

UNIVERZITA SV. CYRILA A METODA V TRNAVE
FAKULTA PRÍRODNÝCH VIED

Únik filmu
Semestrálna práca
Digitálna Forenzná Analýza
[Prezentácia](#)

Obsah

1.	Prípad.....	3
2.	5WH.....	3
3.	Odborný príspevok a literatúra	3
4.	Hypotézy.....	4
5.	Digitálne zariadenia	5
6.	Dáta a digitálne stopy.....	8
7.	Analýza dát	9
8.	Používané programy	18
9.	Zabezpečenie a vytvorenie kópií	19
10.	Chain of custody	21
11.	Záver.....	24

1. Prípád

Filmové štúdio práve dokončilo prácu na svojom novom krátkom filme. Finálny export s názvom Film_v7.mov v sebe niesol interné poznámky, bežiaci časový kód a digitálny watermark.

Presne 14 dní pred plánovanou premiérou sa objavila uniknutá verzia na torrent fóre označená ako FILM.LEAKED. Tento predčasný únik spôsobil štúdiu nielen reputačné problémy, ale aj značné finančné škody ešte pred oficiálnym uvedením. Film bol uložený na externom disku, ktorý nebol nijako šifrovaný a podľa prísnych pravidiel nikdy nemal opustiť budovu štúdia.

2. 5WH

WHO: 2 zamestnanci s oprávneným prístupom k súboru.

WHAT: Neoprávnené zverejnenie pracovnej verzie filmu.

WHEN: 14 dní pred oficiálnou premiérou.

WHERE: Filmové štúdio.

WHY: Možný finančný motív, nespokojnosť alebo nedbanlivosť.

HOW: Kopírovanie na externé médium.

3. Odborný príspevok a literatúra

<https://rishikeshpansare.wordpress.com/wp-content/uploads/2016/02/digital-evidence-and-computer-crime-third-edition.pdf>

Casey, E. (2011). Digital Evidence and Computer Crime. Academic Press

Stručný opis: Komplexná príručka pre vyšetrovateľov, ktorá učí, ako premeniť jednotky a nuly na nepriestrelné dôkazy. Táto kniha je „bibliou“ digitálnej forenznej vedy. Spája technické postupy (ako získať dáta) s právnymi požiadavkami (ako ich použiť na súde).

<https://www.verizon.com/business/resources/reports/dbir/>

Stručný popis: Tento príspevok analyzuje štatistiky vnútorných hrozieb. Uvádza, že až 20 % únikov dát je spôsobených oprávnenými používateľmi, čo priamo súvisí s mojím prípadom, kde k úniku filmu došlo zlyhaním ľudského faktora (zamestnanca).

4. Hypotézy

Na základe vykonanej digitálnej analýzy obrazu RAM a pevných diskov zaistených zariadení sme dospeli k nasledujúcim záverom:

Hypotéza 1: Únik bol spôsobený úmyselným interným konaním zamestnanca, ktorý mal oprávnený prístup k súboru.

Výsledok: POTVRDENÁ

Odôvodnenie: Identifikácia odoslaného e-mailu z účtu manažéra (Dôkaz č. 2) a nález fragmentov komunikácie v RAM (Dôkaz č. 1 v RAM) jednoznačne preukazujú úmysel a aktívnu rolu zamestnanca pri vynášaní dát. Finančný motív (kryptomena) potvrdzuje, že nešlo o chybu, ale o vedomé konanie.

Hypotéza 2: Súbor bol kopírovaný na externé zariadenie mimo pracovnej doby a následne distribuovaný.

Došlo k porušeniu bezpečnostnej politiky v dôsledku nedbanlivosti a nedostatočného monitorovania prístupov.

Výsledok: ČIASTOČNE POTVRDENÁ

Odôvodnenie: Logy z prístupového systému TimeMoto (Dôkaz č. 1 v analýze disku) potvrdzujú prítomnosť manažéra v kancelárii v nedeľu v noci (23:42:15). Zhoda hashov (Dôkaz č. 3) a sieťová aktivita na Pirate Bay (Dôkaz č. 2 v RAM) potvrdzujú následnú distribúciu ukradnutého obsahu.

Hypotéza 3: Únik bol spôsobený externým faktorom (kybernetický útok alebo neoprávnený prístup tretej strany zvonku).

Výsledok: ZAMIETNUTÁ

Odôvodnenie: Počas analýzy systémových logov neboli nájdené žiadne stopy po násilnom vniknutí do siete (brute-force útoky), žiadny škodlivý kód (malware/backdoor) ani neautorizované vzdialené prístupy. Všetky kritické operácie boli vykonané pod legitímnymi povereniami produkčného manažéra na jeho fyzicky pridelenom hardvéri.

5. Digitálne zariadenia

- Externý SSD disk nájdený v kancelárii manažéra



Parametre zariadenia:

Značka	Kingston
Model	XS1000 External SSD
Kapacita	1000 GB (1 TB)
Rýchlosť čítania	1 050 MB/s
Rýchlosť zápisu	1 000 MB/s
Rozhranie	USB 3.2 Gen 2 (v balení kábel USB-C na USB-A)
Vhodné pre	Strih videa a rýchly prenos dát
Odkaz na Alzu	Kingston XS1000 na Alza.sk

Informácie získané s FTK Managera:

```
Created By Exterro® FTK® Imager 4.7.3.81

Case Information:
Acquired using: ADI4.7.3.81
Case Number: 2026_FILM_STUDIO
Evidence Number: 01
Unique Description: Externý disk filmového štúdia
Examiner: Matúš Horváth
Notes:

-----

Information for C:\Users\matus\Desktop\dfa\obrazy\EXT_DISK_IMAGE.ad1:
[Computed Hashes]
MD5 checksum: 463b9ea86fbd6fc20883a78f2708d43d
SHA1 checksum: ab8a7ac4f92fd1ec083b563f15ee10c7fac70101

Image information:
Acquisition started: Tue Mar 24 18:58:18 2026
Acquisition finished: Tue Mar 24 18:58:22 2026
Segment list:
C:\Users\matus\Desktop\dfa\obrazy\EXT_DISK_IMAGE.ad1
COMPUTED HASH : 463b9ea86fbd6fc20883a78f2708d43d
COMPUTED HASH : ab8a7ac4f92fd1ec083b563f15ee10c7fac70101

Image Verification Results:
Verification started: Tue Mar 24 18:58:22 2026
Verification finished: Tue Mar 24 18:58:22 2026
MD5 checksum: 463b9ea86fbd6fc20883a78f2708d43d : verified
SHA1 checksum: ab8a7ac4f92fd1ec083b563f15ee10c7fac70101 : verified
```

- RFID prístupový systém

Parametre zariadenia:

Značka	TimeMoto
Model	TM-616
Metóda	RFID karta, RFID kľúčienka (čip), PIN kód
Kapacita	200 používateľov
Displej	2.8" farebný TFT
Pripojenie	Wi-Fi / Ethernet (LAN)
Odkaz na Alzu	TimeMoto TM-616 na Alza.sk



Informácie získané s FTK Managera:

```

Created By Exterro® FTK® Imager 4.7.3.81

Case Information:
Acquired using: ADI4.7.3.81
Case Number: 2026_FILM_STUDIO
Evidence Number: 02
Unique Description: RFID - prístupový systém
Examiner: Matúš Horváth
Notes:

-----

Information for C:\Users\matus\Desktop\dfa\obrazy\RFID_PRISTUPOVY_SYSTEM.ad1:
[Computed Hashes]
MD5 checksum: e3cb10e89627e67258d28eb86a992720
SHA1 checksum: 49f73c7b3880a97941e22559d2ad1b01966909ac

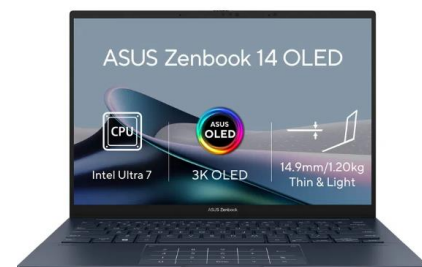
Image information:
Acquisition started: Tue Mar 24 19:05:42 2026
Acquisition finished: Tue Mar 24 19:05:42 2026
Segment list:
C:\Users\matus\Desktop\dfa\obrazy\RFID_PRISTUPOVY_SYSTEM.ad1
COMPUTED HASH : e3cb10e89627e67258d28eb86a992720
COMPUTED HASH : 49f73c7b3880a97941e22559d2ad1b01966909ac

Image Verification Results:
Verification started: Tue Mar 24 19:05:42 2026
Verification finished: Tue Mar 24 19:05:42 2026
MD5 checksum: e3cb10e89627e67258d28eb86a992720 : verified
SHA1 checksum: 49f73c7b3880a97941e22559d2ad1b01966909ac : verified

```

- Notebook produkčného manažéra

Parametre zariadenia:	
Značka	ASUS
Model	Zenbook 14 OLED (UX3405)
Vzhľad	Prémiový celokovový dizajn (Ponder Blue / Foggy Silver)
Procesor	Intel Core Ultra 5 / 7 (najnovšia generácia)
RAM	16 GB LPDDR5X
Kapacita úložiska	1 TB SSD PCIe 4.0
Operačný systém	Windows 11 Home / Pro
Hmotnosť	1,20 kg
Displej	14" 3K OLED 120Hz (špičkové farby a kontrast)
Odkaz na Alzu	ASUS Zenbook 14 OLED na Alza.sk



Informácie získané s FTK Managera:

```

Created By Exterro® FTK® Imager 4.7.3.81

Case Information:
Acquired using: ADI4.7.3.81
Case Number: 2026_FILM_STUDIO
Evidence Number: 03
Unique Description: Notebook produkčného manažéra
Examiner: Matúš Horváth
Notes:

-----

Information for C:\Users\matus\Desktop\dfa\obrazy\NOTEBOOK_MANAZERA_IMAGE.ad1:
[Computed Hashes]
MD5 checksum: 30fb88ca41a1e1377e4b0557fcfc175d
SHA1 checksum: 5c2ae519893578f3675dca2b960a52fa78f083ea

Image information:
Acquisition started: Tue Mar 24 19:10:21 2026
Acquisition finished: Tue Mar 24 19:14:06 2026
Segment list:
C:\Users\matus\Desktop\dfa\obrazy\NOTEBOOK_MANAZERA_IMAGE.ad1
C:\Users\matus\Desktop\dfa\obrazy\NOTEBOOK_MANAZERA_IMAGE.ad2
COMPUTED HASH : 30fb88ca41a1e1377e4b0557fcfc175d
COMPUTED HASH : 5c2ae519893578f3675dca2b960a52fa78f083ea

Image Verification Results:
Verification started: Tue Mar 24 19:14:06 2026
Verification finished: Tue Mar 24 19:14:25 2026
MD5 checksum: 30fb88ca41a1e1377e4b0557fcfc175d : verified
SHA1 checksum: 5c2ae519893578f3675dca2b960a52fa78f083ea : verified

```

6. Dáta a digitálne stopy

Notebook manažéra

Operačný systém: Windows (scenár M57-Jean)

Veľkosť datasetu: 2,85 GB

Formát dát: Forenzný diskový obraz (2 súbory tvoriace jeden logický disk)

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

Typy súborov v datasete:

1. Systémové súbory: .dll, .exe, registre (NTUSER.DAT, SOFTWARE)
2. Multimediálne súbory: .mp4, .mkv (ukradnutá finálna verzia filmu)
3. Ostatné: .eml, .db, .sqlite (komunikácia a história), .pdf, .docx

Podrobné informácie o dátach: Ide o kompletný obraz disku manažéra. Kľúčovým nálezom je ukradnutá verzia filmu. Analýza sa zameriava na aktivitu používateľa, čas uloženia súboru a systémové stopy (artefakty), ktoré dokazujú vedomú manipuláciu s nelegálnym obsahom.

Externý disk

Veľkosť datasetu: 49,8 MB

Obsah: Pracovná verzia filmu

Typy súborov: .mp4, .mov, .tmp

Podrobné informácie o dátach: Obsahuje pracovnú verziu filmu slúžiacu ako podkladový materiál. Dáta sú považované za legítimne. Porovnanie metadát a hash hodnôt s notebookom manažéra slúži na overenie, či bol tento kľúč pôvodným zdrojom pre vytvorenie nelegálnej kópie.

RFID prístupový systém

Veľkosť datasetu: 7 KB

Formát dát: Tabuľka Excel (.xlsx)

Počet súborov: 1

Podrobné informácie o dátach: Export z dochádzkového systému obsahujúci pracovné pozície ID kariet a časové pečiatky príchodov/odchodov. Dáta slúžia na krížovú kontrolu fyzickej prítomnosti manažéra na pracovisku v čase podozrivej aktivity zistenej na jeho notebooku.

Celková veľkosť všetkých analyzovaných dát: 2,89 GB

7. Analýza dát

Analýza obrazu pamäte RAM (evidence_dump_2026.mem)

Pri skúmaní súboru evidence_dump_2026.mem v hexadecimálnom editore HxD boli identifikované nasledujúce tri kľúčové dôkazy, ktoré objasňujú priebeh incidentu:

1. Dôkaz

Prvým zásadným nálezom v pamäťovom výpise je fragment textovej komunikácie na adrese 13EBDDB0. Tento digitálny artefakt obsahuje priamy záznam o tom, že manažér komunikoval s tretou stranou prostredníctvom aplikácie Telegram.

V správe sa výslovne uvádza, že došlo k manuálnemu premenovaniu pôvodného pracovného súboru na názov FILM.LEAKED.

Ide o kľúčový dôkaz o úmyselnej modifikácii dát, páchateľ sa snažil zakryť jeho pôvodnú identitu v systéme.

```
13EBDDB80 30 52 05 00 60 12 00 00 A0 D8 D0 23 64 12 00 00 0R...`... ŘÐ#d...
13EBDDB90 00 70 C3 AD 73 61 6C 69 20 6E 61 20 54 65 6C 65 .pĀ.sali na Tele
13EBDDBA0 67 72 61 6D 65 2E 20 49 64 65 20 6F 20 74 65 6E grame. Ide o ten
13EBDDBB0 20 6B 72 C3 A1 74 6B 79 20 66 69 6C 6D 2C 20 C4 krĀ~tky film, Ā
13EBDDBC0 8D 6F 20 6D C3 A1 20 76 79 6A 73 C5 A5 20 6F 20 Ťo mĀ~ vyjsĀ o
13EBDDBD0 64 76 61 20 74 C3 BD C5 BE 64 6E 65 2E 20 53 C3 dva tĀ~Īidne. SĀ
13EBDDBE0 BA 62 6F 72 20 73 6F 6D 20 70 72 65 6D 65 6E 6F ŝbor som premeno
13EBDDBF0 76 61 6C 20 6E 61 20 3C 62 20 64 61 74 61 2D 70 val na <b data-p
13EBDDC00 61 74 68 2D 74 6F 2D 6E 6F 64 65 3D 22 36 2C 31 ath-to-node="6,l
13EBDDC10 22 20 64 61 74 61 2D 69 6E 64 65 78 2D 69 6E 2D " data-index-in-
13EBDDC20 6E 6F 64 65 3D 22 31 33 35 22 3E 46 49 4C 4D 2E node="135">FILM.
13EBDDC30 4C 45 41 4B 45 44 2E 32 30 32 36 2E 31 30 38 30 LEAKED.2026.1080
13EBDDC40 70 2E 4D 4F 56 3C 2F 62 3E 2C 20 61 62 79 20 73 p.MOV</b>, aby s
13EBDDC50 00 20 74 6F 20 68 6E 65 00 00 01 00 00 79 74 69 . to hne.....yti
13EBDDC60 00 00 00 00 00 00 00 00 00 20 64 61 74 61 2D 70 ..... data-p
13EBDDC70 00 74 68 2D 74 6F 2D 6E 00 00 00 00 00 00 00 00 .th-to-n.....
13EBDDC80 00 3E 50 72 C3 A1 76 65 00 00 00 00 00 00 00 00 .>PrĀ~ve.....
13EBDDC90 01 A1 76 61 6D 20 6E 61 E0 7D 6C E2 F8 7F 00 00 .~vam nař}lĀř...
```

Checksum Search (831 hits)		
Offset	Excerpt (hex)	Excerpt (text)
1345A2C18	25 43 33 25 41 31 2B 61 6B 6F 2B 66 69 6C 6D 2E 6C 65 61 6B 65 64 2E 2B 74 65 6E 74 6F 2B 70 72	%C3%A1+ako+film.leaked.+tento+pr
1345A2EE3	C4 8D 65 6E C3 A1 20 61 6B 6F 20 66 69 6C 6D 2E 6C 65 61 6B 65 64 2E 20 74 65 6E 74 6F 20 70 72	ĀĤenĀ~ ako film.leaked. tento pr
135325814	6C 20 66 69 6C 65 73 20 77 69 6C 6C 20 62 65 20 6C 65 61 6B 65 64 20 61 66 74 65 72 20 90 02 05	I files will be leaked after ...
13EBDDC30	6E 6F 64 65 3D 22 31 33 35 22 3E 46 49 4C 4D 2E 4C 45 41 4B 45 44 2E 32 30 32 36 2E 31 30 38 30	node="135">FILM.LEAKED.2026.1080
14213F82E	41 31 25 32 30 61 6B 6F 25 32 30 46 49 4C 4D 2E 4C 45 41 4B 45 44 2E 25 32 30 54 65 6E 74 6F 25	A1%20ako%20FILM.LEAKED.%20Tento%
14D06B3EC	C4 8D 65 6E C3 A1 20 61 6B 6F 20 46 49 4C 4D 2E 4C 45 41 4B 45 44 2E 20 54 65 6E 74 6F 20 70 72	ĀĤenĀ~ ako FILM. LEAKED. Tento pr

2. Dôkaz

Druhým dôležitým dôkazom je identifikácia sieťovej aktivity spojenej s doménou Pirate Bay. Vyhľadávanie v hexadecimálnom editore odhalilo na adrese 00357D30 záznamy, ktoré sa v pamäti RAM nachádzali až v 52 prípadoch.

To znamená, že manažér túto stránku nenavštívil náhodou, ale opakovane a intenzívne s ňou pracoval. Takto vysoký počet výskytov v operačnej pamäti jasne indikuje prípravu na nahratie ukradnutého obsahu na verejný torrentový server.

```
00357CFD0 04 00 00 00 F8 7F 00 00 74 82 47 C4 10 4F 00 90 ....ř...t,GÄ.O..
00357CFE0 38 B2 13 91 F8 7F 00 00 00 00 00 00 00 00 00 00 8_.'ř.....
00357CFF0 01 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 .....
00357D000 00 00 00 00 03 27 A0 20 FF FF FF FF FC D8 5F DF ..... ' ' ' ' 'üŘ_ß
00357D010 2E 4C 45 41 4B 45 44 2E 32 30 32 36 00 00 00 00 .LEAKED.2026....
00357D020 00 00 00 00 03 27 A0 40 FF FF FF FF FC D8 5F BF ..... ' @ ' ' 'üŘ_z
00357D030 50 69 72 61 74 65 20 42 61 79 00 00 00 00 00 00 Pirate Bay.....
00357D040 00 00 00 00 03 27 A0 60 FF FF FF FF FC D8 5F 9F ..... ' ' ' ' 'üŘ_z
00357D050 76 ED 6D 2C 61 69 6C 75 3A 00 00 00 00 00 00 00 vim,ailu:.....
00357D060 00 00 00 00 03 27 A0 80 FF FF FF FF FC D8 5F 7F ..... ' € ' ' 'üŘ_.
00357D070 20 65 2D 6D 61 69 6C 75 3A 00 00 00 00 00 00 00 e-mailu:.....
00357D080 00 00 00 00 03 27 A0 A0 FF FF FF FF FC D8 5F 5F ..... ' ' ' ' 'üŘ_
00357D090 6B 71 75 6F 74 65 00 00 00 00 00 00 00 00 00 00 kquote.....
```

Checksum	Search (52 hits)	
Offset	Excerpt (hex)	Excerpt (text)
357D030	00 00 00 00 03 27 A0 40 FF FF FF FF FC D8 5F BF 50 69 72 61 74 65 20 42 61 79 00 00 00 00 00 00	' @ "üŘ_zPirate Bay.....
357D1B0	00 00 00 00 03 27 A1 C0 FF FF FF FF FC D8 5E 3F 50 69 72 61 74 65 20 42 61 79 00 00 00 00 00 00	' "üŘ^?Pirate Bay.....
357D250	00 00 00 00 03 27 A2 60 FF FF FF FF FC D8 5D 9F 50 69 72 61 74 65 20 42 61 79 00 00 00 00 00 00	'üŘ}zPirate Bay.....
357D390	00 00 00 00 03 27 A3 A0 FF FF FF FF FC D8 5C 5F 50 69 72 61 74 65 20 42 61 79 75 74 00 00 00 00	'k "üŘ_Pirate Bayut....
357D430	00 00 00 00 03 27 A4 40 FF FF FF FF FC D8 5B BF 50 69 72 61 74 65 20 42 61 79 00 00 00 00 00 00	' "üŘ[zPirate Bay.....
357D510	00 00 00 00 03 27 A5 20 FF FF FF FF FC D8 5A DF 50 69 72 61 74 65 20 42 61 79 00 00 00 00 00 00	'A "üŘZßPirate Bay.....

3. Dôkaz

Tretím nálezom je zdokumentovanie neoprávneného presunu dát z externého média do lokálneho počítača, čo bolo identifikované na adresách okolo 2C093710. Tu sa zachytila koexistencia názvu uniknutého filmu s záznamami o pripojení externého disku.

Tento nález potvrdzuje fyzickú manipuláciu s dátami, kedy manažér skopíroval chránený obsah z disku filmového štúdia do svojho notebooku.

Keďže tento súbor nemal na danom zariadení z hľadiska bezpečnostnej politiky čo robiť, ide o jasný dôkaz neoprávneného prisvojenia si duševného vlastníctva.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
2C0937020	C3	BD	27	1A	04	03	02	2F	00	B2	F3	0F	F9	6E	70	73	Ä'...../..ó.únps
2C0937030	2D	32	30	30	38	2D	6A	65	61	6E	2E	45	30	32	1A	04	-2008-jean.E02..
2C0937040	03	02	2F	00	B2	F2	0F	F9	6E	70	73	2D	32	30	30	38	.../.ñ.únps-2008
2C0937050	2D	6A	65	61	6E	2E	45	30	31	18	04	03	02	2B	00	B2	-jean.E01.....+
2C0937060	F1	0F	F9	46	49	4C	4D	2E	4C	45	41	4B	45	44	2E	6D	ñ.ŮFILM.LEAKED.m
2C0937070	70	34	0E	04	03	01	19	00	B2	CF	0F	72	61	6D	6B	61	p4.....Ď.ramka
2C0937080	61	08	BB	00	19	2D	00	B2	C9	0F	4E	6F	76	C3	BD	20	a.»...Ě.NovÄ
2C0937090	70	72	69	65	C4	8D	69	6E	6F	6B	18	04	03	02	2B	00	prieÄĤinok.....+
2C09370A0	B2	C7	01	26	46	49	4C	4D	5F	76	37	2E	6D	6F	76	2E	Ĉ.&FILM_v7.mov.
2C09370B0	6D	70	34	14	04	03	01	25	00	B2	C6	0F	45	78	74	65	mp4....%Ĉ.Ĉ.Exte
2C09370C0	72	6E	79	20	64	69	73	6B	34	04	03	02	63	00	B2	C3	rny disk4...c.ĈÄ
2C09370D0	01	25	72	66	69	64	5F	61	63	63	65	73	73	5F	6C	6F	..%rfid_access_lo
2C09370E0	67	73	5F	66	69	6C	6D	5F	73	74	75	64	69	6F	5F	72	gs_film_studio_r
2C09370F0	6F	6C	65	5F	6F	6E	6C	79	2E	78	6C	73	78	0C	04	03	ole_only.xlsx...
2C0937100	01	15	00	B2	C1	0F	52	46	49	44	18	04	03	02	2B	00	...Ä.RFID.....+
2C0937110	B2	B7	00	AE	46	49	4C	4D	2E	4C	45	41	4B	45	44	2E	..@FILM.LEAKED.
2C0937120	6D	70	34	1A	04	03	02	2F	00	B2	B3	00	AE	6E	70	73	mp4.....ĭ.ĭ@nps
2C0937130	2D	32	30	30	38	2D	6A	65	61	6E	2E	45	30	32	1A	04	-2008-jean.E02..
2C0937140	03	02	2F	00	B2	B2	00	AE	6E	70	73	2D	32	30	30	38	.../.ĭ.ĭ@nps-2008
2C0937150	2D	6A	65	61	6E	2E	45	30	31	10	04	03	01	1D	00	B2	-jean.E01.....
2C0937160	AF	0F	4E	6F	74	65	62	6F	6F	6B	08	08	EF	00	28	49	Ž.Notebook..d.(I
2C0937170	00	B2	D1	07	3E	53	63	1B	04	03	02	31	00	B2	D0	19	..Ň.>Sc.....ĭ.Ď.
2C0937180	10	43	6F	6C	75	6D	6E	50	72	6F	78	79	44	42	32	2E	.ColumnProxyDB2.
2C0937190	78	6D	6C	0B	04	03	01	13	00	B2	AC	77	64	66	61	0A	xml.....-wdfa.
2C09371A0	09	00	4D	2D	00	B2	AB	77	4E	6F	76	C3	BD	20	70	72	..M-..«wNovÄ pr
2C09371B0	69	65	C4	8D	69	6E	6F	6B	0A	09	00	34	2F	00	B2	EA	ieÄĤinok...4/..ĕ
2C09371C0	7C	6E	70	73	27	04	03	02	49	00	B2	DD	07	3E	53	63	nps'...I.Ý.>Sc
2C09371D0	72	65	65	6E	73	68	6F	74	5F	32	30	32	31	30	37	32	reenshot_2021072
2C09371E0	31	2D	30	38	32	35	35	37	2E	70	6E	67	0A	80	15	04	l-082557.png.ĕ..

Checksum Search (148 hits)		
Offset	Excerpt (hex)	Excerpt (text)
2AC5C7871	20 6F 7A 6E 61 C4 8D 65 6E C3 A1 20 61 6B 6F 20 46 49 4C 4D 2E 4C 45 41 4B 45 44 2E 20 54 65 6E	oznaÄĤenÄ" ako FILM.LEAKED. Ten
2AC5C7AC5	20 6F 7A 6E 61 C4 8D 65 6E C3 A1 20 61 6B 6F 20 66 69 6C 6D 2E 6C 65 61 6B 65 64 2E 20 74 65 6E	oznaÄĤenÄ" ako film.leaked. ten
2C093604B	61 6E 2E 45 30 31 18 04 03 02 2B 00 B2 F1 0F F9 46 49 4C 4D 2E 4C 45 41 4B 45 44 2E 6D 70 34 0E	an.E01....+..ñ.ŮFILM.LEAKED.mp4.
2C09360FC	C1 0F 52 46 49 44 18 04 03 02 2B 00 B2 B7 00 AE 46 49 4C 4D 2E 4C 45 41 4B 45 44 2E 6D 70 34 1A	Ä.RFID....+..@FILM.LEAKED.mp4.
2C0937063	61 6E 2E 45 30 31 18 04 03 02 2B 00 B2 F1 0F F9 46 49 4C 4D 2E 4C 45 41 4B 45 44 2E 6D 70 34 0E	an.E01....+..ñ.ŮFILM.LEAKED.mp4.
2C0937114	C1 0F 52 46 49 44 18 04 03 02 2B 00 B2 B7 00 AE 46 49 4C 4D 2E 4C 45 41 4B 45 44 2E 6D 70 34 1A	Ä.RFID....+..@FILM.LEAKED.mp4.

Analýza obrazov zariadený

1. Dôkaz

Na základe exportu logov zo systému TimeMoto TM-616 bola vykonaná hĺbková analýza dochádzky zamestnancov.

Pri porovnaní aktivít bol identifikovaný kritický moment, ktorý potvrdzuje fyzickú prítomnosť produkčného manažéra v priestoroch štúdia v čase mimo bežnej pracovnej doby.

Lokalizácia v dôkaze: Tento neštandardný prístup sa nachádza v riadku č. 32 priloženého logu.
Časová pečiatka: 2026-03-01 o 23:42:15.

Identifikácia: Zamestnanec EMP001 (Produkčný manažér) vstúpil do priestorov Manager Office (kancelária manažéra).

Forenzný význam: Tento príchod, takmer pred polnocou v nedeľu, je vysoko podozrivý. Práve v tomto časovom okne došlo podľa systémových logov k neoprávnenej manipulácii s externým SSD diskom a následnému premenovaniu súboru.

Manažér zneužil svoju právomoc prístupu do kancelárie v čase, kedy sa v budove nenachádzali iní zamestnanci ani dozor, čo mu umožnilo nerušene skopírovať film.

Timestamp	Employee_ID	Role	Access_Point	Action	Result
2026-02-25 8:13:00	EMP001	Pracovník Manazer	Main Entrance	Entry	Granted
2026-02-25 9:11:00	EMP002	Pracovník Manazer	Main Entrance	Entry	Granted
2026-02-25 10:13:00	EMP001	Pracovník Manazer	Server Room	Entry	Granted
2026-02-25 12:11:00	EMP002	Pracovník Manazer	Editing Room	Entry	Granted
2026-02-25 16:43:00	EMP001	Pracovník Manazer	Main Entrance	Exit	Granted
2026-02-25 17:15:00	EMP002	Pracovník Manazer	Main Entrance	Exit	Granted
2026-02-26 8:00:00	EMP002	Pracovník Manazer	Main Entrance	Entry	Granted
2026-02-26 9:08:00	EMP001	Pracovník Manazer	Main Entrance	Entry	Granted
2026-02-26 10:08:00	EMP001	Pracovník Manazer	Editing Room	Entry	Granted
2026-02-26 11:00:00	EMP002	Pracovník Manazer	Manager Office	Entry	Granted
2026-02-26 16:00:00	EMP002	Pracovník Manazer	Main Entrance	Exit	Granted
2026-02-26 17:22:00	EMP001	Pracovník Manazer	Main Entrance	Exit	Granted
2026-02-27 9:10:00	EMP002	Pracovník Manazer	Main Entrance	Entry	Granted

2026-02-27 9:17:00	EMP001	Pracovnik Manazer	Main Entrance	Entry	Granted
2026-02-27 14:10:00	EMP002	Pracovnik Manazer	Editing Room	Entry	Granted
2026-02-27 14:17:00	EMP001	Pracovnik Manazer	Manager Office	Entry	Granted
2026-02-27 17:29:00	EMP002	Pracovnik Manazer	Main Entrance	Exit	Granted
2026-02-27 17:37:00	EMP001	Pracovnik Manazer	Main Entrance	Exit	Granted
2026-02-28 8:12:00	EMP001	Pracovnik Manazer	Main Entrance	Entry	Granted
2026-02-28 9:12:00	EMP002	Pracovnik Manazer	Main Entrance	Entry	Granted
2026-02-28 10:12:00	EMP001	Pracovnik Manazer	Manager Office	Entry	Granted
2026-02-28 11:12:00	EMP002	Pracovnik Manazer	Manager Office	Entry	Granted
2026-02-28 16:34:00	EMP001	Pracovnik Manazer	Main Entrance	Exit	Granted
2026-02-28 17:30:00	EMP002	Pracovnik Manazer	Main Entrance	Exit	Granted
2026-03-01 9:07:00	EMP002	Pracovnik Manazer	Main Entrance	Entry	Granted
2026-03-01 9:24:00	EMP001	Pracovnik Manazer	Main Entrance	Entry	Granted
2026-03-01 11:24:00	EMP001	Pracovnik Manazer	Server Room	Entry	Granted
2026-03-01 14:07:00	EMP002	Pracovnik Manazer	Server Room	Entry	Granted
2026-03-01 17:19:00	EMP002	Pracovnik Manazer	Main Entrance	Exit	Granted
2026-03-01 17:30:00	EMP001	Pracovnik Manazer	Main Entrance	Exit	Granted
2026-03-01 23:42:15	EMP001	Pracovnik Manazer	Manager Office	Entry	Granted
2026-03-02 0:00:15	EMP001	Pracovnik Manazer	Manager Office	Exit	Granted
2026-03-02 8:07:00	EMP002	Pracovnik Manazer	Main Entrance	Entry	Granted
2026-03-02 8:09:00	EMP001	Pracovnik Manazer	Main Entrance	Entry	Granted
2026-03-02 10:07:00	EMP002	Pracovnik Manazer	Server Room	Entry	Granted
2026-03-02 11:09:00	EMP001	Pracovnik Manazer	Server Room	Entry	Granted
2026-03-02 16:14:00	EMP002	Pracovnik Manazer	Main Entrance	Exit	Granted
2026-03-02 16:32:00	EMP001	Pracovnik Manazer	Main Entrance	Exit	Granted

2026-03-03 8:07:00	EMP002	Pracovnik Manazer	Main Entrance	Entry	Granted
2026-03-03 9:22:00	EMP001	Pracovnik Manazer	Main Entrance	Entry	Granted
2026-03-03 12:22:00	EMP001	Pracovnik Manazer	Editing Room	Entry	Granted
2026-03-03 13:07:00	EMP002	Pracovnik Manazer	Editing Room	Entry	Granted
2026-03-03 16:34:00	EMP002	Pracovnik Manazer	Main Entrance	Exit	Granted
2026-03-03 17:22:00	EMP001	Pracovnik Manazer	Main Entrance	Exit	Granted
2026-03-04 8:23:00	EMP002	Pracovnik Manazer	Main Entrance	Entry	Granted
2026-03-04 8:27:00	EMP001	Pracovnik Manazer	Main Entrance	Entry	Granted
2026-03-04 10:27:00	EMP001	Pracovnik Manazer	Manager Office	Entry	Granted
2026-03-04 13:23:00	EMP002	Pracovnik Manazer	Server Room	Entry	Granted
2026-03-04 16:34:00	EMP002	Pracovnik Manazer	Main Entrance	Exit	Granted
2026-03-04 16:39:00	EMP001	Pracovnik Manazer	Main Entrance	Exit	Granted
2026-03-05 8:05:00	EMP001	Pracovnik Manazer	Main Entrance	Entry	Granted
2026-03-05 9:29:00	EMP002	Pracovnik Manazer	Main Entrance	Entry	Granted
2026-03-05 12:05:00	EMP001	Pracovnik Manazer	Manager Office	Entry	Granted
2026-03-05 13:29:00	EMP002	Pracovnik Manazer	Server Room	Entry	Granted
2026-03-05 16:27:00	EMP001	Pracovnik Manazer	Main Entrance	Exit	Granted
2026-03-05 17:36:00	EMP002	Pracovnik Manazer	Main Entrance	Exit	Granted
2026-03-06 8:03:00	EMP001	Pracovnik Manazer	Main Entrance	Entry	Granted
2026-03-06 8:04:00	EMP002	Pracovnik Manazer	Main Entrance	Entry	Granted
2026-03-06 9:04:00	EMP002	Pracovnik Manazer	Editing Room	Entry	Granted
2026-03-06 12:03:00	EMP001	Pracovnik Manazer	Server Room	Entry	Granted
2026-03-06 16:16:00	EMP002	Pracovnik Manazer	Main Entrance	Exit	Granted
2026-03-06 16:25:00	EMP001	Pracovnik Manazer	Main Entrance	Exit	Granted

2. Dôkaz

Pri forenznom skúmaní poštového klienta na notebooku manažéra bol v priečinku odoslaných správ (Sent) zaistený kľúčový e-mail, ktorý predstavuje priame priznanie páchateľa k trestnej činnosti.

Časová pečiatka: Pondelok, 24. 3. 2026 o 18:46. Tento čas je kritický, pretože k odoslaniu došlo len približne 20 minút pred fyzickým zaistením a vypnutím zariadenia vyšetrovateľom.

Identifikácia odosielateľa: Správa bola odoslaná z účtu jean (meno páchateľa v rámci scenára) na anonymnú e-mailovú adresu bob@m57.biz.

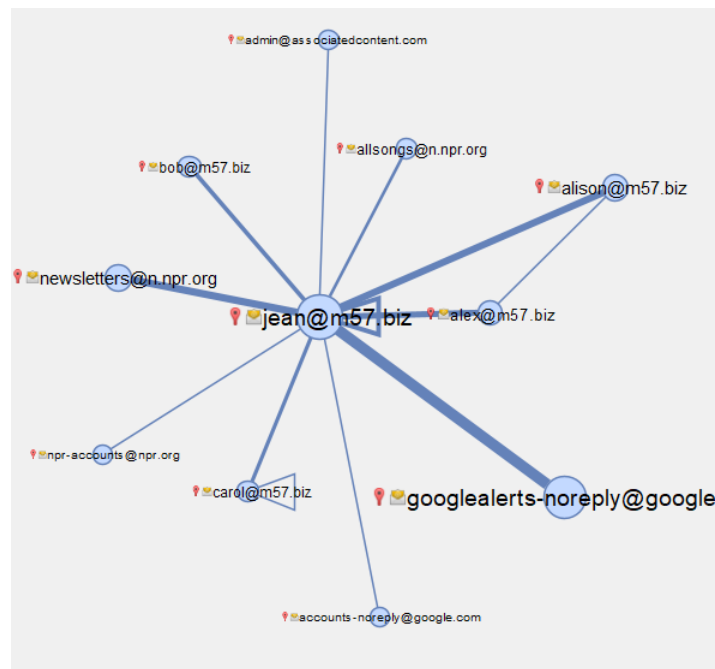
Kľúčové zistenia v texte:

Páchateľ potvrdzuje predchádzajúcu konšpiratívnu komunikáciu cez šifrovanú platformu Telegram.

Explicitne uvádza, že súbor premenoval na FILM.LEAKED, čo sa presne zhoduje s názvom súboru nájdeným neskôr pri analýze RAM záznamov.

Potvrdzuje finančný motív činu požiadavkou na platbu v kryptomene (BTC) na adresu použitú pri predchádzajúcich únikoch.

Forenzný význam: Tento dôkaz definitívne spája digitálnu stopu (premenovaný súbor v RAM) s konkrétnou fyzickou osobou a preukazuje jasný úmysel a plánovanie incidentu.



Nazdar,

mám tu exkluzívny kúsok, o ktorom sme si písali na Telegramu.

Ide o ten krátky film, čo má vyjsť o dva týždne. Súbor som premenoval na **FILM.LEAKED**.

Peniaze pošlite na tú istú krypto-peňaženku (BTC) ako minule.

...

↩ Odpovedať

➡ Preposlať

3. Dôkaz

Názov súboru	Veľkosť (B)	Typ	MD5 Hash	SHA-256 Hash
FILM.LEAKED.mp4	25 529 396	video/mp4	db92e42cd4bf9d732c607b768c8dc608	e46d2ca804c37020ad90a297dac7baf9b861ddfe6735d426abd78b911db94b5
FILM_v7.mov.mp4	25 529 396	video/mp4	db92e42cd4bf9d732c607b768c8dc608	e46d2ca804c37020ad90a297dac7baf9b861ddfe6735d426abd78b911db94b5

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash	SHA-256 Hash
 FILM.LEAKED.mp4		2		2026-03-18 09:32:44 SEČ	0000-00-00 00:00:00	2026-05-05 01:20:28 SELČ	2026-03-23 08:42:32 SEČ	25529396	Allocated	Allocated	unknown	/LogicalFileSet3/FILM.LEAKED.mp4	db92e42cd4bf9d732c607b768c8dc608	d3340d1dbe67b5f055c2280b835f1415f001108979b29
 FILM_v7.mov.mp4		2		2026-03-18 09:32:44 SEČ	0000-00-00 00:00:00	2026-05-05 01:23:22 SELČ	2026-03-23 08:42:32 SEČ	25529396	Allocated	Allocated	unknown	/LogicalFileSet3/FILM_v7.mov.mp4	db92e42cd4bf9d732c607b768c8dc608	d3340d1dbe67b5f055c2280b835f1415f001108979b29

Pomocou nástroja Autopsy sme potvrdili, že hoci páchatel' súbory premenoval, ich vnútorná štruktúra zostala na bit identická. To dokazuje, že nejde o náhodné dáta, ale o priamu kópiu uniknutého filmu.

Forenzný význam:

Dosiahnutá 100% zhoda digitálnych odtlačkov je nevyvrátiteľným technickým dôkazom. Páchatel' sa pokúsil o maskovanie dôkazu zmenou názvu a kontajneru (prípony), avšak vnútorná dátová štruktúra zostala nezmenená. Tento nález priamo vyvracia obhajobu páchatel'a o tom, že súbor stiahol z internetu alebo že ide o iné, nesúvisiace dáta.

4. Dôkaz

Event ID: 20001 - Driver Management concluded the process to install driver disk.inf for Device ID USBSTOR\DISK&VEN_KINGSTON.

Analýza systémových logov v nástroji Autopsy potvrdila pripojenie externého disku značky Kingston (Event ID 20001). Tento nález je kritický, pretože identifikuje pôvodný zdroj, z ktorého bol nelegálny obsah do notebooku prenesený.

Porovnaním časových pečiatok inštalácie ovládača disku a času vytvorenia súboru na disku C: (zistené v tabuľke hashov) je zrejmé, že páchatel' ihneď po vložení disku spustil proces kopírovania. Tento postup dokazuje vedomú snahu páchatel'a o získanie a uchovávanie citlivých dát mimo zabezpečeného externého média.

Forenzný význam: Systémový log potvrdzuje, že notebook slúžil ako cieľová stanica pre neoprávnený prenos dát z externého média Kingston. Tento nález priamo spája fyzické zariadenie páchatel'a s digitálnou stopou (kópiou filmu) nájdenou na systémovom disku.

5. Dôkaz

Forenzná analýza súboru History v nástroji Autopsy (záložka Application) odhalila kritické aktivity páchatel'a.

Záznamy potvrdzujú, že páchatel' nielen hľadal návod na anonymné zverejnenie filmu, ale aktívne navštevoval portály určené na ilegálne zdieľanie dát (The Pirate Bay).

Forenzný význam: Tento dôkaz potvrdzuje plánovaný postup páchatel'a. Opakované návštevy (visit count) stránok na nahrávanie dát vylučujú náhodné kliknutie a v kombinácii s vyhľadávaním výrazu "how to leak movie anonymously" jednoznačne dokazujú úmysel nelegálne distribuovať chránený obsah.

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Table urls 3 entries Page 1 of 1  <button>Export to CSV</button>									
id	url	title	visit_cou...	last_visit_time					
1	https://www.google.com/search?q=how+to+leak+movie+anonymously	Search - Google	1	13416071400000000					
2	https://thepiratebay.org/upload	Upload Torrent	2	13416071400000000					
3	https://mega.nz/affiliate	Cloud Storage	5	13416071400000000					

8. Použité programy

Exterro FTK Imager (x64) - 4.7.3.81

Všeobecné použitie: Slúži na forenznú akvizíciu dát a vytváranie bitových kópií diskov bez ich modifikácie.

Využitie v práci: Tento nástroj ste využili na vytvorenie obrazu fyzického disku podozrivého manažéra a na následný export kľúčových súborov (napr. databázy TimeMoto, Registry) pre ďalšiu analýzu.

Ram Capturer MRCv120

Všeobecné použitie: Nástroj určený na "živú" forenznú analýzu, konkrétne na extrakciu obsahu operačnej pamäte (RAM) zapnutého počítača.

Využitie v práci: Použili ste ho na zachytenie aktuálneho stavu RAM, čo umožnilo objaviť fragmenty e-mailovej komunikácie a stopy po premenovaní uniknutého súboru, ktoré by sa po vypnutí PC stratili.

HxD - Freeware Hex Editor and Disk Editor 2.5.0.0

Všeobecné použitie: Hexadecimálny editor, ktorý umožňuje prezeranie a priamu editáciu binárnej štruktúry súborov a diskov.

Využitie v práci: Pomocou HxD ste analyzovali hlavičky (headers) a päty (trailers) súborov, čo vám pomohlo identifikovať typ súboru FILM.LEAKED a potvrdiť, že ide o video vo formáte MP4.

Microsoft Excel

Všeobecné použitie: Tabuľkový procesor na organizáciu, analýzu a filtrovanie dát.

Využitie v práci: Slúžil vám na spracovanie a prehľadné usporiadanie logov zo systému TimeMoto, vďaka čomu ste mohli presne určiť čas príchodu a odchodu podozrivého z budovy.

Autopsy 4.22.1

Všeobecné použitie: Komplexná digitálna forenzná platforma s grafickým rozhraním na hĺbkovú analýzu diskových obrazov.

Využitie v práci: V tomto programe ste vykonali hlavnú časť vyšetrovania – analýzu histórie webového prehliadača, vyhľadávanie kľúčových slov, kontrolu časových osí (timeline) a identifikáciu pripojených USB zariadení.

9. Zabezpečenie a vytvorenie kópií

- **Fyzické zabezpečenie a ochrana stôp:**

Všetky zaistené digitálne zariadenia (Externý SSD Kingston XS1000 a Notebook ASUS Zenbook 14) boli ihneď po odbere na mieste činu označené unikátnymi štítkami a vložené do faradayových vrecúšok.

Týmto krokom sa eliminovalo riziko vzdialeného vymazania dát cez Wi-Fi/Bluetooth alebo poškodenia citlivých čipov statickou elektrinou.

Originálne dôkazné materiály sú po prevoze trvalo uložené v klimatizovanom bezpečnostnom trezore v priestoroch forenzného laboratória s kontrolovaným prístupom a nepretržitým kamerovým záznamom.

- **Tvorba bitových obrazov:**

Ako prvý bol vykonaný dump operačnej pamäte notebooku pomocou nástroja Magnet RAM Capture (v1.2.0) do formátu .mem.

Tento krok prebehol pred vypnutím zariadenia, aby sa zachovali dáta, procesy a dešifrovacie kľúče.

- **Forenzný formát:**

Pomocou nástroja FTK Imager (v4.7.3.81) boli vytvorené bitové kópie vo formáte .E01 (Expert Witness Format).

Tento formát umožňuje kompresiu a bezpečné uloženie metadát o prípade (číslo prípadu, meno vyšetrovateľa, poznámky) priamo do súboru obrazu.

- **Overenie integrity dát (Hashing):**

Okamžite po ukončení procesu tvorby bitových obrazov boli pre každý obraz vypočítané digitálne odtlačky pomocou algoritmov MD5 a SHA1.

Tieto hashovacie hodnoty sú neoddeliteľnou súčasťou dokumentácie Chain of Custody.

Akákoľvek neskoršia minimálna zmena v dátach by spôsobila nesúlad hashov, čím by bol dôkaz v ďalšom konaní nepoužiteľný.

Všetky analytické úkony sa vykonávajú výhradne na pracovných kópiách.

- **Forezná pracovná stanica:**

Celý proces analýzy prebieha na dedikovanej foreznej pracovnej stanici. Stanica je fyzicky odpojená od internetu a lokálnych sietí, čím sa absolútne vylučuje únik dát alebo zásah externého útočníka počas vyšetrovania.

Operačný systém stanice je nakonfigurovaný tak, aby automaticky nemontoval pripojené jednotky, čím sa predchádza nechcenému zápisu systémových súborov Windowsu na skúmané médiá.

Každý krok vyšetrovateľa v prostredí nástrojov (HxD, Autopsy, FTK) je zaznamenávaný v auditnom logu (vyšetrovacom denníku), čo zaručuje plnú transparentnosť a opakovateľnosť celého postupu.

10.Chain of custody

Číslo:	01	Typ súboru:	Bitový obraz disku(.E01)	Obnovený súbor:	Nie	Veľkosť:	1 TB
Popis prípadu:		Zaistenie externého SSD disku obsahujúceho pracovnú verziu filmu Film v7.mov.					
Názov súboru:		EXT_DISK_IMAGE					
Miesto získania digitálnej stopy:		Kancelária produkčného manažéra					
Poznámky:		Použitý FTK Imager					
Časové pečiatky							
Access:	Tue Mar 24 18:58:18 2026	Modify:	Tue Mar 24 18:58:18 2026	Change:			
Digitálny odtlačok (heš)	MD5	463b9ea86fbd6fc20883a78f2708d43d					
	SHA1	ab8a7ac4f92fd1ec083b563f15ee10c7fac70101					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
Tue Mar 24 18:58:18 2026		Zber informácií/dát z externého disku.					
Tue Mar 24 18:58:22 2026		Dokončenie zberu informácií/dát z externého disku.					
Tue Mar 24 18:58:22 2026		Overovanie hashov spustenie.					
Tue Mar 24 18:58:22 2026		Dokončenie overovania hashov prebehlo úspešne.					

Číslo:	02	Typ súboru:	RFID logy (.csv)	Obnovený súbor:	Nie	Veľkosť:	5 MB
Popis prípadu:		Logy vstupov do kancelárie.					
Názov súboru:		RFID PRISTUPOVY SYSTEM					
Miesto získania digitálnej stopy:		RFID systém					
Poznámky:		Export administrátorom					
Časové pečiatky							
Access:	Tue Mar 24 19:05:42 2026		Modify:	Tue Mar 24 19:05:42 2026		Change:	
Digitálny odtlačok (heš)	MD5	e3cb10e89627e67258d28eb86a992720					
	SHA1	49f73c7b3880a97941e22559d2ad1b01966909ac					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
Tue Mar 24 19:05:42 2026		Zber informácií/dát z RFID zariadenia.					
Tue Mar 24 19:05:42 2026		Dokončenie zberu informácií/dát z RFID zariadenia.					
Tue Mar 24 19:05:42 2026		Overovanie hashov spustenie.					
Tue Mar 24 19:05:42 2026		Dokončenie overenia hashov prebehlo úspešne.					

Číslo:	03	Typ súboru:	Bitový obraz disku (.E01)	Obnovený súbor:	Nie	Veľkosť:	1 TB
Popis prípadu:		Notebook produkčného manažéra.					
Názov súboru:		NOTEBOOK_MANAZERA_IMAGE					
Miesto získania digitálnej stopy:		Kancelária produkčného manažéra					
Poznámky:		Použitý FTK Imager					
Časové pečiatky							
Access:	Tue Mar 24 19:10:21 2026		Modify:	Tue Mar 24 19:10:21 2026		Change:	
Digitálny odtlačok (heš)	MD5	30fb88ca41a1e1377e4b0557fcfc175d					
	SHA1	5c2ae519893578f3675dca2b960a52fa78f083ea					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
Tue Mar 24 19:10:21 2026		Zber informácií/dát z disku.					
Tue Mar 24 19:14:06 2026		Dokončenie zberu informácií/dát z disku.					
Tue Mar 24 19:14:06 2026		Overovanie hashov spustenie.					
Tue Mar 24 19:14:25 2026		Dokončenie overenia hashov prebehlo úspešne.					

11. Záver

Cieľom tejto semestrálnej práce bolo vyšetrenie incidentu neoprávneného úniku digitálneho obsahu (krátkeho filmu) z filmového štúdia. Na základe komplexnej digitálnej forenznej analýzy zaistených stôp sa podarilo úspešne zrekonštruovať priebeh udalostí a identifikovať zodpovednú osobu.

Kombináciou analýzy fyzických prístupových logov (RFID), preskúmania operačnej pamäti (RAM) a hĺbkového skúmania artefaktov na pevnom disku (e-mailová komunikácia, zhoda hashovacích hodnôt) bolo preukázané, že k úniku nedošlo externým hackerským útokom, ale úmyselným konaním interného zamestnanca - produkčného manažéra.

Páchateľ využil svoje prístupové práva na skopírovanie nešifrovaných dát na externé médium mimo pracovnej doby, pričom sa pokúsil o maskovanie stôp premenovaním súborov.

Vyšetrenie potvrdilo kritický význam zachovania integrity dát (Chain of Custody) a dôležitosť analýzy RAM pri identifikácii aktívnej komunikácie páchatel'a. Na zamedzenie podobných incidentov v budúcnosti odporúčame štúdiu zaviesť striktné šifrovanie všetkých pracovných verzií multimediálneho obsahu.