

Únik filmu

Digitálna forenzná analýza

Matúš Horváth

2. ročník APIN FPV UCM

Akademický rok 2025/2026

Prípad

- **Predmet úniku:** finálna verzia filmu (Film_v7.mov)
- **Časový rámec:** súbor bol zverejnený na torrent fórach 14 dní pred plánovanou premiérou
- **Spôsob vykonania:** neoprávnený prístup k nešifrovanému externému disku, ktorý sa nachádzal v priestoroch štúdia
- **Hlavné pochybenie:** obsah disku nebol digitálne chránený, čo umožnilo páchatelovi skopírovať dáta na iné médium priamo v objekte
- **Následky:** predčasné zverejnenie diela viedlo k závažným finančným stratám a poškodeniu dobrého mena štúdia

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.

Odborný príspevok a literatúra

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

- Komplexná príručka pre vyšetrovateľov zameraná na transformáciu digitálnych dát na právne uznateľné dôkazy
- Spája technické postupy získavania dát s právnymi normami
- <https://rishikeshpansare.wordpress.com/wp-content/uploads/2016/02/digital-evidence-and-computer-crime-third-edition.pdf>

Verizon Data Breach Investigations Report (DBIR)

- Analytická správa o štatistikách kybernetických hrozieb
- Potvrďuje, že až 20 % únikov dát spôsobujú interní zamestnanci, čo reflektuje tento prípad
- <https://www.verizon.com/business/resources/reports/dbir/>

Hypotézy

Hypotéza 1: Interný páchatel'

- **Stav:** POTVRDENÁ
- **Dôkazy:** Fragmenty e-mailov v RAM a odoslaná pošta z účtu manažéra
- **Motív:** Finančný zisk (potvrdené stopy po platbe v kryptomene)

Hypotéza 2: Kopírovanie a distribúcia

- **Stav:** ČIASTOČNE POTVRDENÁ
- **Dôkazy:** Systém TimeMoto potvrdil prítomnosť manažéra v nedeľu v noci (23:42).
- Zhoda hashov súborov a sieťová aktivita na The Pirate Bay
- Súbor bol skopírovaný na firemný notebook

Hypotéza 3: Externý kyberútok

- **Stav:** ZAMIETNUTÁ
- **Odôvodnenie:** Nulový výskyt malvéru, backdoorov alebo pokusov o prelomenie hesla
- **Záver:** Všetky kroky boli vykonané pod legitímnym prístupom manažéra na jeho zariadení

Digitálne zariadenia a dáta



EXTERNÝ SSD DISK

Kingston XS1000 – 1 TB

- Vymeniteľné médium exfiltrácie
- USB 3.2 Gen 2 (USB-C / USB-A)
- Obsah: Film_v7.mov (pracovná verzia)
- Veľkosť datasetu: 49,8 MB
- Typy súborov: .mp4, .mov, .tmp



NOTEBOOK MANAŽÉRA

ASUS Zenbook 14 OLED (UX3405)

- OS: Windows 11 / scenár M57-Jean
- RAM: 16 GB LPDDR5X | SSD: 1 TB PCIe 4.0
- Súborový systém: NTFS
- Dataset: 2,85 GB (.E01 forenzný obraz)
- Typy: .dll, .exe, .eml, .mp4, .mkv, .sqlite



RFID PRÍSTUPOVÝ SYSTÉM

TimeMoto TM-616

- Metóda: RFID karta / kľúčienka / PIN
- Pripojenie: Wi-Fi / Ethernet (LAN)
- Export: tabuľka Excel (.xlsx)
- Veľkosť datasetu: 7 KB
- Obsahuje: timestampy príchodov/odchodov



Analýza dát

1. Analýza obrazu pamäte RAM (evidence_dump_2026.mem)
2. Analýza obrazov zariadený

Analýza obrazu pamäte RAM

- Dôkaz č. 1: Fragment komunikácie (premenovanie súboru)

```
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
```

- Dôkaz č. 2: Sieťová aktivita domény Pirate Bay (52 výskytov)

```
00357D020 00 00 00 00 03 27 A0 40 FF FF FF FF FC D8 5F BF .....UR_2
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 .....uR_z
```

- Dôkaz č. 3: Záznam o presune dát z externého média do notebooku

```
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..../.1.0nps
```

Analýza obrazov zariadený

Dôkaz č. 1: Logy prístupového systému TimeMoto (fyzická prítomnosť)

2026-03-01 23:42:15	EMP001	Pracovník Manazer	Manager Office	Entry	Granted
2026-03-02 0:00:15	EMP001	Pracovník Manazer	Manager Office	Exit	Granted

Dôkaz č. 2: E-mailové priznanie a požiadavka na platbu v BTC

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 minútu.

Dôkaz č. 3: Hashovacia analýza (potvrdenie 100% bitovej zhody)

Názov súboru	Veľkosť (B)	Typ	MD5 Hash	SHA-256 Hash
FILMLEAKED.mp4	25 529 396	video/mp4	db92e42cd4bf9d732c607b768c8dc608	e46d2ca804c37020ad90a297dac7ba9b861ddfe67356426babd78b911db94b5
FILM_v7.mov.mp4	25 529 396	video/mp4	db92e42cd4bf9d732c607b768c8dc608	e46d2ca804c37020ad90a297dac7ba9b861ddfe67356426babd78b911db94b5

Dôkaz č. 4: Systémový log pripojenia externého disku Kingston

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

Dôkaz č. 5: História prehliadača (návody na anonymný únik)

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Table		urls	3 entries		Page 1 of 1		Export to CSV		
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	3	13416071400000000					

Použité programy

RAM Capturer MRCv120

Dump operačnej pamäte (.mem)

Zachytenie volatilnej pamäte notebooku PRED jeho vypnutím. Umožnilo objaviť fragmenty Telegram komunikácie a stopy premenovaného súboru, ktoré by sa inak stratili.

Microsoft Excel

Spracovanie RFID logov (.xlsx)

Organizácia a filtrovanie dochádzkových záznamov TimeMoto. Identifikácia kritického záznamu v riadku 32: EMP001 o 23:42:15 mimo pracovnej doby.

HxD Hex Editor 2.5.0.0

Hexadecimálna analýza RAM

Prezeranie binárnej štruktúry RAM dumpu. Identifikácia adries 13EBDD80 (Telegram), 00357D30 (Pirate Bay), 2C093710 (prenos súboru). Overenie súborových hlavičiek.

Exterro FTK Imager 4.7.3.81

Bitové kópie zariadení (.E01)

Forenzná akvizícia diskov bez modifikácie. Write-blocker podpora, výpočet MD5/SHA1 hashov. Export registrov a kľúčových súborov (NTUSER.DAT, databázy TimeMoto).

Autopsy 4.22.1

Komplexná analýza diskových obrazov

Hlavná analytická platforma – historia prehliadača, kľúčové slová, USB artefakty, e-mailová komunikácia, hashové porovnanie súborov, časová os udalostí.

Zabezpečenie a vytvorenie kópií

1. Zaistenie a ochrana stôp

- **Fyzická ochrana:** Zariadenia (SSD Kingston, ASUS Zenbook) uložené vo **Faradayových vrecúškach** (ochrana pred vzdialeným zmazaním/statickou elektrinou)
- **Bezpečné úložisko:** Originály sú v trezore s riadenou teplotou a nepretržitým kamerovým monitoringom

2. Akvizícia dát (Získavanie dôkazov)

- **Dump RAM:** Vykonaný ako prvý (nástroj Magnet RAM Capture) pred vypnutím notebooku (zachovanie procesov a kľúčov).
- **Forenzné kópie:** Vytvorené bitové obrazy diskov vo formáte **.E01** (nástroj FTK Imager)
- **Hashovanie:** Okamžitý výpočet **MD5** a **SHA1** pre overenie integrity (Chain of Custody)

3. Analytické prostredie

- **Forenzná stanica:** Izolovaná jednotka bez prístupu k internetu (Air-gapped).
- **Ochrana proti zápisu:** Systém upravený tak, aby zabránil akémukoľvek zápisu na skúmané médiá.
- **Transparentnosť:** Každý úkon (HxD, Autopsy, FTK) je automaticky logovaný vo vyšetrovacom denníku pre zabezpečenie opakovateľnosti.

Chain of custody

Císlo:	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	463b9ea86fdb6fc20883a78f2708d43d					
	SHA1	ab8a7ac4f92fd1ec083b563f15ee10c7fac70101					
Časová pečiatka							
Tue Mar 24 18:58:18 2026		Akcia vykonaná s digitálnou stopou					
Tue Mar 24 18:58:22 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 overenia hashov prebehlo úspešne.					

Císlo:	02	Typ súboru:	RFID logy (.csv)	Obnovený súbor:	Nie	Veľkosť:	5 MB
Popis prípadu:	Logy vstupov do kancelárie.						
Názov súboru:	RFID PRISTUPOVÝ 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							
Tue Mar 24 19:05:42 2026		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.					

Cislo:	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							
Tue Mar 24 19:10:21 2026		Akcia vykonaná s digitálnou stopou					
Tue Mar 24 19:14:06 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.					

Záver

- **Výsledok:** identifikácia páchatel'a (produkčný manažér) a vyvrátenie teórie o hackerskom útoku
- **Metóda:** analýza RAM, diskov, RFID prístupov a e-mailovej komunikácie
- **Odporúčanie:** zavedenie striktného šifrovania dát na zamedzenie zneužitia interných právomocí

Ďakujem za pozornosť