

KRÁDEŽ VO VLAKU

Digitálna forenzná analýza (DFA)

Fakulta prírodných vied a informatiky, UCM Trnava

Michal Rýzek

Akademický rok 2025/2026

1. Názov prípadu a zhrnutie

Prípad: Krádež batohu počas cestovnej vlakovou súpravou Os 3412 na trati Trnava – Kúty

Dátum incidentu: 17. apríla 2026

Dátum zahájenia vyšetrovania: 18. apríla 2026

1.1 Zhrnutie prípadu (model 5WH)

Otázka	Opis
Kto (Who)	Neznámy páchateľ (ďalej NP), obeť: Jana Kováčová, cestujúca na vlaku Os 3412
Čo (What)	Odcudzenie batohu (čierna taška Osprey Farpoint 40 L) obsahujúceho notebook, doklady a peňaženku
Kedy (When)	Krádež sa odohrala medzi zastávkami Smolenice (15:59) a Kúty (16:57), 17. 4. 2026
Kde (Where)	Vlak Os 3412, vozňový rad 2, sedadlá 14–18, úsek trate Smolenice – Kúty
Prečo (Why)	Pravdepodobne majetkový trestný čin – krádež s cieľom zisku
Ako (How)	Páchateľ využil moment, keď obeť zaspala (doložené HRV dátami z hodínok), a batoh odniesol bez priameho fyzického kontaktu s obeťou

1.2 Predmet a ciele vyšetrovania

Predmetom vyšetrovania je digitálna forenzná analýza dostupných elektronických dôkazov za účelom identifikácie páchateľa krádeže batohu. Ciele sú:

- Rekonštruovať chronologický priebeh udalostí na základe digitálnych stôp.
- Identifikovať podozrivú osobu prostredníctvom analýzy CCTV záznamov, Wi-Fi logov a RAM obrazu smarthodínok obete.
- Overiť stanovené forenzné hypotézy.
- Zachovať integritu dôkazov a vytvoriť chain of custody pre prípadné trestné konanie.

1.3 Odborný príspevok z DFRWS

Relevantný vedecký príspevok: Nickson M. Karie, Hein S. Venter: "Toward a General Ontology for Digital Forensic Disciplines", DFRWS 2015 (Journal of Digital Forensics, Security and Law, 2015). Príspevok definuje všeobecnú ontológiu pre digitálne forenzné disciplíny vrátane analýzy IoT a nositeľných zariadení. Je priamo relevantný pre náš prípad, keďže smarthodinky obete predstavujú IoT/wearable zariadenie, z ktorého bol získaný RAM obraz, a príspevok poskytuje metodologický rámec pre spracovanie dát z takýchto zariadení v súlade s medzinárodne uznávanými forenznými princípmi.

2. Forenzné hypotézy

2.1 Hypotéza H1 – Páchateľ vystúpil na prvej zastávke po krádeži

Atribút	Popis
Súvisiace zariadenia	CCTV kamery na nástupištiach Štefanov a Kúty; GPS log z vlaku (NMEA súbory)
Digitálne stopy	Záznamy z kamery č. 4 (výstupné dvere, vozňový rad 2); Wi-Fi DHCP logy (odpojenie zariadenia)
Nástroj a postup	Autopsy – analýza videosúborov .mp4;

2.2 Hypotéza H2 – Ku krádeži nedošlo a obeť si to vymyslela

Atribút	Popis
Súvisiace zariadenia	Wi-Fi router TP-Link TL-WR902AC (vlakový)
Digitálne stopy	DHCP logy, RADIUS autentifikačné záznamy, MAC adresa zariadenia, pridelené IP adresy
Nástroj a postup	VLC

2.3 Hypotéza H3 – Obeť v čase krádeže spala a nevšimla si že bola okradnutá (doložené biosenzormi hodínok)

Atribút	Popis
Súvisiace zariadenia	Smart hodinky Garmin Forerunner 245 Music obeť (RAM obraz)
Digitálne stopy	RAM artefakty: záznamy srdcovej frekvencie (HRV), akcelerometrické dáta, GPS súradnice, sleep detection dáta
Nástroj a postup	FTK Imager – získanie RAM obrazu; HxD – hex analýza .img súboru; Belkasoft RAM Analyzer – extrakcia štruktúrovaných artefaktov

2.4 Hypotéza H4 – Obeť zabudla kde sedí a jej veci ostali na jej originálnom mieste

Atribút	Popis
Súvisiace zariadenia	IP kamery Hikvision DS-2CD2143G2-I vo vlaku (celkovo 4 ks)
Digitálne stopy	Videosúbory .mp4 (H.264), časové pečiatky, záznamy pohybu
Nástroj a postup	VLC

3. Digitálne zariadenia

3.1.1 Kamerový systém – Hikvision DS-2CD2143G2-I

Parameter	Hodnota
Výrobca / Model	Hikvision / DS-2CD2143G2-I
Sériové číslo	DS-2CD2143G2-I-SN20260417A
Inštalácia vo vlaku	4 kusy: predná kabína (×1), prechod medzi vozňami (×2), zadný vozňový rad (×1)
Rozlíšenie	4 MP (2688 × 1520 px), farebný snímač CMOS 1/3"
Formát záznamu	H.264+, kontajner .mp4
Snímkovacia frekvencia	25 fps
Kapacita NVR úložiska	2 TB (WD Purple HDD); rotačná smyčka 72 hodín
Prístupová doba	≈ 12 ms (HDD rotačné médium)
Rýchlosť čítania / zápisu	130 MB/s čítanie / 90 MB/s zápis
Protokol prenosu	RTSP / onvif



Toto je kamerový systém ktorý sa vo vlakoch ktoré jazdia na trase Trnava – Kúty zvyčajne nachádza

3.1.2 Wi-Fi Router – TP-Link TL-WR902AC

Parameter	Hodnota
Výrobca / Model	TP-Link / TL-WR902AC
Sériové číslo	2196G-WR902AC-001A
Firmware verzia	3.16.9 Build 200727 Rel.55495n
Frekvenčné pásmo	2.4 GHz + 5 GHz (dual-band)
SSID	VlakNet_OS3412
Logy uložené na	Interná flash pamäť 16 MB + externý USB kľúč Kingston 32 GB
Logovaná dáta	DHCP lease záznamy, autentifikácia (RADIUS), MAC adresy, časy pripojenia/odpojenia, pridelené IP
Prístupová doba	< 1 ms (flash)
Rýchlosť čítania	≈ 300 MB/s (USB 3.0)



Toto je router ktorí sa nachádza vo vlaku ktorí jazdí na trase Trnava – Kúty v ktorom sa náš prípad odohral a na ktorom bola ako obeť tak aj páchatel pri najväčšej pravdepodobnosti pripojený.

3.1.3 Smart hodinky – Garmin Forerunner 245 Music (obet')

Parameter	Hodnota
Výrobca / Model	Garmin / Forerunner 245 Music
Sériové číslo	3BE123456789
Kapacita internej pamäte	3,5 GB (storage) + 64 MB RAM (LPDDR3)
Senzory	GPS/GLONASS, Eleveo HR (optický snímač TF), akcelerometer, barometer, kompas
Operačný systém	Garmin OS (proprietárny, Linux kernel 4.4)
Súborový systém	FAT32 (interné úložisko), exFAT (externá karta)
Konektivita	ANT+, Bluetooth 4.0, Wi-Fi 2.4 GHz
Rýchlosť čítania (USB)	≈ 18 MB/s
Batéria v čase zaistenia	62 %



Toto sú hodinky ktoré mala obäť na sebe v dobe krádeže. Zariadenie bolo aj spárované s telefónom obeťe. Toto zariadenie má integrované ložisko, podporu pre hudbu, GPS, meranie tepu, párovanie s mobilnými zariadeniami. Toto zariadenie má odhadovanú životnosť batérie 7 dní vo smart režime, 24 hodín s GPS a 6 hodín so zapnutou hudbou a GPS.

4. Prehľad dát a datasetov

4.1 Typy súborov a datasety

Všetky dáta boli vygenerované AI asistentom Claude (Sonnet 4.6).

Zdroj zariadenia	Počet súborov	Celková veľkosť	Poznámka
CCTV NVR Hikvision	4	14,2 GB	Záznamy zo 4 kamier, úsek 15:00–17:30
Wi-Fi router TP-Link	3	1,2 MB	dhcp.log, auth.log, syslog
RAM hodínok Garmin	1	64,0 MB	Binárny RAW obraz pamäte
Garmin Forerunner 245	1	88 kB	Aktivitný súbor Garmin FIT (binárny)
Export GPS hodinky	1	24 kB	GPS track obeť (exportovaný cez Garmin Connect)
Snímky z CCTV (Autopsy)	47	31,5 MB	Kľúčové snímky extrahované z .mp4
Wi-Fi DHCP export	1	8 kB	Parsovaný zoznam DHCP lease záznamov
GPS trasa páchatel'a (sim.)	1	6 kB	Simulovaná GPS trasa podozrivého

Celková veľkosť datasetu: 14,30 GB | Celkový počet súborov: 59

4.2 Simulované dáta

Vzhľadom na simulovaný charakter prípadu boli nasledovné dáta vytvorené synteticky tak, aby verne odrážali reálny priebeh udalostí a boli logicky konzistentné s ostatnými digitálnymi stopami:

- RAM obraz Garmin – Simulovaný obraz obsahuje realistické artefakty: GPS súradnice pozdĺž trate Trnava–Kúty, HRV dáta s potvrdením spánku, fragmenty Wi-Fi sieťových konfigurácií a notifikačné záznamy.
- DHCP/Wi-Fi logy – Synteticky vygenerované záznamy odrážajúce pripojenie zariadenia s MAC 3C:2E:F9:A1:7B:4D od 15:47 do 16:59. Časy sú konzistentné s CCTV zábermi.
- KML GPS trasa páchatel'a – Simulovaná trasa z vlaku do centra Kútov, vytvorená v Google Maps na základe reálnych geografických dát OpenStreetMap.
- Garmin FIT súbor obeť – Binárny súbor aktivity, generovaný nástrojom fit-file-writer (Node.js), obsahuje HRV, krokomery a GPS dáta pre časový úsek 14:30–17:15 v deň incidentu.

5. Image RAM – analýza a artefakty

5.1 Postup získania RAM obrazu

RAM obraz bol získaný dňa 18. 4. 2026 o 09:14 UTC analytikom Bc. M. Novákom za prítomnosti svedka. Postup:

- Smarthodinky boli prijaté v zaistenom stave (vypnuté, v antistatickom vrecku) s potvrdenou batériou 62 %.
- Zariadenie bolo pripojené cez USB s fyzickým hardvérovým blokovačom zápisu CRU WiebeTech USB Write Blocker v3, čím bola zaručená integrita originálu.
- FTK Imager 4.7.1.2 vytvoril RAW .img obraz celého úložného priestoru zariadenia vrátane obsahu zachyteného cez USB DFU (Device Firmware Upgrade) mode.
- Ihneď po vytvorení obrazu boli vypočítané hashe MD5 a SHA-1 a zaznamenané do forenzného protokolu.
- Obraz bol uložený na forezný HDD (evidence drive č. 1) a jeho záloha na evidence drive č. 2; oba disky uzamknuté v trezore.

5.2 Artefakty z RAM obrazu

Artefakt RAM-01: GPS súradnice v čase krádeže

Offset v obraze: 0x00A3F200 – 0x00A3F240

Interpretácia: Záznamy GPS súradníc zapísané v 30-sekundových intervaloch. Reťazec v čase 16:12:44 zodpovedá polohe medzi zastávkami Štefanov a Kúty, čo koreluje s časom zaznamenaným na CCTV.

Offset	Hex dump	ASCII
00A3F200	47 50 53 3A 34 38 2E 35 36 37 32 4E 2C 31 37 2E	GPS:48.5672N,17.
00A3F210	32 33 34 38 45 2C 31 36 3A 31 32 3A 34 34 2C 53	2348E,16:12:44,S
00A3F220	50 44 3D 35 2E 32 6D 2C 41 43 43 3D 30 2E 30 32	PD=5.2m,ACC=0.02

Dekódovaný obsah: GPS:48.5672N,17.2348E | Čas: 16:12:44 UTC | Presnosť: 5,2 m

Forenzný význam: Poloha 48.5672°N, 17.2348°E zodpovedá katastrálnemu územiu medzi zastávkami Štefanov nad Oravou a Kúty, čo potvrdzuje, že obeť sa v tomto čase nachádzala na inkriminovanom úseku trate. Táto GPS stopa koreluje s CCTV záberom o 16:12.

Artefakt RAM-02: Záznam srdcovej frekvencie (HRV) – detekcia spánku

Offset v obraze: 0x01B7C080 – 0x01B7C0C0

Interpretácia: Blok obsahuje sekvenciu hodnôt tepovej frekvencie (v BPM, unsigned 8-bit integers) v 1-minútovom rozlíšení. Hodnoty pod 62 BPM s nízkou variabilitou sú indikátorom ľahkého spánku podľa Garmin Sleep Algorithm.

Offset	Hex dump	Dekódovanie
01B7C080	48 52 3A 37 32 2C 37 30 2C 36 38 2C 36 35 2C 36	HR:72,70,68,65,6
01B7C090	32 2C 35 39 2C 35 38 2C 53 4C 3A 31 36 3A 30 37	2,59,58,SL:16:07
01B7C0A0	2C 53 54 3A 4C 49 47 48 54 2C 48 52 56 3A 4C 4F	,ST:LIGHT,HRV:LO

Dekódovaný obsah: HR: 72, 70, 68, 65, 62, 59, 58 BPM (15:58 – 16:04) | Sleep onset: 16:07 | Sleep type: LIGHT | HRV: LOW (spánkový stav)

Forenzný význam: Progresívny pokles TF z 72 na 58 BPM a aktivácia sleep-detection algoritmu o 16:07 potvrdzujú H3 – obeť zaspala pred samotnou krádežou o 16:12. Toto je kľúčový dôkaz, ktorý vysvetľuje, prečo nezaregistrovala odcudzenie batohu.

Artefakt RAM-03: Fragment Wi-Fi sieťového profilu

Offset v obraze: 0x02C4A500 – 0x02C4A560

Interpretácia: RAM obsahuje fragment sieťového profilu Wi-Fi uloženého v operačnej pamäti hodínok. Obsahuje SSID vlakového routera a hash hesla, čo dokumentuje, že hodinky boli pripojené k sieťovej infraštruktúre vlaku.

02C4A500	57	49	46	49	3A	56	6C	61	6B	4E	65	74	5F	4F	53	33	WIFI:VlakNet_OS3
02C4A510	34	31	32	2C	50	53	4B	3A	62	37	64	32	61	31	65	39	412,PSK:b7d2a1e9
02C4A520	66	33	63	38	62	30	37	34	2C	4D	41	43	3A	42	38	3A	f3c8b074,MAC:B8:

Dekódovaný obsah: SSID: VlakNet_OS3412 | PSK hash: b7d2a1e9f3c8b074 | MAC hodínok: B8:3E:59:AD:2C:1F

Forenzný význam: Potvrdenie, že hodinky boli pripojené k Wi-Fi sieti vlaku. MAC adresa hodínok obete (B8:3E:59:AD:2C:1F) sa nachádza aj v DHCP logoch routera, čo umožňuje korelačnú analýzu a vylúčenie zámeny zariadení.

6. Image zariadení – hlavné dôkazy

Dôkaz D-01: CCTV záznam – identifikácia krádeže (16:12–16:14)

Atribút	Hodnota
Zdroj	CCTV kamera č. 3 (vozňový rad 2, zadná časť), súbor: cam3_20260417_1500.mp4
Časová pečiatka	17. 4. 2026, 16:12:07 – 16:14:23
Popis obsahu	Na zázname je viditeľná mužská postava (tmavá bunda, tmavé vlasy, výška cca 175 cm) prechádzajúca uličkou. O 16:12:07 sa priblížil ku sedadlu v rade 16, kde leží batoh. O 16:12:27 odchádza s batohom zavesným na pravom ramene.
Formát	H.264, 2688×1520px, 25fps
MD5 hash súboru	9f2e3c1a8b4d7e0f5a2c6b9d1e3f7a4c
Podporuje hypotézu	H1 (páchateľ odišiel s batohom), H3 (fyzická identifikácia na CCTV)

Dôkaz D-02: CCTV záznam – výstup páchatel'a (stanica Kúty, 16:59)

Atribút	Hodnota
Zdroj	CCTV kamera nástupišťa Kúty (externá, ŽSR), súbor: kutynastupistypatform2_20260417.mp4
Časová pečiatka	17. 4. 2026, 16:59:14
Popis obsahu	Tá istá mužská postava (identická bunda, rovnaký batoh) vystupuje z vlaku na 2. nástupišti v Kútoch. Batoh zodpovedá popisu odcudzeného (čierna Osprey, veľkosť 40 L, žltý prívěsok na zips).
MD5 hash súboru	3c7a9f2e1b4d8c0e5f7a3b6d9e1f2c4a
Podporuje hypotézu	H1 (potvrdenie výstupu páchatel'a na prvej zastávke po krádeži)

Dôkaz D-03: Wi-Fi DHCP log – pripojenie podozrivého zariadenia

Atribút	Hodnota
Zdroj	Wi-Fi router TP-Link, súbor: dhcp.log
Relevantné záznamy	15:47:03 DHCP OFFER 192.168.1.14 -> 3C:2E:F9:A1:7B:4D (Samsung)\n16:59:01 DHCP RELEASE 192.168.1.14 <- 3C:2E:F9:A1:7B:4D
Popis	MAC adresa 3C:2E:F9:A1:7B:4D (OUI prefixom Samsung Electronics) sa pripojila k Wi-Fi o 15:47. Zariadenie sa odpojilo o 16:59:01 – čo je 47 sekúnd po zaznamenávaní výstupu z vlaku na CCTV (16:59:14 – rozdiel je v latencii DHCP release oproti fyzickému pohybu).
Nástroj analýzy	Wireshark 4.2, Python 3.11 (pandas korelačný skript)
MD5 hash súboru	b1c4e8f2a7d3e9f0c5b2a4d7e3f1c8b9
Podporuje hypotézu	H2 (digitálna stopa páchatel'a v sieti)

Dôkaz D-04: HRV a sleep-detection dáta z hodínok obeť

Atribút	Hodnota
Zdroj	RAM obraz DFA-2026-001_GARMIN_RAM.img, artefakt RAM-02
Popis	Pokles tepovej frekvencie zo 72 BPM (15:58) na 58 BPM (16:04), aktivácia sleep-detection algoritmu o 16:07. Hodnoty HRV poklesli pod prahovú hodnotu 30 ms RMSSD, čo Garmin klasifikuje ako ľahký spánok (LIGHT sleep stage).
Nástroj analýzy	HxD 2.5, Belkasoft RAM Analyzer 9.0, Python fitparse knižnica
Podporuje hypotézu	H3 (obeť spala v čase krádeže) – POTVRDENÁ

Dôkaz D-05: GPS korelácia – poloha obeť a páchateľ

Atribút	Hodnota
Zdroj	RAM artefakt RAM-01 (GPS hodínok obeť) + simulovaná KML trasa páchateľ
Popis	GPS hodínok obeť: 48.5672°N, 17.2348°E o 16:12:44 (medzi Štefanovom a Kútmi). Koreluje s CCTV záberom krádeže. Simulovaná trasa páchateľ po výstupe v Kútoch vedie smer mesto Kúty, centrum (vzdialenosť od nástupišťa cca 1,2 km, čas pešo ≈ 15 min).
Nástroj analýzy	Google Maps
Podporuje hypotézu	H1 a H3 – geografická a časová konzistencia dôkazov

Dôkaz D-06: Garmin FIT súbor – aktívny záznam obeť

Atribút	Hodnota
Zdroj	activity_20260417_143022.fit (exportovaný z hodínok cez Garmin Connect)
Popis	FIT súbor zaznamenáva kompletnú aktivitu obeť od 14:30 do 17:15. Krokometry ukazujú nízku aktivitu od 16:07 (menej ako 2 kroky/min), čo potvrdzuje sedavú/spiaci polohu v čase krádeže.
Hash MD5	e4f1c8a2b7d9e3f0c6b4a8d2e7f3c1b5
Podporuje hypotézu	H3 (potvrdenie spánku z iného zdroja ako RAM)

Dôkaz D-07: RADIUS autentifikačný log – identifikácia účtu

Atribút	Hodnota
Zdroj	Wi-Fi router, súbor: auth.log
Relevantný záznam	15:47:01 RADIUS ACCEPT user=samsung_j71@vlaknet MAC=3C:2E:F9:A1:7B:4D VLAN=guests
Popis	Autentifikačný log obsahuje username samsung_j71@vlaknet, ktorý bol zaregistrovaný prostredníctvom captive portálu vlaku. Prihlasovacie meno bolo ďalej preverené u vlakového dopravcu a koreluje s osobou, ktorá si zakúpila lístok na trasu Trnava–Kúty platobnou kartou.
Podporuje hypotézu	H2 (identita páchateľ prostredníctvom digitálnej stopy v sieti) – silný nepriamy dôkaz

7. Softvérové nástroje a ich účel

Nástroj	Verzia	Účel v tomto prípade
Exterro FTK Imager	4.7.1.2	Vytvorenie bitových kópií (.img, .E01) zariadení; kalkulácia MD5/SHA-1 hashov; bol použitý pre RAM obraz hodínok a pre zálohu CCTV NVR disku
HxD Hex Editor	2.5.0.0	Manuálna analýza binárnych artefaktov v RAM obraze; vyhľadávanie ASCII/HEX reťazcov (GPS súradnice, HR hodnoty, Wi-Fi SSID fragmenty)
Autopsy	4.21.0	Komplexná analýza a indexácia súborov; extrakcia metadát; timeline analýza udalostí; analýza CCTV .mp4 súborov a FIT súborov
Belkasoft RAM Analyzer	9.0.4984	Automatizovaná extrakcia štruktúrovaných artefaktov z RAM obrazu (hodinky Garmin); identifikácia procesov, sietí, reťazcov
VLC Media Player	3.0.20	Vizuálna kontrola CCTV videozáznamov; prehrávanie s presnou časovou navigáciou

8. Bezpečnostné opatrenia a reťazec dôvery

8.1 Bitové kópie zariadení

Zariadenie	Počet kópií	Umiestnenie	MD5 Hash	SHA-1 Hash	Čas vytvorenia
CCTV NVR disk	2	Forenzný HDD #1 (trezor A), HDD #2 (trezor B)	9f2e3c1a8b4d7e0f	d84e2a910f3b7c6e45d1	18.4.2026 08:32 UTC
Wi-Fi router flash	2	Forenzný HDD #1 (trezor A), HDD #2 (trezor B)	b1c4e8f2a7d3e9f0	a3c5b0e1d2f9a84f3e2c	18.4.2026 09:01 UTC
Smart hodinky RAM	2	Forenzný HDD #1 (trezor A), HDD #2 (trezor B)	a3f8c2e1d7b904f5	d84e2b910f3b7c6e45d1	18.4.2026 09:14 UTC
Smart hodinky interné úložisko	2	Forenzný HDD #1 (trezor A), HDD #2 (trezor B)	e4f1c8a2b7d9e3f0	b9c2e7f3a1d5e8c4b6a2	18.4.2026 09:28 UTC

8.2 Chain of Custody

Císlo:	001	Typ súboru:	Video .mp4	Obnovený súbor:	Nie	Veľkosť:	14,2 GB
Popis prípadu:	Krádež batohu vo vlaku Os 3412 na trati Trnava–Kúty dňa 17. 4. 2026. Vyšetrovanie krádeže.						
Názov súboru:	cam1_20260417_1500.mp4, cam2_20260417_1500.mp4, cam3_20260417_1500.mp4, cam4_20260417_1500.mp4						
Miesto získania digitálnej stopy:	Vlak Os 3412, bezpečnostný systém (model Hikvision DS-7608NI-K2), depo Kúty, vozňový rad 2.						
Poznámky:	Záznamy pokrývajú časový úsek 15:00–17:30 zo štyroch kamier. Originálne médiá uložené vo Faradayovom vrecku, plomba č. F-001.						
Časové pečiatky							
Access:	17. 4. 2026 18:15 UTC	17. 4. 2026 17:30 UTC	17. 4. 2026 18:32 UTC	Change:			
Digitálna odtlačok (heš)	MD5	9f2e3c1a8b4d7e0f5a2c6b9d1e3f7a4c					
	SHA1	c91f3b820e4a5d7f28e392b4f1c7d3a5e8b2f096					
Časová pečiatka	Akcia vykonaná s digitálnou stopou						
18. 4. 2026 08:55 UTC	Vytvorenie bitovej kópie č.2 (E01) na forezný HDD #2 – záloha						
18. 4. 2026 10:15 UTC	Analýza videosúborov v Autopsy 4.21 – extrakcia kľúčových snímok						

Číslo:	002	Typ súboru:	Log .log	Obnovený súbor:	Nie	Veľkosť:	1,2 MB + 16 MB
Popis prípadu:		Krádež batohu vo vlaku Os 3412 na trati Trnava–Kúty dňa 17. 4. 2026. Vyšetrovanie krádeže.					
Názov súboru:		dhcp.log, auth.log, syslog, router_flash.img					
Miesto získania digitálnej stopy:		Vlak Os 3412, server rack za kabínou strojvodcu. Wi-Fi router TP-Link TL-WR902AC, SN: 2196G-WR902AC-001A.					
Poznámky:		Router zaistený vo vypnutom stave, vložený do Faradayovho vrečka, plomba č. F-002. Logy exportované cez SSH pred vypnutím zariadenia.					
Časové pečiatky							
Access:	17. 4. 2026 18:22 UTC	17. 4. 2026 16:59 UTC	17. 4. 2026 18:22 UTC	Change:			
Digitálna odtlačok (heš)	MD5	b1c4e8f2a7d3e9f0c5b2a4d7e3f1c8b9					
	SHA1	a7d3f1c8b9e2f4a5c0b7d3e9f1a4c8b2e5d7f093					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
18. 4. 2026 09:05 UTC		Vytvorenie bitovej kópie flash pamäte routera (.img) – FTK Imager					
18. 4. 2026 11:00 UTC		Analýza logov v Wireshark 4.2 – filtrácia DHCP a RADIUS záznamov					

Číslo:	003	Typ súboru:	RAM image	Obnovený súbor:	Áno – artefakty z RAM	Veľkosť:	64 MB RAM + 3,5 GB storage
Popis prípadu:	Krádež batohu vo vlaku Os 3412 na trati Trnava–Kúty dňa 17. 4. 2026. Vyšetrovanie krádeže.						
Názov súboru:	DFA-2026-001_GARMIN_RAM.img, activity_20260417_143022.fit, gps_track_obet.csv						
Miesto získania digitálnej stopy:	Zariadenie (Garmin Forerunner 245 Music, SN: 3BE123456789) odovzdala obeť Jana Kováčová dobrovoľne dňa 17. 4. 2026 o 19:45. Batéria v čase odovzdania: 62 %.						
Poznámky:	Hodinky prijaté vo vypnutom stave, uložené v antistatickom vrecku. RAM obraz získaný cez USB DFU mode s aktívnym write-blockerom. Hash overený 3× (vytvorenie, uloženie HDD #1, pred analýzou) – všetky zhodné.						
Časové pečiatky							
Access:	18. 4. 2026 09:14 UTC	17. 4. 2026 16:57 UTC	18. 4. 2026 09:14 UTC	Change:			
Digitálna odtlačok (heš)	MD5	a3f8c2e1d7b904f5a1cc83e290f74b62					
	SHA1	d84e2a910f3b7c6e45d1892f7a3c5b0e1d2f9a84					
Časová pečiatka	Akcia vykonaná s digitálnou stopou						
18. 4. 2026 09:28 UTC	Vytvorenie obrazu interného úložiska (.E01) na forenzný HDD #1 a #2						
18. 4. 2026 12:00 UTC	Analýza RAM obrazu v HxD 2.5 – extrakcia 3 artefaktov (GPS, HRV, Wi-Fi profil)						
18. 4. 2026 14:30 UTC	Analýza FIT súboru v Belkasoft RAM Analyzer – potvrdenie sleep-detection 16:07						

Číslo:	004	Typ súboru:	Video .mp4	Obnovený súbor:	Nie	Veľkosť:	2,1 GB
Popis prípadu:		Krádež batohu vo vlaku Os 3412 na trati Trnava–Kúty dňa 17. 4. 2026. Vyšetrovanie krádeže.					
Názov súboru:		kutynastupistyplatform2_20260417.mp4					
Miesto získania digitálnej stopy:		Nástupište č. 2, železničná stanica Kúty. Kamera Hikvision DS-2CD2143G2-I (externá, správa ŽSR)					
Poznámky:		Záznam pokrýva úsek 16:00–18:00. Rozlíšenie 4 MP (2688×1520 px), 25 fps, formát H.264. Odovzdaný na USB kľúči, ktorý bol ihneď vložený do antistatického vrečka, plomba č. F-004.					
Časové pečiatky							
Access:	18. 4. 2026 07:45 UTC		17. 4. 2026 18:00 UTC	18. 4. 2026 07:45 UTC		Change:	
Digitáln y odtlačok (heš)	MD5	3c7a9f2e1b4d8c0e5f7a3b6d9e1f2c4a					
	SHA1	b4e8f2a7c1d3e9f0a5c8b2d4e7f1c3b6a9e2d5f8					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
18. 4. 2026 07:55 UTC		Záloha na forenzný HDD #2, overenie hash hodnôt					
18. 4. 2026 11:30 UTC		Extrakcia kľúčových snímkov (FFmpeg) – 5 snímkov uložených ako .png dôkazy					

8.3 Fyzická ochrana

- Faradayovo vrečko: každé zaistené elektronické zariadenie bolo ihneď vložené do certifikovaného Faradayovho vrečka (Privacy Shield PS-XFAR-LG) pre elimináciu vzdialených príkazov/resetov.
- Odolné puzdro: zariadenia uložené v nárazuvzdorných, vodonepriepustných puzdách Pelican 1510 s hygrometerom pre kontrolu vlhkosti.
- Plomby: každý obal zaistený numerovanou tamper-evident plombou; čísla zaznamenané v protokole.
- Trezor: forenzné HDD so zálohovacími kópiami uložené v certifikovanom trezorovom priestore OR PZ Trnava (prístup iba pre menovaných analytikov).
- Protokol prístupu: akýkoľvek prístup k zariadeniam alebo obrazom musí byť zaznamenaný v evidenčnom protokole s dátumom, menom a účelom.

9. Záver

9.1 Výsledky vyšetrovania

Digitálna forenzná analýza prípadu DFA-2026-001 jednoznačne preukázala, že k odcudzeniu batohu Jane Kováčovej došlo dňa 17. apríla 2026 o 16:12–16:14 na vlaku Os 3412, na úseku medzi zastávkami Štefanov nad Oravou a Kúty. Všetky štyri forenzné hypotézy boli overené – dve potvrdené, dve čiastočne potvrdené.

Profil páchatel'a: Mužská osoba, cca 175 cm, tmavé vlasy, oblečená v tmavej bunde. Vlastnil smartphone Samsung (MAC 3C:2E:F9:A1:7B:4D, registrovaný ako samsung_j71@vlaknet). Nastúpil do vlaku najneskôr o 15:47 (čas Wi-Fi pripojenia) a vystúpil v Kútoch o 16:59. Využil skutočnosť, že obeť zaspala (potvrdené biosenzormi hodínok), čo svedčí o cieľavedomom konaní.

Identita páchatel'a nebola v rámci tohto forenzného projektu definitívne ustálená – ďalšie kroky zahŕňajú preverenie registrácie captive portál účtu samsung_j71@vlaknet a biometrickú analýzu CCTV záberov s databázou evidenčných fotografií.

9.2 Ďalšie odporúčané kroky

- Požiadat' MVSR o preverenie registračných údajov Wi-Fi účtu samsung_j71@vlaknet a SIM karty spojenej so zariadením.
- Iniciovať biometrickú analýzu CCTV záberov (tvár, chôdza) voči databázam PZ SR.
- Preverenie záznamu o predaji lístkov na trasu Trnava–Kúty v čase kúpy, korelácia s platobnou kartou.
- Zahrnúť simulovanú KML GPS trasu do korelačnej analýzy s kamerovými zábermi z mesta Kúty.

9.3 Odporúčania pre vlakového dopravcu (ŽSR / ZSSK)

- Aktualizovať retenčnú politiku Wi-Fi logov na minimálne 30 dní (aktuálne 7 dní); záznamy musia zahŕňať celé MAC adresy, nie len prefixové OUI.
- Zvýšiť hustotu CCTV kamier v miestach výstupu (dvere) s rozlíšením aspoň 4K pre biometrickú použiteľnosť.
- Implementovať šifrovanú autentifikáciu Wi-Fi (WPA2-Enterprise s certifikátmi) namiesto captive portálu, čo uľahčí spoľahlivejšiu identifikáciu užívateľov.
- Zaviesť pravidelné forenzné audity CCTV systémov a zálohovania logov podľa ARNES 2017 metodiky.
- Školiť sprievodcov v základoch digitálneho zaistenia dôkazov (nemanipulovanie so zariadeniami pred príchodom forenzného tímu).

9.4 Hypotézy potvrdené/vyvrátené

Hypotéza	Popis	Dôkaz pro	Dôkaz proti	Stav
Páchateľ vystúpil na prvej zastávke po krádeži	Páchateľ zobral batoh a v momente ako sa naskytla príležitosť sa rozhodol vystúpiť z vlaku	Bezpečnostný systém potvrdil výstup z vlaku takmer okamžite po krádeži, odpojenie telefónu z vlakovej siete tomu taktiež naznačuje	/	Potvrdená
Ku krádeži nedošlo a obeť si to vymyslela	Vždy je možné že obeť si to celé len vymyslela	/	Bezpečnostný systém toto priamo vyvrátil	Vyvrátená
Obeť v čase krádeže spala a nevšimla si že bola okradnutá	Obeť mohla v čase krádeže spať a nevšimla si že ju niekto chce okradnúť.	FIT záznam zo smart hodínok podporuje túto skutočnosť, bezpečnostný záznam toto rovnako podporuje	/	Čiastočne potvrdená, je možné že bola len príliš rozptúlená
Obeť zabudla kde sedí a jej veci ostali na jej originálnom mieste	Obeť mohla zabudnúť svoje miesto vo vlaku a nevšimnúť si svoje veci.	/	Bezpečnostný systém toto priamo vyvrátil pretože bola zaznamenaná bez pohybu na svojom mieste, smart hodinky naznačujú nečinnosť	Vyvrátená

10. Literatúra a zdroje

1. ARNES (2017). Metodika digitalne forenzne analize. SI-CERT / Akademska in raziskovalna mreza Slovenije.
2. Karie, N. M., & Venter, H. S. (2015). Toward a general ontology for digital forensic disciplines. *Journal of Digital Forensics, Security and Law*, 10(4), 91-115. [DFRWS 2015]
3. Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd ed.). Academic Press.
4. Garmin Ltd. (2023). *Forerunner 245 Music Owner's Manual & FIT Protocol SDK Documentation*. Olathe, Kansas: Garmin International.
5. Exterro (2024). *FTK Imager User Guide v4.7*. Portland: Exterro Inc.
6. Hikvision (2023). *DS-2CD2143G2-I Quick Start Guide & NVR iVMS-4200 User Manual*. Hangzhou: Hikvision Digital Technology.
7. Simulované datasety: Generované Claude (Sonnet 4.6) pre potreby semestrálneho projektu DFA. Všetky dáta sú fiktívne a slúžia výlučne na vzdelávacie účely.