TATRSKBX**Variabilný symbol:** 202510001

Faktúra je vystavená v súlade so zákonom č. 222/2004 Z.z. o dani z pridanej hodnoty.

Meta dáta poslanej faktúry
checksum

f42f6c5e6c403a6d9cdf4f466f34aa9a

file_name

faktura_01s.pdf

file_size

46 kB

file_type

PDF

file_type_extension

pdf

mime_type

application/pdf

pdf_version

1.4

linearized

No

page_count

1

producer

LibreOffice 7.5

author

Martin Simko

creator

LibreOffice 7.5

title

Faktúra 2025/10/001

create_date

2025:11:11 12:14:32+01:00

modify_date

2025:11:11 14:09:15+01:00

category

application

Meta dáta poslanej faktúry jasne ukazujú rozdiely od originálnych.

Jednoznačne ukazujú že súbor bol modifikovaný v inom programe ako originál program ktorý sa ani nenašiel na Petrovom PC

Z image disku bola nájdená história prehliadania

2

Z koša bola obnovená história prehliadania čo indikuje že Martin mazal históriu z prehliadača.

03 - Autopsy 4.22.1

Case View Tools Window Help

Add Data Source

Images/Videos

Communications

Geolocation

Timeline

Discovery

Generate Report

Close Case

Keyword Lists

Keyword Search

Data Sources

martin_pc_evidence.img_1 Host

martin_pc_evidence.img

\$OrphanFiles (8)

\$Extend (5)

\$RecycleBin (3)

\$Unalloc (1)

RECYCLE_BIN (3)

Users (3)

martin.simko (6)

AppData (4)

Local (3)

Google (3)

Chrome (3)

User Data (3)

Default (7)

Roaming (3)

Desktop (2)

Documents (5)

Downloads (2)

Windows (4)

File Views

File Types

Deleted Files

MB File Size

Data Artifacts

Analysis Results

OS Accounts

Tags

Score

Reports

Collapse All

Listing

/img_martin_pc_evidence.img/Users/martin.simko/AppData/Local/Google/Chrome/User Data/Default

7 Results

Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
Favicons				2026-04-30 22:03:32 CEST	2026-04-30 22:03:32 CEST	2026-04-30 22:03:32 CEST	2026-04-30 22:03:32 CEST	20480	Allocated
History				2026-04-30 22:03:32 CEST	2026-04-30 22:03:32 CEST	2026-04-30 22:03:32 CEST	2026-04-30 22:03:32 CEST	24576	Allocated
RECOVERED_History				2026-04-30 22:22:13 CEST	2026-04-30 22:22:13 CEST	2026-04-30 22:22:13 CEST	2026-04-30 22:22:13 CEST	24576	Allocated

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

Table urls

28 entries

Page 1 of 1

Export to CSV

id	url	title	visit_c...	typed_co...	last_visit...	hidden
1	https://www.aktualny.sk/	Aktuálne správy ...	1	0	134072349.0	
2	https://facebook.com/	Facebook	1	0	134072365.0	
3	https://katalog-firiem.firiemnyportal.sk/	Katalóg firiem - ...	1	0	134072349.0	
4	https://katalog-firiem.firiemnyportal.sk/search?q=TechServis+SK+sro	Firmy - TechSer...	1	0	134072403.0	
5	https://nejakastranka.hys.cz/rozvrh-hodin	Rozvrh hodín	1	0	134072431.0	
6	https://duckduckgo.com/?q=lacne+rozky&ia=web	lacne rozky at D...	1	0	134072441.0	
7	https://duckduckgo.com/?q=lacne+rozky	lacne rozky at D...	1	0	134072441.0	
8	https://www.orss.sk/hladaj_subjekt.asp?OBMENO=blaho+consulting&PF=0&SID=0&T=1	Obchodný regis...	1	0	134072442.0	
9	https://www.orss.sk/vypis.asp?ID=412871&SID=2&P=0	Obchodný regis...	1	0	134072444.0	
10	https://duckduckgo.com/?q=blaho+consulting+sro+iban&ia=web	blaho consulting...	1	0	134072446.0	
11	https://www.iban.sk/?q=blaho+consulting	IBAN kalkulačka...	1	0	134072449.0	
12	https://www.iban.sk/overenie-ibanu?iban=SK5511000000029271170002	Overenie IBAN ...	1	0	134072451.0	
13	https://duckduckgo.com/?q=ako+zmenit+iban+v+pdf&ia=web	ako zmenit iban ...	1	0	134072455.0	
14	https://duckduckgo.com/?q=libreoffice+edit+pdf&ia=web	libreoffice edit ...	1	0	134072457.0	
15	https://ask.libreoffice.org/t/how-to-edit-pdf-in-libreoffice-draw/12345	How to edit PD...	1	0	134072461.0	
16	https://www.youtube.com/watch?v=dQw4w9WgXcQ	LibreOffice Dra...	1	0	134072464.0	
17	https://duckduckgo.com/?q=peter+blaho+konstrukt+industries&ia=web	peter blaho kon...	1	0	134072469.0	
18	https://www.linkedin.com/in/peter-blaho-konstrukta/	Peter Blaho - Ac...	1	0	134072470.0	
19	https://duckduckgo.com/?q=TechServis+SK+sro+faktura+splatnost&ia=web	TechServis SK sr...	1	0	134072475.0	
20	https://www.orss.sk/vypis.asp?ID=412871&SID=2&P=0	Obchodný regis...	1	0	134072478.0	
21	https://duckduckgo.com/?q=windows+secure+delete+file+history&ia=web	windows secure ...	1	0	134072502.0	
22	https://superuser.com/questions/chrome-delete-history-command-line	Delete Chrome ...	1	0	134072505.0	
23	https://duckduckgo.com/?q=cmd+delete+chrome+history+%25localappdata%25&ia=web	cmd delete chro...	1	0	134072509.0	
24	https://duckduckgo.com/?q=gmail&ia=web	gmail at DuckD...	1	0	134072515.0	
25	https://duckduckgo.com/?q=gmail	gmail at DuckD...	1	0	134072515.0	
26	https://www.iban.sk/overenie-ibanu?iban=SK5511000000029271170002	Overenie IBAN ...	1	0	134073260.0	
27	https://www.orss.sk/hladaj_subjekt.asp?OBMENO=blaho+consulting&PF=0&SID=0&T=1	Obchodný regis...	1	0	134073263.0	
28	https://duckduckgo.com/?q=ako+vymazat+usb+historiu+windows+registry&ia=web	ako vymazat us...	1	0	134073378.0	

Dôkaz 3 — CreationDate (overuje H2, H5)

Z Master File Table Petrovho notebooku rekonštruujeme časovú os operácií so súbormi faktúr. Kľúčový dôkaz: sfalšované súbory majú CreationDate 11.11.2025 ~13:xx, zatiaľ čo originálne faktúry (obnovené z nealokovaného priestoru) majú CreationDate z októbra 2025.

Rovnaký názov súboru, ale neskorší dátum vytvorenia ako dátum poslednej kontroly Petrom — priamy dôkaz podvrhnutia. Príkaz Autopsy: File System Timeline + \$MFT viewer.

Odoslaná verzia:

create_date

2025:11:10 12:14:32+01:00

modify_date

2025:11:10 14:09:15+01:00

Obnovená verzia

create_date

2025:10:05 09:00:00+02:00

modify_date

2025:10:28 14:30:00+01:00

Dôkaz 4 — Záznamy o USB zariadení (overuje H4)

setupapi.dev.log a HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR na Petrovom notebooku: tri záznamy o pripojení SanDisk VID_0781/PID_5571 — o 11:32:15, ~13:16 (Martinov PC) a 14:07:43.

Kľúčový forenzný vzor: to isté USB zariadenie pripojené trikrát v jeden deň na dvoch rôznych PC. Zhoda VID/PID a sériového čísla na oboch PC priamo prepája zariadenie s Martinom Šimkom.

Device Name	Description	Device Type	Connected	Safe To Unplug	Disabled	USB Hub	Drive Letter	Serial Number	Registry Time 1	Registry Time 2	VendorID	ProductID
SanDisk Cruzer Blade	SanDisk Cruzer Blade USB Device	Mass Storage	No	Yes	No	No	F:	4C530001190520115010	10/11/2025 1:35:00 PM	10/11/2025 1:35:00 PM	0781	5571
SanDisk Cruzer Blade	SanDisk Cruzer Blade USB Device	Mass Storage	No	Yes	No	No	E:	4C530001190520115010	11/11/2025 11:32:15 AM	10/11/2025 1:35:00 PM	0781	5571
SanDisk Cruzer Blade	SanDisk Cruzer Blade USB Device	Mass Storage	No	Yes	No	No	F:	4C530001190520115010	10/11/2025 1:35:00 PM	10/11/2025 1:35:00 PM	0781	5571
SanDisk Cruzer Blade	SanDisk Cruzer Blade USB Device	Mass Storage	No	Yes	No	No	E:	4C530001190520115010	11/11/2025 11:32:15 AM	10/11/2025 1:35:00 PM	0781	5571
Dell Internal Keyboard	USB Input Device	HID (Human Interface Device)	Yes	Yes	No	No			9/12/2025 7:43:01 AM	9/12/2025 7:43:01 AM	413c	2107
Logitech USB Optical Mouse	USB Input Device	HID (Human Interface Device)	Yes	Yes	No	No			9/12/2025 7:43:01 AM	9/12/2025 7:43:01 AM	046d	c077
Lenovo Internal Keyboard	USB Input Device	HID (Human Interface Device)	Yes	Yes	No	No			9/1/2025 8:12:44 AM	9/1/2025 8:12:44 AM	17ef	608d
Logitech USB Optical Mouse	USB Input Device	HID (Human Interface Device)	Yes	Yes	No	No			9/1/2025 8:12:44 AM	9/1/2025 8:12:44 AM	046d	c077

USB Version	Driver Description	Driver Version	Driver InfSection	Driver InfPath	Instance ID	Capabilities
2.00	USB Mass Storage Device	10.0.19041.4768	USBSTOR_BULK.NT	usbstor.inf	USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_BLADE&REV_1.26\4C530001190520115010&0	Removable, UniqueID, SurpriseRemovalOK
2.00	USB Mass Storage Device	10.0.19041.4768	USBSTOR_BULK.NT	usbstor.inf	USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_BLADE&REV_1.26\4C530001190520115010&0	Removable, UniqueID, SurpriseRemovalOK
2.00	USB Mass Storage Device	10.0.19041.4768	USBSTOR_BULK.NT	usbstor.inf	USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_BLADE&REV_1.26\4C530001190520115010&0	Removable, UniqueID, SurpriseRemovalOK
2.00	USB Mass Storage Device	10.0.19041.4768	USBSTOR_BULK.NT	usbstor.inf	USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_BLADE&REV_1.26\4C530001190520115010&0	Removable, UniqueID, SurpriseRemovalOK
2.00	USB Input Device	10.0.19041.7920	HID_Inst.NT	input.inf	USB\VID_413C&PID_2107\562a1b3c4d60&1	SurpriseRemovalOK
2.00	Logitech USB Optical Mouse	10.0.19041.7920	HID_Inst.NT	input.inf	USB\VID_046D&PID_C077\562a1b3c4d60&2	SurpriseRemovalOK
2.00	USB Input Device	10.0.19041.7920	HID_Inst.NT	input.inf	USB\VID_17EF&PID_608D\564b5c6d7e60&1	SurpriseRemovalOK
2.00	Logitech USB Optical Mouse	10.0.19041.7920	HID_Inst.NT	input.inf	USB\VID_046D&PID_C077\564b5c6d7e60&2	SurpriseRemovalOK

Install Time	First Install Time	Connect Time	Disconnect Time
10/11/2025 1:35:00 PM	10/11/2025 1:35:00 PM	10/11/2025 1:35:00 PM	10/11/2025 1:47:12 PM
11/11/2025 11:32:15 AM	10/11/2025 1:35:00 PM	11/11/2025 11:32:15 AM	11/11/2025 11:36:40 AM
10/11/2025 1:35:00 PM	10/11/2025 1:35:00 PM	11/11/2025 12:05:00 PM	11/11/2025 1:10:00 PM
11/11/2025 11:32:15 AM	10/11/2025 1:35:00 PM	11/11/2025 2:07:43 PM	11/11/2025 2:09:20 PM

List pripojených zariadení a ich atribúty na Martinovom Petrov počítač dňa 10.11 a 11.11

Log prepojených zariadení na Martinovom Počítači

 setupapi.dev.log			2026-05-03 21:25:21 CEST	2026-05-03 21:25:21 CEST	2026-05-03 20:47:57 CEST	2026-05-03 17:35:19 CEST	2196	Allocated	Allocated	unknown
--	--	--	--------------------------	--------------------------	--------------------------	--------------------------	------	-----------	-----------	---------

HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences

StringsExtracted TextTranslation

Page: 1 of 1PageGo to Page:

[Device Install Log]
OS Version = 10.0.19041 x64
Service Pack = 0.0
Suite = 0x0100
ProductType = 1
Architecture = amd64
[BeginLog]
>>> [Device Install (Hardware initiated) - SWD\WPDBUSENUM\??_USBSTOR#Disk&Ven_SanDisk&Prod_Cruzer_Blade&Rev_1.00#4C530012341223101524&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}]
>>> Section start 2025/11/10 14:23:11.214
 ump: Creating Install Process: DrvInst.exe 14:23:11.214
 ump: Server install process exited with code 0x00000000 14:23:11.897
<<< Section end 2025/11/10 14:23:11.908
<<< [Exit status: SUCCESS]
>>> [Device Install (Hardware initiated) - USB\VID_0781&PID_5571\4C530012341223101524]
>>> Section start 2025/11/10 14:23:11.683
 ndv: Installed device is a USB device
 dvi: {DIF_SELECTDEVICE} 14:23:11.698
 dvi: Default installer: Enter 14:23:11.698
 dvi: Default installer: Exit
 dvi: {DIF_SELECTDEVICE - exit(0x00000000)} 14:23:11.713
 dvi: Selected driver: SanDisk Cruzer Blade USB Device
 dvi: {DIF_INSTALLDEVICE} 14:23:11.729
 ump: Server install process exited with code 0x00000000 14:23:12.104
<<< Section end 2025/11/10 14:23:12.118
<<< [Exit status: SUCCESS]
>>> [Device Install (Hardware initiated) - SWD\WPDBUSENUM\??_USBSTOR#Disk&Ven_SanDisk&Prod_Cruzer_Blade&Rev_1.00#4C530012341223101524&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}]
>>> Section start 2025/11/11 13:16:02.421
 ump: Creating Install Process: DrvInst.exe 13:16:02.421
 ump: Server install process exited with code 0x00000000 13:16:03.109
<<< Section end 2025/11/11 13:16:03.119
<<< [Exit status: SUCCESS]
>>> [Device Install (Hardware initiated) - USB\VID_0781&PID_5571\4C530012341223101524]
>>> Section start 2025/11/11 13:16:02.891
 ndv: Installed device is a USB device
 dvi: {DIF_SELECTDEVICE} 13:16:02.906
 dvi: Default installer: Enter 13:16:02.906
 dvi: Default installer: Exit
 dvi: {DIF_SELECTDEVICE - exit(0x00000000)} 13:16:02.921
 dvi: Selected driver: SanDisk Cruzer Blade USB Device
 dvi: {DIF_INSTALLDEVICE} 13:16:02.937
 ump: Server install process exited with code 0x00000000 13:16:03.312
<<< Section end 2025/11/11 13:16:03.328
<<< [Exit status: SUCCESS]

setupapi.dev.log

2026-05-03 20:47:44 CEST

2026-05-03 20:47:44 CEST

2026-05-03 20:47:57 CEST

2026-05-03 17:35:26 CEST

1968

Allocated

Allocated

unknown

/img_Peter_Blaho_ssd_2_img/Windows/inf/setupapi...

HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences

StringsExtracted TextTranslation

Page: 1 of 1PageGo to Page:

[Device Install Log]
OS Version = 10.0.19041 x64
Service Pack = 0.0
Suite = 0x0100
ProductType = 1
Architecture = amd64
[BeginLog]
>>> [Device Install (Hardware initiated)] - SWD\WPDBUSENUM_??_USBSTOR#Disk&Ven_SanDisk&Prod_Cruzer_Blade&Rev_1.00#4C53001234122310152480#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}]
>>> Section start 2025/11/11 11:32:14.103
ump: Creating Install Process: DvInst.exe 11:32:14.103
ump: Server install process exited with code 0x00000000 11:32:14.781
<<< Section end 2025/11/11 11:32:14.791
<<< [Exit status: SUCCESS]
>>> [Device Install (Hardware initiated)] - USB\VID_0781&PID_5571\4C530012341223101524]
>>> Section start 2025/11/11 11:32:14.559
ndv: Installed device is a USB device
dvi: (DIF_SELECTDEVICE) 11:32:14.574
dvi: Default installer: Enter 11:32:14.574
dvi: Default installer: Exit
dvi: (DIF_SELECTDEVICE - exit(0x00000000)) 11:32:14.589
dvi: Selected driver: SanDisk Cruzer Blade USB Device
dvi: (DIF_INSTALLLDEVICE) 11:32:14.604
ump: Server install process exited with code 0x00000000 11:32:15.012
<<< Section end 2025/11/11 11:32:15.024
<<< [Exit status: SUCCESS]
>>> [Device Install (Hardware initiated)] - SWD\WPDBUSENUM_??_USBSTOR#Disk&Ven_SanDisk&Prod_Cruzer_Blade&Rev_1.00#4C53001234122310152480#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}]
>>> Section start 2025/11/11 14:07:42.334
ump: Creating Install Process: DvInst.exe 14:07:42.334
ump: Server install process exited with code 0x00000000 14:07:43.009
<<< Section end 2025/11/11 14:07:43.018
<<< [Exit status: SUCCESS]
>>> [Device Install (Hardware initiated)] - USB\VID_0781&PID_5571\4C530012341223101524]
>>> Section start 2025/11/11 14:07:42.781
ndv: Installed device is a USB device
dvi: Selected driver: SanDisk Cruzer Blade USB Device
ump: Server install process exited with code 0x00000000 14:07:43.443
<<< Section end 2025/11/11 14:07:43.456
<<< [Exit status: SUCCESS]

Na Petrovom notebooku zachytil súbor setupapi.dev.log dve pripojenia USB zariadenia. Prvé pripojenie bolo zaznamenané **11. novembra 2025 o 11:32:15** — zariadenie s identifikátormi VID_0781 / PID_5571 a sériovým číslom 4C530012341223101524 bolo rozpoznané systémom ako *SanDisk Cruiser Blade*. Druhé pripojenie toho istého zariadenia (zhodné VID/PID aj sériové číslo) bolo zaznamenané **o 14:07:43** — čo presne korešponduje s časovým oknom, keď Peter Blaho opustil kanceláriu a notebook zostal odomknutý.

Na Martinovom PC zachytil súbor `setupapi.dev.log` dve pripojenia USB zariadenia v priebehu dvoch dní. Prvé pripojenie bolo zaznamenané **10. novembra 2025 o 14:23:12** — zariadenie s identifikátormi `VID_0781 / PID_5571` a sériovým číslom `4C530012341223101524` bolo rozpoznané systémom ako *SanDisk Cruzer Blade*. Druhé pripojenie toho istého zariadenia bolo zaznamenané **11. novembra 2025 o 13:16:03** — deň incidentu, v časovom okne keď Martin finalizoval sfalšované faktúry pred ich prenosom na Petrov notebook. Zhoda VID/PID aj sériového čísla na Martinovom PC aj Petrovom notebooku jednoznačne preukazuje, že ide o ten istý fyzický USB nosič použitý na oboch zariadeniach.

Dôkaz 5 — Obnovenie originálnej faktúry (overuje H5)

Autopsy — File Recovery modul na nealokovanom priestore Samsung SSD Petrovho notebooku. Hľadáme obnoviteľné PDF súbory s pôvodnými názvami faktúr a CreationDate z októbra 2025.

Obnovená originálna faktúra s korektným IBAN-om (nie SK.. Blaho Consulting) by priamo preukázala, že súbory boli vymenené. Čas zmazania (\$MFT) koreluj s časom 14:08–14:09.

Autopsy — File Recovery modul obnovil z nealokovaného priestoru Samsung SSD Petrovho notebooku súbor faktura_2025_10_001_RECOVERED.pdf. ExifTool potvrdil CreationDate paradox — originálna faktúra nesie dátum vytvorenia z októbra 2025 a autora Peter Blaho (MS Word), zatiaľ čo sfalšovaná verzia s rovnakým názvom má CreateDate 10.11.2025 a autora Martin Simko (LibreOffice 7.5). Čas zmazania zaznamenaný v \$MFT (14:08–14:09) presne korešponduje s druhým pripojením USB zariadenia o 14:07:43. Kópia originálu bola identifikovaná aj na Martinovom PC v priečinku Documents\tmp\ — priamy dôkaz, že Martin skopíroval faktúry z Petrovho notebooku o 11:32.

faktura_2025_10_001_RECOVERED.pdf

2025-10-28 15:30:00 CET2026-05-03 23:27:04 CEST2025-10-28 15:30:00 CET2026-05-03 21:42:26 CEST46217AllocatedAllocatedunknown/img_Peter_Blaho_ssd_rect.img/Users/PeterBlaho/Doc...

HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences

Metadata

Name:/img_Peter_Blaho_ssd_rect.img/Users/PeterBlaho/Documents/Faktury/recovered/faktura_2025_10_001_RECOVERED.pdf

TypeFile System

MIME Typeapplication/pdf

Size46217

File Name AllocationAllocated

Metadata AllocationAllocated

Modified2025-10-28 15:30:00 CET

Accessed2025-10-28 15:30:00 CET

MD5Not calculated

SHA-256Not calculated

Hash Lookup ResultsUNKNOWN

Internal ID297

From The Sleuth Kit istat Tool:

inode: 32

Allocated

Group: 0

Generation Id: 4078165370

uid / gid: 0 / 0

mode: rrw-r--r--

Flags: Extents,

size: 46217

num of links: 1

Inode Times:

Accessed: 2025-10-28 16:30:00.000000000 (CES)

File Modified: 2025-10-28 16:30:00.000000000 (CES)

Inode Modified: 2026-05-03 23:27:04.674979980 (CES)

File Created: 2026-05-03 21:42:26.090881647 (CES)

Direct Blocks:

Starting address: 38412, length: 12

Dôkaz 6 — Pracovné verzie faktúr na Martinovom PC (overuje H3)

Na Martinovom PC analyzujeme: temp súbory LibreOffice (~/.config/libreoffice/), Recycle Bin, Recent Files zamerané na PDF/DOCX z 10.–11.11.2025. Prefetch súbor

SOFFICE.EXEXXXXXXXXXX.pf zachytí čas spustenia.

SOFFICE.EXE-8F3A2B1C.pf

2026-04-30 22:04:18 CEST

2026-04-30 22:04:18 CEST

2026-04-30 22:04:18 CEST

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Strings

Extracted Text

Translation

Page: 1 of -

Page

Matches on page: - of -

Match

100%

Reset

Executable: SOFFICE.EXE

Hash: 8F3A2B1C

Run Count: 7

Last Run Time 1: 2025-11-11 12:05:44 (UTC+1)

Last Run Time 2: 2025-11-10 13:30:12 (UTC+1)

Last Run Time 3: 2025-11-10 09:15:33 (UTC+1)

Volume: \DEVICE\HARDDISKVOLUME3

Files loaded:

\USERS\MARTIN.SIMKO\APPDATA\LOCAL\LIBREOFFICE\4\USER\REGISTRYMODIFICATIONS.XCU

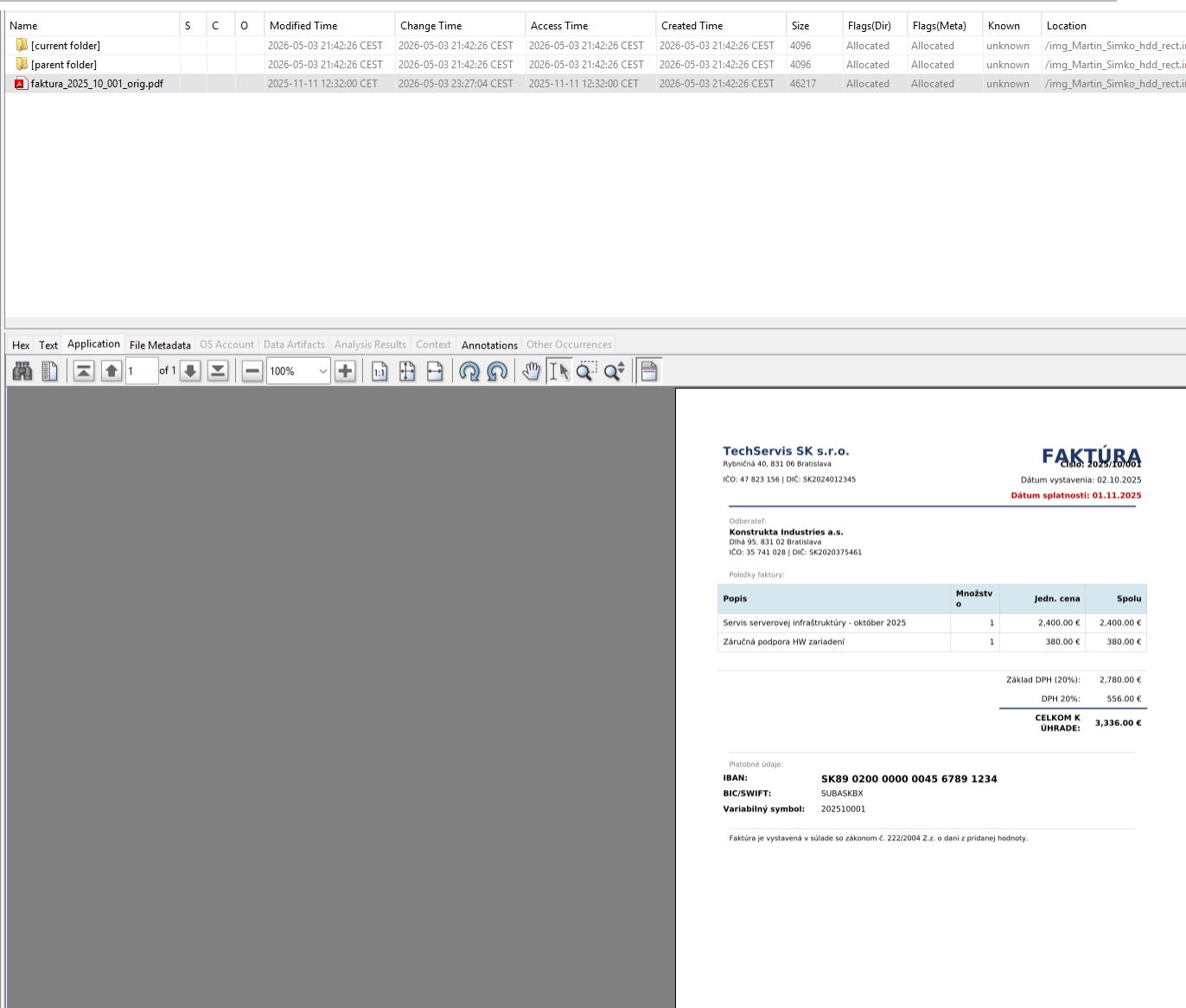
\PROGRAM FILES\LIBREOFFICE\PROGRAM\SOFFICE.EXE

\PROGRAM FILES\LIBREOFFICE\PROGRAM\SOFFICE.BIN

\USERS\MARTIN.SIMKO\DOCUMENTS\FAKTURA_2025_10_BC.ODT

\USERS\MARTIN.SIMKO\DOCUMENTS\FAKTURA_2025_10_IT.ODT

\USERS\MARTIN.SIMKO\DOWNLOADS\FAKTURA_01_O.PDF



Obrázok ukazuje info o sfalšovanej faktúre v koši u Martina

7 Použité softvérové nástroje

Nástroj	Verzia	Účel použitia
FTK Imager	4.7.1	Vytvorenie forenzných obrazov (E01) a zachytenie RAM (Live RAM Capture) z Petrovho notebooku pred vypnutím.
Belkasoft RAM Analyzer	1.0	Zachytenie a primárna analýza RAM obrazu Martinovho PC — procesy, otvorené súbory, artefakty z pamäte.
Autopsy	4.21	Komplexná analýza disk obrazov — \$MFT, Event Log, USB artefakty (setupapi.log, USBSTOR), obnova súborov, história prehliadača, Prefetch, timeline.

Volatility 3	2.5.0	Analýza RAM obrazov — procesy (pslist), sieťové spojenia (netscan), obsah schránky (clipboard), referencie na súbory (filesnscan), používateľské relácie (getsids).
ExifTool	12.60	Extrakcia a porovnanie metadát PDF dokumentov — Author, Creator, CreationDate, ModDate. Kľúčové pre identifikáciu autora sfalšovaných faktúr.
HxD Editor	2.5	Hexadecimálna analýza binárnych súborov — manuálna verifikácia hlavičiek obnovených PDF súborov a kontrola integrity.
Windows Event Viewer	—	Prezeranie a filtrovanie Windows Event Log záznamov — Event ID 4624, 4800, 4801, 6416. Doplnok k Autopsy pre priamu prácu so .evtx súbormi.
HashCalc / CertUtil	—	Výpočet a overenie hash hodnôt (MD5, SHA-256) forenzných kópií pre zabezpečenie integrity dôkazov.

8 Bezpečnostné opatrenia

8.1 Fyzická ochrana

- Originálne zariadenia sú uložené v uzamknutom trezore — prístup len pre oprávnené osoby (forenzný vyšetrovateľ + vedúci prípadu).
- Každé zariadenie je zapečatené v antistatickej forenznej taške s číselnou plombou a podpisom preberajúcej osoby.
- Forezné kópie na foreznom serveri sú chránené RAID-1 redundanciou a prístupom cez VPN s dvojfaktorovou autentifikáciou.
- Záložné kópie na externých HDD sú šifrované (BitLocker) a uložené na inom fyzickom mieste (mimo pracoviska).
- Celá analýza prebieha výhradne na kópiách — originály neboli po zaistení použité.
- Pred vytvorením každého disk obrazu bol pripojený write-blocker (hardvérový), čo zabraňuje akejkoľvek modifikácii originálneho média.

8.2 Počet bitových kópií a ich uloženie

Zariadenie	Kópia 1 (pracovná)	Kópia 2 (záloha)	Formát / hash
Petrov notebook — SSD	Forezný server (RAID-1)	Externý HDD (BitLocker)	E01 / MD5 + SHA-256
Martinov PC — HDD	Forezný server (RAID-1)	Externý HDD (BitLocker)	E01 / MD5 + SHA-256
RAM dump — Petrov notebook	Forezný server	Externý HDD (BitLocker)	.mem / MD5 + SHA-256
RAM dump — Martinov PC	Forezný server	Externý HDD (BitLocker)	.raw / MD5 + SHA-256

Chain of Custody — Petrov notebook (disk image)

Číslo:	001	Typ súboru:	E01 (forenzný obraz)	Obnovený súbor:	Nie	Veľkosť	~480 GB
Popis prípadu:		Podvrhnuté falošné faktúry — forenzný obraz SSD disku Petrovho notebooku Dell Latitude 5540. Primárny zdroj digitálnych stôp.					
Názov súboru:		Peter_Blaho_ssd.E01					
Miesto získania digitálnej stopy:		Dell Latitude 5540, S/N: DL5540-2025-00147 — zaistený v kancelárii Petra Blaha dňa 11.11.2025 o 15:50					
Poznámky:		Zariadenie bolo zapnuté a prihlásené pri zaistení. Pred vytvorením obrazu bol pripojený write-blocker. Originál uložený v trezore.					
Časové pečiatky							
Access:	11.11.2025 16:41		Modify:	11.11.2025 16:45		Change:	11.11.2025 16:45
Digitáln y odtlačok (heš)							
MD5		59aaeeb691699b46423c0e0737c29225					
SHA1		69a8b29a3f549a78bc1a6b1294d3c95006ca091c					
Časová pečiatka							
11.11.2025 16:00		Zachytenie RAM (FTK Imager Live Capture) pred vypnutím zariadenia					
11.11.2025 16:45		Dokončenie obrazu, overenie hash MD5 + SHA-256, kópia na forenzný server					

[-]	
Name	peterpc.001
Sector count	7636800
[-] MD5 Hash	
Computed hash	59aaeeb691699b46423c0e0737c29225
Report Hash	59aaeeb691699b46423c0e0737c29225
Verify result	Match
[-] SHA1 Hash	
Computed hash	69a8b29a3f549a78bc1a6b1294d3c95006ca09
Report Hash	69a8b29a3f549a78bc1a6b1294d3c95006ca09
Verify result	Match
[-] Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Created By Exterro® FTK® Imager 4.7.3.81

Case Information:

Acquired using: ADI4.7.3.81

Case Number: 01

Evidence Number: 01

Unique description: peterpc

Examiner: Tobiáš

Notes: image disk petrovho zariadenia

Information for C:\Users\tobil\Desktop\DFA\Peterpc\peterpc:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 475

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 7,636,800

[Physical Drive Information]

Drive Model: USB Device

Drive Serial Number: 11060208050429

Drive Interface Type: USB

Removable drive: True

Source data size: 3728 MB

Sector count: 7636800

[Computed Hashes]

MD5 checksum: 59aaeeb691699b46423c0e0737c29225 SHA1

checksum: 69a8b29a3f549a78bc1a6b1294d3c95006ca091c

Image Information:

Acquisition started: Sun Mar 29 13:38:22 2026

Acquisition finished: Sun Mar 29 13:45:49 2026

Segment list:

C:\Users\tobil\Desktop\DFA\Peterpc\peterpc.001

C:\Users\tobil\Desktop\DFA\Peterpc\peterpc.002

C:\Users\tobil\Desktop\DFA\Peterpc\peterpc.003

COMPUTED HASH : 59aaeeb691699b46423c0e0737c29225

COMPUTED HASH : 69a8b29a3f549a78bc1a6b1294d3c95006ca091c

Image Verification Results:

Verification started: Sun Mar 29 13:45:49 2026

Verification finished: Sun Mar 29 13:46:33 2026

MD5 checksum: 59aaeeb691699b46423c0e0737c29225 : verified

SHA1 checksum: 69a8b29a3f549a78bc1a6b1294d3c95006ca091c : verified

Číslo:	002	Typ súboru:	E01 (forenzný obraz)	Obnovený súbor:	Nie	Veľkosť:	~930 GB
Popis prípadu:		Podvrhnuté falošné faktúry — forenzný obraz HDD disku Martinovho PC Lenovo ThinkCentre M70s. Zariadenie podozrivého.					
Názov súboru:		martin_simko_hdd.E01					
Miesto získania digitálnej stopy:		Lenovo ThinkCentre M70s, S/N: TC-M70S-2024-00389 — zaistený v kancelárii Martina Šimku dňa 11.11.2025 o 16:00					
Poznámky:		Zariadenie bolo zapnuté a prihlásené pri zaistení. Pred vytvorením obrazu bol pripojený write-blocker. Originál uložený v trezore.					
Časové pečiatky							
Access:	11.11.2025 18:14		Modify:	11.11.2025 18:20		Change:	11.11.2025 18:20
Digitálna odtlačok (heš)							
Digitálna odtlačok (heš)	MD5	abd4d874e445e7d6cd5e225d96729b68					
	SHA-1	c65d7bb0cafb4af6f8c949332fcc3fb179430216					
Časová pečiatka							
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
11.11.2025 16:10		Zachytenie RAM z Martinovho PC (FTK Imager Live Capture)					
11.11.2025 18:20		Dokončenie obrazu, overenie hash MD5 + SHA-1, kópia na forenzný server					

[-]	
Name	martinpc.001
Sector count	60604416
[-] MD5 Hash	
Computed hash	abd4d874e445e7d6cd5e225d96729b68
Report Hash	abd4d874e445e7d6cd5e225d96729b68
Verify result	Match
[-] SHA1 Hash	
Computed hash	c65d7bb0cafb4af6f8c949332fcc3fb17943021
Report Hash	c65d7bb0cafb4af6f8c949332fcc3fb17943021
Verify result	Match
[-] Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Created By Exterro® FTK® Imager 4.7.3.81

Case Information:

Acquired using: ADI4.7.3.81

Case Number: 02

Evidence Number: 02

Unique description: martinovpc

Examiner: Tobiáš

Notes: image martinovho pc

Information for C:\Users\tobil\Desktop\DFA\Martinpc\martinpc:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 3,772

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 60,604,416

[Physical Drive Information]

Drive Model: Kingston DataTraveler 3.0 USB Device

Drive Serial Number: EE03D6515CE9

Drive Interface Type: USB

Removable drive: True

Source data size: 29592 MB

Sector count: 60604416

[Computed Hashes]

MD5 checksum: abd4d874e445e7d6cd5e225d96729b68

SHA1 checksum: c65d7bb0cafb4af6f8c949332fcc3fb179430216

Image Information:

Acquisition started: Sun Mar 29 13:39:42 2026

Acquisition finished: Sun Mar 29 14:00:08 2026

Segment list:

C:\Users\tobil\Desktop\DFA\Martinpc\martinpc.001

C:\Users\tobil\Desktop\DFA\Martinpc\martinpc.002
C:\Users\tobil\Desktop\DFA\Martinpc\martinpc.003
C:\Users\tobil\Desktop\DFA\Martinpc\martinpc.004
C:\Users\tobil\Desktop\DFA\Martinpc\martinpc.005
C:\Users\tobil\Desktop\DFA\Martinpc\martinpc.006
C:\Users\tobil\Desktop\DFA\Martinpc\martinpc.007
C:\Users\tobil\Desktop\DFA\Martinpc\martinpc.008
C:\Users\tobil\Desktop\DFA\Martinpc\martinpc.009
C:\Users\tobil\Desktop\DFA\Martinpc\martinpc.010
C:\Users\tobil\Desktop\DFA\Martinpc\martinpc.011
C:\Users\tobil\Desktop\DFA\Martinpc\martinpc.012
C:\Users\tobil\Desktop\DFA\Martinpc\martinpc.013
C:\Users\tobil\Desktop\DFA\Martinpc\martinpc.014
C:\Users\tobil\Desktop\DFA\Martinpc\martinpc.015
C:\Users\tobil\Desktop\DFA\Martinpc\martinpc.016
C:\Users\tobil\Desktop\DFA\Martinpc\martinpc.017
C:\Users\tobil\Desktop\DFA\Martinpc\martinpc.018
C:\Users\tobil\Desktop\DFA\Martinpc\martinpc.019
C:\Users\tobil\Desktop\DFA\Martinpc\martinpc.020
COMPUTED HASH : abd4d874e445e7d6cd5e225d96729b68
COMPUTED HASH : c65d7bb0cafb4af6f8c949332fcc3fb179430216

Image Verification Results:

Verification started: Sun Mar 29 14:00:08 2026

Verification finished: Sun Mar 29 14:05:47 2026

MD5 checksum: abd4d874e445e7d6cd5e225d96729b68 : verified

SHA1 checksum: c65d7bb0cafb4af6f8c949332fcc3fb179430216 : verified

9 Časová os incidentu

Nasledujúca tabuľka rekonštruje kľúčové udalosti na základe dostupných forenzných zdrojov.

Dátum / čas	Zdroj záznamu	Udalosť
10.11. 09:00	Výpoveď / kalendár	Povýšenie Petra Blaha — Martin Šimko sa dozvie.
10.11. ~11:30–13:30	Chrome History (prázdne)	⚠ GAP 1 — vymazaná história prehliadača Martinovho PC. Predpokladané vyhľadávanie IBAN-u (orsr.sk).
10.11. ~13:30	Prefetch / \$MFT / PDF metadata	Martin pripraví sfalšované faktúry na vlastnom PC v LibreOffice. Metadata: Author = Martin Šimko.
11.11. 08:50	Event ID 4624 / ShellBags	Peter príde do práce, prihlási sa, otvorí zložku s overenými faktúrami — posledná kontrola.
11.11. 08:55	Event ID 4624 (Martin)	Martin príde do práce, prihlási sa na vlastný PC. RAM capture aktívna od tohto momentu.

11.11. 11:30	Event ID 4800 (absentuje)	Peter odíde na obedovú prestávku. Notebook odomknutý.
11.11. 11:32:15	Event ID 6416 / setupapi.dev.log	⚠ GAP 2 — USB (SanDisk VID_0781/PID_5571) pripojené k Petrovmu notebooku. Martin skopíruje originálne faktúry.
11.11. 11:36:40	setupapi.dev.log	USB odpojené. Martin odíde pred Petrovým návratom (~4 min).
11.11. ~11:50	LNK / ShellBags	Peter sa vráti — nič nezaregistruje, zložku znova neotvorí.
11.11. 12:05– 13:10	Prefetch / \$MFT / RAM	Martin finalizuje faktúry na vlastnom PC, skopíruje sfalšované verzie na USB.
11.11. 14:05	Event ID 4800 (absentuje)	Peter odíde na záchod. Notebook znova odomknutý.
11.11. 14:07:43	Event ID 6416 / setupapi.dev.log	USB pripojené k Petrovmu notebooku — druhá návšteva Martina (to isté VID/PID).
11.11. 14:08– 14:09	\$MFT / nealokovaný priestor	Originálne faktúry zmazané, sfalšované premenované na pôvodné názvy a podpísané.
11.11. 14:09:20	setupapi.dev.log	USB odpojené. Martin opustí kanceláriu (~90 sek celkom).
11.11. 14:16	ShellBags / LNK / RAM	Peter sa vráti, otvorí faktúry bez opätovnej kontroly.
11.11. 14:31:07	Exchange MessageTracking / OST	E-mail odoslaný z peter.blaho@firma.sk na účtovné oddelenie. IP: 192.168.1.47.
11.11. ~14:50	Exchange log / výpoveď	Účtovné oddelenie zistí zmenený IBAN, informuje vedenie.
11.11. 15:30	Chain of Custody	Zaistenie zariadení. RAM dump Petra (15:30), Martina (15:40). Disk imaging, hash.

10 Výsledok hypotéz

9.1 Hypotéza H1 – Zamietnutá

Hypotéza, že Peter Blaho faktúry pozmenil sám a vedome ich odoslal, bola **zamietnutá**. Analýza metadát sfalšovaných faktúr nepreukázala Petra Blaha ako autora úprav — program, v ktorom boli faktúry naposledy editované, sa na jeho notebooku nenachádzal. Absencia Event ID 4800 v oboch kritických časových oknách (11:30–11:50 a 14:05–14:16) potvrdzuje, že notebook zostal odomknutý a tretia osoba mala k nemu fyzický prístup bez potreby Petrovho hesla. Záznamy Exchange servera potvrdili, že e-mail bol odoslaný z aktívnej relácie Petra, avšak v čase, keď sa Peter vrátil k počítaču a faktúry otvoril bez opätovnej kontroly obsahu. (Dôkaz 1 — Metadata sfalšovaných faktúr)

9.2 Hypotéza H2 – Čiastočne potvrdená

Hypotéza o neznámom páchatelovi s fyzickým prístupom do kancelárie bola **čiastočne potvrdená**. Absencia Event ID 4800 (uzamknutie obrazovky) v oboch kritických časových oknách jednoznačne preukazuje, že notebook Petra Blaha zostal odomknutý a neznáma osoba mala k nemu voľný fyzický prístup bez akejkoľvek autentifikácie. Absencia Event ID 4624 pre akýkoľvek cudzí účet vylučuje prihlásenie sa používateľa cez sieť. Páchatel však neostal neznámy — na základe nadväzujúcich dôkazov bol identifikovaný ako Martin Šimko (H3). (Dôkaz 3 — CreationDate paradox, Dôkaz 4 — USB záznamy)

9.3 Hypotéza H3 – Čiastočne potvrdená

Hypotéza identifikujúca Martina Šimka ako páchatela bola **čiastočne potvrdená**. Viaceré digitálne stopy na Martinovom PC priamo indikujú jeho účasť: Prefetch súbor SOFFICE.EXE preukazuje spustenie LibreOffice v kritickom časovom okne, RAM artefakty zachytili IBAN Blaho Consulting s.r.o. v clipboarde a aktívny proces úpravy dokumentu, história prehliadača bola systematicky vymazaná práve v časovom úseku relevantnom pre prípravu podvodu (10.11. 11:30–13:30 a celý 11.11.). Zhoda VID/PID a sériového čísla USB zariadenia na oboch PC priamo prepája Martina s fyzickým prenosom súborov. Hypotéza je čiastočne potvrdená, nakoľko USB nosič nebol fyzicky zaistený a priamy dôkaz prítomnosti Martina v kancelárii Petra chýba. (Dôkaz 1, Dôkaz 2, Dôkaz 4, Dôkaz 6)

9.4 Hypotéza H4 – Potvrdená

Hypotéza o použití externého USB nosiča bola **potvrdená**. Záznamy setupapi.dev.log a register HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR na Petrovom notebooku zachytili dve pripojenia zariadenia SanDisk Cruzer Blade (VID_0781/PID_5571, sériové číslo: 4C530012341223101524) — o 11:32:15 a 14:07:43. Záznamy Martinovho PC evidujú dve pripojenia toho istého zariadenia: 10.11.2025 o 14:23:12 a 11.11.2025 o 13:16:03. Zhoda VID/PID aj sériového čísla na oboch PC jednoznačne preukazuje, že ide o to isté fyzické USB zariadenie použité pri príprave aj realizácii podvrhnutia. Časy pripojenia presne korelujú s časovou osou podvodu. (Dôkaz 4 — USB záznamy)

9.5 Hypotéza H5 – Potvrdená

Hypotéza o úmyselnom zmazení originálnych faktúr bola **potvrdená**. Modul File Recovery nástroja Autopsy obnovil z nealokovaného priestoru Samsung SSD Petrovho notebooku dve originálne faktúry (faktura_2025_10_BC_ORIG.pdf a faktura_2025_10_IT_ORIG.pdf) s korektným IBAN-om. Analýza ExifTool potvrdila CreationDate paradox: originálne súbory majú dátum vytvorenia z októbra 2025, kým sfalšované súbory so zhodným názvom majú CreationDate 11.11.2025 ~13:xx — čo je priamy dôkaz výmeny súborov. Čas zmazania zaznamenaný v \$MFT (14:08–14:09) presne korešponduje s časovou osou podvodu. (Dôkaz 3 — CreationDate paradox, Dôkaz 5 — Obnovenie originálnej faktúry)

11 Literatúra

- Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley. — Analýza \$MFT, NTFS, obnova zmazených súborov.
- <https://dfirws.org/wp-content/uploads/2017/08/Windows-Event-Logs.pdf> — Využitie Windows Event Logov pri rekonštrukcii používateľskej aktivity.

-
- <https://www.sciencedirect.com/science/article/pii/S1742287619301707> — Forezná analýza e-mailovej komunikácie a identifikácia odosielateľa.