

UNIVERZITA SV. CYRILA A METODA V TRNAVE

FAKULTA PRÍRODNÝCH VIED

ÚSTAV POČÍTAČOVÝCH TECHNOLOGIÍ A INFORMATIKY

KRÁDEŽ FOTOGRAFIÍ Z PRACOVNÉHO POČÍTAČA

SEMESTRÁLNY PROJEKT

[Prezentácia](#)

Ročník: 2.

Krúžok: 6

Ak. rok: 2025/2026

Simona Hamárová

Obsah

1	Prípád	3
1.1	Opis prípadu	3
1.2	Predmet vyšetrovania.....	3
1.3	Cieľ vyšetrovania.....	3
1.4	Metóda 5WH	4
1.4.1	WHO (Kto)	4
1.4.2	WHAT (Čo)	4
1.4.3	WHEN (Kedy)	4
1.4.4	WHERE (Kde).....	4
1.4.5	WHY (Prečo)	4
1.4.6	HOW (Ako)	4
1.5	Odborný príspevok – DFRWS.....	5
2	Hypotézy	6
2.1	Hypotéza 1	6
2.1.1	Výsledok hypotézy 1 – potvrdená.....	6
2.2	Hypotéza 2.....	6
2.2.1	Výsledok hypotézy 2 – potvrdená.....	6
2.3	Hypotéza 3	6
2.3.1	Výsledok hypotézy 3 – potvrdená.....	6
3	Zaistené zariadenia	7
3.1	Notebook – Tomáš Urban (poškodený).....	7
3.1.1	Fotografia a vlastnosti zariadenia	7
3.1.2	Chain of custody EVID-001	8
3.2	USB – Martin Kováč (podozrivý)	8
3.2.1	Fotografia a vlastnosti zariadenia	8
3.2.2	Chain of custody	9
3.3	Notebook – Martin Kováč (podozrivý)	9
3.3.1	Fotografia a vlastnosti zariadenia	9
4	Dáta	10

5	Zber dôkazov	12
5.1	Notebook – Tomáš Urban (poškodený).....	12
5.1.1	Logy USB - Autopsy	12
5.1.2	Evidencia USB zariadení	12
5.1.3	Autopsy	13
5.1.4	Obraz RAM.....	14
5.2	USB – Martin Kováč (podozrivý)	15
5.2.1	Autopsy	15
5.3	Notebook – Martin Kováč (podozrivý)	16
5.3.1	Autopsy	16
5.3.2	Obraz RAM.....	18
6	Image zariadení	21
6.1	Notebook – Tomáš Urban (poškodený).....	21
6.2	USB – Martin Kováč (podozrivý)	22
6.3	Notebook – Martin Kováč (podozrivý)	23
7	Softvérové nástroje.....	24
8	Bezpečnostné opatrenia.....	25
8.1	Bitové kópie.....	25
8.1.1	Notebook – Tomáš Urban (poškodený)	25
8.1.2	USB – Martin Kováč (podozrivý).....	25
8.1.3	Notebook – Martin Kováč (podozrivý).....	25
8.2	Chain of custody	26
8.2.1	Notebook – Tomáš Urban (poškodený)	26
8.2.2	USB – Martin Kováč (podozrivý).....	27
8.2.3	Notebook – Martin Kováč (podozrivý).....	28

1 Prípád

1.1 Opis prípadu

Zamestnanec v marketingovej agentúre odišiel 29.3.2026 počas obeda z kancelárie a nechal notebook odomknutý. Kolega, ktorý vedel o uložených osobných fotografiách, sa posadil k notebooku, pripojil firemný USB kľúč a fotografie skopíroval. Originály presunul do koša, no nestihol ho vyprázdniť. Na svojom notebooku fotografie zverejnil cez falošný profil na sociálnej sieti s cieľom poškodiť kolegovu reputáciu. Poškodený sa o zverejnení dozvedel od kolegov a vo svojom notebooku našiel vymazaný priečinok s fotografiami, ktorý obnovil.

1.2 Predmet vyšetrovania

Vyšetrovanie sa zameriava na neoprávnené použitie notebooku poškodeného zamestnanca marketingovej agentúry a krádež jeho osobných fotografií. Predmetom analýzy sú tri zaistené zariadenia – notebook poškodeného (EVID-001), firemný šifrovaný USB kľúč podozrivého (EVID-002) a notebook podozrivého (EVID-003). Kľúčovou úlohou je prepojiť digitálne stopy na týchto zariadeniach s konkrétnou osobou a vytvoriť časový priebeh incidentu.

1.3 Cieľ vyšetrovania

Cieľom je forenzne preukázať, že podozrivý využil neprítomnosť poškodeného počas obedovej prestávky, neoprávnene použil jeho notebook a skopíroval osobné fotografie na firemné šifrované USB zariadenie. Konkrétne výsledky, ktoré má vyšetrovanie priniesť:

- identifikácia USB zariadenia pripojeného k notebooku poškodeného na základe sériového čísla a firemnej evidencie zariadení,
- potvrdenie kopírovania fotografií na USB zariadenie podozrivého, preukázanie prítomnosti odcudzených fotografií na notebooku a zaznamenanými prihlasovacími údajmi k falošným účtom,
- potvrdenie aktivity spojenej s vytvorením falošného Gmail a Instagram účtu a zverejnením fotografií prostredníctvom analýzy RAM pamäte notebooku podozrivého.

1.4 Metóda 5WH

1.4.1 WHO (Kto)

Poškodeným je zamestnanec marketingovej agentúry. Podozrivým je jeho kolega zo spoločnej kancelárie, ktorý s ním súperí o vyššiu pracovnú pozíciu. Je identifikovaný cez firemnú evidenciu USB zariadení — sériové číslo z logov notebooku patrí práve jemu.

1.4.2 WHAT (Čo)

Neoprávnené použitie cudzieho notebooku (Tomáša Urbana), skopírovanie osobných fotografií na firemný šifrovaný USB kľúč, ich vymazanie do koša bez vyprázdnenia a zverejnenie cez falošný profil na sociálnej sieti na notebooku podozrivého (Martina Kováča).

1.4.3 WHEN (Kedy)

Krádež fotografií prebehla počas obednej prestávky poškodeného. Zverejnenie fotografií prebehli po skončení pracovnej zmeny.

1.4.4 WHERE (Kde)

Krádež: kancelária poškodeného.

Zverejnenie: sociálna sieť cez falošný profil.

1.4.5 WHY (Prečo)

Kariérna rivalita o vyššiu pracovnú pozíciu a snaha poškodiť reputáciu kolegu.

1.4.6 HOW (Ako)

Využitím odomknutého notebooku poškodeného, kopírovaním fotografií na vlastný firemný šifrovaný USB kľúč, vymazaním originálov do koša (bez vyprázdnenia), vytvorením falošného profilu a zverejnením fotografií poškodeného s negatívnymi popismi pod príspevkom, čím cielene poškodzoval reputáciu kolegu a firmy.

1.5 Odborný príspevok – DFRWS

<https://dfrws.org/presentation/duck-hunt-memory-forensics-of-usb-attack-platforms>

Tento článok sa zaoberá tým, ako sa dajú zistiť stopy po použití USB zariadení v počítači. Ukazuje, že aj po odpojení USB kľúča zostávajú v systéme rôzne informácie, napríklad identifikátory zariadenia alebo záznamy o jeho použití. Tieto údaje vie forenzný analytik použiť na zistenie, či bolo USB pripojené a čo sa mohlo diať. V praxi sa to využíva napríklad pri prípadoch, keď niekto skopíruje dáta (napr. fotografie) na USB zariadenie bez povolenia.

2 Hypotézy

2.1 Hypotéza 1

Počas neprítomnosti poškodeného v priebehu obedovej prestávky došlo k neoprávnenému použitiu pracovného počítača a odcudzeniu fotografií zamestnancom.

2.1.1 Výsledok hypotézy 1 – potvrdená

Dňa 29.3.2026 v priebehu obedovej prestávky bolo o 11:37:49 k notebooku poškodeného pripojené USB zariadenie so sériovým číslom 60A44C425569FD71F21A2A27&0 a odpojené o 11:39:09 (dôkaz v podkapitole 5.1.1). Na základe firemnej evidencie USB zariadení bolo toto zariadenie identifikované ako USB kľúč patriaci Martinovi Kováčovi (dôkaz v podkapitole 5.1.2). Analýzou obrazu disku USB zariadenia bolo preukázané, že v čase 11:38:55 — teda medzi pripojením a odpojením zariadenia — došlo ku kopírovaniu priečinka s názvom „fotky“ z notebooku poškodeného (dôkaz v podkapitole 5.2.1).

2.2 Hypotéza 2

Odcudzené fotografie sa nachádzajú na zariadení podozrivého.

2.2.1 Výsledok hypotézy 2 – potvrdená

Vymazaný priečink s fotografiami bol nájdený na USB zariadení Martina Kováča (dôkaz v podkapitole 5.2.1). Fotografie boli následne objavené aj na notebooku podozrivého (EVID-003), a to v priečinku, ktorý okrem fotografií obsahoval aj dokumenty nasvedčujúce tomu, že podozrivý po určitú dobu sledoval pohyb poškodeného Tomáša Urbana počas prestávky. V rovnakom priečinku boli nájdené aj zaznamenané prihlasovacie údaje k falošnému Gmail a Instagram účtu (dôkazy v podkapitole 5.3.1).

2.3 Hypotéza 3

Podozrivý zverejnil fotografie na sociálnu sieť cez falošný profil.

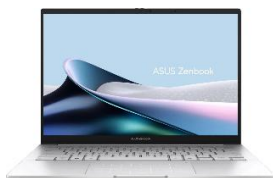
2.3.1 Výsledok hypotézy 3 – potvrdená

Analýzou obrazu RAM pamäte notebooku podozrivého bola zachytená aktivita spojená s vytváraním falošného Gmail a Instagram účtu a tvorbou príspevkov na Instagrame (dôkaz v podkapitole 5.3.2). Analýza obrazu RAM pamäte notebooku poškodeného žiadnu podobnú aktivitu s falošnými prihlasovacími údajmi nepreukázala (dôkaz v podkapitole 5.1.4), čím bolo vylúčené, že by táto činnosť pochádzala zo zariadenia Tomáša Urbana.

3 Zaistené zariadenia

3.1 Notebook – Tomáš Urban (poškodený)

3.1.1 Fotografia a vlastnosti zariadenia



Identifikácia zariadenia	
Model	ASUS Zenbook 14 UX3405CA
Procesor (CPU)	
Model procesora	Intel Core Ultra 7 255H (Series 2, Arrow Lake-H)
Operačná pamäť (RAM)	
Kapacita	16 GB
Úložisko (sekundárna pamäť)	
Kapacita SSD	512 GB (podľa konfigurácie)
Displej	
Uhlopriečka	14,0"
Rozlíšenie / pomer strán	WUXGA 1920 × 1200, 16:10
Panel	OLED (Lumina OLED), dotykový
Obnovovacia frekvencia	60 Hz
Grafická karta (GPU)	
Model	Intel Arc Graphics (integrovaná)
Konektivita a porty	
USB-A	1× USB 3.2 Gen 1 Type-A
Operačný systém a batéria	
Operačný systém	Windows 11 Home / Pro
Parametre relevantné pre vyšetrenie	
Rozhranie disku	NVMe PCIe 4.0 (nie SATA) – write-blocker musí podporovať M.2/PCIe
RAM (volatilná pamäť)	16 GB LPDDR5X – pri vypnutom zariadení obsah stratený
Secure Boot / TPM	TPM 2.0, Secure Boot (UEFI)

3.1.2 Chain of custody EVID-001

3.2 USB – Martin Kováč (podozrivý)

3.2.1 Fotografia a vlastnosti zariadenia



Identifikácia zariadenia	
Výrobca / Model	Kingston DataTraveler 2.0 USB Device 8GB
Technické parametre	
Kapacita	8 GB (nominálna)
Typ pamäte	Flash (NAND)
Rozhranie / verzia USB	USB 2.0 High-Speed (spätne kompatibilné s USB 3.0/3.1)
Konektor	USB-A (Type-A), štandardný
LED indikátor	Áno – svieti pri pripojení, bliká pri prenose dát
Parametre relevantné pre vyšetrovanie	
Typ rozhrania	USB 2.0 – write-blocker musí podporovať USB mass storage
Sériové číslo	60A44C425569FD71F21A2A27&0 (zaznamenané v USBSTOR registri notebooku)
Odporúčaný postup	Pripojiť cez USB write-blocker, vytvoriť .E01 obraz (FTK Imager), overiť MD5/SHA1 hash
Volatilita	Nie – flash pamäť je nevolatilná (obsah zachovaný aj bez napájania)

3.2.2 Chain of custody

3.3 Notebook – Martin Kováč (podozrivý)

3.3.1 Fotografia a vlastnosti zariadenia

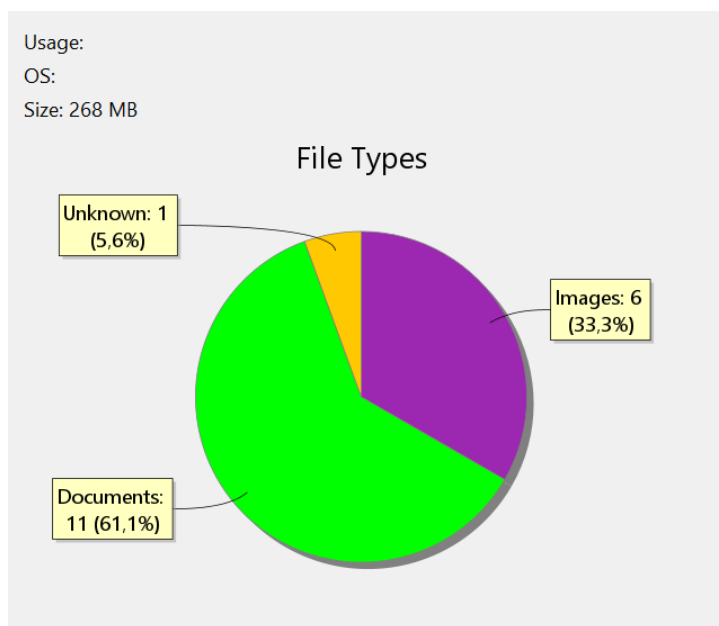


Identifikácia zariadenia	
Model	ASUS Zenbook 14 UX3405CA
Procesor (CPU)	
Model procesora	Intel Core Ultra 7 255H (Series 2, Arrow Lake-H)
Operačná pamäť (RAM)	
Kapacita	16 GB
Úložisko (sekundárna pamäť)	
Kapacita SSD	512 GB (podľa konfigurácie)
Displej	
Uhlopriečka	14,0"
Rozlíšenie / pomer strán	WUXGA 1920 × 1200, 16:10
Panel	OLED (Lumina OLED), dotykový
Obnovovacia frekvencia	60 Hz
Typ	Integrovaná (iGPU)
Konektivita a porty	
USB-C / Thunderbolt	2× Thunderbolt™ 4 (40 Gbps, display + PD)
HDMI	1× HDMI 2.1 TMDS
Kapacita batérie	75 Wh
Výdrž (výrobca)	až ~15 hodín (video playback)
RAM (volatilná pamäť)	16 GB LPDDR5X – pri vypnutom zariadení obsah stratený

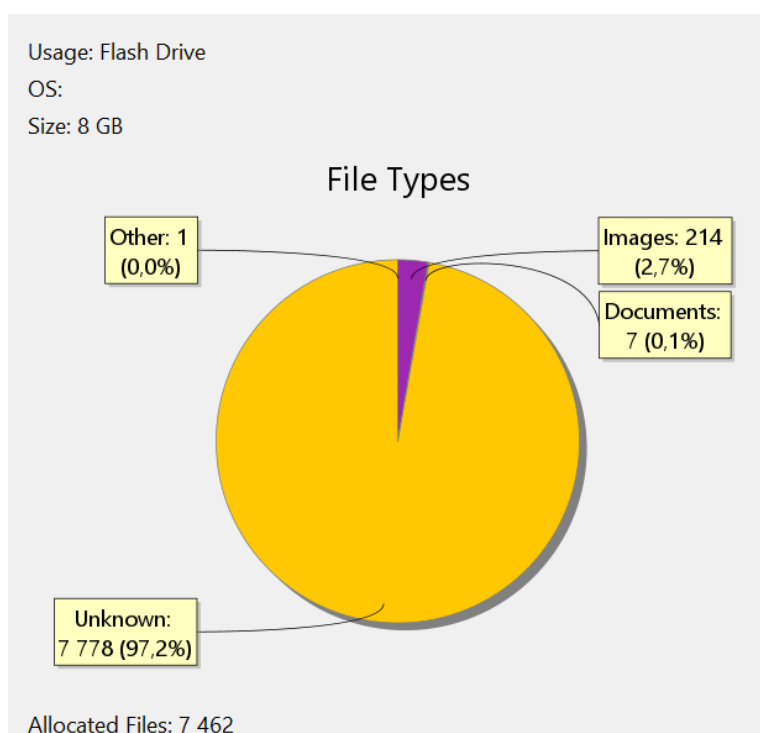
4 Dáta

- Z tohto odkazu https://cfreds-archive.nist.gov/data_leakage_case/data-leakage-case.html boli stiahnuté datasety:
 - Notebook poškodeného: [pc.E01](#) (1,99GB) – využitý na vytvorenie obrazu disku v Exterro FTK Imager 4.7.3.81
 - Notebook podozrivého: [pc.E03](#) (1,99GB) – využitý na vytvorenie obrazu disku v Exterro FTK Imager 4.7.3.81
- USB podozrivého: vlastné dáta – využitý na vytvorenie obrazu disku v Exterro FTK Imager 4.7.3.81 a analýzu v Autopsy
- Fotografie: generované pomocou ChatGPT
- Úprava EXIF metadát fotografií: <https://metadata-editor.com>
- Obrazy diskov notebookov poškodeného a podozrivého, ktoré obsahujú logy USB, word a textový dokument, priecinok s fotografiami: generované pomocou Claude (Sonnet 4.6) – využité na analýzu v Autopsy (268MB)

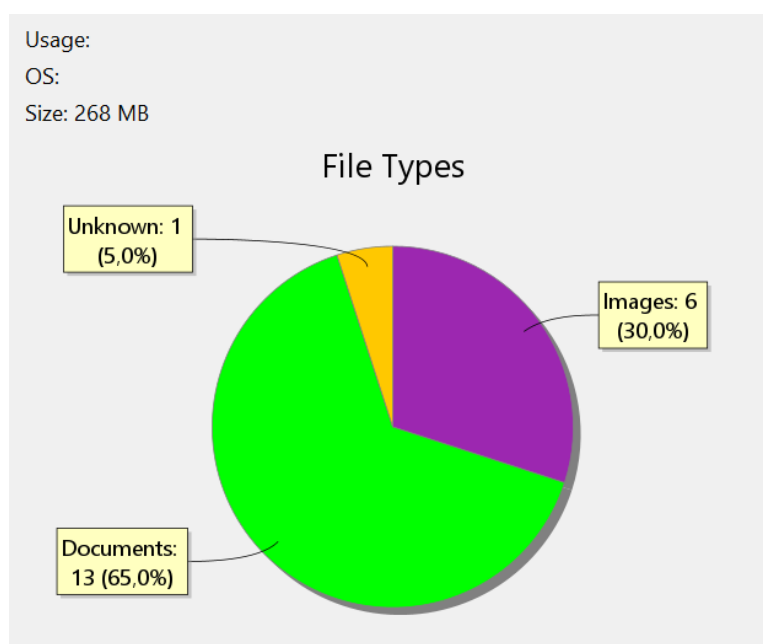
Celkovo bolo analyzovaných na obraze disku notebooku poškodeného (Tomáša Urbana):



Celkovo bolo analyzovaných na obrazu disku USB podozrivého (Martina Kováča):



Celkovo bolo analyzovaných na obrazu disku notebooku podozrivého (Martina Kováča):

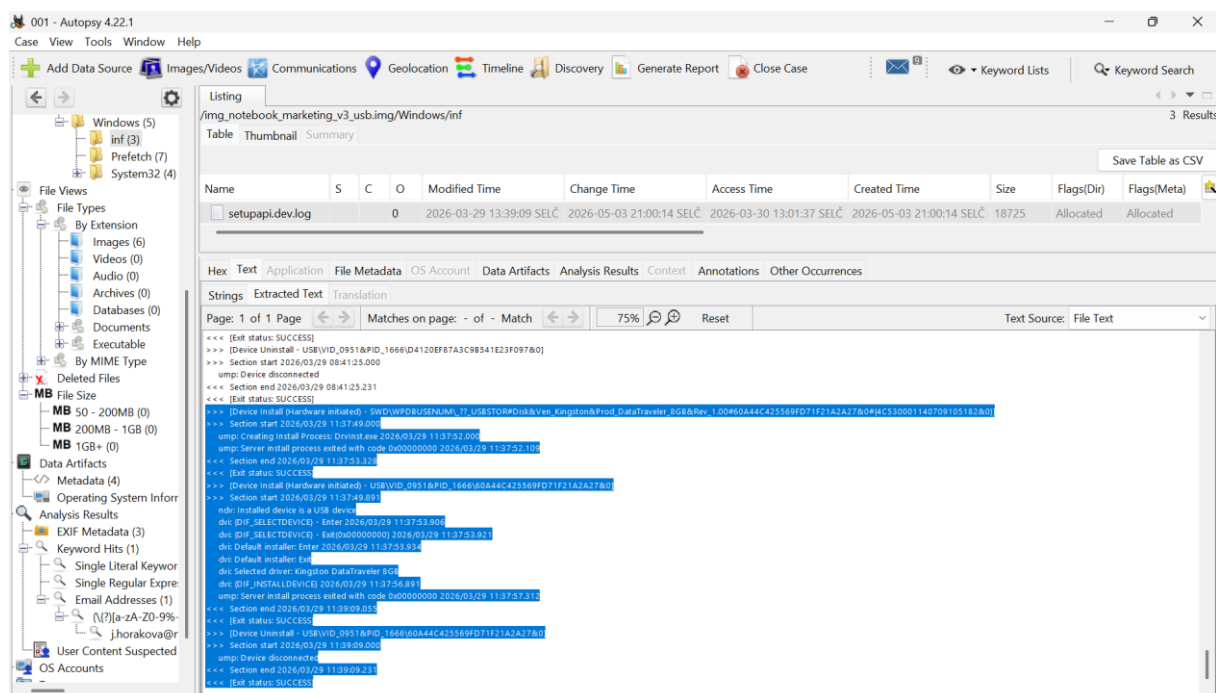


5 Zber dôkazov

5.1 Notebook – Tomáš Urban (poškodený)

5.1.1 Logy USB - Autopsy

Podľa analýzy USB logov bolo dňa 29. 3. 2026 počas obedovej prestávky pripojené USB zariadenie Kingston DataTraveler 8 GB so sériovým číslom 60A44C425569FD71F21A2A27&0, a to v čase 11:37:49, pričom odpojené bolo o 11:39:09. Operačný systém Windows pri pripojení nainštaloval ovládač, čo naznačuje, že toto zariadenie bolo k danému systému pripojené prvýkrát.



5.1.2 Evidencia USB zariadení

Na základe firemnej evidencie USB zariadení poskytnutej zamestnávateľom bolo USB so sériovým číslom 60A44C425569FD71F21A2A27&0 identifikované ako zariadenie pridelené zamestnancovi Martinovi Kováčovi.

Meno zamestnanca	Pridelené zariadenie	Sériové číslo
Jana Bieliková	Kingston DataTraveler 8GB	B7F23190CC5D4A8E2F014B62&0
Martin Kováč	Kingston DataTraveler 8GB	60A44C425569FD71F21A2A27&0
Andrej Král	Kingston DataTraveler 8GB	F19234DC6A0B8E57310CF2A4&0
Peter Novák	Kingston DataTraveler 8GB	AA00D987B3C14E2F19AB3301&0
Lucia Novotná	Kingston DataTraveler 8GB	9B4E270FD83C1A650E72BC34&0
Veronika Šimková	Kingston DataTraveler 8GB	8C3F00A21B7D5E94CF301A88&0
Tomáš Urban	Kingston DataTraveler 8GB	D4120EF87A3C9B541E23F097&0
Katarína Vargová	Kingston DataTraveler 8GB	3E70B14A9C2D5F836E01AD50&0

5.1.3 Autopsy

Po analýze priečinka „fotky“ boli identifikované tri fotografie, na ktorých sa nachádza Tomáš Urban (poškodený) a EXIF metadáta sa zhodujú s EXIF metadátami fotografií Tomáša Urbana.

EVID_001 - 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

Listing

/img_notebook_poskodeny-Tomas_Urban.img/fotky

Table Thumbnail Summary

Page: 1 of 1 Pages: Go to Page: Images: 1-3 Medium Thumbnails Sort Sorted by: ---

dovolenka.jpg hokej.jpg praca.jpg

/img_notebook_poskodeny-Tomas_Urban.img/fotky/dovolenka.jpg

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

Item: dovolenka.jpg

Aggregate Score: Not Notable

Analysis Result 1

Score: Not Notable

Type: EXIF Metadata

Configuration:

Conclusion:

Justification:

Device Make: Apple

Device Model: iPhone14

Latitude: 36.21748

Longitude: 27.57148

Analysis Result 2

EVID_001 - 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

Listing

/img_notebook_poskodeny-Tomas_Urban.img/fotky

Table Thumbnail Summary

Page: 1 of 1 Pages: Go to Page: Images: 1-3 Medium Thumbnails Sort Sorted by: ---

dovolenka.jpg hokej.jpg praca.jpg

/img_notebook_poskodeny-Tomas_Urban.img/fotky/hokej.jpg

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

Item: hokej.jpg

Aggregate Score: Not Notable

Analysis Result 1

Score: Not Notable

Type: EXIF Metadata

Configuration:

Conclusion:

Justification:

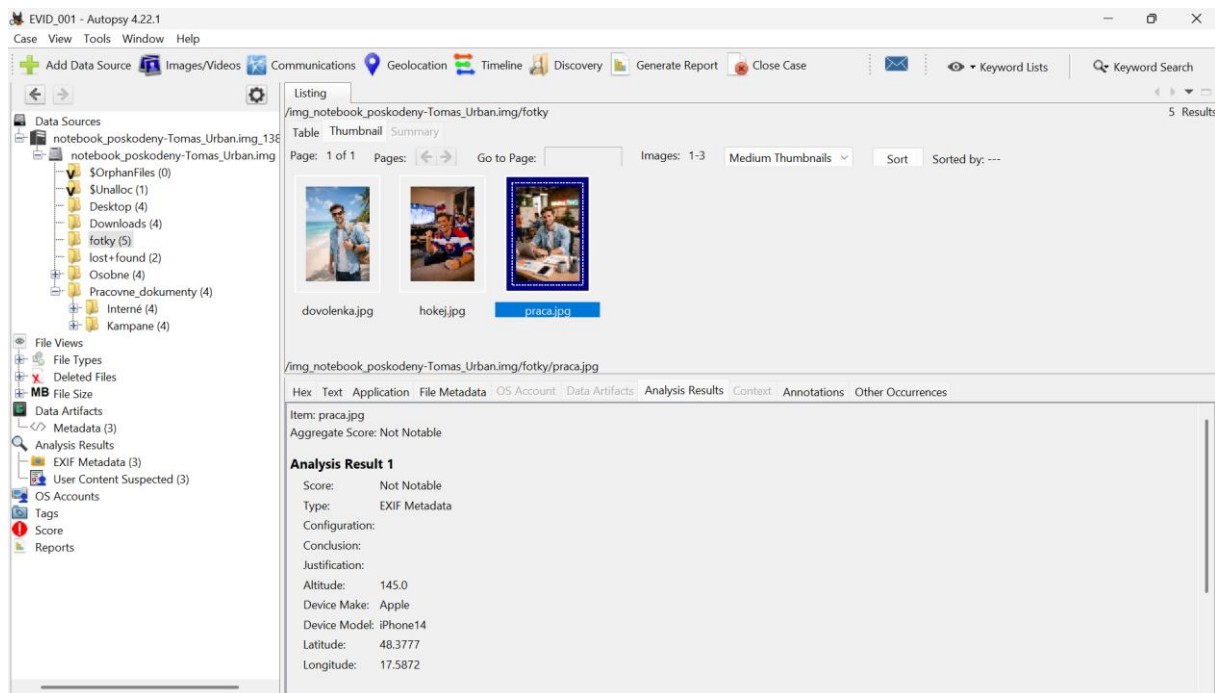
Device Make: Apple

Device Model: iPhone14

Latitude: 48.379645500054416

Longitude: 17.579924500103072

Analysis Result 2



Autopsy Forensic Rep- x

file:///C:/Users/Admin/Desktop/skola%20-%20APIN/2.%20ročník%20LS/Digitalná%20forenzná%20analýza/Daatsety/Notebook%

EXIF Metadata

Date Taken	Device Manufacturer	Device Model	Latitude	Longitude	Altitude	Source File
	Apple	iPhone14	36.21748	27.57148		/img_notebook_poskodeny-Tomas_Urban.img/fotky/dovolenka.jpg
	Apple	iPhone14	48.3777	17.5872	145.0	/img_notebook_poskodeny-Tomas_Urban.img/fotky/praca.jpg
	Apple	iPhone14	48.379645500054416	17.579924500103072		/img_notebook_poskodeny-Tomas_Urban.img/fotky/hokej.jpg

5.1.4 Obraz RAM

Analýza obrazu RAM neodhalila žiadnu aktivitu pod prihlasovacím menom „urban.tomas“.

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text

```

78F772430 74 20 28 32 4B 4F 4D 55 2D 42 63 45 32 33 29 00 t (2KOMU-BcE23)..
78F772440 06 00 07 03 00 00 D5 B1 BC 00 13 00 C0 2F 6F 3D .....ôL...r/o=
78F772450 45 78 63 68 61 6E 67 65 4C 61 62 73 2F 6F 75 3D ExchangeLabs/ou=
78F772460 45 78 63 68 61 6E 67 65 20 41 64 6D 69 6E 69 73 Exchange Adminis
78F772470 74 72 61 74 69 76 65 20 47 72 6F 75 70 20 28 46 trative Group (F
78F772480 59 44 49 42 4F 48 46 32 33 53 50 44 4C 54 29 2F YDIBOHF23SPDLT)/
78F772490 63 6E 3D 52 65 63 69 70 69 65 6E 74 73 2F 63 6E cn=Recipients/cn
78F7724A0 3D 64 64 31 36 32 61 61 36 64 34 61 62 34 35 31 =dd162aa6d4ab451
78F7724B0 38 38 35 38 61 61 36 30 39 62 37 62 62 66 38 34 8858aa609b7bbf84
78F7724C0 61 2D 33 30 30 31 39 39 00 74 6F 6D 61 73 2E 66 a-300199.tomas.f
78F7724D0 61 72 6B 61 73 40 75 63 6D 2E 73 6B 00 06 53 49 arkas@ucm.sk..SI
78F7724E0 50 3A 33 30 30 31 39 39 40 75 63 6D 2E 73 6B 00 P:300199@ucm.sk.
78F7724F0 53 4D 54 50 3A 74 6F 6D 61 73 2E 66 61 72 6B 61 SMTP
78F772500 73 40 75 63 6D 2E 73 6B 00 53 50 4F 3A 53 50 4F s@ucm
78F772510 5F 30 35 39 30 32 61 61 66 2D 37 31 36 32 2D 34 _059
78F772520 63 66 34 2D 39 65 35 38 2D 64 65 34 37 64 36 30 CF4-
78F772530 36 32 62 62 40 53 50 4F 5F 64 31 35 64 31 31 62bb
78F772540 30 30 2D 64 37 34 34 2D 34 62 30 39 2D 38 61 66 00-d
78F772550 39 2D 35 38 31 38 34 30 64 36 34 34 35 30 00 53 9-58
78F772560 50 4F 3A 53 50 4F 5F 65 63 33 64 34 66 33 33 2D P0:SI
78F772570 32 62 39 31 2D 61 39 61 32 2D 65 36 66 30 2D 63 2b91
78F772580 31 66 64 39 34 37 63 31 34 62 65 40 53 50 4F 5F 1fd94
78F772590 64 31 35 64 31 31 30 30 2D 64 37 34 34 2D 34 62 d15d1100-d744-4b
78F7725A0 30 39 2D 38 61 66 39 2D 35 38 31 38 34 30 64 36 09-8af9-581840d6

```

Information

Can't find 'urban.tomas'.

OK

Data inspector

Binary (8 bit) 01110100

Int8 go.to: 116

UInt8 go.to: 116

Int16 go.to: 28532

UInt16 go.to: 28532

Int24 go.to: 7171956

UInt24 go.to: 7171956

Int32 go.to: 1634561908

UInt32 go.to: 1634561908

Int64 go.to: Invalid

UInt64 go.to: Invalid

LEB128 go.to: -12

ULEB128 go.to: 116

AnsiChar / char8_t t

UnicodeChar / char16_t

Byte order

☒ Little endian ☐ Big endian

☐ Hexadecimal basis (for integral numbers)

Checksum Search (0 hits)

Offset Excerpt (hex) Excerpt (text)

Offset(h): 78F7724F5 Block(h): 78F7724F5-78F7724F9 Length(h): 5 Overwrite

5.2 USB – Martin Kováč (podozrivý)

5.2.1 Autopsy

Z analýzy obrazu disku USB vyplýva, že sa na ňom nachádzal vymazaný priečinok „fotky“, ktorý bol vytvorený dňa 29. 3. 2026 o 11:38:55 počas prestávky.

The screenshot shows the Autopsy software interface. On the left is a 'Data Sources' tree with a folder named 'Martin' expanded, showing subfolders like '\$OrphanFile', '\$Unalloc (', 'O: - \$R', '0-WYLA', '1_sy_pri', 'creeny', and '_otky'. The main pane displays a 'Listing' of files in the '/img_D/_otky' directory. Below the listing is a 'Metadata' section for the selected file '_otky'.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	MDS Hash
0-WYLA				2021-06-15 22:06:48 SELČ	0000-00-00 00:00:00	2025-02-24 01:00:00 SELČ	2021-06-15 22:06:46 SELČ	0	Unallocated	Unallocated	unknown	
1_sy_prih				2021-01-03 18:04:48 SELČ	0000-00-00 00:00:00	2021-01-03 01:00:00 SELČ	2021-01-03 18:38:55 SELČ	4096	Allocated	Allocated	unknown	
creeny				2023-06-13 13:39:28 SELČ	0000-00-00 00:00:00	2023-06-13 01:00:00 SELČ	2023-06-13 13:39:27 SELČ	0	Unallocated	Unallocated	unknown	
_otky				2026-03-29 11:22:34 SELČ	0000-00-00 00:00:00	2026-03-29 11:38:55 SELČ	2026-03-29 11:38:55 SELČ	0	Unallocated	Unallocated	unknown	

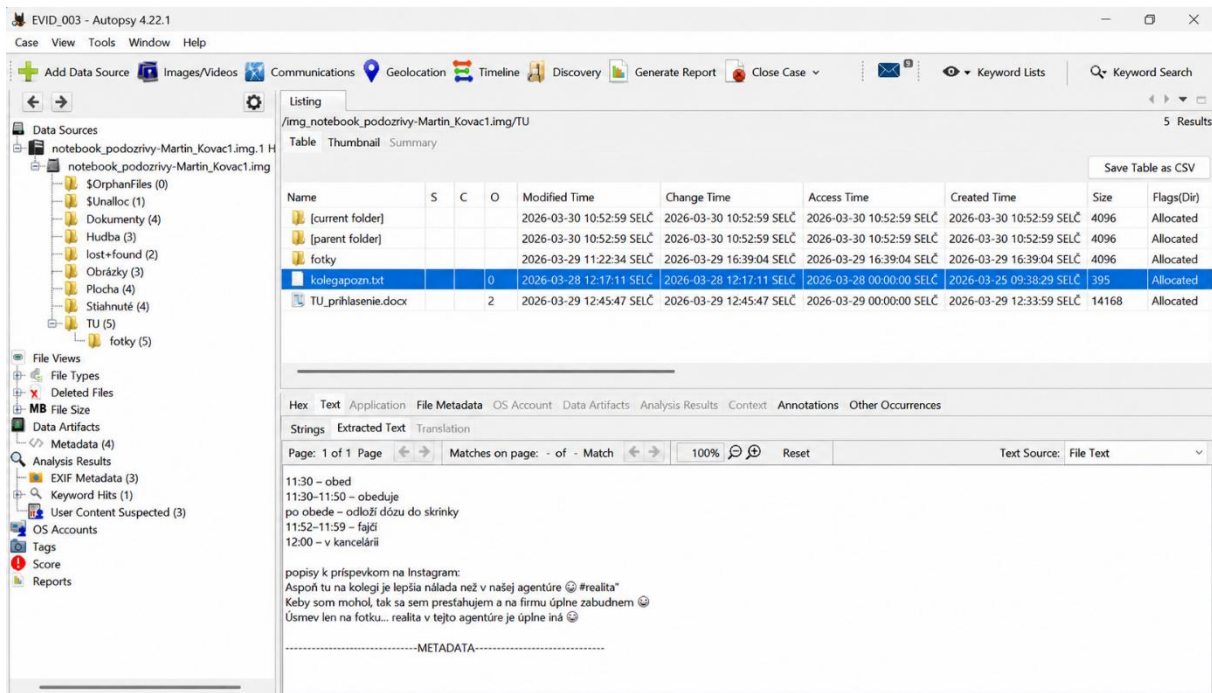
Metadata

Name: /img_D/_otky
Type: File System
MIME Type: null
Size: 0
File Name Allocation: Unallocated
Metadata Allocation: Unallocated
Modified: 2026-03-29 11:22:34 SELČ
Accessed: 2026-03-29 11:38:55 SELČ
Created: 2026-03-29 11:38:55 SELČ
Changed: 0000-00-00 00:00:00
MDS: Not calculated
SHA-256: Not calculated
Hash Lookup Results: UNKNOWN
Internal ID: 798

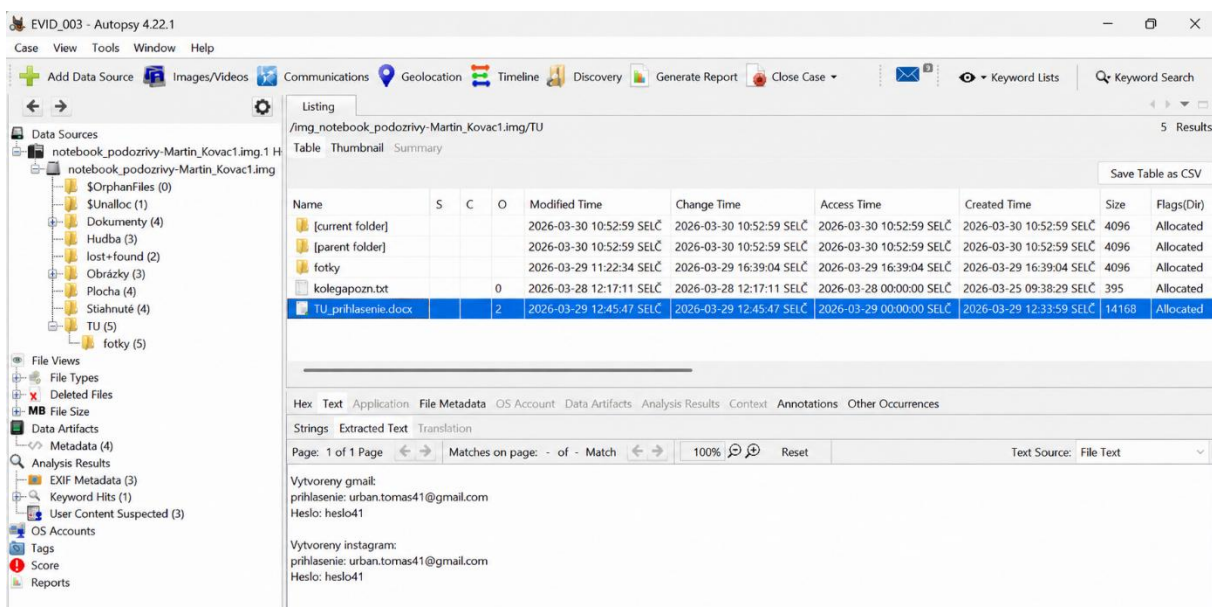
5.3 Notebook – Martin Kováč (podozrivý)

5.3.1 Autopsy

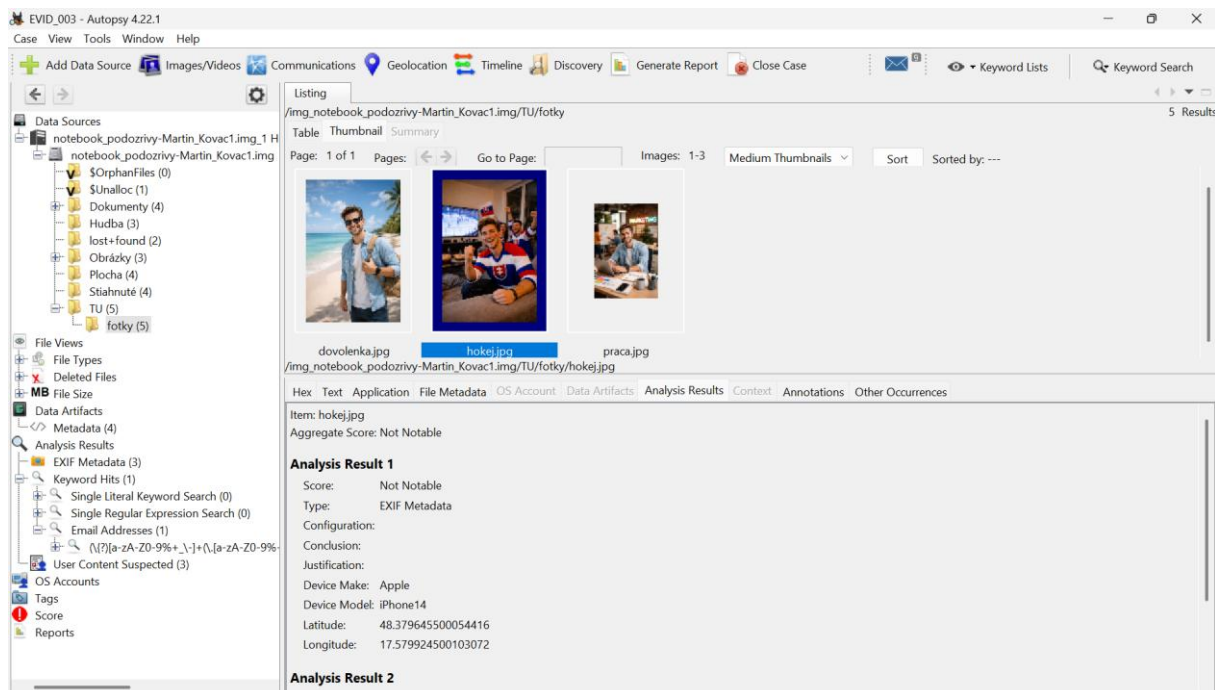
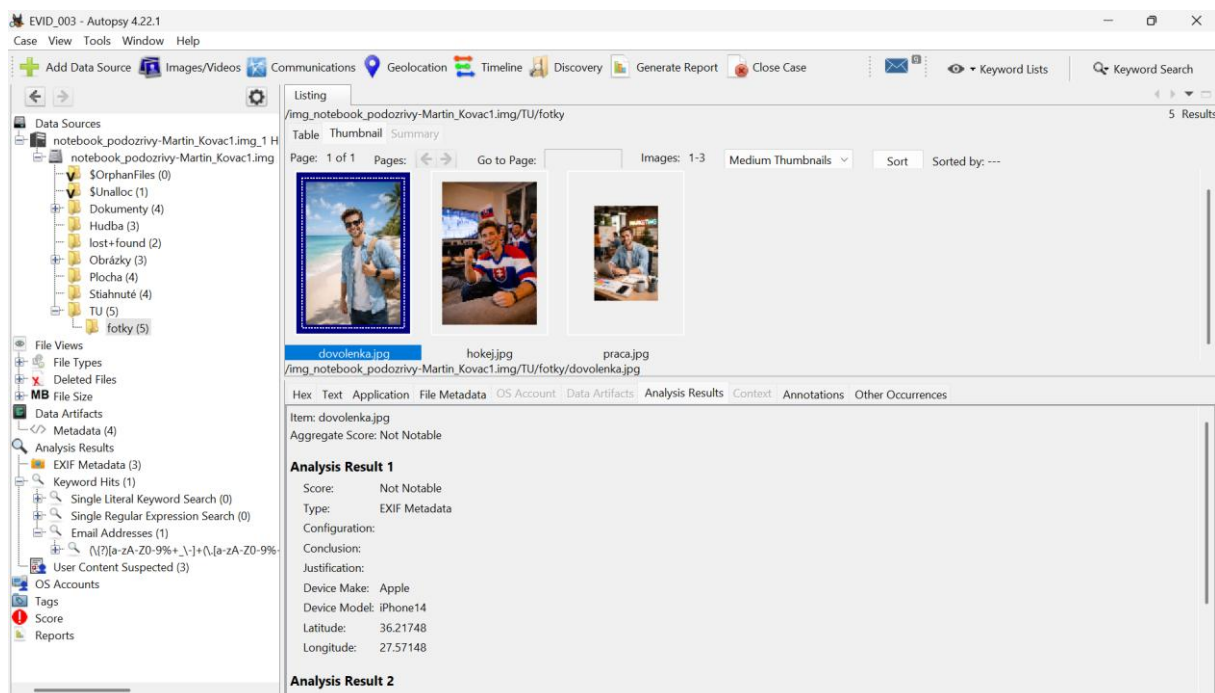
Na základe analýzy textového dokumentu „kolegapozn.txt“, ktorý bol nájdený v priečinku „TU“, možno usudzovať, že Martin Kováč určitý čas sledoval bežnú rutinu Tomáša Urbana počas prestávok a zároveň si vopred pripravoval popisy k príspevkom na Instagram, pravdepodobne s cieľom poškodiť jeho reputáciu vo firme.

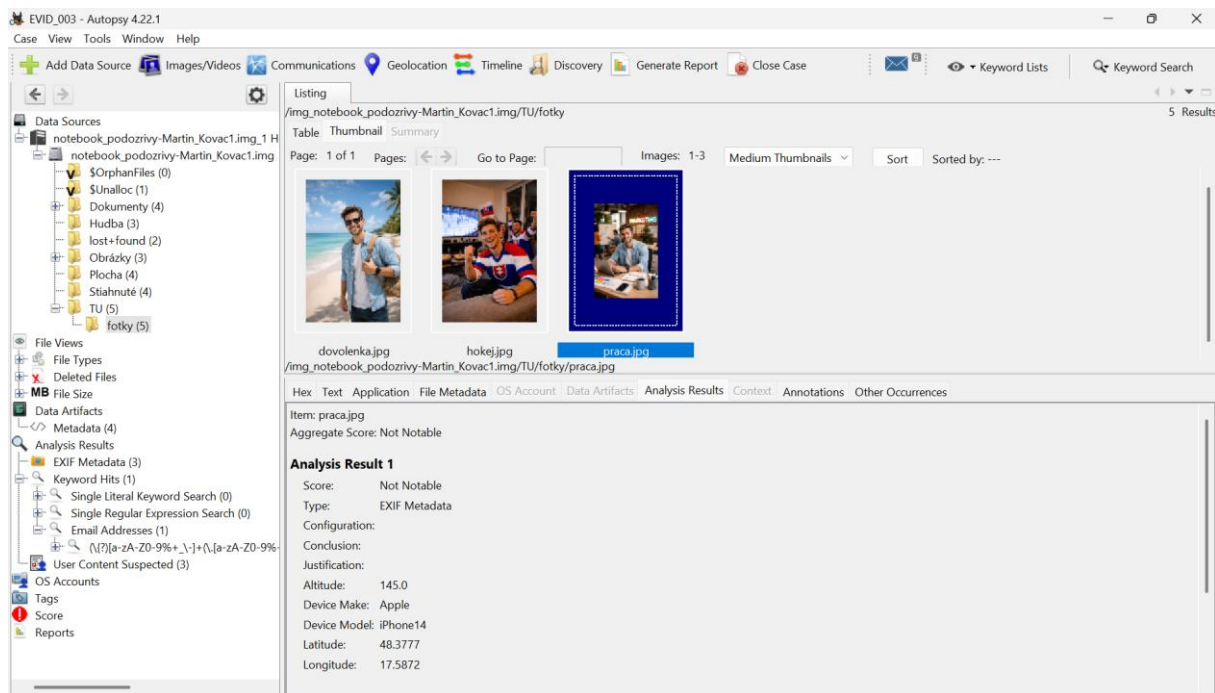


V tom istom priečinku bol taktiež nájdený dokument „TU_prihlasenie.docx“, ktorý obsahuje prihlasovacie údaje k falošnému Gmail a Instagram účtu.



V priečinku „TU“ bol následne nájdený totožný priečinok s názvom „fotky“, ktorý obsahoval rovnaké fotografie s identickými súradnicami ich vyhotovenia, aké sa nachádzali aj u Tomáša Urbana (poškodeného).





Autopsy Forensic Rep: x

file:///C:/Users/Admin/Desktop/skola%20-%20APIN/2.%20ročník%20S/Digitálna%20forenzná%20analýza/Daatsety/Notebook%

EXIF Metadata

Date Taken	Device Manufacturer	Device Model	Latitude	Longitude	Altitude	Source File
	Apple	iPhone14	36.21748	27.57148		/img_notebook_podozrivy-Martin_Kovac1.img/TU/fotky/dovolenka.jpg
	Apple	iPhone14	48.3777	17.5872	145.0	/img_notebook_podozrivy-Martin_Kovac1.img/TU/fotky/praca.jpg
	Apple	iPhone14	48.379645500054416	17.579924500103072		/img_notebook_podozrivy-Martin_Kovac1.img/TU/fotky/hokej.jpg

Report Navigatic

Case

Summary

5.3.2 Obraz RAM

Pri analýze obrazu RAM notebooku podozrivého boli vyhľadávaním reťazca „vytvorenie“ identifikované stopy po vytváraní účtov v prehliadači Opera – konkrétne Gmail a Instagram.

```

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
119FE69F0 61 00 2F 00 69 00 6E 00 64 00 65 00 78 00 2E 00 a./i.n.d.e.x...
119FE6A00 68 00 74 00 00 00 00 00 00 00 00 00 01 00 00 00 h.t.....
119FE6A10 68 00 74 00 00 00 00 00 00 00 00 00 01 00 00 00 h.t.t.p.s.:././
119FE6A20 62 00 63 00 73 00 74 00 75 00 64 00 65 00 6E 00 b.c.s.t.u.d.e.n.
119FE6A30 74 00 2E 00 66 00 70 00 76 00 75 00 63 00 6D 00 .s.k./r.t.e.s.
119FE6A40 2E 00 73 00 6B 00 2F 00 7E 00 74 00 65 00 73 00 t.u.s.e.r./d.f.
119FE6A50 74 00 75 00 73 00 65 00 72 00 7F 00 64 00 66 00 .t.j.f.....
119FE6A60 61 00 2F 00 69 00 6E 00 64 00 65 00 78 00 2E 00 a./i.n.d.e.x...
119FE6A70 00 00 89 04 7C 34 00 00 00 00 00 00 01 00 00 00 .t.j.f.....
119FE6A80 68 74 74 70 73 3A 2F 2F 77 77 2E 6F 6F 6F 6F https://www.goog
119FE6A90 6C 65 2E 63 6F 6D 2F 73 65 61 72 63 68 3F 63 6C le.com/search?cl
119FE6AA0 69 65 6E 74 3D 6F 70 65 72 61 26 71 3D 76 79 74 ient=opera&q=vyt
119FE6AB0 76 6F 72 65 6E 69 65 2B 67 6D 61 69 6C 2B 75 63 vorenie+gmail+uc
119FE6AC0 65 74 26 73 6F 75 72 63 65 69 64 3D 6F 70 65 72 et&sourceid=oper
119FE6AD0 61 26 69 65 3D 55 54 46 2D 38 26 6F 65 3D 55 54 a&ie=UTF-8&oe=UTF

```

Data inspector

Binary (8 bit) 01110110

Int8	go.to:	118
Int8	go.to:	118
Int16	go.to:	31094
Int16	go.to:	31094
Int24	go.to:	7633270
Int24	go.to:	7633270
Int32	go.to:	1987344758
Int32	go.to:	1987344758
Int64	go.to:	7954890139874130294
Int64	go.to:	7954890139874130294

Offset(h)

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

Decoded text

03E9F0D0 32 36 30 37 33 30 36 35 01 15 43 8C 22 06 00 81 26073065..C\$"...
03E9F0E0 03 02 08 68 74 74 70 73 3A 2F 2F 68 65 6C 70 2E ...https://help.
03E9F0F0 69 6E 73 74 61 67 72 61 6D 2E 63 6F 6D 2F 31 38 instagram.com/18
03E9F100 32 34 39 32 33 33 31 38 38 36 39 31 33 2F 3F 68 2492381886913/7h
03E9F110 65 6C 70 72 65 66 3D 68 63 5F 66 6E 61 76 01 14 elpref=hc fnav..
03E9F120 32 8C 21 05 00 63 02 08 68 74 74 70 73 3A 2F 2F 2\$1...c..https://
03E9F130 68 65 6C 70 2E 69 6E 73 74 61 67 72 61 6D 2E 63 help.instagram.c
03E9F140 6F 6D 2F 31 35 35 39 34 30 35 33 34 35 36 38 37 om/1559405345687
03E9F150 35 33 2F 01 14 6E 8C 20 06 00 81 5B 01 08 68 74 53/..n\$...l..ht
03E9F160 74 70 73 3A 2F 2F 77 77 77 2E 67 6F 6F 67 6C 65 tps://www.google
03E9F170 2E 63 6F 6D 2F 73 65 61 72 63 68 3F 63 6C 69 65 .com/search?clie
03E9F180 6E 74 3D 6F 70 65 72 61 26 71 3D 69 6E 73 74 61 nt=opera&q=insta
03E9F190 67 72 61 6D 2B 76 79 74 76 6F 72 65 6E 69 65 2B gram=vytvoreni+
03E9F1A0 75 63 74 75 26 73 6F 75 72 63 65 69 64 3D 6F 70 uctu&sourceid=op
03E9F1B0 65 72 61 26 69 65 3D 55 54 46 2D 38 26 6F 65 3D erasie=UTF-8&oe=
03E9F1C0 55 54 46 2D 38 17 8C 36 8C 1F 06 00 98 69 02 09 UTF-8.565....i..
03E9F1D0 68 74 74 70 73 3A 2F 2F 6D 79 61 63 63 6F 75 6E https://myaccoun
03E9F1E0 74 2E 67 6F 6F 67 6C 65 2E 63 6F 6D 2F 61 63 63 t.google.com/acc
03E9F1F0 67 75 6E 74 73 2F 53 65 74 4F 53 49 44 3F 61 75 ounts/SetOSID7au
03E9F200 74 68 75 73 65 72 3D 32 26 63 6F 6E 74 69 6E 75 thuser=24contin
03E9F210 65 3D 68 74 74 70 73 3A 2F 2F 61 63 63 6F 75 6E e=https://accoun
03E9F220 74 73 2E 79 6F 75 74 75 62 65 2E 63 6F 6D 2F 61 ts.youtube.com/a
03E9F230 63 63 6F 75 6E 74 73 2F 53 65 74 53 49 44 3F 73 ccounts/SetOSID7s
03E9F240 73 64 63 25 33 44 31 25 32 36 73 69 64 74 25 33 sdck3D1k26s1dtk3

Data inspector

Binary (8 bit)

01110110

Int8 go.to: 118

UInt8 go.to: 118

Int16 go.to: 31094

UInt16 go.to: 31094

Int24 go.to: 7633270

UInt24 go.to: 7633270

Int32 go.to: 1987344758

UInt32 go.to: 1987344758

Int64 go.to: 7954890139874130294

UInt64 go.to: 7954890139874130294

LEB128 go.to: -10

ULEB128 go.to: 118

AnsiChar / char8_t v

UnicodeChar / char16_t 18

Byte order

☒ Little endian
☐ Big endian

☐ Hexadecimal basis (for integral numbers)

Checksum Search (446 hits)

Offset

Excerpt (hex)

Excerpt (text)

3A942F1A 6E C3 A9 3A 20 25 73 00 5A 6C 79 68 61 6C 6F 20 76 79 74 76 6F 72 65 6E 69 65 20 6F 62 6A 65 6B nÃ©: %s.Zlyhalo vytvorenie obje
3C394433 61 7C 70 72 65 6A 73 C5 A5 7C 73 69 65 C5 A5 7C 76 79 74 76 6F 72 65 6E 69 65 20 73 69 65 74 65 alprejsiÃ(sieÃ)vytvorenie siete
3E9EF195 65 72 61 26 71 3D 69 6E 73 74 61 67 72 61 6D 2B 76 79 74 76 6F 72 65 6E 69 65 2B 75 63 74 75 26 erag=instagram+ vytvorenie+uctu
41651284 64 78 3B 76 69 72 74 20 64 69 73 68 00 00 00 00 56 79 74 76 6F 72 65 6E 69 65 20 76 69 72 74 75 dcvirt disk...Vytvorenie virtu
4675E7B1 63 74 75 72 65 43 61 6D 65 72 61 26 26 4E 61 20 76 79 74 76 6F 72 65 6E 69 65 20 6F 62 72 C3 A1 cturedCamera&Na vytvorenie obrÃ
47DFA969 41 63 74 69 76 69 74 79 4C 69 73 74 11 94 24 8E 76 79 74 76 6F 72 65 6E 69 65 20 61 6C 65 62 6F ActivityList."SŽvytvorenie alebo
47DFA9EF 74 69 76 69 74 79 4C 69 73 74 0F A0 24 8E 6F 20 76 79 74 76 6F 72 65 6E 69 65 20 61 6C 65 62 6F tivityList.SŽo vytvorenie alebo
47DFAA81 AC 24 8E 70 6F C5 BE 69 61 64 61 6C 69 20 6F 20 76 79 74 76 6F 72 65 6E 69 65 20 61 6C 65 62 6F ~SŽpoÃiadali o vytvorenie alebo

Offset(h): 3E9EF195

Block(h): 3E9EF195-3E9EF19E

Length(h): A

Overwrite

Vyhľadávaním reťazca „tomas“ boli v RAM zachytené prihlasovacie údaje k falošnému instagramovému profilu: e-mail urban.tomas41@gmail.com a prihlasovacie meno urban.tomas41. Z tohto profilu bolo zverejnených niekoľko príspevkov.

Offset(h)

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

Decoded text

746363370 33 31 32 45 43 36 46 34 33 5C 22 2C 5C 22 72 65 312E06F49\\",\"re
746363380 76 69 73 69 6F 6E 49 64 5C 22 3A 5C 22 32 30 30 visionId\\":\"200
746363390 34 33 31 38 30 37 31 5C 22 2C 5C 22 66 69 6C 65 4318071\\",\"file
7463633A0 45 78 74 65 6E 73 69 6F 6E 5C 22 3A 5C 22 2E 64 Extension\\":\".d
7463633B0 6F 63 78 5C 22 7D 2C 5C 22 65 6C 65 6D 65 6E 74 ocx\\"),\"element
7463633C0 73 5C 22 3A 5B 7B 5C 22 74 65 78 74 5C 22 3A 5C s\\":{\\\"text\\\":\\
7463633D0 22 56 79 74 76 6F 72 65 6E 79 20 69 6E 73 74 61 \"Vytvoreny insta
7463633E0 67 72 61 6D 3A 20 70 72 69 68 6C 61 73 65 6E 69 gram: prihlasi
7463633F0 65 3A 20 20 20 20 20 20 20 20 20 20 20 20 20 20 e:
746363400 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
746363410 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
746363420 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
746363430 6F 6D 61 75 34 31 20 40 67 6D 61 69 6C 2E 63 6F urban.41
746363440 6D 20 5C 22 2C 5C 22 74 65 78 74 55 6E 69 74 5C m \",\"textUnit
746363450 22 3A 34 7D 5D 2C 5C 22 73 75 62 54 79 70 65 5C \":41\\\",\"subType
746363460 22 3A 30 7D 7D 2C 2C 22 43 6F 72 72 65 6C 61 74 \":0\\\"),\"Correlat
746363470 69 6F 6E 56 65 63 74 6F 72 22 3A 22 46 59 4F 6A ionVector\\\":Ffioj
746363480 54 74 37 67 6F 45 79 49 6C 6A 47 66 6C 76 46 34 Tc7goEy1jGflvF4
746363490 67 77 2E 32 32 33 32 2E 35 2D 7D 5D 25 04 00 00 gw.2232.5\\\"))%...
7463634A0 EE 22 D9 6F 05 00 00 00 A0 0D 00 00 61 0A 00 00 i\"0o.....a...
7463634B0 25 04 00 00 EE E7 89 D2 09 00 00 00 BD F2 4A 00 %...ighN....\"AJ.
7463634C0 89 0A 00 00 64 00 00 00 65 05 00 00 08 00 00 00 h...d...e...o...
7463634D0 51 F6 1A 00 FD 34 36 02 61 00 00 00 61 00 00 00 00 Q0..y4e.a...a...
7463634E0 AD BD 18 00 CD 06 00 00 C9 34 36 02 08 00 00 00 00 .\".I...E4e.....

Data inspector

Binary (8 bit)

01110100

Int8 go.to: 116

UInt8 go.to: 116

Int16 go.to: 28532

UInt16 go.to: 28532

Int24 go.to: 7171956

UInt24 go.to: 7171956

Int32 go.to: 1634561908

UInt32 go.to: 1634561908

Int64 go.to: Invalid

UInt64 go.to: Invalid

LEB128 go.to: -12

ULEB128 go.to: 116

AnsiChar / char8_t t

UnicodeChar / char16_t 18

Byte order

☒ Little endian
☐ Big endian

☐ Hexadecimal basis (for integral numbers)

Checksum Search (1280 hits)

Offset

Excerpt (hex)

Excerpt (text)

7413DEB75 61 67 72 61 6D 2E 63 6F 6D 2F 75 72 62 61 6E 2E 74 6F 6D 61 73 34 31 2F 1A 58 68 74 74 70 73 3A agram.com/urban.tomas41/./https:
746360F6E 20 20 20 20 20 20 20 20 20 20 75 72 62 61 6E 2E 74 6F 6D 61 73 34 31 20 40 67 6D 61 69 6C 2E 63 urban.tomas41 @gmail.c
74636144A 20 20 20 20 20 20 20 20 20 20 75 72 62 61 6E 2E 74 6F 6D 61 73 34 31 20 40 67 6D 61 69 6C 2E 63 urban.tomas41 @gmail.c
746361B7A 20 20 20 20 20 20 20 20 20 20 75 72 62 61 6E 2E 74 6F 6D 61 73 34 31 20 40 67 6D 61 69 6C 2E 63 urban.tomas41 @gmail.c
74636342F 20 20 20 20 20 20 20 20 20 20 75 72 62 61 6E 2E 74 6F 6D 61 73 34 31 20 40 67 6D 61 69 6C 2E 63 urban.tomas41 @gmail.c
74636369E 20 20 20 20 20 20 20 20 20 20 75 72 62 61 6E 2E 74 6F 6D 61 73 34 31 20 40 67 6D 61 69 6C 2E 63 urban.tomas41 @gmail.c
746363B1A 20 20 20 20 20 20 20 20 20 20 75 72 62 61 6E 2E 74 6F 6D 61 73 34 31 20 40 67 6D 61 69 6C 2E 63 urban.tomas41 @gmail.c
746365B8B 20 20 20 20 20 20 20 20 20 20 75 72 62 61 6E 2E 74 6F 6D 61 73 34 31 20 40 67 6D 61 69 6C 2E 63 urban.tomas41 @gmail.c

Offset(h): 74636342F

Block(h): 74636342F-746363433

Length(h): 5

Overwrite

Offset(h)

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

Decoded text

7C3243400

68 6F 69 63 65 22 09 49 6E 73 74 61 67 72 61 6D

hoice".Instagram

7C3243410

30 00 40 C7 07 48 C4 B4 CE B0 D3 33 50 00 58 00

0.8q.HA.f"0SP.X.

7C3243420

60 00 78 AB B9 E3 A8 98 96 EB 17 8A 01 3D 68 74

".xeqA".-E.S.wh

7C3243430

74 70 73 3A 2F 2F 73 74 61 74 69 63 2E 63 64 6E

tps://static.odn

7C3243440

69 6E 73 74 61 67 72 61 6D 2E 63 6F 6D 2F 72 73

instagram.com/rs

7C3243450

72 63 2E 70 68 70 2F 79 34 2F 72 2F 51 61 42 6C

rc.php/y4/z/QaBl

7C3243460

49 30 4F 5A 69 6B 73 2E 69 63 6F A0 01 C8 01 C8

I00Ziks.ico .C.C

7C3243470

01 01 D0 01 01 3A E5 01 12 28 68 74 74 70 73 3A

..B...i..(https:

7C3243480

2F 2F 77 77 77 2E 69 6E 73 74 61 67 72 61 6D 2E

//www.instagram.

7C3243490

63 6F 6D 2F 75 72 62 61 6E 2E 74 6F 6D 61 73 34

com/urban.tomas4

7C32434A0

31 2F 1A 28 68 74 74 70 73 3A 2F 2F 77 77 77 2E

l/. (https://www.

7C32434B0

69 6E 73 74 61 67 72 61 6D 2E 63 6F 6D 2F 75 72

instagram.com/ur

7C32434C0

62 61 6E 2E 74 6F 6D 61 73 34 31 2F 22 28 56 79

ban.tomas41/"(Vy

7C32434D0

74 76 6F 72 69 C5 A5 20 6E 6F 76 C3 BD 20 70 72

tvorila novA" pr

7C32434E0

C3 AD 73 70 65 76 6F 6B 20 E2 80 A2 20 49 6E 73

A.spevok eE" Ins

7C32434F0

74 61 67 72 61 6D 30 00 38 01 40 8F 08 48 9E B5

tagram0.8.8Z.H2u

7C3243500

A9 C9 D3 33 50 00 58 00 60 00 78 97 F6 20 AF D9

@E03P.X."x-u2D

7C3243510

97 EB 17 8A 01 3D 68 74 74 70 73 3A 2F 2F 73 74

-E.S.whhttps://st

7C3243520

61 74 69 63 2E 63 64 6E 69 6E 73 74 61 67 72 61

atic.odninstagra

7C3243530

6D 2E 63 6F 6D 2F 72 73 72 63 2E 70 68 70 2F 79

m.com/rsrc.php/y

7C3243540

34 2F 72 2F 51 61 42 6C 49 30 4F 5A 69 6B 73 2E

4/z/QaBlI00Ziks.

7C3243550

69 63 6F A0 01 C8 01 C8 01 01 D0 01 01 3A 8B 02

ico .C.C.B...<

7C3243560

12 28 68 74 74 70 73 3A 2F 2F 77 77 77 2E 69 6E

.(https://www.in

7C3243570

73 74 61 67 72 61 6D 2E 63 6F 6D 2F 61 63 63 6F

stagram.com/acco

Data inspector

Binary (8 bit)

01110100

Int8

go.to: 116

UInt8

go.to: 116

Int16

go.to: 28532

UInt16

go.to: 28532

Int24

go.to: 7171956

UInt24

go.to: 7171956

Int32

go.to: 1634561908

UInt32

go.to: 1634561908

Int54

go.to: Invalid

UInt54

go.to: Invalid

LEB128

go.to: -12

ULEB128

go.to: 116

AnsiChar / char8_t

t

UnicodeChar / char16_t

3W

Byte order

Little endian

Big endian

Hexadecimal basis (for integral numbers)

Checksum Search (1280 hits)

Results

Offset

Excerpt (hex)

Excerpt (text)

7B647AF32

00 00 04 37 6F 50 FF FF FF FF FB C8 90 AF 6E 2E 74 6F 6D 61 73 34 31 40 67 6D 61 69 6C 2E 63 6F

...ToP" uC.Zn.tomas41@gmail.co

7C32432A4

61 67 72 61 6D 2E 63 6F 6D 2F 75 72 62 61 6E 2E 74 6F 6D 61 73 34 31 2F 1A 58 68 74 74 70 73 3A

agram.com/urban.tomas41/.(https:

7C324349A

61 67 72 61 6D 2E 63 6F 6D 2F 75 72 62 61 6E 2E 74 6F 6D 61 73 34 31 2F 1A 28 68 74 74 70 73 3A

agram.com/urban.tomas41/.(https:

7C32434C4

61 67 72 61 6D 2E 63 6F 6D 2F 75 72 62 61 6E 2E 74 6F 6D 61 73 34 31 2F 22 28 56 79 74 76 6F 72

agram.com/urban.tomas41/"(Vytvor

7C3243DB7

61 67 72 61 6D 2E 63 6F 6D 2F 75 72 62 61 6E 2E 74 6F 6D 61 73 34 31 2F 1A 58 68 74 74 70 73 3A

agram.com/urban.tomas41/.(https:

7C3243FAD

61 67 72 61 6D 2E 63 6F 6D 2F 75 72 62 61 6E 2E 74 6F 6D 61 73 34 31 2F 1A 28 68 74 74 70 73 3A

agram.com/urban.tomas41/.(https:

7C3243FD7

61 67 72 61 6D 2E 63 6F 6D 2F 75 72 62 61 6E 2E 74 6F 6D 61 73 34 31 2F 22 28 56 79 74 76 6F 72

agram.com/urban.tomas41/"(Vytvor

Offset(h): 7C32434C4

Block(h): 7C32434C4-7C32434C8

Length(h): 5

Overwrite

6 Image zariadení

6.1 Notebook – Tomáš Urban (poškodený)

Drive/Image Verify Results	
Name	notebook-poskodeny.001
Sector count	245760000
MDS Hash	
Computed hash	f8cd417a0234eba5a09b076636f1b4ba
Report Hash	f8cd417a0234eba5a09b076636f1b4ba
Verify result	Match
SHA1 Hash	
Computed hash	953a4b46feab900da6366ee4e08f11ea915e272f
Report Hash	953a4b46feab900da6366ee4e08f11ea915e272f
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: 001
Evidence Number: 001
Unique Description:
Examiner: Simona
Notes: Notebook poškodeného
-----

Information for C:\Users\Admin\Desktop\škola - APIN\2. ročník LS\Digitálna forenzná analýza\Daatsety\Notebook poškodeného\notebook-poskodeny:

Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 15 297
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 245 760 000
[Physical Drive Information]
Drive Model: PHILIPS USB Device
Drive Serial Number: FC306E4366773
Drive Interface Type: USB
Removable drive: True
Source data size: 120000 MB
Sector count: 245760000
[Computed Hashes]
MD5 checksum: f8cd417a0234eba5a09b076636f1b4ba
SHA1 checksum: 953a4b46feab900da6366ee4e08f11ea915e272f

Image Information:
Acquisition started: Mon Mar 30 10:36:44 2026
Acquisition finished: Mon Mar 30 10:52:59 2026
Segment list:
C:\Users\Admin\Desktop\škola - APIN\2. ročník LS\Digitálna forenzná analýza\Daatsety\Notebook poškodeného\notebook-poskodeny.001
COMPUTED HASH : f8cd417a0234eba5a09b076636f1b4ba
COMPUTED HASH : 953a4b46feab900da6366ee4e08f11ea915e272f

Image Verification Results:
Verification started: Mon Mar 30 10:53:00 2026
Verification finished: Mon Mar 30 11:01:37 2026
MD5 checksum: f8cd417a0234eba5a09b076636f1b4ba : verified
SHA1 checksum: 953a4b46feab900da6366ee4e08f11ea915e272f : verified
```

6.2 USB – Martin Kováč (podozrivý)

Drive/Image Verify Results	
[-]	
Name	USB-podozrivy.001
Sector count	15131636
[-] MD5 Hash	
Computed hash	4afc2f10b801618c6509291d4d650bd6
Report Hash	4afc2f10b801618c6509291d4d650bd6
Verify result	Match
[-] SHA1 Hash	
Computed hash	4f10d1feb363e1436f84089d71edbca2f0fc584c
Report Hash	4f10d1feb363e1436f84089d71edbca2f0fc584c
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: 002
Evidence Number: 002
Unique Description:
Examiner: Simona
Notes: USB podozrivého

-----

Information for C:\Users\Admin\Desktop\škola - APIN\2. ročník LS\Digitálna forenzná analýza\Daatsety\USB podozrivého\USB-podozrivy:

Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 941
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 15 131 636
[Physical Drive Information]
Drive Model: Kingston DataTraveler 2.0 USB Device
Drive Serial Number: 60A44C425569FD71F21A2A27&0
Drive Interface Type: USB
Removable drive: True
Source data size: 7388 MB
Sector count: 15131636
[Computed Hashes]
MD5 checksum: 4afc2f10b801618c6509291d4d650bd6
SHA1 checksum: 4f10d1feb363e1436f84089d71edbca2f0fc584c

Image Information:
Acquisition started: Mon Mar 30 11:19:14 2026
Acquisition finished: Mon Mar 30 11:26:50 2026
Segment list:
C:\Users\Admin\Desktop\škola - APIN\2. ročník LS\Digitálna forenzná analýza\Daatsety\USB podozrivého\USB-podozrivy.001
COMPUTED HASH : 4afc2f10b801618c6509291d4d650bd6
COMPUTED HASH : 4f10d1feb363e1436f84089d71edbca2f0fc584c

Image Verification Results:
Verification started: Mon Mar 30 11:26:51 2026
Verification finished: Mon Mar 30 11:28:22 2026
MD5 checksum: 4afc2f10b801618c6509291d4d650bd6 : verified
SHA1 checksum: 4f10d1feb363e1436f84089d71edbca2f0fc584c : verified
```

6.3 Notebook – Martin Kováč (podozrivý)

Drive/Image Verify Results	
[-]	
Name	notebook-podozrivy.001
Sector count	245760000
[-] MD5 Hash	
Computed hash	a547dd461b317087783dcaa1bacc0828
Report Hash	a547dd461b317087783dcaa1bacc0828
Verify result	Match
[-] SHA1 Hash	
Computed hash	a55c46a7ba86077f9cf96d27d0eaf218ee9b462
Report Hash	a55c46a7ba86077f9cf96d27d0eaf218ee9b462
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: 003
Evidence Number: 003
Unique Description:
Examiner: Simona
Notes: Notebook podozrivého

Information for C:\Users\Admin\Desktop\škola - APIN\2. ročník LS\Digitálna forenzná analýza\Daatsety\Notebook podozrivého\notebook-podozrivy:

Physical Evidentiary Item (Source) Information:

[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 15 297
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 245 760 000
[Physical Drive Information]
Drive Model: PHILIPS USB Device
Drive Serial Number: FC306E4366773
Drive Interface Type: USB
Removable drive: True
Source data size: 120000 MB
Sector count: 245760000
[Computed Hashes]
MD5 checksum: a547dd461b317087783dcaa1bacc0828
SHA1 checksum: a55c46a7ba86077f9cf96d27d0eaf218ee9b462

Image Information:

Acquisition started: Mon Mar 30 12:23:54 2026
Acquisition finished: Mon Mar 30 12:37:24 2026
Segment list:
C:\Users\Admin\Desktop\škola - APIN\2. ročník LS\Digitálna forenzná analýza\Daatsety\Notebook podozrivého\notebook-podozrivy.001
COMPUTED HASH : a547dd461b317087783dcaa1bacc0828
COMPUTED HASH : a55c46a7ba86077f9cf96d27d0eaf218ee9b462

Image Verification Results:

Verification started: Mon Mar 30 12:37:25 2026
Verification finished: Mon Mar 30 12:47:13 2026
MD5 checksum: a547dd461b317087783dcaa1bacc0828 : verified
SHA1 checksum: a55c46a7ba86077f9cf96d27d0eaf218ee9b462 : verified

7 Softvérové nástroje

- Exterro FTK Imager 4.7.3.81 – vytváranie obrazov diskov
- Belkasoft Live RAM Capturer – vytváranie obrazu RAM pamäte notebooku podozrivého a poškodeného
- HxD – analýza obsahu RAM pamäte notebookov podozrivého a poškodeného
- Autopsy 4.22.1 – analýza obrazov diskov (priechinky, súbory, logy)

8 Bezpečnostné opatrenia

8.1 Bitové kópie

8.1.1 Notebook – Tomáš Urban (poškodený)

Vytvorené v programe: Exterro FTK Imager 4.7.3.81

Počet kópií: 2 (pracovná kópia + archívna kópia)

Dátum a čas vytvorenia: 30.3.2026 10:55

MD5: f8cd417a0234eba5a09b076636f1b4ba

SHA1: 953a4b46feab900da6366ee4e08f11ea915e272f

Uložené: Pracovná kópia – forenzná pracovná stanica analytika
Archívna kópia – odovzdaná zamestnávateľovi, externý disk uložený v trezore

8.1.2 USB – Martin Kováč (podozrivý)

Vytvorené v programe: Exterro FTK Imager 4.7.3.81

Počet kópií: 2 (pracovná kópia + archívna kópia)

Dátum a čas vytvorenia: 30.3.2026 11:30

MD5: 4afc2f10b801618c6509291d4d650bd6

SHA1: 4f10d1feb363e1436f84089d71edbca2f0fc584c

Uložené: Pracovná kópia – forenzná pracovná stanica analytika
Archívna kópia – odovzdaná zamestnávateľovi, externý disk uložený v trezore

8.1.3 Notebook – Martin Kováč (podozrivý)

Vytvorené v programe: Exterro FTK Imager 4.7.3.81

Počet kópií: 2 (pracovná kópia + archívna kópia)

Dátum a čas vytvorenia: 30.3.2026 12:50

MD5: a547dd461b317087783dcaa1bacc0828

SHA1: a55c46a7ba86077f9cf96d27d0eaef218ee9b462

Uložené: Pracovná kópia – forenzná pracovná stanica analytika
Archívna kópia – odovzdaná zamestnávateľovi, externý disk uložený v trezore

8.2 Chain of custody

8.2.1 Notebook – Tomáš Urban (poškodený)

Číslo:	EVID-001	Typ súboru:	Bitový obraz disku (.E01)	Obnovený súbor:	Nie	Veľkosť:	117 GB
Popis prípadu:		Notebook poškodeného zamestnanca (Tomáš Urban) bol počas jeho obednej prestávky neoprávnene použitý kolegom (Martin Kováč). Z notebooku boli na USB kľúč skopírované osobné fotografie. Originály boli presunuté do koša bez vyprázdnenia.					
Názov súboru:		notebook-poskodeny.001					
Miesto získania digitálnej stopy:		Kancelária Tomáša Urbana, pracovisko marketingovej agentúry					
Poznámky:		Model: ASUS Zenbook 14 UX3405CA (Foggy Silver)					
Časové pečiatky							
Access:	30.03.2026 11:03		Modify:	30.03.2026 11:03		Change:	-
Digitálny odtlačok (heš)	MD5	f8cd417a0234eba5a09b076636f1b4ba					
	SHA1	953a4b46feab900da6366ee4e08f11ea915e272f					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
30.03.2026 09:30		Vytvorenie obrazu RAM					
30.03.2026 10:36		Vytvorenie bitového obrazu disku (FTK Imager)					
30.03.2026 11:01		Dokončenie obrazu, výpočet a overenie hash hodnôt (MD5, SHA1)					
30.03.2026 11:03		Zaistenie notebooku, vloženie do antistatického vrečka, zapečatenie páskou T-001					

8.2.2 USB – Martin Kováč (podozrivý)

Číslo:	EVID-002	Typ súboru:	Bitový obraz disku (.E01)	Obnovený súbor:	Nie	Veľkosť:	7,21 GB
Popis prípadu:		Firemný šifrovaný USB kľúč pridelený podozrivému zamestnancovi (Martin Kováč). Zariadenie bolo podľa logov Windows pripojené k notebooku poškodeného o 11:38:46 a použité na skopírovanie osobných fotografií. Sériové číslo zariadenia bolo identifikované v registroch Windows (USBSTOR) notebooku poškodeného a spárované s firemnou evidenciou pridelených zariadení.					
Názov súboru:		USB-podozrivy.001					
Miesto získania digitálnej stopy:		Kancelária Martina Kováča, pracovisko marketingovej agentúry					
Poznámky:		Model: Kingston DataTraveler 2.0 USB Device 8GB					
Časové pečiatky							
Access:	30.03.2026 11:30	Modify:	30.03.2026 11:30	Change:	-		
Digitálny odtlačok (heš)	MD5	4afc2f10b801618c6509291d4d650bd6					
	SHA1	4f10d1feb363e1436f84089d71edbca2f0fc584c					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
30.03.2026 11:19		Vytvorenie bitového obrazu disku (FTK Imager)					
30.03.2026 11:28		Dokončenie obrazu, výpočet a overenie hash hodnôt (MD5, SHA1)					
30.03.2026 11:30		Vloženie do dôkazného vrečka, zapečatenie páskou T-002					

8.2.3 Notebook – Martin Kováč (podozrivý)

Číslo:	EVID-003	Typ súboru:	Bitový obraz disku (.E01)	Obnovený súbor:	Nie	Veľkosť:	117 GB
Popis prípadu:		Firemný notebook podozrivého zamestnanca (Martin Kováč). Po skončení pracovnej zmeny podozrivý pripojil USB kľúč (EVID-002) k vlastnému notebooku, skopíroval fotografie a zverejnil ich na falošnom instagramovom profile. V RAM boli identifikované stopy po vytváraní falošných účtov (Gmail, Instagram) a prihlasovacie údaje k profilu urban.tomas41.					
Názov súboru:		USB-podozrivy.001					
Miesto získania digitálnej stopy:		Kancelária Martina Kováča, pracovisko marketingovej agentúry					
Poznámky:		Model: ASUS Zenbook 14 UX3405CA (Ponder Blue)					
Časové pečiatky							
Access:	30.03.2026 11:30		Modify:	30.03.2026 11:30		Change:	-
Digitálny odtlačok (heš)	MD5	a547dd461b317087783dcaa1bacc0828					
	SHA1	a55c46a7ba86077f9cf96d27d0eaef218ee9b462					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
30.03.2026 11:10		Vytvorenie obrazu RAM					
30.03.2026 12:23		Vytvorenie bitového obrazu disku (FTK Imager)					
30.03.2026 12:47		Dokončenie obrazu, výpočet a overenie hash hodnôt (MD5, SHA1)					
30.03.2026 12:50		Vloženie do antistatického vrečka, zapečatenie páskou T-003					