

UNIVERZITA SV. CYRILA A METODA V TRNAVE

FAKULTA PRÍRODNÍCH VIED

Ústav počítačových technológií a informatiky

NEZVESTNÁ OSOBA

Semestrálna práca

prezentácia

Ročník: 2

Skupina: 06

Trnava 2026

Stanislav Šunderlík

Obsah

Popis prípadu Identifikácia a úvodná analýza incidentu	4
Stručný popis prípadu.....	4
Popis prípadu.....	4
5WH	5
Ciele vyšetrovania	5
Potenciálne digitálne stopy:	6
Literatúra	6
Pracovné hypotézy	8
1. Hypotéza A (Cudzie zavinenie):.....	8
2. Hypotéza B (Inscenované zmiznutie):	8
3. Hypotéza C (Priemyselná špionáž):	8
Zaistene digitálne zariadenia	9
Zoznam dôkazových zariadení:.....	9
Laptop obete	9
Mobil obete	10
USB kľúč.....	11
Špecifikácia dát	12
Objem a zloženie dát	12
Analýza volatílnej pamäte	13
Analýza nevolatílnej pamäte	17
Záver.....	27
Vyhodnotenie hypotéz	27
Hypotéza A: Cudzie zavinenie	27
Hypotéza B: Inscenované zmiznutie	27
Hypotéza C: Priemyselná špionáž.....	28

Použité nástroje	29
Nástroje pre akvizíciu a integritu dát	29
1. FTK Imager:.....	29
2. Magnet RAM Capture:	29
3. Winpmem:.....	29
Nástroje pre hĺbkovú analýzu a verifikáciu.....	29
1. Hex Editor (HxD):	29
2. Visual Studio Code + Hex Editor Plugin:	30
3. Autopsy:.....	30
4. Volatility Workbench.....	30
Bezpečnostné opatrenia a CoC.....	31
Bezpečnostné opatrenia.....	31
Zaistenie volatílnej pamäte (RAM) a prvotná akvizícia	31
Laboratórne spracovanie a tvorba bitových kópií nevolatívnych pamätí.....	31
Analýza na pracovných kópiách	32
Zoznam hashov	32
Laptop (operačná pamäť):	32
Laptop:	32
Mobil:	32
USB:	32
Chain of Custody (CoC).....	33
Laptop (operačná pamäť)	33
Laptop.....	34
Mobil	35
USB	36

Popis prípadu Identifikácia a úvodná analýza incidentu

Stručný popis prípadu

Obeť (Adam K.) bola naposledy videná vo svojom byte, odkiaľ zmizla bez stôp násilného vniknutia. Interiér vykazuje anomálie: rozhádzané dokumenty a pohodené USB médium pod notebookom, čo naznačuje náhlu manipuláciu s dátami. Balkónové dvere do záhrady zostali otvorené pri mrazu. Kľúčovými digitálnymi stopami sú cielene vymazaný archív bezpečnostných kamier a telefón v režime „Lietadlo“. Prítomnosť tretej osoby potvrdzuje nález cudzej stopy a fakt, že digitálne príkazy na mazanie dát prebehli až po predpokladanom zmiznutí obete.

Popis prípadu

Obeť (Adam K.) bola naposledy videná vo večerných hodinách vo svojom byte. Nasledujúci deň sa nedostavil do zamestnania a jeho telefón zostal nedostupný. Prvotná obhliadka bydliska nepreukázala žiadne známky násilného vniknutia cez hlavný vchod a v celom objekte neboli zistené žiadne stopy po fyzickom napadnutí, zápase či inej forme násilia.

Interiér však vykazoval neobvyklé anomálie. Pracovný stôl bol v značnom neporiadku. Rôzne dokumenty a kancelárske papiere boli rozhádzané po celej ploche stola a vo veľkom množstve sa nachádzali aj pohodené na podlahe v okolí stoličky. Na stole sa nachádzal notebook a priamo na zemi pod ním ležalo pohodené neoznačené USB médium, čo naznačuje buď unáhlenú manipuláciu, alebo fyzickú konfrontáciu počas prenosu dát. Balkónové dvere vedúce do záhrady zostali dokorán otvorené, hoci vonkajšia teplota bola pod bodom mrazu. Podozrenie umocňuje fakt, že domáca bezpečnostná kamera nevykazuje v archíve žiadne uložené videá ani fotografie – dáta boli cielene vymazané. Na nočnom stolíku bol nájdený mobilný telefón, ktorý bol manuálne prepnutý do režimu „Lietadlo“.

Podľa predbežnej policajnej správy existuje dôvodné podozrenie na prítomnosť tretej osoby v objekte. Toto podozrenie sa opiera o nález cudzej stopy v blízkosti záhradného vchodu a fakt, že digitálne príkazy na mazanie archívu kamery boli vykonané v čase, kedy už mala byť obeť podľa svedkov nezvestná.

5WH

- **Who (Kto):** Obeť Adam K. a neidentifikovaná osoba.
- **What (Čo):** Nevysvetlené zmiznutie osoby sprevádzané neautorizovaným prístupom k laptopu a IoT zariadeniam.
- **Where (Kde):** Dom obete
- **When (Kedy):** 28.01.2026, časové okno 21:30 – 3:15 nasledujúceho dňa (29.01.2026).
- **Why (Prečo):** Podozrenie na krádež citlivých dát (využitie USB kľúča) alebo plánovaný odchod za asistencie tretej strany.
- **How (Ako):** Fyzický prístup k zariadeniam v objekte, následná exfiltrácia dát a opustenie miesta.

Ciele vyšetrovania

1. **Rekonštrukcia časovej osi:** Stanoviť presný chronologický sled digitálnych a fyzických udalostí v čase incidentu (21:30 – 03:15).
2. **Identifikácia neznámeho subjektu:** Získať informácie o tretej osoby, ktorá sa pripojila do domácej siete.
3. **Analýza integrity dát:** Zistiť, aké súbory boli kopírované na nájdený USB kľúč a či došlo k ich trvalému odstráneniu z laptopu.
4. **Obnova vymazaných záznamov:** Pokúsiť sa o obnovu logov alebo fragmentov obrazových dát z IP kamery.
5. **Určenie smeru pátrania:** Identifikovať poslednú známu polohu a trasu pohybu nezvestného

Potenciálne digitálne stopy:

1. **Súborové artefakty:** Monitoring súborov vytvorených alebo modifikovaných v čase incidentu na notebooku a USB kľúči.
2. **Windows Registry & LNK súbory:** Záznamy o pripojení USB zariadení (USBSTOR) a zoznam naposledy otvorených súborov z externého média.
3. **ShellBags & Event Logs:** Systémové záznamy Windows o manipulácii s adresármi

Literatúra

- <https://dfrws.org/presentation/data-remnants-analysis-of-document-files-in-windows-microsoft-365-as-a-case-study/>
 - Tento vedecký príspevok sa zaoberá analýzou dátových zvyškov (data remnants) po dokumentoch v systéme Windows, konkrétne v prostredí Microsoft 365. Autori predstavujú rámec na identifikáciu stôp po súboroch, ktoré boli úmyselne vymazané alebo prepísané anti-forenznými nástrojmi. Pre náš prípad je táto štúdia kľúčová, pretože umožňuje rekonštruovať históriu manipulácie s dokumentmi na laptopu Adama K. aj v prípade, že útočník (alebo obeť) po skopírovaní dát na USB kľúč pôvodné súbory vymazal. Metodika opísaná v článku pomáha identifikovať „stopy po činnosti používateľa“

- <https://dfrws.org/presentation/windows-memory-forensics-identification-of-malicious-modifications-in-memory-mapped-image-files/>
 - Tento vedecký príspevok sa zameriava na pokročilú forenznú analýzu operačnej pamäte (RAM) so špeciálnym zreteľom na detekciu neoprávnených zmien v súboroch namapovaných v pamäti (ako sú .exe a .dll súbory). Autori predstavujú novú metodiku a nástroj (plugin imgmalfind), ktorý dokáže s presnosťou na jednotlivé bajty identifikovať modifikácie kódu vykonané malvérom alebo útočníkom, ktoré bežné forenzné nástroje často prehliadajú.
- <https://dfrws.org/presentation/a-contemporary-investigation-of-ntfs-file-fragmentation/>
 - Tento vedecký príspevok prináša modernú analýzu fragmentácie súborov v systéme NTFS na základe skúmania reálnych používateľských dát. Autori preukazujú, že veľká časť fragmentovaných súborov nie je v pamäti uložená v správnom poradí (out-of-order fragmentácia), čo zásadne komplikuje ich následnú rekonštrukciu. Pre náš prípad je táto štúdia kľúčová, pretože upozorňuje na limity bežných forenzných nástrojov pri obnove dokumentov a multimédií, ktoré mohli byť z notebooku Adama K. odstránené. Metodika opísaná v článku definuje nové metriky na meranie miery fragmentácie, čo vyšetrovateľom pomáha pochopiť, prečo sa niektoré zmazané dôkazy môžu javiť ako nečitateľné alebo poškodené, a navrhuje cesty k ich úspešnejšej manuálnej rekonštrukcii.

Pracovné hypotézy

1. Hypotéza A (Cudzie zavinenie):

- **Znenie:**
 - Tretia osoba vnikla do objektu cez záhradu s cieľom získať citlivé dáta z laptopu. Obeť bola konfrontovaná a následne z objektu odvedená, pričom útočník sa pokúsil zahľadiť stopy manipuláciou s kamerou a mobilným telefónom.
- **Výsledok:**
 - Zamietnutá

2. Hypotéza B (Inscenované zmiznutie):

- **Znenie:**
 - Obeť (Adam K.) zinscenovala vlastné zmiznutie. Rozhádzaný stôl a otvorené dvere majú slúžiť ako zmätočné stopy. Režim „Lietadlo“ a mazanie kamery vykonal sám, aby sťažil svoje vypátranie.
- **Výsledok:**
 - Potvrdená

3. Hypotéza C (Priemyselná špionáž):

- **Znenie:**
 - Obeť bola cieľom útoku zameraného na konkrétne dáta (USB kľúč). Útočník využil znalosť prostredia a prístupových kódov k domácej sieti, čo vysvetľuje absenciu stôp násilia pri vstupe.
- **Výsledok:**
 - Čiastočne potvrdená (Došlo k úniku citlivých dát, avšak v opačnej réžii)

Zaistene digitálne zariadenia

Zoznam dôkazových zariadení:

1. **Laptop obete**
2. **Mobil obete**
3. **USB kľúč**

Laptop obete

Model	MSI GF63
CPU	Intel Core i5-11400H
Operačná pamäť	8GB DDR4
Grafická karta	NVIDIA GeForce GTX 1650
Kapacita úložiska	500 GB
Operačný systém	Windows 11 home



Obrázok 1: Laptop obete

Mobil obete

Model	Samsung Galaxy S20
CPU	Octa-core (2x2.73 GHz Mongoose M5 & 2x2.50 GHz Cortex-A76 & 4x2.0 GHz Cortex-A55)
Operačná pamäť	8GB
Grafická karta	Mali-G77 MP11
Kapacita úložiska	128 GB
Operačný systém	Android 13



Obrázok 2: Mobil obete

USB ključ

Model	Kingston DataTraveler 3.0 USB
Kapacita úložiska	64 GB



Obrázok 3: USB

Špecifikácia dát

Dáta použité v tejto forenzej analýze vznikli kombináciou manuálnej prípravy, generovania za pomoci umelej inteligencie (AI) a integrácie štandardizovaných forenzných datasetov.

- **Manuálna príprava a AI asistované generovanie:** Kľúčové dôkazové materiály, ako sú zmluvy, interná komunikácia v JSON formáte a konfiguračné skripty, boli navrhnuté a vygenerované za pomoci AI. Tento postup zabezpečil vysokú mieru detailov a presnú logickú nadväznosť medzi motívom a samotným činom páchatel'a.
- **Využitie referenčných datasetov (NIST CFReDS):** Pre simuláciu realistického správania operačného systému a súborových štruktúr boli využité vybrané datasety z portálu CFReDS (Computer Forensic Reference Data Sets), spravovaného inštitútom NIST.
 - <https://cfreds.nist.gov/>

Objem a zloženie dát

Celkový dataset pozostáva zo 700 GB dát, ktoré sú rozdelené nasledovne:

- **Laptop (Operačná pamäť): 8 GB** surových dát (RAM dump).
- **Laptop (Systémový disk): 500 GB** bitová kópia pevného disku.
- **Mobilné zariadenie: 128 GB** bitová kópia vnútornej pamäte.
- **USB médium: 64 GB** bitová kópia externého úložiska.

Analýza volatílnnej pamäte

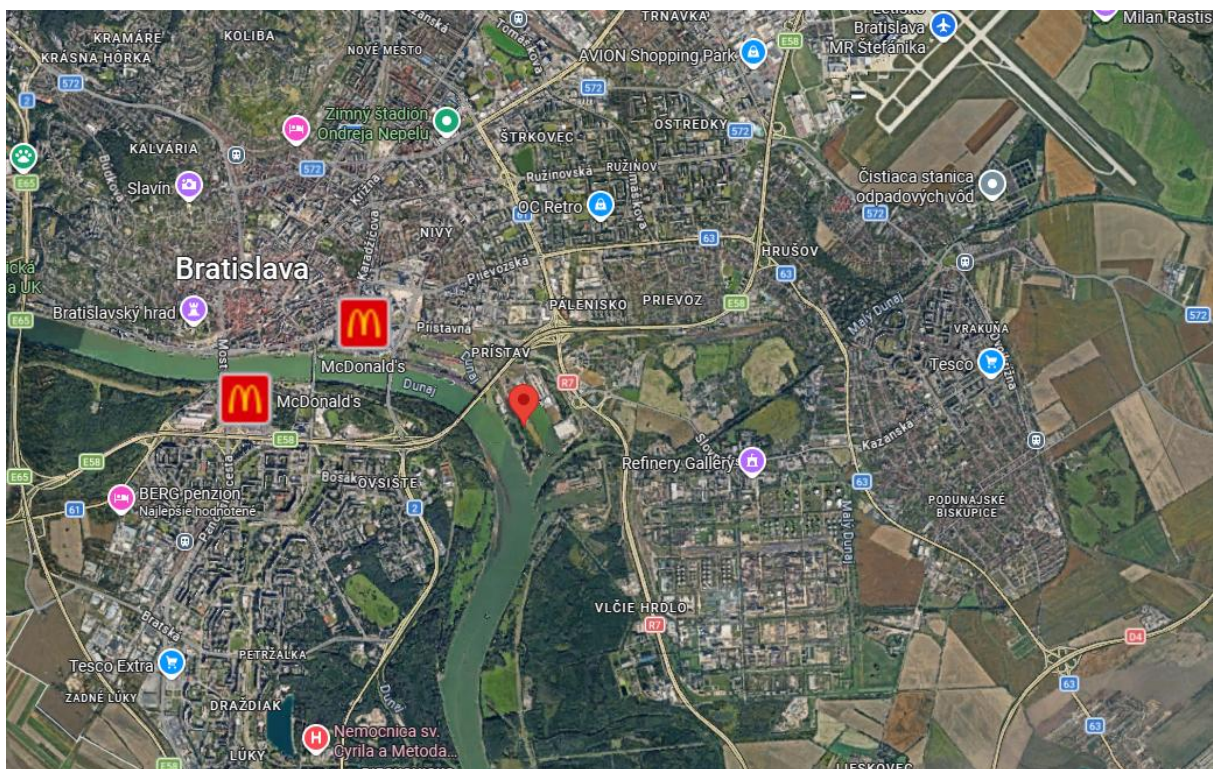
09A3ACC0	82	5B 02 68 74 74 70 73 3A 2F 2F 77 77 77 2E 67	.	[. h t t p s : / / w w w . g
09A3ACD0	6F 6F 67 6C 65 2E 63 6F 6D 2F 6D 61 70 73 2F 70			o o g l e . c o m / m a p s / p
09A3ACE0	6C 61 63 65 2F 34 38 2E 31 33 32 38 2B 31 37 2E			l a c e / 4 8 . 1 3 2 8 + 1 7 .
09A3ACF0	31 34 37 32	2F 40 34 38 2E 33 37 37 35 36 30 31		1 4 7 2 / @ 4 8 . 3 7 7 5 6 0 1
09A3AD00	2C 31 38 2E 30 31 38 39 33 32 39 2C 34 34 30 36			, 1 8 . 0 1 8 9 3 2 9 , 4 4 0 6
09A3AD10	6D 2F 64 61 74 61 3D 21 33 6D 31 21 31 65 33 21			m / d a t a = ! 3 m 1 ! 1 e 3 !
09A3AD20	34 6D 32 21 33 6D 31 21 37 65 32 3F 61 75 74 68			4 m 2 ! 3 m 1 ! 7 e 2 ? a u t h
09A3AD30	75 73 65 72 3D 30 26 65 6E 74 72 79 3D 74 74 75			u s e r = 0 & e n t r y = t t u
09A3AD40	26 67 5F 65 70 3D 45 67 6F 79 4D 44 49 32 4D 44			& g _ e p = E g o y M D I 2 M D
09A3AD50	55 78 4D 43 34 77 49 4B 58 4D 44 53 6F 41 53 41			U x M C 4 w I K X M D S o A S A
09A3AD60	46 51 41 77 25 33 44 25 33 44 4F 39 81 5C 04 83			F Q A w % 3 D % 3 D 0 9 . \ . .
09A3AD70	39 02 68 74 74 70 73 3A 2F 2F 77 77 77 2E 67 6F			9 . h t t p s : / / w w w . g o
09A3AD80	6F 67 6C 65 2E 63 6F 6D 2F 6D 61 70 73 2F 70 6C			o g l e . c o m / m a p s / p l
09A3AD90	61 63 65 2F 34 38 25 43 32 25 42 30 30 37 27 35			a c e / 4 8 % C 2 % B 0 0 7 ' 5

Obrázok 4: analýza ram pamäte, vyhľadávanie súradníc

Pri hĺbkovej analýze súboru `laptopram.mem` bol v pamäťovom bloku na adrese `09A3ACC0` identifikovaný fragment URL adresy smerujúcej na Google Maps.

Technické detaily nálezů:

- **Identifikovaný reťazec:**
`https://www.google.com/maps/place/48.1328+17.1472.`
- **Súradnice:** GPS poloha **48.1328, 17.1472.**



Obrázok 5: zobrazenie súradníc na mape



Obrázok 6: zobrazenie súradníc na mape (približené)

Na základe extrahovaných údajov z RAM bola vykonaná vizualizácia a overenie súradníc v mapových podkladoch.

Identifikovaná lokalita:

- **Súradnice:** 48.1328, 17.1472.
- **Geografická poloha:** Bratislava, mestská zóna „Prístav“, v blízkosti Nákladného prístavu a rafinérie Apollo.

```
0A9198C0 32 34 66 65 64 41 6B 6F 20 66 75 6E 67 75 6A C3 2 4 f e d A k o   f u n g u j .
0A9198D0 BA 20 73 70 69 72 69 74 62 6F 78 79 3F 20 2D 20 .   s p i r i t b o x y ?   -
0A9198E0 47 6F 6F 67 6C 65 20 47 65 6D 69 6E 69 00 2F B0 G o o g l e   G e m i n i . / .
0A9198F0 1E D7 A7 79 68 63 81 9E 3F 08 00 5D 63 09 08 06 . . . y h c . . ? . . ] c . .
0A919900 08 68 74 74 70 73 3A 2F 2F 6E 6F 72 64 70 61 73 .   h t t p s : / / n o r d p a s
0A919910 73 2E 63 6F 6D 2F 68 61 76 65 2D 69 2D 62 65 65 s . c o m / h a v e - i - b e e
0A919920 6E 2D 68 61 63 6B 65 64 2F 48 61 76 65 20 49 20 n - h a c k e d / H a v e   I
0A919930 62 65 65 6E 20 68 61 63 6B 65 64 3F 20 46 69 6E b e e n   h a c k e d ?   F i n
0A919940 64 20 6F 75 74 20 6E 6F 77 20 7C 20 4E 6F 72 64 d   o u t   n o w   |   N o r d
0A919950 50 61 73 73 00 2F B0 38 9E 8B 7F F9 00 00 00 82 P a s s . / . 8 . . . . .
0A919960 16 81 9E 34 09 00 83 63 41 09 08 06 08 68 74 74 . . . 4 . . . c A . . . . h t t
0A919970 70 73 3A 2F 2F 77 77 77 2E 67 6F 6F 67 6C 65 2E p s : / / w w w . g o o g l e .
0A919980 63 6F 6D 2F 6D 61 70 73 2F 70 6C 61 63 65 2F 41 c o m / m a p s / p l a c e / A
0A919990 6F 6B 69 67 61 68 61 72 61 2F 40 33 35 2E 34 37 o k i g a h a r a / @ 3 5 . 4 7
0A9199A0 30 30 35 30 38 2C 31 33 38 2E 36 33 32 33 37 37 0 0 5 0 8 , 1 3 8 . 6 3 2 3 7 7
0A9199B0 34 2C 38 34 33 33 6D 2F 64 61 74 61 3D 21 33 6D 4 , 8 4 3 3 m / d a t a = ! 3 m
0A9199C0 31 21 31 65 33 21 34 6D 36 21 33 6D 35 21 31 73 1 ! 1 e 3 ! 4 m 6 ! 3 m 5 ! 1 s
0A9199D0 30 78 36 30 31 62 65 37 32 31 65 39 31 32 64 62 0 x 6 0 1 b e 7 2 1 e 9 1 2 d b
0A9199E0 37 37 3A 30 78 65 64 30 34 33 34 39 33 63 38 61 7 7 : 0 x e d 0 4 3 4 9 3 c 8 a
0A9199F0 64 39 32 65 31 21 38 6D 32 21 33 64 33 35 2E 34 d 9 2 e 1 ! 8 m 2 ! 3 d 3 5 . 4
0A919A00 37 35 32 31 38 33 21 34 64 31 33 38 2E 36 34 30 7 5 2 1 8 3 ! 4 d 1 3 8 . 6 4 0
0A919A10 35 30 31 34 21 31 36 7A 4C 32 30 76 4D 44 6C 69 5 0 1 4 ! 1 6 z L 2 0 v M D l i
0A919A20 4E 57 4D 7A 3F 65 6E 74 72 79 3D 74 74 75 26 67 N W M z ? e n t r y = t t u & g
0A919A30 5F 65 70 3D 45 67 6F 79 4D 44 49 32 4D 44 55 77 _ e p = E g o y M D I 2 M D U w
0A919A40 4E 69 34 77 49 4B 58 4D 44 53 6F 41 53 41 46 51 N i 4 w I K X M D S o A S A F Q
0A919A50 41 77 25 33 44 25 33 44 41 6F 6B 69 67 61 68 61 A w % 3 D % 3 D A o k i g a h a
0A919A60 72 61 20 E2 80 93 20 4D 61 70 79 20 47 6F 6F 67 r a . . .   M a p y   G o o g
```

Obrázok 7: ďalšie záznamy vyhľadávania

Pri ďalšom skúmaní súboru `laptopram.mem` na adrese 0A919900 boli identifikované ďalšie fragmenty webovej aktivity.

- **Identifikovaná URL:** <https://nordpass.com/have-i-been-hacked/>.
- **Kontextový text:** „Have I been hacked? Find out now | NordPass“.

Vyhľadávanie „Have I been hacked“ naznačuje, že Adam mal podozrenie na narušenie svojho súkromia alebo bezpečnosti svojich účtov.

Dalšie nálezy vo vyhľadávaní

- **Interakcia s AI nástrojmi:** Identifikovaný reťazec „Google Gemini“ v spojení s dopytom „Ako funguj.. spiritboxy?“ potvrdzuje, že subjekt aktívne využíval umelú inteligencia na hĺbkové štúdium technických princípov zariadení. Tento dopyt naznačuje Adamov záujem o netradičné komunikačné technológie a ich technické fungovanie.
- **Vyhľadávanie izolovaných lokalít:** Na adrese 0A919970 bola zachytená URL adresa smerujúca na súradnice lokality Aokigahara v Japonsku. Ide o les známi ako „les samovrahov“.

07B1CD90	55 72 6C 22 3A	22 68 74 74 70 73 3A 2F 2F 77 77	U r l " : " h t t p s : / / w w
07B1CDA0	77 2E 67 6F 6F 67 6C 65 2E 63 6F 6D 2F 73 65 61		w . g o o g l e . c o m / s e a
07B1CDB0	72 63 68 3F 71 3D 68 6F 77 2B 74 6F 2B 64 65 6C		r c h ? q = h o w + t o + d e l
07B1CDC0	65 74 65 2B 63 61 6D 65 72 61 2B 72 65 63 6F 72		e t e + c a m e r a + r e c o r
07B1CDD0	64 73 26 73 63 61 5F 65 73 76 3D 36 34 66 31 39		d s & s c a _ e s v = 6 4 f 1 9

Obrázok 8

Pri pokračujúcej analýze súboru `laptopram.mem` na adrese 07B1CD90 bol identifikovaný kritický reťazec, ktorý potvrdzuje priamy úmysel subjektu poškodiť integritu monitorovacieho systému.

Technické detaily nálezů:

- **Identifikovaná URL:**
<https://www.google.com/search?q=how+to+delete+camera+records>.
- **Formát dát:** Fragment JSON objektu alebo histórie prehliadača zachytený v RAM.
- **Kľúčové slová:** "how to delete camera records" (ako vymazať záznamy z kamier).

Analýza nevolatílnej pamäte

address	person	date	date_sent	protocol	read	status	type	reply_pa...	subject	body
244444		1643148518098	0		1	-1	2			(OgPqTeDunuet) Google is verifying the phone# of this device as part of setup. Learn more: ...
3342924739		1643425656177	1643425654000	0	1	-1	1	0		<#> Here is your PIN: 037431.Please do not disclose this code to anyone.Tech bit: z6NZ55X/...
3342924739		1643836844544	1643836843000	0	1	-1	1	0		<#> Here is your PIN: 278311.Please do not disclose this code to anyone.Tech bit: z6NZ55X/...
teresafader46gu@outlook.com		1643897062738	1643897060000	0	0	-1	1	0		ow.ly/vN5t50HLrXX????????zeq#comments .comment .comment-actions,subs
4159095630		1643942141492	1643942140000	0	1	-1	1	0		Your Discord security code is: 950849 tzD9jY28Wrn
4154032806		1643944331476	1643944329000	0	1	-1	1	0		Your Discord security code is: 326152
611611		1644256993158	1644256992000	0	0	-1	1	0		Welcome back to Total Wireless! Your phone number is 6202950585, your last day of service i...
244444		1644257283639	1644257284000	0	1	-1	1	0		Your Messenger verification code is G-212954
2243264888		1644388649283	1644388647000	0	1	-1	1	0		<#> Snapchat Code: 543220. Happy Snapping! qunyt57f5Rf
6318898841		1644738777749	1644738775000	0	1	-1	1	0		[#][TikTok] 304321 is your verification codefJpzQvK2eu1
22395		1644741140530	1644741138000	0	0	-1	1	0		<#> Your SIGNAL verification code is: 276498doDiFGKPO1r
CCDC-Security		1643878800000	1643878800000		1	-1	1	0		Lokalizacia uspesna. Nasli sme vas. Ocavame vas zajtra rano v centrale na pohovore.
CCDC-Security		1643911200000	1643911200000		1	-1	1	0		Viete, co mate urobit. Nezkousajte odist, monitorujeme vsetky pristupy.
+421944555666		1643810400000	1643810400000		1	-1	1	0		Ak na to pridu, budeme to musiet spravit. Inej cesty niet.
+421944555666		1643918400000	1643918400000		1	-1	2	0		Uz nemozeme cakat. Musime ist.
+421944555666		1643919000000	1643919000000		1	-1	1	0		Suhlas. Stretname sa na tom pive ako sme vpravli. Okna nechaj dokoran.
+421944555666		1643928000000	1643928000000		1	-1	1	0		Som na mieste. Vypni svetla a pod.
Pizza-Donaska		1643821200000	1643821200000		1	-1	1	0		Vasa objednavka cislo 445 bola prijata. Kurier pride do 30 minut.
Mama		1643835600000	1643835600000		1	-1	1	0		Ahoj, nezabudni sa ozvat, ked dopises tu analyzu. Davaj na seba pozor.

Obrázok 9: sms komunikácia

address	body
244444	(OgPqTeDunuet) Google is verifying the phone# of this device as part of setup. Learn more: ...
3342924739	<#> Here is your PIN: 037431.Please do not disclose this code to anyone.Tech bit: z6NZ55X/...
3342924739	<#> Here is your PIN: 278311.Please do not disclose this code to anyone.Tech bit: z6NZ55X/...
teresafader46gu@outlook.com	ow.ly/vN5t50HLrXX????????zeq#comments .comment .comment-actions,subs
4159095630	Your Discord security code is: 950849 tzD9jY28Wrn
4154032806	Your Discord security code is: 326152
611611	Welcome back to Total Wireless! Your phone number is 6202950585, your last day of service i..
244444	Your Messenger verification code is G-212954
2243264888	<#> Snapchat Code: 543220. Happy Snapping! qunyt57f5Rf
6318898841	[#][TikTok] 304321 is your verification codefJpzQvK2eu1
22395	<#> Your SIGNAL verification code is: 276498doDiFGKPO1r
CCDC-Security	Lokalizacia uspesna. Nasli sme vas. Ocavame vas zajtra rano v centrale na pohovore.
CCDC-Security	Viete, co mate urobit. Nezkousajte odist, monitorujeme vsetky pristupy.
+421944555666	Ak na to pridu, budeme to musiet spravit. Inej cesty niet.
+421944555666	Uz nemozeme cakat. Musime ist.
+421944555666	Suhlas. Stretname sa na tom pive ako sme vpravli. Okna nechaj dokoran.
+421944555666	Som na mieste. Vypni svetla a pod.
Pizza-Donaska	Vasa objednavka cislo 445 bola prijata. Kurier pride do 30 minut.
Mama	Ahoj, nezabudni sa ozvat, ked dopises tu analyzu. Davaj na seba pozor.

Obrázok 10: sms komunikácia (adresy a obsah správ)

Analýza databázy správ v mobilnom zariadení odhalila komunikáciu, ktorá potvrdzuje kritický stav subjektu pred incidentom.

Nátlak zo strany organizácie (CCDC-Security):

- **Správa č. 12:** *"Lokalizacia uspesna. Nasli sme vas. Ocavame vas zajtra rano v centrale na pohovore."*
- **Správa č. 13:** *"Viete, co mate urobit. Nezkousajte odist, monitorujeme vsetky pristupy."*
- Tieto správy jasne dokazujú, že Adam bol pod neustálym dohľadom bezpečnostného oddelenia CCDC.

Analýza vybraných správ:

- **Správa č. 14:** *"Ak na to prídu, budeme to musieť spraviť. Inej cesty niet."* – Táto správa naznačuje existenciu záložného plánu v prípade odhalenia subjektu.
- **Správa č. 15:** *"Uz nemozeme cakat. Musime ist."* - Táto správa pôsobí ako impulz k akcii. Zatiaľ čo predchádzajúca správa (č. 14) hovorila o tom, že to "budú musieť spraviť, ak na to prídu", správa č. 15 signalizuje, že čas na váhanie vypršal.
- **Správa č. 16:** *"Suhlas. Stretneme sa na tom pive ako sme vraveli. Okna nechaj dokoran."* – Použitie spojenia „pivo“ v tomto kontexte pôsobí neštandardne.
- **Správa č. 17:** *"Som na mieste. Vypni svetla a pod."* – Záznam potvrdzuje fyzickú prítomnosť druhej osoby na mieste, ktoré nateraz nie je špecifikované.

_id	account_name	account_type	data_set
1	rafaelshell124@gmail.com	com.google	

Obrázok 11: analýza používateľských účtov

Pri skúmaní databázy účtov v mobilnom zariadení (`accounts2.db`) bol identifikovaný hlavný Google účet priradený k zariadeniu.

Technické detaily nálezu:

- **Identifikovaný účet:** `rafaelshell124@gmail.com`.
- **Typ účtu:** `com.google`.
- **ID záznamu:** 1 (naznačuje, že ide o primárny účet nastavený v zariadení).

Počas analýzy bol zistený významný nesúlad medzi úradnou identitou subjektu a jeho digitálnym profilom:

- **Skutočné meno:** Adam K.
- **Digitálna identita:** rafaelshell24@gmail.com.

number	presenta...	post_dial...	via_num...	date	duration	data_usa...	type
CCDC-Security	1			1643878850000	0		3
+421944555666	1			1643918500000	42		1
Mama	1			1643835700000	115		2

Obrázok 12: zoznam volaní

V databáze hovorov boli identifikované tri kľúčové záznamy, ktoré korelujú s psychologickým tlakom na subjekt a fázou prípravy incidentu.

1. Kontakt: CCDC-Security

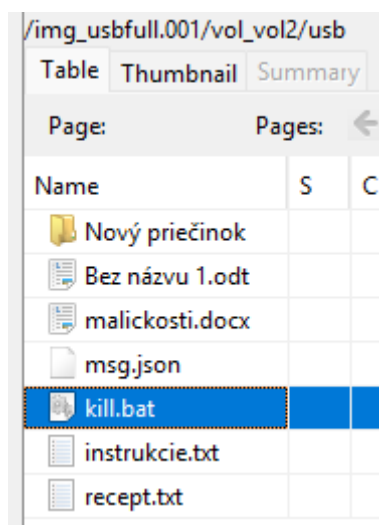
- **Trvanie (duration):** 0.
- **Typ (type):** 3 (Zmeškaný hovor).
- **Interpretácia:** Subjekt ignoroval pokus o kontakt zo strany bezpečnostného oddelenia firmy. Tento zmeškaný hovor časovo sedí k výhražným SMS o „lokalizácii“. Ignorovanie hovoru potvrdzuje Adamovu snahu o odpútanie sa od vplyvu organizácie.

2. Kontakt: +421944555666 (Predpokladaný komplic)

- **Trvanie (duration):** 42 sekúnd.
- **Typ (type):** 1 (Prichádzajúci hovor).
- **Interpretácia:** Tento 42-sekundový hovor je najdôležitejším nálezom v tejto sekcii. Prebehol po sérii podozrivých SMS o „pive“ a „otvorených oknách“. Dĺžka hovoru je dostatočná na odovzdanie operatívnej inštrukcie k začatiu akcie.

3. Kontakt: Mama

- **Trvanie (duration):** 115 sekúnd.
- **Typ (type):** 2 (Odchádzajúci hovor).
- **Interpretácia:** Dlhší súkromný hovor, ktorý pravdepodobne súvisí s SMS správou, v ktorej ho mama nabádala k opatrnosti. Je to posledný zaznamenaný kontakt s rodinou pred Adamovým zmiznutím.



/img_usbfull.001/vol_vol2/usb		
Table	Thumbnail	Summary
Page:		Pages: ←
Name	S	C
Nový priečinok		
Bez názvu 1.odt		
malickosti.docx		
msg.json		
kill.bat		
instrukcie.txt		
recept.txt		

Obrázok 13: štruktúra posledných súborov na USB

Na základe forenznej analýzy priečinka `/usb` boli identifikované tri súbory, ktoré priamo dokumentujú prípravu a vykonanie sabotáže.

- `kill.bat`
- `msg.json`
- `instrukcie.txt`

```
@echo off
net use Z: \\192.168.1.50\C$ /user:admin B3$t_S4f3_H0us3_2026!
taskkill /S 192.168.1.50 /U admin /P B3$t_S4f3_H0us3_2026! /F /IM "cctv_service.exe"
del /S /Q /F "Z:\CCTV\Records\*.avi"
cipher /w:Z:\CCTV\Records\
wmic /node:192.168.1.50 /user:admin /password:B3$t_S4f3_H0us3_2026! process call create "wevtutil cl System"
net use Z: /delete /y
del %0
```

Obrázok 14: kill.bat

Dávkový súbor, ktorý je technickou realizáciou plánu opísaného v predchádzajúcich dvoch súboroch.

- **Funkcia:** Skript sa vzdialene pripája na IP 192.168.1.50, ukončuje proces `cctv_service.exe` a vymazáva videozáznamy `.avi`.
- **Zahladenie stôp:** Obsahuje príkaz `cipher /w`, ktorý prepisuje zmazané dáta, aby ich nebolo možné obnoviť, a príkaz na vymazanie systémových logov.

```
{
  "chat_provider": "Signal_Desktop_Export",
  "export_date": "2026-01-27T23:10:45Z",
  "conversation_with": "+421 9xx xxx xxx",
  "messages": [
    {
      "timestamp": "2026-01-27T19:10:00Z",
      "sender": "Adam",
      "text": "Pocuj, hori mi pod nohami. CCDC po mne ide"
    },
    {
      "timestamp": "2026-01-27T19:12:15Z",
      "sender": "Kontakt",
      "text": "Takze plati to Zmiznutie?"
    },
    {
      "timestamp": "2026-01-27T19:13:50Z",
      "sender": "Adam",
      "text": "Ano. Ked ti napisem, ze 'IDEME NA PIVO', znamena to, ze uz som v safe house"
    },
    {
      "timestamp": "2026-01-27T19:15:30Z",
      "sender": "Kontakt",
      "text": "Rozumiem. 'IDEME NA PIVO' = Kamery su off a ty si na ceste von. Kluc ti dam pri bare zajtra o 15:00."
    },
    {
      "timestamp": "2026-01-27T19:18:00Z",
      "sender": "Kontakt",
      "text": "Script mam na USB. Hned ako budem vnutri, odpalim to a zmiznem."
    }
  ]
}
```

Obrázok 15: msg.json

Tento súbor je exportom šifrovanej komunikácie z aplikácie Signal. Odhaľuje kritické detaily:

- **Motív:** Adam píše, že mu „horí pod nohami“ a že po ňom ide CCDC.
- **Plán „Zmiznutie“:** Komunikácia priamo spomína akciu pod kódovým názvom „Zmiznutie“.
- **Kódové heslá:** Potvrďuje sa význam hlášky „IDEME NA PIVO“. V JSONe je jasne napísané, že to znamená „kamery sú off“ a Adam je na ceste von.
- **Technika:** Adamov kontakt potvrdzuje: „Script mam na USB. Hned ako budem vnútri, odpalim to a zmiznem“.

PROTOKOL: ZMIZNUTIE (28.01.2026)

STRETNUTIE:

- 15:00 pri bare (prevziať kľúče)

POSTUP:

- Smer Safe House (48.1328, 17.1472)

- Spustiť skript z USB (kill.bat)

- HESLO: B3\$!t_S4f3_H0us3_2026!

KÓD PRE KONTAKT:

"IDEME NA PIVO" (= kamery sú off, odchádzam)

Obrázok 16: instrukcie.txt

Tento dokument slúžil ako Adamov presný „ťahák“ pre deň incidentu (28. 1. 2026):

- **Súradnice:** Smer Safe House na presných súradniciach (48.1328, 17.1472).
- **Logistika:** Stretnutie o 15:00 pri bare kvôli prevzatiu kľúčov.
- **Prístupové údaje:** Obsahuje priamo to heslo, ktoré sme videli v skripte:
B3\$!t_S4f3_H0us3_2026!.

ZMLUVA O POSKYTOVANÍ SERVISNÝCH SLUŽIEB A SPRÁVE KAMEROVÉHO SYSTÉMU

Číslo zmluvy: 2024/INV/089-B

Zmluvné strany:

Objednávateľ:

Mesto Metropola
Štefánikova trieda 60
999 01 Metropola
IČO: 11111111
DIČ: 11111111
Zastúpené: Ing. Viktor Zástupca, poverený správca mestskej infraštruktúry

Poskytovateľ:

Central City Defense Corporation (CCDC), s.r.o.
Priemyselná 18
821 09 Bratislava
IČO: 99999999
DIČ: 999999999
IČ DPH: SK1234567890
Zapísaná v OR Mestského súdu Bratislava III, oddiel Sro, vložka č. 145789/B
Zastúpená: Dr. Elias Riaditeľ, výkonný riaditeľ spoločnosti

I. Predmet zmluvy

Poskytovateľ sa zaväzuje zabezpečiť nepretržitý monitoring (24/7) a technickú údržbu 142 monitorovacích bodov (kamier) v mestskej zóne „Prístav“ a príľahlých sektoroch. Súčasťou predmetu zmluvy je aj pravidelná diagnostika zariadení, aktualizácia bezpečnostného softvéru a vzdialená správa systému.

II. Rozsah poskytovaných služieb

Poskytovateľ bude vykonávať preventívne servisné kontroly minimálne raz mesačne. Súčasťou služieb je aj výmena poškodených komponentov, kalibrácia kamerových zariadení a monitoring integrity dátového prenosu.

III. Garancia funkčnosti (SLA)

Poskytovateľ garantuje 99,9 % dostupnosť videosignálu. V prípade poruchy sa poskytovateľ zaväzuje k oprave do 4 hodín od nahlásenia incidentu. Kritické incidenty budú riešené prioritne prostredníctvom nonstop technickej podpory.

IV. Archivácia a ochrana dát

Všetky kamerové záznamy budú archivované po dobu minimálne 14 dní na dedikovaných serveroch Poskytovateľa v režime „Safe House“. Poskytovateľ sa zaväzuje dodržiavať všetky bezpečnostné štandardy a zabezpečiť ochranu údajov pred neoprávneným prístupom.

V. Cena a fakturácia

Zmluvné strany sa dohodli na paušálnej mesačnej odplate vo výške 45 000 EUR bez DPH za správu a údržbu systému. Fakturácia bude vykonávaná mesačne so splatnosťou faktúr 14 dní odo dňa vystavenia.

VI. Povinnosti Objednávateľa

Objednávateľ sa zaväzuje zabezpečiť Poskytovateľovi prístup k monitorovacím bodom a technologickým priestorom v prípade potreby servisného zásahu alebo technickej kontroly.

VII. Mlčanlivosť

Obe zmluvné strany sa zaväzujú zachovávať mlčanlivosť o všetkých technických, prevádzkových a bezpečnostných informáciách získaných počas plnenia tejto zmluvy.

VIII. Sankcie

V prípade preukázania nefunkčnosti systému z viny Poskytovateľa, ktorá nebola nahlásená, prináleží Objednávateľovi zmluvná pokuta vo výške 10 % z mesačnej paušálnej platby za každý deň nefunkčnosti.

IX. Vyššia moc

Za porušenie povinností podľa tejto zmluvy sa nepovažujú udalosti spôsobené vyššou mocou, najmä prírodnými katastrofami, rozsiahlymi výpadkami elektrickej energie alebo kybernetickými útokmi tretích strán.

X. Doba trvania zmluvy

Táto zmluva sa uzatvára na dobu určitú v trvaní 36 mesiacov odo dňa nadobudnutia jej účinnosti. Zmluvu je možné predčasne ukončiť dohodou zmluvných strán alebo výpoveďou s trojmesačnou výpovednou lehotou.

XI. Záverečné ustanovenia

Táto zmluva nadobúda platnosť dňom podpisu oboma zmluvnými stranami. Akékoľvek zmeny alebo dodatky k tejto zmluve musia byť vyhotovené v písomnej forme a podpísané oboma stranami.

V Metropole, dňa: 14.09.2024

Objednávateľ	Poskytovateľ
 Ing. Viktor Zástupca Poverený správca mestskej infraštruktúry	 Dr. Elias Riaditeľ Výkonný riaditeľ spoločnosti CCDC, s.r.o.

Obrázky 17, 18 19: zmluva

```
{
  "channel": "CCDC_Operations_Internal",
  "export_date": "2025-09-16T10:15:30Z",
  "messages": [
    {
      "timestamp": "2025-09-15T08:45:12Z",
      "user": "Technik_Matus",
      "text": "Sektor B (Pristav) je zase kompletne dole. Tie stare firmware-y na 142 bodoch jednoducho padaju."
    },
    {
      "timestamp": "2025-09-15T09:10:05Z",
      "user": "Dr_Elias_Riaditel",
      "text": "Matus, nerieste to teraz. Nemame rozpocet na vymenu komponentov podla clanku II zmluvy. Ak sa niekto z mesta spyta, nahlaste to ako vypadok prudu kvoli pocasiu."
    },
    {
      "timestamp": "2025-09-15T09:12:30Z",
      "user": "Adam",
      "text": "Ale Elias, to je riskantne. V zmluve garantujeme 99,9 % funkcnost. Ak na to pridu, podla clanku VIII zaplatime pokutu 10 % denne. To je cez 4000 eur kazdy den."
    },
    {
      "timestamp": "2025-09-15T09:15:00Z",
      "user": "Dr_Elias_Riaditel",
      "text": "Adam, prestante mudrovat a starajte sa o tie archivy na externom uzle. Tie logy musia sediet s tym, co fakturujeme. Mesto nam plati 45 000 mesacne, tak budte rad, ze mate pracu."
    }
  ]
}
```

Obrazok 20: záznam konverzácie

Analýza dokumentov v „Novom priečinku“ priniesla zásadný zvrat vo vyšetrovaní. Nájsené súbory naznačujú, že subjekt Adam K. (Rafael Shell) disponoval citlivými informáciami o nezákonnej činnosti organizácie CCDC.

- **Súbor `zmluva_dokoncena.pdf`** predstavuje zmluvu ktorú uzavrelo mesto a firma CCDC.
- **Súbor `i_msg.json`**: obsahuje potvrdenia o tom, že firma CCDC falšovala záznamy a dokumentáciu pre mesto.

Záver

Analýza digitálnych stôp potvrdzuje, že Adam K. zinscenoval svoje zmiznutie ako reakciu na odhalenie podvodov vo vnútri firmy CCDC.

Kľúčové body vyšetovania:

- **Úmyselný útek:** Subjekt naplánoval akciu pod kódom „Zmiznutie“. Signál na odchod bol dohodnutý kód „IDEME NA PIVO“.
- **Motív (Whistleblowing):** Na USB kľúči sa našli dokumenty dokazujúce, že firma CCDC falšovala zmluvy s mestom. Adam tieto dôkazy vyniesol, pretože sa cítil ohrozený sledovaním zo strany CCDC-Security.

Vyhodnotenie hypotéz

Hypotéza A: Cudzie zavinenie

- **Znenie:**
 - Tretia osoba vnikla do objektu cez záhradu s cieľom získať citlivé dáta z laptopu. Obet' bola konfrontovaná a následne z objektu odvedená, pričom útočník sa pokúsil zahľadiť stopy manipuláciou s kamerou a mobilným telefónom.
- **Rozšírenie o nálezy:**
 - Táto hypotéza predpokladala externého agresora. Analýza však ukázala, že hoci firma CCDC-Security Adama lokalizovala a vyvíjala naňho nátlak cez SMS, neexistujú dôkazy o fyzickom zápase.
- **Výsledok: VYVRÁTENÁ.**
 - Manipulácia so systémom bola iniciovaná zvnútra, nie útočníkom zvonku.

Hypotéza B: Inscenované zmiznutie

- **Znenie:**
 - Obet' (Adam K.) zinscenovala vlastné zmiznutie. Rozhádzaný stôl a otvorené dvere majú slúžiť ako zmätočné stopy. Režim „Lietadlo“ a mazanie kamery vykonal sám, aby sťažil svoje vypátranie.
- **Rozšírenie o nálezy:**
 - Táto hypotéza sa ukázala ako technicky najpresnejšia. Adam používal pseudonym Rafael Shell a vopred si pripravil "Protokol Zmiznutie". Nájdene súradnice a kódové frázy ako „IDEME NA PIVO“ potvrdzujú, že zmiznutie bolo vopred naplánovanou operáciou na opustenie sféry vplyvu CCDC.
- **Výsledok: POTVRDENÁ.**
 - Celý incident bol riadený subjektom s cieľom bezpečne opustiť monitorovaný priestor.

Hypotéza C: Priemyselná špionáž

- **Znenie:**
 - Obeť bola cieľom útoku zameraného na konkrétne dáta (USB kľúč). Útočník využil znalosť prostredia a prístupových kódov k domácej sieti, čo vysvetľuje absenciu stôp násilia pri vstupe.
- **Rozšírenie o nálezy:**
 - Špionáž sa potvrdila, ale v obrátenom garde. Obeť (Adam) nebola cieľom, ale aktérom, ktorý vynášal dáta. Na USB kľúči sa našli dokumenty o projekte **Sektor B** a zmluvy mesta. Absencia stôp násilia je vysvetlená tým, že Adam mal k objektu legítimny prístup a kľúče si prevzal podľa plánu o 15:00 pri bare.
- **Výsledok: ČIASTOČNE POTVRDENÁ.**
 - Došlo k úniku citlivých dát, avšak v réžii zamestnanca.

Použité nástroje

Nástroje pre akvizíciu a integritu dát

1. FTK Imager:

- Hlavný nástroj použitý na vytváranie bitových kópií diskov a fyzických obrazov USB média. Nástroj zároveň slúžil na prvotný náhľad súborového systému a výpočet kontrolných súčtov pre zabezpečenie integrity dôkazov.

2. Magnet RAM Capture:

- Špecializovaný nástroj použitý na "živý" odber obsahu operačnej pamäte (RAM) z laptopu obete. Bol zvolený pre jeho minimálnu stopu v systéme (low footprint), čím sa minimalizovalo riziko prepísania dôležitých artefaktov v nestálej pamäti.

3. Winpmem:

- Alternatívny nástroj pre akvizíciu RAM, využitý na vytvorenie surového (raw) dumpu pamäte. Jeho schopnosť pracovať s jadrom systému (kernel-level) zabezpečila získanie kompletného obrazu fyzickej pamäte vrátane chránených oblastí.

Nástroje pre hĺbkovú analýzu a verifikáciu

1. Hex Editor (HxD):

- Použitý na nízkoúrovňovú analýzu binárnych dát, vyhľadávanie magických čísel a manuálnu verifikáciu hlavičiek poškodených alebo vymazaných súborov, ktoré nebolo možné otvoriť bežnými prostriedkami.

2. Visual Studio Code + Hex Editor Plugin:

- Bol využitý na analýzu konfiguračných súborov, logov a na prehľadné porovnávanie zmien v textových artefaktoch. Hex Editor plugin v rámci VS Code umožnil rýchlu navigáciu v rozsiahlych binárnych dumpoch z RAM pamäte pri hľadaní kľúčových slov.

3. Autopsy:

- Komplexná digitálna forenzná platforma použitá ako hlavný nástroj pre hĺbkovú analýzu diskových obrazov. Umožňuje automatizované vyhľadávanie artefaktov, obnovu vymazaných súborov (file carving), analýzu časovej osi (Timeline) a efektívnu kategorizáciu kľúčových dôkazov v prehľadnom rozhraní.

4. Volatility Workbench

- Tento nástroj bol použitý na pokročilú analýzu volatílnej pamäte (RAM dump). Hoci primárne textové artefakty boli verifikované pomocou Hex editora, Volatility slúžila na rekonštrukciu stavu systému v čase zaistenia, analýzu bežiacich procesov a kontrolu sieťových artefaktov, čím sa vylúčila prítomnosť cudzieho malvéru alebo neoprávneného vzdialeného prístupu v čase incidentu.

Bezpečnostné opatrenia a CoC

Bezpečnostné opatrenia

Pri manipulácii s digitálnymi dôkazmi bol kladený maximálny dôraz na dodržiavanie forenzných štandardov, aby sa zamedzilo akejkoľvek modifikácii alebo znehodnoteniu pôvodných dát. Celý proces prebiehal v dvoch fázach: na mieste zaistenia (on-site) a v laboratórnom prostredí.

Zaistenie volatílnej pamäte (RAM) a prvotná akvizícia

Vzhľadom na to, že laptop bol v čase príchodu v zapnutom stave, prioritou bolo získanie obsahu operačnej pamäte pred vypnutím zariadenia.

- **Postup na mieste:** Bol vykonaný "živý" odber pamäte pomocou nástrojov Magnet RAM Capture.
- **Bezpečnosť:** Nástroje boli spúšťané priamo z forenzného USB kľúča, aby sa minimalizoval zápis na systémový disk a zabránilo sa prepísaniu relevantných artefaktov v nestálej pamäti.
- **Ostatné zariadenia:** boli izolované v tieniacej (Faradayovej) taške a vložené do bezpečnostných kufrov určené na bezpečný prenos zariadení.

Laboratórne spracovanie a tvorba bitových kópií nevolatívnych pamätí

Po prevoze zaistených zariadení do laboratória sa pristúpilo k vytvoreniu fyzických obrazov (disk imaging) pre účely následnej analýzy.

- **Hardvérová blokácia zápisu:** Pri pripájaní zariadení k analytickej stanici boli použité hardvérové blokátory zápisu (write-blockers). Tieto zariadenia fyzicky znemožňujú operačnému systému vykonať akýkoľvek zápis (vrátane automatických zmien v súborovom systéme alebo aktualizácie časových pečiatok) na pôvodné médium.
- **Tvorba obrazov:** Pomocou nástroja FTK Imager boli vytvorené bitové kópie všetkých médií. Obrazy boli uložené vo formáte IMG.
- **Verifikácia integrity (Hashing):** Okamžite po vytvorení každého obrazu bol vypočítaný kontrolný súčet (hash) pomocou algoritmov MD5 a SHA1. Tieto hodnoty boli zaznamenané a následne porovnané s pôvodným médium, čím sa preukázala 100 % zhoda a integrita vytvorených kópií.

Analýza na pracovných kópiách

Všetky následné analytické kroky v prostředí **Autopsy** a ďalších nástrojoch boli vykonávané výhradne na pracovných kópiách (bitových obrazoch). Originálne pamäťové médiá boli po vytvorení obrazov bezpečne uložené, čím sa eliminovalo riziko ich náhodného poškodenia počas hĺbkovej analýzy.

Zoznam hashov

Laptop (operačná pamäť):

- **MD5:** c6d91d7ab787f7d1e730256b4078bdbf
- **SHA1:** ded9cdb17a0ed7a926764cc26481fd168108d9b1

Laptop:

- **MD5:** 81e6a37dc02df3d62d78b3ac4e2029bf
- **SHA1:** 0d9d55ca35619e9e84ea94fd00475c70c74fc10a

Mobil:

- **MD5:** 6778e01e26a9ca0b48bc99223a993490
- **SHA1:** ba28c273f27052fea247e1a5c93d198f69080072

USB:

- **MD5:** 55032ddd25d6f01213391b1ad5cb6b01
- **SHA1:** 2f9f78f28bfca676933690c441c63bc051dfd4ea

Laptop (operačná pamäť)

Číslo:	00	Typ súboru:	mem	Obnovený súbor:	nie	Veľkosť:	8gb
Názov prípadu:	Nezvestná osoba						
Názov súboru:	laptopram.mem						
Miesto získania digitálnej stopy:	Na stole v pracovni						
Poznámky:	Bitová kópia operačnej pamäti laptopu						
Časové pečiatky							
Access:	29.01.2026 08:30		Modify:	29.01.2026 09:00		Change:	-
Digitálny odtlačok (heš)	MD5	c6d91d7ab787f7d1e730256b4078bdbf					
	SHA1	ded9cdb17a0ed7a926764cc26481fd168108d9b1					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
29.01.2026 08:20		Zaistenie zariadenia					
29.01.2026 9:00		Vytvorenie bitovej kópie a hashu					
29.01.2026 9:05		Vloženie zariadenia do bezpečného úložiska					
29.01.2026 11:45		Analýza dát					

Laptop

Číslo:	01	Typ súboru:	img	Obnovený súbor:	nie	Veľkosť:	500gb
Názov prípadu:	Nezvestná osoba						
Názov súboru:	laptopimg.img						
Miesto získania digitálnej stopy:	Na stole v pracovni						
Poznámky:	Bitová kópia laptopu						
Časové pečiatky							
Access:	29.01.2026 10:00		Modify:	29.01.2026 10:50		Change:	-
Digitálny odtlačok (heš)	MD5	81e6a37dc02df3d62d78b3ac4e2029bf					
	SHA1	0d9d55ca35619e9e84ea94fd00475c70c74fc10a					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
29.01.2026 08:20		Zaistenie zariadenia					
29.01.2026 10:50		Vytvorenie bitovej kópie a hashu					
29.01.2026 10:55		Vloženie zariadenia do bezpečného úložiska					
29.01.2026 14:10		Analýza dát					

Mobil

Číslo:	02	Typ súboru:	img	Obnovený súbor:	nie	Veľkosť:	128gb
Názov prípadu:	Nezvestná osoba						
Názov súboru:	mobilingg.img						
Miesto získania digitálnej stopy:	Na stolíku pri posteli v spálni						
Poznámky:	Bitová kópia mobilu						
Časové pečiatky							
Access:	29.01.2026 10:55		Modify:	29.01.2026 11:10		Change:	-
Digitálny odtlačok (heš)	MD5	6778e01e26a9ca0b48bc99223a993490					
	SHA1	ba28c273f27052fea247e1a5c93d198f69080072					
Časová pečiatka	Akcia vykonaná s digitálnou stopou						
29.01.2026 08:30	Zaistenie zariadenia						
29.01.2026 11:10	Vytvorenie bitovej kópie a hashu						
29.01.2026 11:15	Vloženie zariadenia do bezpečného úložiska						
29.01.2026 16:15	Analýza dát						

USB

Číslo:	03	Typ súboru:	img	Obnovený súbor:	nie	Veľkosť:	64gb
Názov prípadu:		Nezvestná osoba					
Názov súboru:		usbimg.img					
Miesto získania digitálnej stopy:		Pod stolom v pracovni					
Poznámky:		Bitová kópia USB					
Časové pečiatky							
Access:	29.01.2026 11:15		Modify:	29.01.2026 11:28		Change:	-
Digitálny odtlačok (heš)	MD5	55032ddd25d6f01213391b1ad5cb6b01					
	SHA1	2f9f78f28bfca676933690c441c63bc051dfd4ea					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
29.01.2026 08:40		Zaistenie zariadenia					
29.01.2026 11:28		Vytvorenie bitovej kópie a hashu					
29.01.2026 11:32		Vloženie zariadenia do bezpečného úložiska					
29.01.2026 17:00		Analýza dát					