

UNIVERZITA SV. CYRILA A METODA V TRNAVE
FAKULTA PRÍRODNÝCH VIED

Nájdienie vraha na Instagrame

Semestrálna práca

[prezentácia](#)

2025/2026

Roberta Šelestiaková

Obsah

Prípad	3
Metodika 5WH	3
Literatúra – odborné príspevky	3
Hypotézy + ich digitálne stopy a zariadenia, nástroj overenia a postup.....	4
Digitálne zariadenia	7
Digitálne stopy - dáta.....	9
RAM	11
Image Zariadení	11
Nástroje SW ktoré boli použité a na aký účel.....	17
Bezpečnostné opatrenia.....	17
Datasety.....	19

Prípad

Zhrnutie:

Komunita používateľov sociálnej siete Instagram nahlásila polícií podozrivý účet, ktorý zverejšťoval nepríjemné príspevky s fotografiami násilia a ľudskými pozostatkami.

Polícia po prevzatí prípadu začala vyšetrovanie. Predbežné analýzy potvrdili že fotografie na profile zobrazovali skutočné obete. Vyšetrovanie sa zameriava na identifikáciu páchatel'a prostredníctvom digitálnych stôp, najmä lokalizačných údajov a metadát.

Digitálna forenzná analýza však preukázala, že podozrivý sa nenachádzal na miestach činov a fotografie nevytvoril. Výsledkom vyšetrovania bolo zistenie, že osoba nebola páchatel'om násilia, ale iba šířila už existujúci nevhodný obsah na sociálnej sieti.

Metodika 5WH

WHO (kto) ?

- Majiteľ účtu, osoba s cieľom zmiast', neznámy páchatel'.

WHAT (čo) ?

- Zverejšťoval nepríjemné fotografie ukazujúc násilné činy.

WHEN (kedy) ?

- V čase publikovania príspevkov na profile (časové údaje získané z metadát).

WHERE (kde) ?

- Online prostredie sociálnej siete Instagram.

WHY (prečo) ?

- Možný psychologický motív ako je potreba pozornosti, zastrašovanie, manipulácia verejnosti alebo snaha o medializáciu.

HOW (ako)

- Zverejšťovanie už existujúcich fotografií získaných z externých zdrojov alebo vlastne vytvorené pomocou mobilného zariadenia.

Literatúra – odborné príspevky

<https://www.arcjournals.org/pdfs/ajfs/v9-i1/5.pdf>

PDF dokument v ktorom je prehľad techník, metód získavania, uchovávaní digitálnych dôkazov ideálne cez Instagram.

<https://www.sciencedirect.com/science/article/pii/S1742287612000321>

Práca o forenznej analýze sociálnych aplikácií na telefónoch vrátane prístupu k používateľským dátam.

Hypotézy + ich digitálne stopy a zariadenia, nástroj overenia a postup

Hypotéza 1

- Majiteľ Instagram účtu je priamym páchatelom vražd a úmyselne zverejšňoval fotografie ako formu prezentácie alebo výsmechu.

Digitálne stopy a zariadenia :

- Mobilný telefón podozrivého, notebook podozrivého, metadáta fotografií (GPS súradnice, čas vytvorenia, zariadenie), logy prihlásenia (IP adresy, čas, údaje), história komunikácie (správy, komentáre), záznamy o pripojení (Wi-fi alebo mobilné dáta).

Nástroje použité na overenie :

- MAGNET RAM Capture, FTK Imager, HxD, Volatility, Autopsy.

Postup overenia :

- Vytvorenie forenznej kópie zariadení, výpočet hash hodnôt zariadení, extrakcia fotografií a analýza metadát (GPS súradnice, čas), porovnanie GPS údajov s miestami incidentov, analýza údajov od mobilného operátora (poloha zariadenia, pripájanie k internetu), skúmanie súvislostí času vytvorenia a publikovania príspevkov, analýza prihlasovacích IP adries, kontrola komunikácie.

Výsledok : zamietnutá, lokalizačné údaje zariadenia potvrdili, že podozrivý sa v čase vzniku fotografií nenachádzal na mieste činov. Analýza metadát a forezných kópií nepreukázala, že by fotografie boli vytvorené jeho zariadeniami, ale pochádzali z externých zdrojov. Neboli zistené ani žiadne dôkazy v komunikácií či logoch, ktoré by ho spájali s páchaním vražd.

Hypotéza 2

- Majiteľ účtu iba prezdieľal fotografie bez priamej účasti na násilných činoch.

Digitálne stopy a zariadenia :

- Mobilný telefón podozrivého a notebook podozrivého, metadáta fotografií (GPS, čas, zariadenie), história prehliadania a sťahovanie obsahu, logy prihlasovania (čas, údaje) ,IP adresy, záznamy o pripojení.

Nástroje použité na overenie :

- MAGNET RAM Capture, FTK Imager, HxD, Volatility, Autopsy.

Postup overenia :

- Vytvorenie forenznnej kópie zariadení, extrakcia a analýza metadát fotografií, výpočet hash hodnôt zariadení, vyhľadávanie pôvodu obrázkov, kontrola histórie prehliadania, porovnávanie času publikovania s časom vykonania činov spolu s GPS, analýza komunikácie, analýza prihlasovacích IP adries a údajov, analýza údajov od operátora (poloha zariadenia, pripájanie k internetu).

Výsledok : potvrdená, fotografie neboli vytvorené zariadeniami podozrivého, ale pochádzali z externých zdrojov (sťahovanie z internetu). História prehliadania a sieťové artefakty potvrdili ich vyhľadávanie a sťahovanie, pričom časové údaje nezodpovedali času spáchania činov. Lokalizačné dáta zároveň vylúčili prítomnosť podozrivého na miestach incidentov, čím sa potvrdilo, že obsah iba prezdieľal bez priamej účasti na násilí.

Hypotéza 3

- Účet bol vytvorený inou osobou a s cieľom zmiast' vyšetrovanie.

Digitálne stopy a zariadenia :

- Mobilný telefón podozrivého, notebook podozrivého, metadáta (GPS, čas, zariadenie), IP adresy pri registrácii a prihlasovaní do účtu, e-mail použitý pri registrácii, logy, VPN alebo anonymizačné služby.

Nástroje použité na overenie :

- MAGNET RAM Capture, FTK Imager, HxD, Volatility, Autopsy.

Postup overenia:

- Vytvorenie forenznnej kópie zariadení, výpočet hash hodnôt zariadení, extrakcia a analýza metadát fotografií, Analýza IP adries, overenie použitia VPN alebo proxy, porovnanie zariadení použitých na prístup, porovnávanie času publikovania s časom vykonania činov spolu s GPS, analýza komunikácie, analýza údajov od operátora (poloha zariadenia, pripájanie k internetu).

Výsledok : zamietnutá, forenzná analýza zariadení, IP adries a prihlasovacích logov nepreukázala prístup inej osoby k účtu ani vytvorenie účtu z cudzieho zariadenia. Všetky aktivity boli konzistentne spojené s jedným používateľom, bez stôp zdieľania prístupu alebo použitia externého zariadenia.

Hypotéza 4

- Páchateľ využil cudzie zariadenie na zakrytie svojej identity.

Digitálne stopy a zariadenia :

- Mobilný telefón podozrivého, notebook podozrivého, metadáta fotografií (GPS súradnice, čas vytvorenia, zariadenie), logy prihlásenia (IP adresy, čas, údaje), história komunikácie (správy, komentáre), záznamy o pripojení (Wi-fi alebo mobilné dáta).

Nástroje použité na overenie :

- MAGNET RAM Capture, FTK Imager, HxD, Volatility, Autopsy.

Postup overenia :

- Vytvorenie forenznej kópie zariadení, výpočet hash hodnôt zariadení, extrakcia fotografií a analýza metadát (GPS súradnice, čas), porovnanie GPS údajov s miestami incidentov, analýza údajov od mobilného operátora (poloha zariadenia, pripájanie k internetu), skúmanie súvislostí času vytvorenia a publikovania príspevkov, analýza prihlasovacích IP adries, kontrola komunikácie, analýza používateľských účtov v zariadení, identifikácia časov, súvislosti s pohybom a majiteľa zariadenia,

Výsledok : zamietnutá, prihlasovacie logy a IP adresy preukázali konzistentné používanie jedného zariadenia bez známk cudzieho prístupu. Forezná analýza neodhalila žiadne stopy naznačujúce využitie iného zariadenia, jedine notebooku kde uchovával fotografie.

Digitálne zariadenia

V rámci vyšetrovania budú analyzované tieto zariadenia:

Mobilný telefón podozrivej osoby :

Poco X3 6GB/128GB

Parametre :

- Operačný systém a verzia : Android 10
- Možnosť pamäťovej karty
- Nadstavba systému MIUI
- Veľkosť displeja 6.67"
- Rozlíšenie displeja 2400x1080
- Pomer strán displeja 20:9
- Výška 165.3 mm
- Šírka 76.8 mm
- Hrúbka 9.4 mm
- Rozlíšenie fotoaparátu 64 Mpix
- Počet objektívov zadného fotoaparátu 4
- Počet objektívov predného fotoaparátu 1
- Dual SIM
- Kapacita batérie 5160 mAh
- Frekvencia procesoru 2.3 GHz
- Počet jadier procesora 8
- Užívateľská pamäť 128 GB
- Operačná pamäť RAM 6GB
- WIFI
- LTE
- NFC
- GPS modul

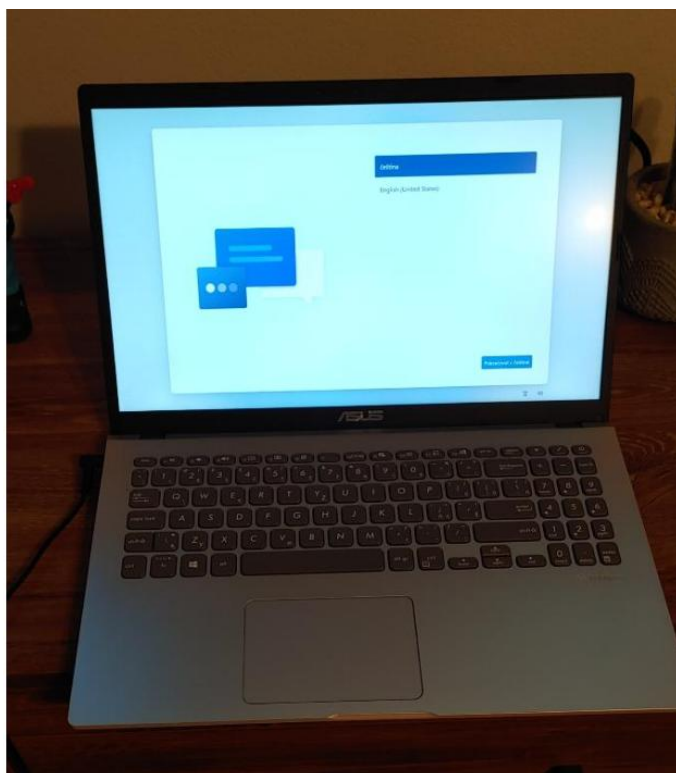


Notebook podozrivej osoby :

ASUS Vivobook 15 OLED M1505YA-OLED389W

Parametre :

- SSD kapacita 1 000 GB
- Typ pamäte DDR4
- Frekvencia pamäte 3 200 MHz
- Veľkosť operačnej pamäte RAM 16 GB
- Modelové označenie procesora AMD Ryzen 7 7730U
- Počet jadier procesora 8
- Frekvencia procesora 2 GHz
- Core Boost frekvencia 4.5 GHz
- Cache procesora 20 MB
- Generácia procesora Zen 3 (5. generácia)
- Frekvencia procesora 2GHz
- Obnovovacia frekvencia displeja 60 Hz
- Uhlopriečka displeja 15.6“
- Pomer strán 16:9
- Rad grafickej karty AMD Radeon
- Operačný systém Windows 11 Home
- Hmotnosť 1.7 kg
- Šírka 356.8 mm
- Výška 19.9 mm
- Hĺbka 227.6 mm
- Rad notebooku Asus VivoBook
- Certifikácia MIL-STD-810H



SIM karta a údaje od mobilného operátora

Parametre :

- IMSI unikátne číslo SIM karty v sieti
- ICCID sériové číslo SIM fyzické
- MSISDN telefónne číslo
- KI tajný kľúč na autentifikáciu
- Aktivita, poloha, komunikácia

Digitálne stopy - dáta

Vyšetovanie sa zameriava na nasledujúce digitálne stopy :

Mobilný telefón podozrivej osoby

Zariadenie: Poco X3 6GB/128GB

Operačný systém: Android 10 (MIUI nadstavba)

Užívateľská pamäť : 128 GB

RAM: 6GB

Výbava: GPS, Wi-Fi, LTE, NFC, Dual SIM, 64 Mpix fotoaparát

Informácie o dátach:

Mobilné zariadenie obsahovalo systémové aj používateľské dáta operačného systému Android, Systémové súbory (APK, DEX, XML, LOG) súvisia s fungovaním aplikácií a systému. Používateľské dáta zahŕňali fotografie, videá, dokumenty a dáta aplikácií sociálnych sietí.

Najdôležitejšie pre forenznú analýzu:

- Fotografie a ich metadáta EXIF údaje, čas vytvorenia, GPS súradnice)
- Logy komunikácie a prihlásení
- Údaje o pripojení k internetu (Wi-Fi, mobilné dáta)

Tieto údaje umožnili rekonštrukciu aktivity používateľa na platforme Instagram a analýzu spôsobu zverejňovania obsahu.

Notebook podozrivej osoby

Zariadenie: ASUS Vivobook 15 OLED M1505YA-OLED389W

Operačný systém: Windows 11 Home

RAM: 16 GB DDR4

SSD: 1TB

Processor: AMD Ryzen 7 7730U (8 jadier)

Informácie o dátach:

Notebook obsahoval systémové súbory Windows a používateľské dáta vrátane dokumentov, archívov, logov a internetovej aktivity. Dôležitú časť tvorili súbory prehliadača, ktoré mohli obsahovať históriu vyhľadávania a stiahnuté dáta.

Najdôležitejšie pre forenznú analýzu:

- História prehliadania a cache prehliadača
- Logy systému a prihlásení
- Stiahnuté súbory a ich metadáta
- Sieťové záznamy komunikácie

Tieto údaje boli využité na overenie pôvodu obrazového materiálu a analýzu online aktivity používateľa.

SIM karta z telefónu podozrivej osoby

Identifikátory SIM karty:

- IMSI (identifikátor účastníka v sieti)
- ICCID (sériové číslo SIM karty)
- MSISDN (telefónne číslo)
- KI (autentifikačný kľúč)

Informácie o dátach:

Údaje od mobilného operátora obsahovali záznamy o polohe zariadenia, časoch pripojenia do siete a komunikácií. Tieto dáta umožnili časovo-priestorovú rekonštrukciu pohybu zariadenia.

Najdôležitejšie pre forenznú analýzu:

- Lokalizačné údaje
- Časové záznamy pripojenia
- IP komunikácia sieťová aktivita

Tieto informácie boli použité na porovnanie s metadátami fotografií a overenie, či sa zariadenie nachádzalo na miestach incidentov.

RAM

Analýza RAM pamäte v tomto prípade nepriniesla žiadne značné dôkazy, preto sú tu len 3 ukážky ktoré mohli súvisieť s prípadom.

Na zariadení notebooku bolo v obraze RAM pamäte vidieť že používateľ navštívil Instagram cez internetový prehliadač.

```
001B21620 02 00 00 00 03 00 FF FF 11 00 00 80 04 00 FF FF .....€...
001B21630 77 77 77 2E 69 6E 73 74 61 67 72 61 6E 2E 63 6F www.instagram.co
001B21640 6D 00 00 00 00 00 00 00 03 00 00 00 03 00 FF FF m.....
```

Podozrivá osoba mohla skúšať aké záznamy sa dokážu nájsť cez obraz RAM pamäte.

```
0 01 1a 14 33 45 42 30 42 42 39 37 31 39 44 45 ....3EB0BB9719DE
1 45 42 31 46 46 35 31 12 1c 0a 1a 48 69 2e 20 1EB1FF51....Hi.
9 20 61 6d 20 74 65 73 74 69 6e 67 20 73 6f 6d I am testing som
5 74 68 69 6e 67 18 95 ce 83 f7 05 20 01 06 75 ething..i+. ..u
```

IP adresy pripojenia

```
00001400 6C 69 62 67 63 6A 2D 31 36 2E 64 6C 6C 00 5F 4A libgcj-16.dll._J
00001410 76 5F 52 65 67 69 73 74 65 72 43 6C 61 73 73 65 v_RegisterClasse
00001420 73 00 00 00 31 39 32 2E 31 36 38 2E 30 2E 31 30 s...192.168.0.10
00001430 31 00 00 00 D0 13 40 00 4D 69 6E 67 77 20 72 75 l...D.@.Mingw ru
00001440 5F 74 69 6D 5E 20 5E 61 69 6C 7E 73 6E 38 03 00 nima failura.
```

Image Zariadení

Pre prácu v digitálnom forenznom analyzovaní sa vytvoril forenzný obraz (image) zariadenia USB ktoré slúži len ako spôsob na ukladanie dôkazov dodaný vyšetrovacím tímom. Na USB kľúči sa nachádzali dôkazy z týchto zariadení :

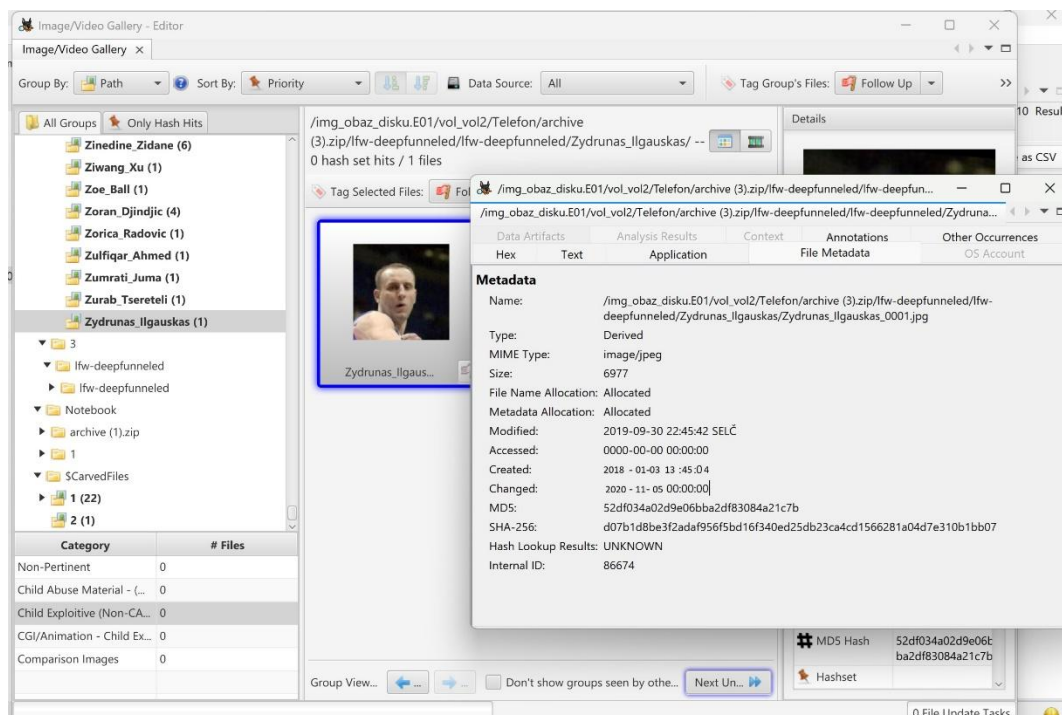
- Mobilný telefón podozrivej osoby (Poco X3 6GB/128GB)
- Notebook podozrivej osoby (ASUS Vivobook 15 OLED)
- SIM karta a údaje od mobilného operátora

Tento obraz bol vytvorený pomocou nástroja FTK Imager s dôrazom na zachovanie integrity dát a elimináciu zásahu do originálnych zariadení. Následná analýza prebiehala s využitím nástrojov: MAGNET RAM Capture, HxD, Volatility, Autopsy.

Dôkaz č. 1 : Pôvod obrazového materiálu

V dátach z notebooku boli nájdené obrazové súbory zhodné s obsahom publikovaným na Instagram účte. Detailná analýza metadát (EXIF) ukázala, že tieto súbory neboli vytvorené zariadením podozrivého ale pochádzali z rôznych iných zariadení a lokalít. Niektoré súbory mali odstránené alebo upravené metadáta, čo naznačuje že už predtým prešli ďalším spracovaním alebo zdieľaním.

Tento dôkaz naznačuje, že podozrivý nebol autorom fotografií, ale ich získal z iných zdrojov. Podporuje hypotézu č. 2 a zároveň spochybňuje hypotézu č. 1.

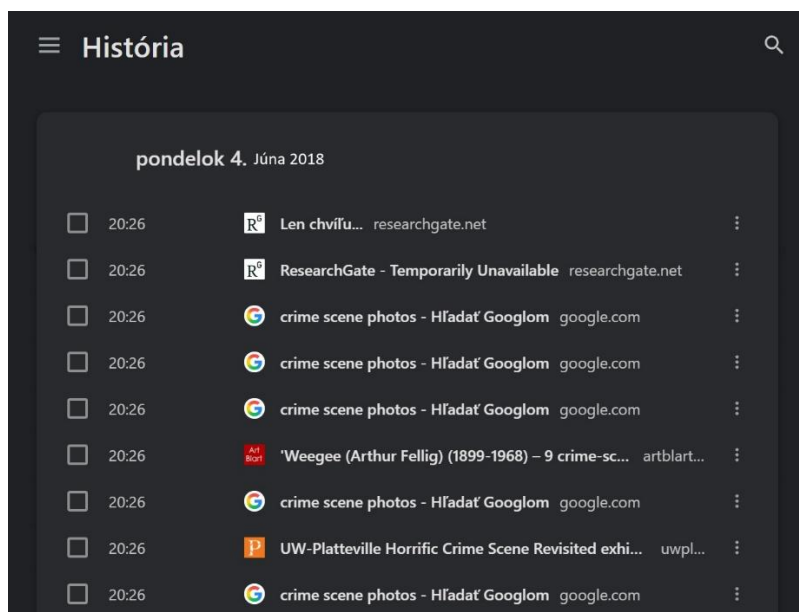


Fotografia so zmenou v metadátach.

Dôkaz č 2. Internetová aktivita a získavanie obsahu

Z analýzy histórie prehliadania vyplynulo, že páchateľ navštevoval stránky obsahujúce násilný vizuálny materiál. V cache a medzi stiahnutými súbormi sa nachádzali obrázky identické alebo veľmi podobné tým ktoré boli neskôr zverejnené na jeho profile. Časové údaje naznačujú, že k ich stiahnutiu došlo ešte pred samotným publikovaním.

Tento dôkaz priamo poukazuje na to, že obsah bol najskôr vyhľadaný a uložený a až potom zverejnený, výrazne to potvrdzuje hypotézu č. 2.



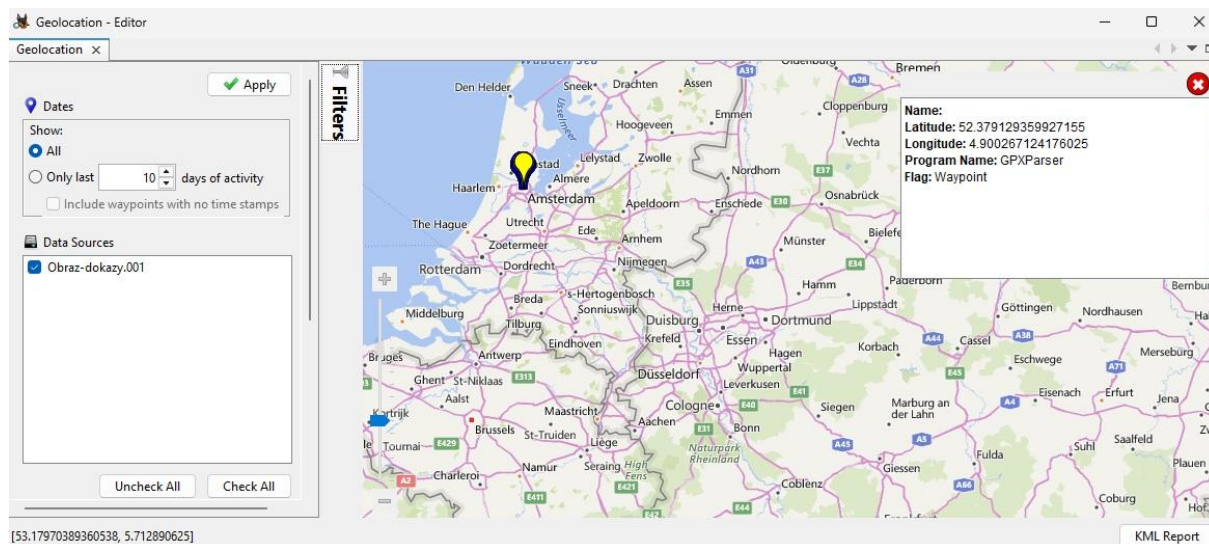
História prehliadania podozrivej osoby

Dôkaz č. 3 Porovnanie lokalizačných údajov

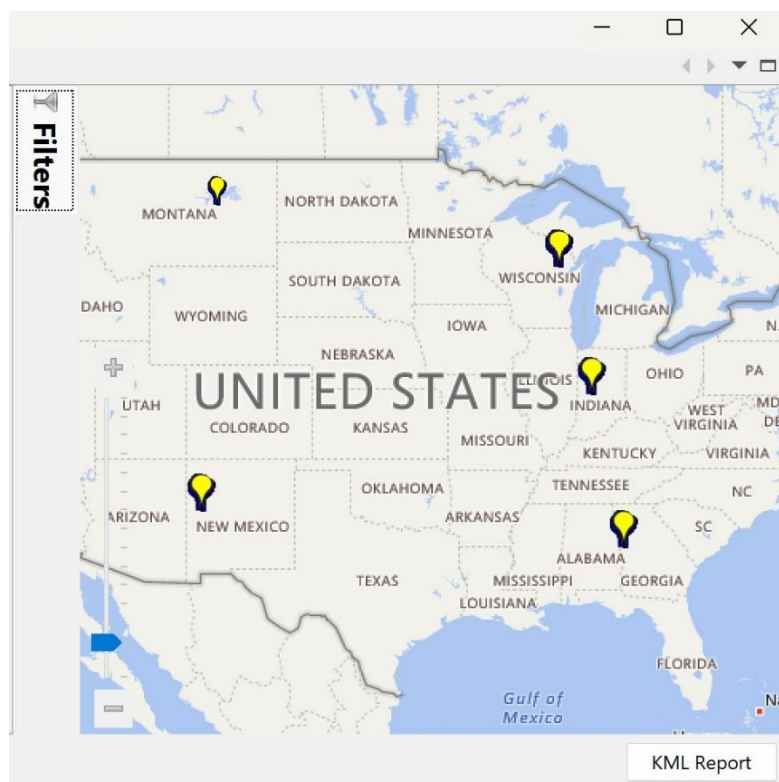
Porovnaním metadát fotografií s lokalizačnými údajmi zo SIM karty a mobilného zariadenia bolo zistené, že poloha podozrivého sa nezhodovala s miestami, kde mali fotografie vzniknúť.

Záznamy od operátora s GPS údajmi konzistentne potvrdzovali inú polohu zariadenia v danom čase.

Tento dôkaz vylučuje fyzickú účasť podozrivého na miestach incidentov, vylučuje hypotézu č. 1 a podporuje hypotézu č. 2



Geo lokácia telefónu a notebooku podozrivej osoby.

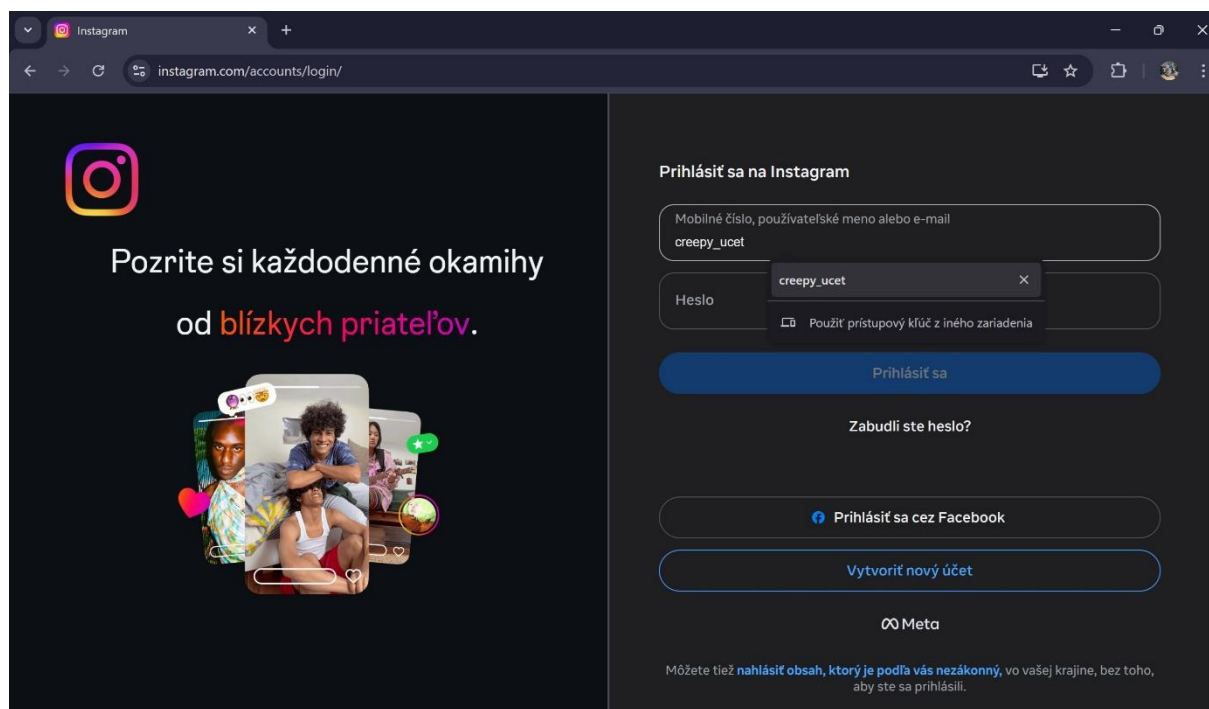


Geo lokácie fotografií z profilu a uložených na notebooku

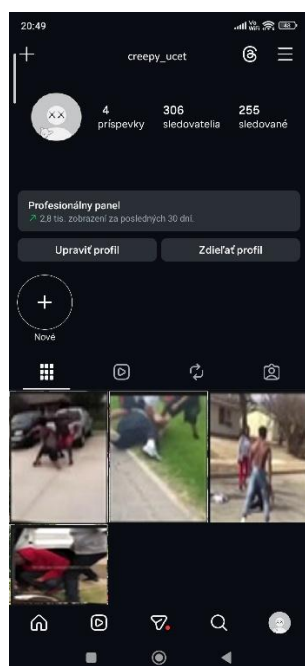
Dôkaz č. 4 Analýza prístupov k účtu

Preskúmanie prihlasovacích logov a IP adries ukázalo, že účet bol používaný z konzistentného prostredia, bez známkov prístupu tretích strán. Neboli identifikované žiadne dôkazy o použití anonymizačných nástrojov, ako sú VPN alebo proxy služby.

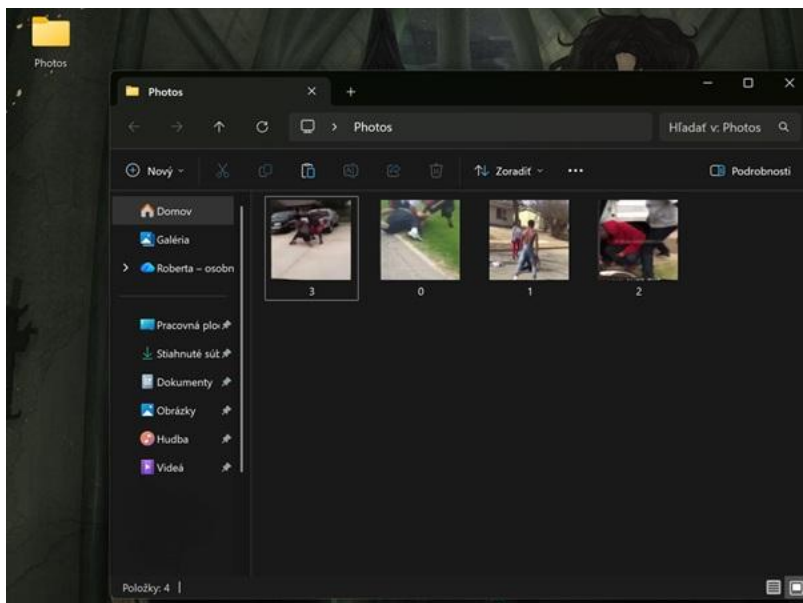
Tento dôkaz naznačuje, že účet nebol zneužitý inou osobou, vyvracia hypotézy č. 3 a č. 4.



Na obrázku je vidieť že prehliadač používateľa na jeho notebooku má zapamätané jeho prihlasovacie meno čo sa zhoduje s menom Instagram účtu používaným na publikáciu fotografií v jeho telefóne.



Prihlásený účet Instagramu na telefónnom zariadení podozrivého.



Fotografie uložené na notebooku ktoré sa zhodujú s tými čo sú zverejnené na účte, stiahnuté zo stránok pri dôkazovom materiáli ukázanom v dôkazy č. 2.

Dôkaz č. 5 Aktivita v mobilnej aplikácii a prehliadači

V mobilnom zariadení boli identifikované artefakty aplikácie Instagram, na notebooku zase návštevy web stránky Instagramu vrátane údajov o prihlásení a histórie používania. Tieto dáta potvrdili, že podozrivý aktívne spravoval svoj účet a zverejňoval obsah. Napriek tomu sa v zariadení nenašli originálne fotografie násilného charakteru vytvorené fotoaparátom zariadenia.

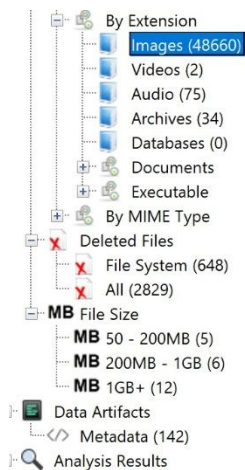
Tento dôkaz potvrdzuje správu účtu podozrivým, no zároveň nepreukazuje jeho účasť na vytváraní obsahu, podporuje hypotézu č. 2

```
001B21620 02 00 00 00 03 00 FF FF 11 00 00 80 04 00 FF FF .....€...
001B21630 77 77 77 2E 69 6E 73 74 61 67 72 61 6D 2E 63 6F www.instagram.co
001B21640 6D 00 00 00 00 00 00 00 03 00 00 00 03 00 FF FF m.....
```

Záznam z RAM pamäte o tom že bol navštevovaný Instagram na internetovom prehliadači.



(3) Instagram znamená že používateľ bol prihlásený na účte.



Name	S	C	O	Modified Time
Abdel_Nasser_Assidi_0001.jpg			2	2019-09-30 23:45:10 SELČ
Abdel_Nasser_Assidi_0002.jpg			2	2019-09-30 23:45:10 SELČ
Abdoulaye_Wade_0001.jpg			2	2019-09-30 23:45:10 SELČ
Abdoulaye_Wade_0002.jpg			2	2019-09-30 23:45:10 SELČ
Abdoulaye_Wade_0003.jpg			2	2019-09-30 23:45:10 SELČ
Abdoulaye_Wade_0004.jpg			2	2019-09-30 23:45:10 SELČ
Abdul_Majeed_Shobokshi_0001.jpg			2	2019-09-30 23:45:10 SELČ
Abdul_Rahman_0001.jpg			2	2019-09-30 23:45:10 SELČ
Abdulaziz_Kamilov_0001.jpg			2	2019-09-30 23:45:10 SELČ
Abdullah_0001.jpg			2	2019-09-30 23:45:10 SELČ
Abdullah_0002.jpg			2	2019-09-30 23:45:10 SELČ
Abdullah_0003.jpg			2	2019-09-30 23:45:10 SELČ
Abdullah_0004.jpg			2	2019-09-30 23:45:10 SELČ
Abdullah_Ahmed_Radwan_0001.jpg			2	2019-09-30 23:45:10 SELČ

Zoznam fotografií v telefóne a notebooku, niektoré boli len uložené na zariadeniach, niektoré aj zverejnené.

Nástroje SW ktoré boli použité a na aký účel

- MAGNET RAM Capture (zachytenie obsahu operačnej pamäte RAM)
- FTK Imager (vytvára kópie diskov)
- HxD (hexadecimálny editor na priamu prácu so súbormi a diskovými obrazmi)
- Volatility (framework na analýzu zachytenej RAM pamäte)
- Autopsy (softvér na analýzu diskov a súborových systémov)

Bezpečnostné opatrenia

Bitové kópie zariadení : Zo zaistených zariadení boli všetky dôkazy premiestnené na USB kľúč, z ktorého za vytvorila bitová kópia.

Vytvorené bitové kópie :

- RAM pamäť telefónneho zariadenia a notebooku.
- Forenzné obrazy telefónu, SIM karty a notebooku

Boli vytvorené 2 kópie jedna ako záložná a druhá s ktorou sa pracovalo na analýze.

Hash hodnoty :

Pre zabezpečenie integrity dát boli vypočítané hash hodnoty MD5 a SHA1 z USB na ktorom sa nachádzali dôkazy, hodnoty :

MD5 : ee9adebe55877407920ea6e27b5e0b0c

SHA1 : db2f221464b5ae9a40179d86c0215ae839ad0078

Fyzická ochrana :

Zaistené zariadenia (mobil, notebook, SIM karta) boli uložené v antistatických obaloch. Následne boli umiestnené v uzamknutej miestnosti. Prístup k nim mal iba oprávnený vyšetrovateľ, ktorý všetky dôkazy prekopíroval na pripravené USB.

Analýza prebiehala výlučne z kópií dát.

Každá manipulácia bola zaznamenaná v Chain of Custody

Chain of custody :

Číslo:	01	Typ súboru:	E01	Obnovený súbor:	-	Veľkosť:	6,74GB
Popis prípadu:		Účet na Instagrame s podozrivou aktivitou.					
Názov súboru:		TOSHIBA TransMemory USB Device					
Miesto získania digitálnej stopy:		Dom podozrivého v Amsterdame					
Poznámky:		SIM, notebook, telefón					
Časové pečiatky							
Access:	25-7-2023		Modify:	-		Change:	-
Digitáln y odtlačok (heš)	MD5	ee9adebe55877407920ea6e27b5e0b0c					
	SHA1	db2f221464b5ae9a40179d86c0215ae839ad0078					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
25-7-2023 --14-20-27--		Zaistenie telefónu					
25-7-2023 --15-26-03--		Zaistenie notebooku					
26-7-2023 --08-10-00--		Vytvorenie bitovej kópie, odovzdanie digitálneho obrazu forenzným analytikom.					
26-7-2023 --11-17-56--		Analýza obsahu					

Dataseťy

Dataseť obsahujúci kybernetické anomálie s časovou informáciou, user_ID, IP adresy, typ aktivity napr. login, modifikáciu súboru vzdialené prihlásenie. 853.7 kB, súbor Microsoft Excelu

<https://www.kaggle.com/datasets/jimohyusuf/cybercrime-forensic-dataset>

Dataseť obsahujúci fotografie násilných činov. 237.79 MB, súbor jpg forografií

<https://www.kaggle.com/datasets/abdulmananraja/real-life-violence-situations>

Dataseť obashujúci zločiny, dátumy k daným zločinom, geografické miesto, klasifikáciu zločinu, použitú zbraň. 246.44 MB, súbor Microsoft Excelu

<https://www.kaggle.com/datasets/saurabhbadole/crime-incidents-in-los-angeles-2020-to-present>

Dataseť s metadáťami ľudských fotografií 117.15 MB, súbor Microsoft Excelu a jpg fotografie

<https://www.kaggle.com/datasets/jessicali9530/lfw-dataset>

Dataseť s históriou aktivity v telefóne. 203.12 kB, súbor KML

<https://www.kaggle.com/datasets/atharvaarya25/phone-usage-dataset>

Dataseťy s geolokačnými údajmi. 26.11 MB a 39.65 kB, súbor GPX

<https://www.kaggle.com/datasets/shaivyac/gps-iot-data-for-data-visualization/data>

<https://www.kaggle.com/datasets/thomasnibb/criminal-location-tracking>