

Bezpečnostný incident: podozrivá aktivita zamestnanca

V rámci štúdia digitálnej forenzej analýzy bol vytvorený fiktívny prípad so scenárom kybernetického bezpečnostného incidentu.

1. Scenár

Organizácia zaznamenala pokusy o neoprávnený prístup k citlivým interným informáciám. V reakcii na to bezpečnostný tím posilnil monitoring IT infraštruktúry. Analýza záznamov zo systému a rozhovory so zamestnancami poukázali na konkrétneho zamestnanca, ktorý mohol spolupracovať s externou stranou.

Zvýšené sledovanie jeho aktivity odhalilo podozrivé správanie v sieti aj na lokálnom systéme. Bezpečnostný tím preto vykonal forenzné zabezpečenie dát vrátane:

- Kopírovania obsahu jeho domovského adresára,
- Vytvorenia obrazu operačnej pamäte,
- Zachytávania paketov sieťovej komunikácie.

2. Motivácia

Cieľom vyšetrovania je zodpovedať nasledujúce otázky:

1. **Aké aktivity používateľ a možno zrekonštruovať a čo z nich vyplýva?**
2. **Existujú dôkazy o nevhodnej alebo podozrivej činnosti v systéme?**
3. **Je preukázaná spolupráca s externou stranou? Ak áno, aké informácie sú o nej dostupné a akým spôsobom komunikácia prebiehala?**
4. **Došlo k odcudzeniu citlivých údajov? Ak áno, aké dáta boli skopírované a akým spôsobom boli prenesené?**

Pre lepšie pochopenie prípadu a zodpovedanie predchádzajúcich otázok použijeme Kiplingovu metódu:

- **Who? (Kto?)**
 - Kto je podozrivý? Kto je dotknutý touto udalosťou?
 - Podozrivý zamestnanec, externý aktér, bezpečnostný tím.
- **What? (Čo?)**
 - Čo sa stalo? Aké dôkazy máme k dispozícii?
 - Neoprávnené pokusy o prístup k citlivým údajom, podozrivá sieťová aktivita.
 - Dôkazy: obraz systémovej pamäte, sieťové pakety, domovský adresár.
- **When? (Kedy?)**
 - Kedy bola podozrivá aktivita zaznamenaná?
 - Kedy bol podozrivý zamestnanec online?
 - Kedy došlo k pokusu o kopírovanie alebo prenos údajov?
- **Where? (Kde?)**
 - Kde sa podozrivá aktivita odohrala?
 - Firemný počítač, vzdialené servery, USB zariadenie, e-mailová komunikácia.
- **Why? (Prečo?)**
 - Prečo by podozrivý mohol vykonať túto činnosť?

- Finančná motivácia? Spolupráca s konkurenciou? Nevedomé konanie?
- Mohol byť účet zamestnanca kompromitovaný?

- **How? (Ako?)**

- Ako bola aktivita vykonaná? Aké technické metódy boli použité?
- Použitie USB disku, vzdialeného prístupu, šifrovaných správ?
- Aké nástroje mohol útočník využiť (VPN, anonymizácia, šifrovanie)?

3. Hypotézy vyšetrovania

1. Zamestnanec vedome spolupracoval s externou stranou na odcudzení údajov.

- Zamestnanec bol v kontakte s neznámou externou stranou prostredníctvom šifrovaných komunikačných kanálov.
- Používal nástroje na obchádzanie bezpečnostných opatrení organizácie, napríklad anonymizačné služby alebo špeciálne softvérové nástroje na extrakciu údajov.
- Skopíroval citlivé súbory a preniesol ich cez externé médium alebo sieť.

2. Podozrivá aktivita bola spôsobená neúmyselným správaním alebo nesprávnym vyhodnotením dôkazov.

- Zamestnanec nevedome vykonal činnosti, ktoré boli interpretované ako podozrivé (napr. sťahovanie veľkých objemov dát v rámci pracovných povinností).
- Infekcia malvérom mohla spôsobiť podozrivú sieťovú aktivitu a prenos údajov na externé servery bez vedomia používateľa.
- Bezpečnostné nástroje mohli nesprávne interpretovať legitímne správanie ako hrozbu.

3. Účet zamestnanca bol kompromitovaný a využitý inou osobou na neoprávnené aktivity.

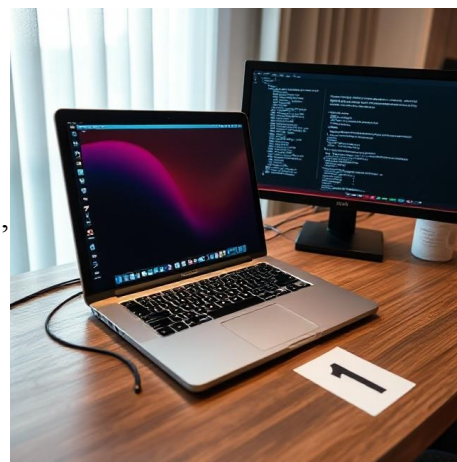
- Iný zamestnanec alebo hacker získal prístup k účtu podozrivého zamestnanca prostredníctvom kompromitovaných prihlasovacích údajov.
- Skutočný páchateľ mohol získať citlivé údaje a pokúsiť sa ich odoslať von z organizácie, pričom falošne nasmeroval podozrenie na nevinného zamestnanca.
- Stopy v záznamoch môžu naznačovať manipuláciu s účtom (napr. prihlasovanie z neobvyklých miest alebo používanie nástrojov na vzdialený prístup).

Forenzná analýza získaných dát pomôže určiť, ktorá z hypotéz je najpravdepodobnejšia a aké kroky by mala organizácia podniknúť na ďalšie zabezpečenie svojich systémov.

4. Identifikácia zariadení:

Firemný notebook zamestnanca AlbertE

- **Model:** HP ProBook 450 G9 (6S6J4EA)
- **Operačný systém:** Windows 7
- **Typ úložiska:** NVMe SSD (WD SN530)
- **Parametre:**
 - **Životnosť SSD:** cca 150–300 TBW (Terabytes Written), ~5 rokov pri bežnom používaní



- **Rýchlosť zápisu/čítania:**
 - **Sekvenčné čítanie:** až 3 000 MB/s
 - **Sekvenčný zápis:** až 2 000 MB/s
- **Prístupová doba:** ~0.03 ms (SSD), prakticky okamžitá
- **RAM (predpokladaná):** 8–16 GB DDR4, ~2666 MHz
- **CPU:** Intel Core i5-1235U (6 jadier, 8 vlákien)
- **Forenzná poznámka:**
 - Nízka prístupová doba a vysoké rýchlosti sťažujú zachytenie všetkých operácií v reálnom čase.
 - SSD používajú TRIM – môže ovplyvniť možnosť obnovy zmazaných dát.
 - Obsahuje podozrivú aktivitu, vrátane súborov, logov a sieťovej komunikácie.
 - Mohol byť použitý na prenos citlivých údajov alebo vzdialený prístup.

USB flash drive zamestnanca AlbertE

- **Model:** Transcend JetFlash 700 USB 3.0 32GB
- **Typ pamäte:** NAND Flash
- **Parametre:**
 - **Životnosť:**
 - ~3 000 – 10 000 prepisov na bunku
 - Približne 3–5 rokov pri bežnom používaní
 - **Rýchlosť prenosu:**
 - **Čítanie:** až 90 MB/s
 - **Zápis:** až 25 MB/s
 - **Prístupová doba:** ~1 ms (vyššia ako SSD, ale stále rýchla)
- **Forenzná poznámka:**
 - Zariadenie bolo detegované medzi pripojenými externými médiami v systéme AlbertE
 - Analyzovať pomocou nástrojov ako Autopsy, FTK Imager, USBDeview (Môže obsahovať skopírované citlivé dáta) - možno analyzovať históriu použitia v systéme a súborové metadáta
 - Flash disk môže obsahovať súbory aj po formátovaní.
 - Možnosť ukrytia dát cez *hidden partitions* alebo šifrované kontajnery - môže obsahovať stopy po šifrovaných alebo skrytých súboroch



Firemný notebook zamestnanca Iaman

- **Model:** HP EliteBook 850 G9
- **Operačný systém:** Windows 7
- **Typ úložiska:** NVMe SSD (WD SN740)
- **Parametre:**
 - **Životnosť SSD:** cca 300–600 TBW (vyššia odolnosť, biznis segment)
 - **Rýchlosť zápisu/čítania:**
 - **Sekvenčné čítanie:** až 6 600 MB/s (PCIe Gen4)
 - **Sekvenčný zápis:** až 5 000 MB/s
 - **Prístupová doba:** ~0.03 ms (SSD), prakticky okamžitá
 - **RAM (predpokladaná):** 16–32 GB DDR4, 4800 MHz
 - **CPU:** Intel Core i7-1265U (10 jadier, 12 vlákien)
- **Forenzná poznámka:**
 - Capture RAM neurobené, notebook bol vypnutý
 - Zariadenie bolo identifikované na základe metadát súborov s vlastníctvom viazaným na SID 1000, ktorý sa štandardne viaže na prvý lokálny účet systému
 - Rovnaký SID (1000) sa nachádzal aj v metadátach dokumentu cyberbullying_by_proxy.doc, pochádzajúceho z konta zamestnanca AlbertE
 - Tieto údaje naznačujú možný presun alebo otvorenie dokumentu na inom zariadení, ktorého vlastníkom je Iaman, čím vzniká podozrenie na manipuláciu alebo spolupodielanie sa na prenose dokumentu



USB flash drive zamestnanca Iaman

- **Model:** Kingston DataTraveler Kyson USB 3.2 Gen 1 – 64 GB
- **Typ pamäte:** NAND Flash
- **Parametre:**
 - **Životnosť:**
 - ~3 000 – 10 000 prepisov na bunku
 - 5+ rokov pri strednom používaní
 - **Rýchlosť prenosu:**
 - **Čítanie:** až 200 MB/s
 - **Zápis:** až 60 MB/s
 - **Prístupová doba:** ~0.5 – 1 ms (štandardná pre USB NAND)



- **Forenzná poznámka:**

- Zariadenie bolo identifikované ako osobný majetok podozrivého č. 2 (Iaman)
- Zariadenie bude podrobené ďalšej analýze s cieľom zistiť stopy po súboroch, ktoré súvisia s prešetrovanou udalosťou, ako aj potenciálne vymazané alebo ukryté dáta

5. Zaist'ovanie a zber dát

Zber digitálnych dôkazov prebiehal systematicky s cieľom uchovať integritu dát a zároveň minimalizovať riziko ich znehodnotenia. Forenzný analytik postupoval v súlade s internými postupmi organizácie a metodikou digitálnej forenznej analýzy.

Postup zberu:

1. Zariadenie podozrivého č. 1 – AlbertE (firemný notebook):

- RAM capture bol vykonaný ako prvý krok, kým bol notebook ešte zapnutý, aby bolo možné zachytiť obsah pamäte vrátane potenciálne bežiacich procesov, sieťových relácií a dešifrovaných údajov.

- **Evidenčné číslo: 01**

- Následne bol vytvorený forenzný obraz disku z interného úložiska (NVMe SSD).

- **Evidenčné číslo: 02**

- Po vypnutí zariadenia bol spravený obraz USB flash disku, ktorý bol identifikovaný ako používaný zariadením podozrivého č. 1.

- **Evidenčné číslo: 03**

2. Zariadenie podozrivého č. 2 – Iaman (notebook nadriadeného):

- Dva dni po zbere dát od podozrivého č. 1 bolo rozhodnuté o zaistení ďalších zariadení na základe analýzy získaných dôkazov.
- Notebook podozrivého č. 2 bol v čase zaistenia vypnutý, preto RAM capture nebolo možné vykonať.
- Vytvorený bol forenzný obraz disku.

- **Evidenčné číslo: 04**

- Zároveň bol zaistený aj USB flash disk, patriaci podozrivému č. 2, ktorý mohol obsahovať citlivé firemné dáta.

- **Evidenčné číslo: 05**

Poznámky k integrite dát:

- Všetky obrazy boli vytvorené pomocou nástrojov umožňujúcich zachovanie forenznej integrity, pričom boli následne overené kontrolnými súčtami (MD5 a SHA-1).
- Dáta boli uložené v bezpečnom formáte (E01) a uložené do zabezpečenej databázy prípadu v rámci forenzného nástroja Autopsy.

6. Uchovanie dôkazov

V tomto prípade boli použité štandardné metódy, ktoré zaisťujú integritu dát a ich právnu použiteľnosť.

Postupy pri uchovávaní:

- **Zabezpečenie dôkazov** prebehlo bez zmeny pôvodného systému – použité boli write-blockery a forenzné nástroje na čítanie dát.
- **Hashovanie** (SHA-1 a MD5) bolo použité na overenie integrity získaných dát
- **Zálohovanie dôkazov** do viacerých bezpečných úložísk (offline a šifrované archívy).
- **Katalogizácia dôkazov** v evidenčnom systéme s presným časom, dátumom a osobou, ktorá dôkaz získala.
- **Retenčné pravidlá** boli stanovené na dobu minimálne 5 rokov v súlade s internými politikami a legislatívou.

Nástroje použité na uchovanie:

- FTK Imager - vytváranie bitových kópií.
- EnCase image - formát pri digitálnej forenzike.

Detailný reťazec dôkaznej väzby (chain of custody) je uvedený ďalej v prehľadnej tabuľke.

Tabuľka 1: Chain of custody: Firemný PC zamestnanca AlbertE: RAM

Číslo:	01	Typ súboru:	mem	Obnovený súbor:	nie	Veľkosť:	297,8 MB
Popis prípadu:	Bezpečnostný incident						
Názov súboru:	challenge						
Miesto získania digitálnej stopy:	Firemný PC zamestnanca AlbertE						
Poznámky:	Dump operačnej pamäte (RAM)						
Časové pečiatky							
Access:	May 2,2017 19:02	Modify:	Apr 20, 2025 17:53	Change:	-		
Digitálny odtlačok (heš)	MD5	a77a5e8833e124067abfcf5d46e0e8d6					
	SHA1	3d52e7d1331af0e7016877798bdc b2be4eeb834e					
Časová pečiatka	Akcia vykonaná s digitálnou stopou						
May 2, 2017	Vytvorené 3 kópie digitálnej stopy						
May 2, 2017	Analýza digitálnej stopy pomocou nástroja Autopsy						
Apr 20, 2025 20:57	Kontrola zhody digitálnych otláčkov, MD5 a SHA 1 súhlasia						
<pre>matik@matik-book: \$ sha1sum /home/matik/Dokumenty/skola/Digitalna_forenzna_analyza/Case2/dfrws2008-challenge/response_data/challenge.mem 3d52e7d1331af0e7016877798bdc b2be4eeb834e /home/matik/Dokumenty/skola/Digitalna_forenzna_analyza/Case2/dfrws2008-challenge/response_data/challenge.mem matik@matik-book: \$ md5sum /home/matik/Dokumenty/skola/Digitalna_forenzna_analyza/Case2/dfrws2008-challenge/response_data/challenge.mem a77a5e8833e124067abfcf5d46e0e8d6 /home/matik/Dokumenty/skola/Digitalna_forenzna_analyza/Case2/dfrws2008-challenge/response_data/challenge.mem matik@matik-book: - \$</pre>							

Listing

challenge.mem_519 Host

TableThumbnailSummary

Name	Type	Size (Byt...	Sector Size (Bytes)	Timezone	
 challenge.mem	Image	297795584	512	Europe/Bratislava	06c6aa8c-ace7-4121-95f1-132048015faf

Data Content

HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther

Metadata

Name: /img_challenge.mem

Type: Raw Single

Size: 297795584

MD5: a77a5e8833e124067abfcf5d46e0e8d6

SHA1: 3d52e7d1331af0e7016877798bdc b2be4eeb834e

Tabuľka 2: Chain of custody: Firemný PC zamestnanca AlbertE

Číslo:	02	Typ súboru:	E01	Obnovený súbor:	nie	Veľkosť:	500 MB												
Popis prípadu:	Bezpečnostný incident																		
Názov súboru:	NTFS Pract 2017																		
Miesto získania digitálnej stopy:	Firemný PC zamestnanca AlbertE																		
Poznámky:	Podozrivá sieťová činnosť																		
Časové pečiatky																			
Access:	May 2, 2017 19:14	Modify:	Apr 20, 2025 17:53	Change:	-														
Digitálny odtlačok (heš)	MD5	eb4393cfcc4fca856e0edbf772b2aa7d																	
	SHA1	094123df4792b18a1f0f64f1e2fc609028695f85																	
Časová pečiatka	Akcia vykonaná s digitálnou stopou																		
May 2, 2017	Vytvorené 3 kópie digitálnej stopy																		
May 2, 2017	Analýza digitálnej stopy pomocou nástroja Autopsy																		
Apr 20, 2025 17:53:53	Export obrazu disku .E01 do .raw, pre účel kontroly zhody digitálnych otláčkov																		
Apr 20, 2025 17:53:55	Export ukončený, MD5 a SHA 1 súhlasia																		
Export started at: Apr 20, 2025 17:53:53 This could take a while. Export completed at: Apr 20, 2025 17:53:55 Written: 500 MiB (524288000 bytes) in 2 second(s) with 250 MiB/s (262144000 bytes/second). MD5 hash calculated over data: eb4393cfcc4fca856e0edbf772b2aa7d ewfexport: SUCCESS <pre>matik@matik-book:~\$ sha1sum /home/matik/Dokumenty/škola/Digitalna_forenzna_analyza/Case2/NTFS_Pract_2017_E01/NTFS_Pract_2017/NTFS_Pract_2017.raw 094123df4792b18a1f0f64f1e2fc609028695f85 /home/matik/Dokumenty/škola/Digitalna_forenzna_analyza/Case2/NTFS_Pract_2017_E01/NTFS_Pract_2017/NTFS_Pract_2017.raw matik@matik-book:~\$</pre>																			
<table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Size (Bytes)</th> <th>Sector Size (Bytes)</th> <th>Timezone</th> <th></th> </tr> </thead> <tbody> <tr> <td> NTFS_Pract_2017.E01</td> <td>Image</td> <td>524288000</td> <td>512</td> <td>Europe/Bratislava</td> <td>5b89e60c-ef7c-464b-9ec0-2872508fb3e5</td> </tr> </tbody> </table>								Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone		 NTFS_Pract_2017.E01	Image	524288000	512	Europe/Bratislava	5b89e60c-ef7c-464b-9ec0-2872508fb3e5
Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone															
 NTFS_Pract_2017.E01	Image	524288000	512	Europe/Bratislava	5b89e60c-ef7c-464b-9ec0-2872508fb3e5														
Data Content Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences Metadata Name: /img_NTFS_Pract_2017.E01 Type: E01 Size: 524288000 MD5: eb4393cfcc4fca856e0edbf772b2aa7d SHA1: Not calculated																			

Tabul'ka 3: Chain of custody: USB flash drive zamestnanca AlbertE

Číslo:	03	Typ súboru:	E01	Obnovený súbor:	nie	Veľkosť:	3,7 GB												
Popis prípadu:	Bezpečnostný incident																		
Názov súboru:	cfreds_2015_data_leakage_rm#2																		
Miesto získania digitálnej stopy:	USB flash drive zamestnanca AlbertE																		
Poznámky:	Podozrivá sieťová činnosť																		
Časové pečiatky																			
Access:	May 2,2017 19:27	Modify:	Apr 20, 2025 18:01	Change:	-														
Digitálny odtlačok (heš)	MD5	b4644902acab4583a1d0f9f1a08faa77																	
	SHA1	048961a85ca3eced8cc73f1517442d31d4dca0a3																	
Časová pečiatka	Akcia vykonaná s digitálnou stopou																		
May 2, 2017	Vytvorené 3 kópie digitálnej stopy																		
May 2, 2017	Analýza digitálnej stopy pomocou nástroja Autopsy																		
Apr 20, 2025 18:17:44	Export obrazu disku .E01 do .raw, pre účel kontroly súčtov MD5 a SHA1																		
Apr 20, 2025 18:18:04	Export ukončený, MD5 a SHA 1 súhlasia																		
Export completed at: Apr 20, 2025 18:18:04 Written: 3.7 GiB (4004511744 bytes) in 20 second(s) with 190 MiB/s (200225587 bytes/second). MD5 hash calculated over data: b4644902acab4583a1d0f9f1a08faa77 ewfexport: SUCCESS matik@matik-book: \$ sha1sum /home/matik/Dokumenty/škola/Digitalna_forenzna_analyza/Case2/DFA_dataset/cfreds_2015_data_leakage_rm#2.raw 048961a85ca3eced8cc73f1517442d31d4dca0a3 /home/matik/Dokumenty/škola/Digitalna_forenzna_analyza/Case2/DFA_dataset/cfreds_2015_data_leakage_rm#2.raw matik@matik-book: \$																			
<table><tr><th>Name</th><th>Type</th><th>Size (Bytes)</th><th>Sector Size (Bytes)</th><th>Timezone</th><th></th></tr><tr><td> cfreds_2015_data_leakage_rm#2.E01</td><td>Image</td><td>4004511744</td><td>512</td><td>Europe/Bratislava</td><td>ec83d36a-9ad1-48e0-b842-07b6a9832606</td></tr></table>								Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone		 cfreds_2015_data_leakage_rm#2.E01	Image	4004511744	512	Europe/Bratislava	ec83d36a-9ad1-48e0-b842-07b6a9832606
Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone															
 cfreds_2015_data_leakage_rm#2.E01	Image	4004511744	512	Europe/Bratislava	ec83d36a-9ad1-48e0-b842-07b6a9832606														
Data Content <table><tr><td>Hex</td><td>Text</td><td>Application</td><td>File Metadata</td><td>OS Account</td><td>Data Artifacts</td><td>Analysis Results</td><td>Context</td><td>Annotations</td><td>Other Occurrences</td></tr></table> Metadata Name: /img_cfreds_2015_data_leakage_rm#2.E01 Type: E01 Size: 4004511744 MD5: b4644902acab4583a1d0f9f1a08faa77 SHA1: 048961a85ca3eced8cc73f1517442d31d4dca0a3								Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences		
Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences										

Tabuľka 4: Chain of custody: Firemný PC zamestnanca Iaman

Číslo:	04	Typ súboru:	E01	Obnovený súbor:	nie	Veľkosť:	20 GB												
Popis prípadu:	Bezpečnostný incident																		
Názov súboru:	cfreds_2015_data_leakage_pc																		
Miesto získania digitálnej stopy:	Firemný PC zamestnanca Iaman																		
Poznámky:	Podozrivý z predaja firemných dát konkurencii																		
Časové pečiatky																			
Access:	May 4, 2017 16:52	Modify:	Apr 20, 2025 17:20	Change:	-														
Digitálny odtlačok (heš)	MD5	a49d1254c873808c58e6f1bcd60b5bde																	
	SHA1	afe5c9ab487bd47a8a9856b1371c2384d44fd785																	
Časová pečiatka	Akcia vykonaná s digitálnou stopou																		
May 4, 2017	Vytvorené 3 kópie digitálnej stopy																		
May 4, 2017	Analýza digitálnej stopy pomocou nástroja Autopsy																		
Apr 20, 2025 17:20:25	Export obrazu disku .E01 do .raw, pre účel kontroly súčtov MD5 a SHA1																		
Apr 20, 2025 17:23:25	Export ukončený, MD5 a SHA 1 súhlasia																		
Export completed at: Apr 20, 2025 17:23:25 Written: 20 GiB (21474836480 bytes) in 3 minute(s) and 0 second(s) with 113 MiB/s (119304647 bytes/second). MD5 hash calculated over data: a49d1254c873808c58e6f1bcd60b5bde ewfexport: SUCCESS matik@matik-book: \$ sha1sum /home/matik/Dokumenty/skola/Digitalna_forenzna_analyza/Case2/DFA_dataset/cfreds_2015_data_leakage_pc.raw afe5c9ab487bd47a8a9856b1371c2384d44fd785 /home/matik/Dokumenty/skola/Digitalna_forenzna_analyza/Case2/DFA_dataset/cfreds_2015_data_leakage_pc.raw matik@matik-book: \$																			
<table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Size (Bytes)</th> <th>Sector Size (Bytes)</th> <th>Timezone</th> <th></th> </tr> </thead> <tbody> <tr> <td> cfreds_2015_data_leakage_pc.E01</td> <td>Image</td> <td>21474836480</td> <td>512</td> <td>Europe/Bratislava</td> <td>6361258b-746f-4d45-ac9d-2053986ccb35</td> </tr> </tbody> </table>								Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone		 cfreds_2015_data_leakage_pc.E01	Image	21474836480	512	Europe/Bratislava	6361258b-746f-4d45-ac9d-2053986ccb35
Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone															
 cfreds_2015_data_leakage_pc.E01	Image	21474836480	512	Europe/Bratislava	6361258b-746f-4d45-ac9d-2053986ccb35														
Data Content Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences Metadata Name: /img_cfreds_2015_data_leakage_pc.E01 Type: E01 Size: 21474836480 MD5: a49d1254c873808c58e6f1bcd60b5bde SHA1: afe5c9ab487bd47a8a9856b1371c2384d44fd785																			

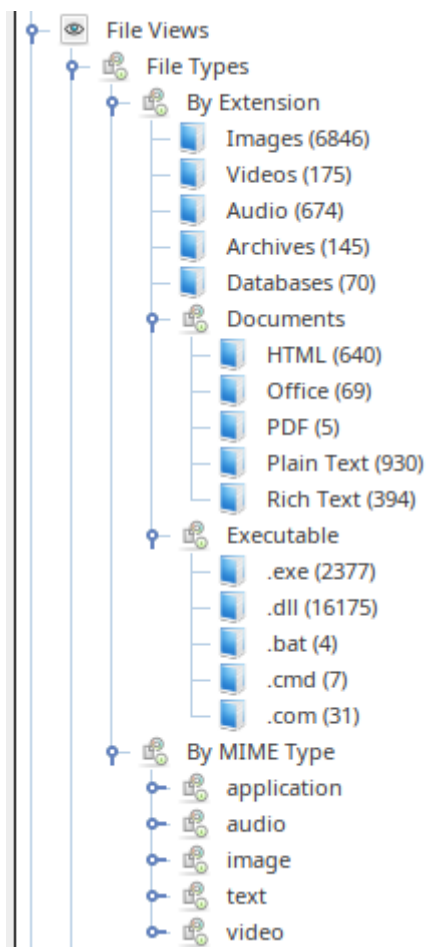
Tabul'ka 5: Chain of custody: USB flash drive zamestnanca Iaman

Číslo:	05	Typ súboru:	E01	Obnovený súbor:	nie	Veľkosť:	3,7 GB												
Popis prípadu:	Bezpečnostný incident																		
Názov súboru:	cfreds_2015_data_leakage_pc																		
Miesto získania digitálnej stopy:	USB flash drive zamestnanca Iaman																		
Poznámky:																			
Časové pečiatky																			
Access:	May 4, 2017 16:59	Modify:	Apr 20, 2025 18:01	Change:															
Digitálny odtlačok (heš)	MD5	8bfa4230bf4e35db966b8c1a9321a0b1																	
	SHA1	f6bb840e98dd7c325af45539313fc3978fff812c																	
Časová pečiatka	Akcia vykonaná s digitálnou stopou																		
May 4, 2017	Vytvorené 3 kópie digitálnej stopy																		
May 4, 2017	Analýza digitálnej stopy pomocou nástroja Autopsy																		
Apr 20, 2025 18:01:29	Export obrazu disku .E01 do .raw, pre účel kontroly súčtov MD5 a SHA1																		
Apr 20, 2025 18:01:50	Export ukončený, MD5 a SHA 1 súhlasia																		
Export completed at: Apr 20, 2025 18:01:50																			
Written: 3.7 GiB (4004511744 bytes) in 21 second(s) with 181 MiB/s (190691035 bytes/second). MD5 hash calculated over data: 8bfa4230bf4e35db966b8c1a9321a0b1 ewfexport: SUCCESS matik@matik-book: \$ sha1sum /home/matik/Dokumenty/škola/Digitalna_forenzna_analyza/Case2/DFA_dataset/cfreds_2015_data_leakage_rm#1.raw f6bb840e98dd7c325af45539313fc3978fff812c /home/matik/Dokumenty/škola/Digitalna_forenzna_analyza/Case2/DFA_dataset/cfreds_2015_data_leakage_rm#1.raw matik@matik-book: \$																			
<table><tr><th>Name</th><th>Type</th><th>Size (Bytes)</th><th>Sector Size (Bytes)</th><th>Timezone</th><th></th></tr><tr><td> cfreds_2015_data_leakage_rm#1.E01</td><td>Image</td><td>4004511744</td><td>512</td><td>Europe/Bratislava</td><td>7b985dec-8bf2-413f-b8c7-f932cc8b6079</td></tr></table>								Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone		 cfreds_2015_data_leakage_rm#1.E01	Image	4004511744	512	Europe/Bratislava	7b985dec-8bf2-413f-b8c7-f932cc8b6079
Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone															
 cfreds_2015_data_leakage_rm#1.E01	Image	4004511744	512	Europe/Bratislava	7b985dec-8bf2-413f-b8c7-f932cc8b6079														
Data Content																			
<table><tr><th>Hex</th><th>Text</th><th>Application</th><th>File Metadata</th><th>OS Account</th><th>Data Artifacts</th><th>Analysis Results</th><th>Context</th><th>Annotations</th><th>Other Occurrences</th></tr></table>								Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences		
Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences										
Metadata																			
Name: /img_cfreds_2015_data_leakage_rm#1.E01																			
Type: E01																			
Size: 4004511744																			
MD5: 8bfa4230bf4e35db966b8c1a9321a0b1																			
SHA1: f6bb840e98dd7c325af45539313fc3978fff812c																			

7. Analýza

Všetky zozbierané dáta boli analyzované pomocou forenzného programu Autopsy.

Hierarchia analyzovaných dát v Autopsy:



1. Analýza dôkazového materiálu č. 01

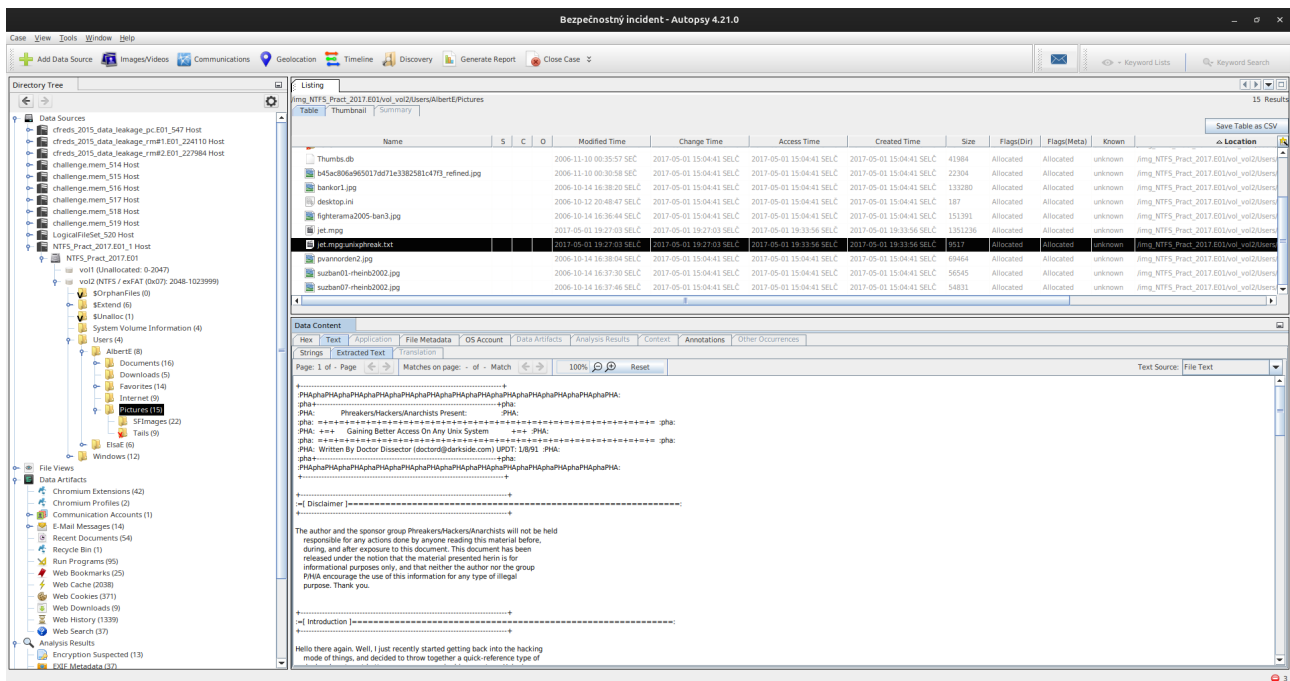
Analýza RAM nepotvrdila žiadne neoprávnené aktivity.

2. Analýza dôkazového materiálu č. 02

- Podorivý súbor **jet.mpg:unixphreak.txt**:

Textový dokument podrobne popisuje techniky, ako získať vyššie oprávnenia (napr. root) na Unixových systémoch:

- Manipulácia s prístupovými právami a cron jobmi
- Použitie SUID bitov
- Vytváranie trojanov
- Čítanie terminálov iných používateľov
- Použitie bežných bináriek na eskaláciu práv



Obrázok 1: jet.mpg:unixphreak.txt

Text je podpísaný skupinou „Phreakers/Hackers/Anarchists“ a autorom „Doctor Dissector“. To sú pseudonymy typické pre underground scénu z 90. rokov.

Je tu aj zmienka o „PHRACK“ — známy undergroundový hackerský e-zin, ktorý často obsahoval technické návody a exploitové popisy.

Aj keď text pochádza z roku 1991, niektoré princípy môžu stále platiť na zle zabezpečených alebo starších systémoch. Môže byť použitý ako návod útočníkom, ale aj ako súčasť vzdelávania.

Vzhľadom na to, že sa nachádza na bežnom používateľskom počítači bez kontextu, je podozrivý. Je uložený v priečinku Pictures používateľa AlbertE, čo je veľmi netypické miesto pre textový dokument s návodom na hackovanie. Môže indikovať prítomnosť útočníka, testera, alebo niekoho so záujmom o neautorizovaný prístup.

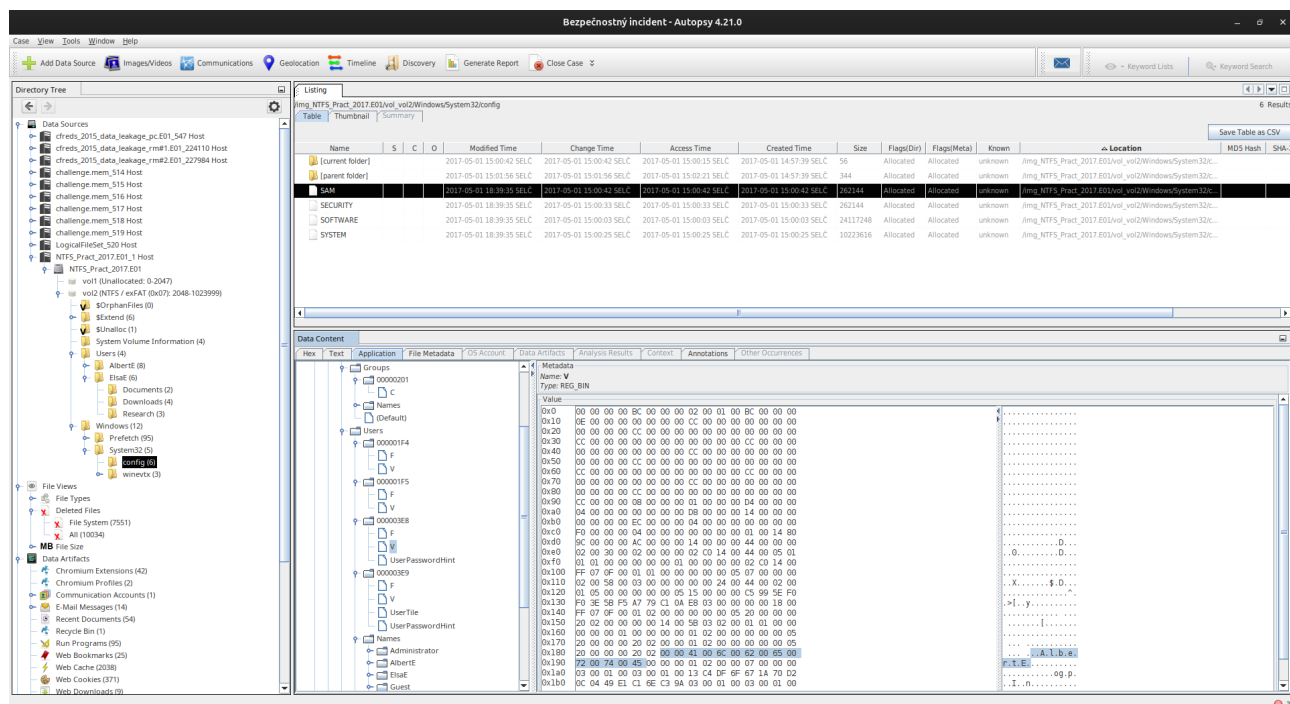
Súbor je uložený ako Alternate Data Stream (ADS) v NTFS k hlavnému súboru jet.mpg. ADS je špecifická vlastnosť NTFS súborového systému, kde môže byť pridaný „neviditeľný“ obsah k bežnému súboru. Takéto streamy nie sú bežne viditeľné vo Windows Exploreri ani pri klasickom prehľade obsahu adresára. To je technika, ktorá sa často využíva na skrývanie podozrivých súborov – vrátane malvéru alebo hackerských nástrojov. Vyzerá to, že niekto zámerne skryl textový súbor ako alternatívny dátový stream v .mpg súbore, pravdepodobne kvôli zakrytiu pred bežným antivírusom alebo používateľom v snahe ukryť nevhodný alebo potenciálne nelegálny obsah.

Časové známky:

- **Vytvorené:** 2017-05-01 19:33:56
- **Modifikované:** 2017-05-01 19:27:03
- **Prístup:** 2017-05-01 19:33:56

Prístup a vytvorenie sú tesne po sebe, čo značí, že súbor bol skopírovaný alebo importovaný z iného systému.

Z metadát sa zistilo, že SID končí na 1004, čo značí iného používateľa ako predtým (AlbertE má SID končiaci na 1000). To môže znamenať, že bol otvorený/uložený iným používateľom (napr. cez iný účet), alebo pôvodne vytvorený mimo aktuálneho profilu.



Obrázok 2: Výpis z databázy SAM

Na základe toho výpisu môžeme presne priradiť SIDy k používateľom:

AlbertE: SID: S-1-5-21-4032731589-4116397808-180451751-1000
(Nachádza sa pri položke AlbertE a 000003E8, čo je hexadecimálne 1000)

ElsaE: SID: S-1-5-21-4032731589-4116397808-180451751-1001
(Priradené k ElsaE a 000003E9 → 1001)

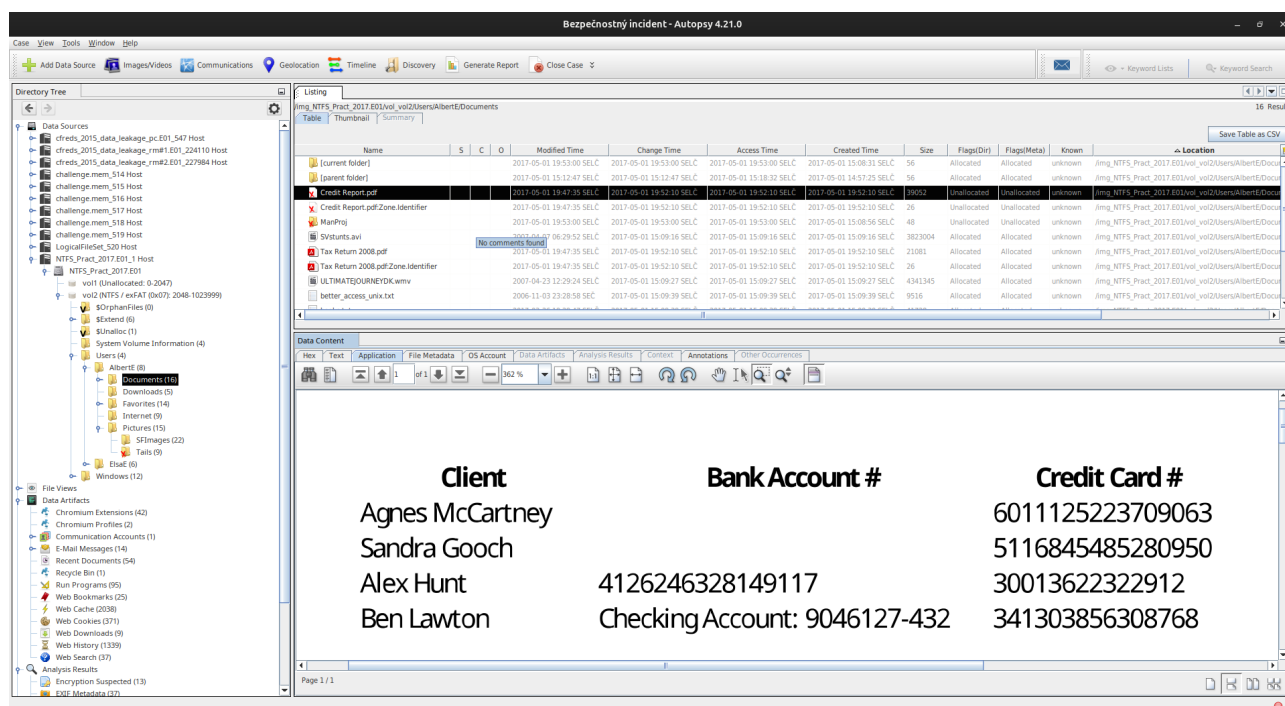
Vo výpise sa nenašla priama asociácia s -1004, tzn., že buď nepatrí bežnému používateľovi, ale ide o účet mimo štandardného zoznamu (napr. zmazaný, doménový účet, testovací profil, atď.) alebo bol zmazaný pred extrakciou, takže v SAM databáze už nie je, ale jeho SID mohol zostať pri súboroch alebo v metadátach. SID -1004 môže patriť niekomu z IT oddelenia, ak šlo o dočasné konto.

- Podorivý súbor **Credit Report.pdf**:

Toto je pravdepodobne starý výpis osobných alebo finančných údajov, vzhľad textu a formátovania nasvedčuje, že šlo o export z Excelu do PDF. Pravdepodobne bol získaný bez vedomia dotknutých osôb. Ide o veľmi vážny únik alebo nelegálne získanie dát.

Obsahuje:

- Údaje osôb – plné mená ako *Agnes McCartney, Sandra Gooch, Alex Hunt,...*
- Citlivé finančné údaje:
 - Čísla kreditných kariet (napr. 6011..., 5116..., 4126...)
 - Číslo bankového účtu (napr. 9046127-432)



Obrázok 3: Credit Report.pdf

Časové známky:

- **Vytvorené:** 2017-05-01 19:52:10
- **Modifikované:** 2017-05-01 19:47:35
- **Prístup:** 2017-05-01 19:52:10

Prístup a vytvorenie sú tesne po sebe, čo značí, že súbor bol skopírovaný alebo importovaný z iného systému, následne uložený alebo skopírovaný do priečinka používateľa *AlbertE*.

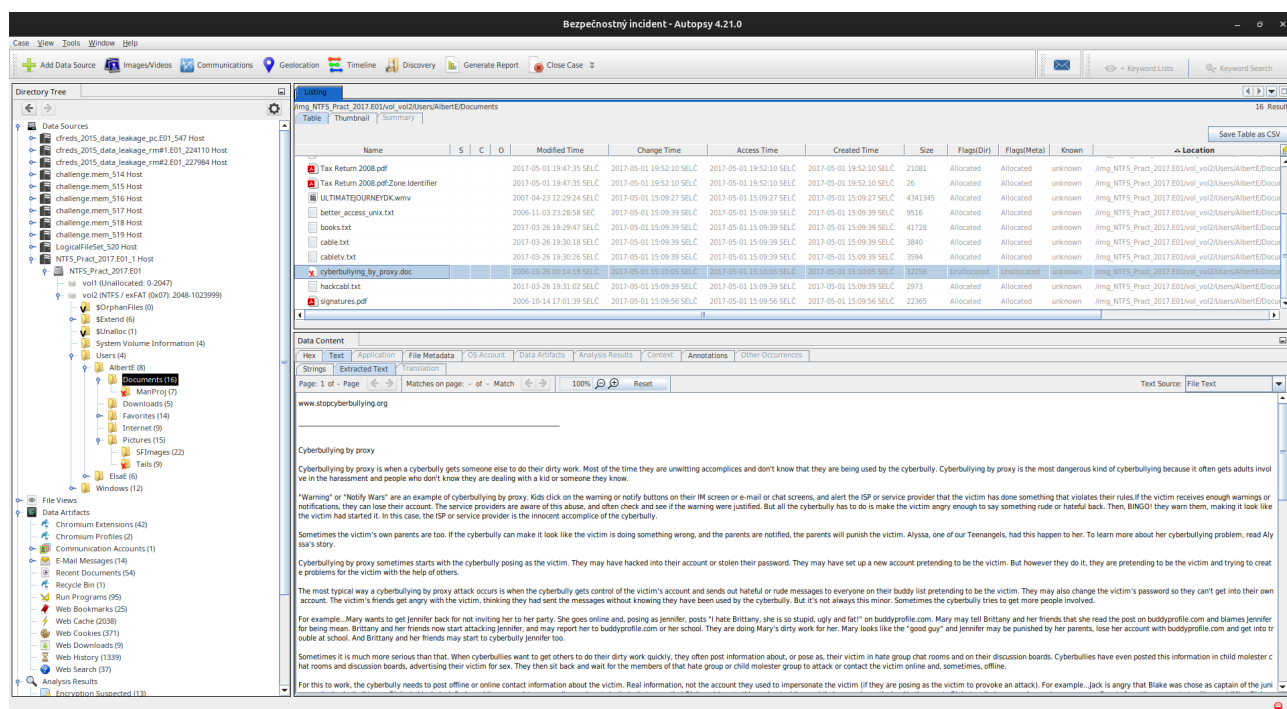
Súbor je nealokovaný, teda používateľ alebo systém ho zmazal, možno na zakrytie stôp.

Zone.Identifier je NTFS Alternate Data Stream, ktorý Windows pridáva k súborom stiahnutým z netu/emailu.

- Podorivý súbor **cyberbullying_by_proxy.doc**:

Článok z webu www.stopcyberbullying.org vysvetľuje mechanizmy a nebezpečenstvá tzv. "kyberšikany prostredníctvom tretích osôb". Popisuje praktiky ako:

- Falošné identifikovanie sa ako obeť.
- Získanie hesiel, kontrola nad účtami.
- Využitie cudzích osôb (vrátane rodičov, ISP, či dokonca pedofilných fór alebo extrémistických skupín) na útok voči obeti.
- Uvádzanie reálnych kontaktných údajov obete za účelom vyvolania útoku.



Obrázok 4: *cyberbullying_by_proxy.doc*

Tento dokument sám o sebe nie je dôkazom trestného činu, ale jeho prítomnosť medzi zmazanými súbormi (indikátor vedomého odstraňovania) a fakt, že je v kontexte ďalších podozrivých dokumentov a osobných údajov ho robí relevantným pre vyšetrovanie.

Súbor bol vytvorený alebo obnovený do image až v máji 2017, ale jeho reálna posledná editácia prebehla v októbri 2006. Rozpor medzi dátumami (1995–2006 vs. 2017) naznačuje, že dokument bol pravdepodobne stiahnutý z webového archívu, získaný cez torrent alebo iné p2p alebo bol súčasťou balíka dokumentov používaných pri kybernetických útokoch (napr. manuály, návody).

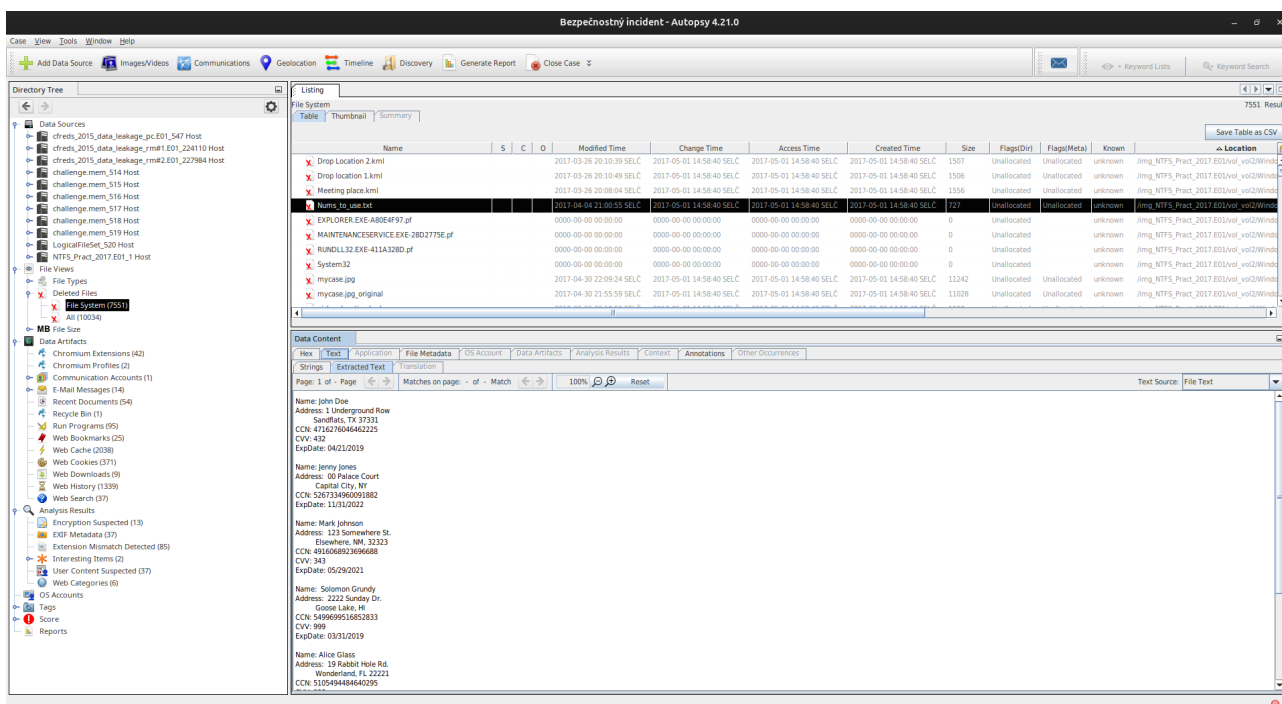
Súbor bol vymazaný alebo inak neprístupný cez bežný súborový systém. Silný znak, že niekto chcel dokument odstrániť – možno kvôli obsahu.

Metadáta ukazujú, že SID pre tento súbor je 0, patrí systémovým procesom ako SYSTEM, LOCAL SERVICE, atď., nie bežným používateľom. Naznačuje, že súbor bol buď zmazaný používateľom, ktorý už v systéme neexistuje (profil bol odstránený), alebo bol vytvorený mimo Windows.

- Podorivý súbor **Nums_to_use.txt**:

Súbor obsahuje citlivé údaje:

- Celé mená osôb
- Adresy
- Čísla kreditných kariet (CCN – Credit Card Number)
- CVV kódy
- Dátumy expirácie kariet



Obrázok 5: Nums_to_use.txt

Citlivé údaje nemajú byť uložené v nezašifrovanej forme nikde v systéme, a už vôbec nie v bežných logoch alebo dokumentoch. Vyzerá to ako výpis z databázy alebo zachytené dáta, ktoré boli nelegálne získané (napr. prostredníctvom keyloggeru, malware-u, alebo kompromitovanej webovej aplikácie). Niektoré z týchto kariet (napr. MasterCard/Discover/Visa) zodpovedajú reálnym BIN rozsahom, aj keď expirácie sú už minulé, čo naznačuje, že ide o únik alebo zber citlivých údajov.

Tento nález veľmi pravdepodobne potvrdzuje, že počítač bol kompromitovaný, používaný na uchovávanie alebo prenos odcudzených dát alebo na ňom prebiehala činnosť súvisiaca s kybernetickou kriminalitou (napr. phishing, carding).

Podobne ako v predchádzajúcom prípade, aj tu metadáta ukazujú, že SID pre tento súbor je 0, čo len potvrdzuje hypotézu, že účet mohol byť kompromitovaný.

3. Analýza dôkazového materiálu č. 03

Analýza USB flash drive patriaceho AlbertoviE nepotvrdila žiadne neoprávnené aktivity.

Zhodnotenie dôkazového materiálu č. 02 vo vzťahu k hypotézam vyšetrovania

- **Hypotéza 1:** *Zamestnanec vedome spolupracoval s externou stranou na odcudzení údajov.*

Podporené dôkazmi:

- **jet.mpg:unixphreak.txt** – Dokument popisuje techniky eskalácie oprávnení, skrývania prítomnosti a manipulácie s právami v Unix systémoch. Je ukrytý v Alternate Data Stream, čo naznačuje vedomé úsilie o utajenie. Použitie ADS je typické pre pokročilých používateľov alebo útočníkov.
- **Credit Report.pdf + Nums_to_use.txt** – Obe obsahujú veľmi citlivé údaje (finančné, osobné) a sú nealokované, teda zmazané. To môže indikovať snahu o zahľadanie stôp.
- **cyberbullying_by_proxy.doc** – Aj keď sám o sebe nie je nezákonný, jeho obsah a kontext (zmazaný stav, starý pôvod, umiestnenie) naznačuje záujem o manipuláciu alebo zneužitie tretích strán – čo môže byť formou útoku.
- **Časové známky** naznačujú, že všetky súbory boli skopírované alebo importované z externého zdroja, nie vytvorené priamo používateľom. To môže podporovať verziu o prenose dát z iného zariadenia alebo systému.

Záver: Táto hypotéza je **silno podporená** – najmä kombináciou skrývania obsahu (ADS), citlivých údajov, snahy o zahľadanie stôp a povahy dokumentov. Znaky vedomej prípravy na kybernetické aktivity a možného úniku dát sú výrazné.

- **Hypotéza 2:** *Podozrivá aktivita bola spôsobená neúmyselným správaním alebo nesprávnym vyhodnotením dôkazov.*

Čiastočne podporené, ale slabé:

- **Prítomnosť starších dokumentov** (napr. článok z 2006, hackerský manuál z 1991) by teoreticky mohla byť výsledkom sťahovania archívnych materiálov na študijné účely.
- **cyberbullying_by_proxy.doc** je verejne dostupný dokument, čo by mohlo byť legitímne.
- Možnosť, že niektoré súbory boli náhodne zachytené alebo importované zo zálohovaných USB, torrentov alebo archívnych stránok.

Ale:

- Skutočnosť, že sú uložené v ADS alebo zmazané, spolu s obsahom dokumentov, naznačuje úmyselné skrytie alebo zahľadanie stôp. Tieto techniky nie sú typické pre bežného používateľa.
- Súbor **Nums_to_use.txt** s plnými CC údajmi nie je možné vysvetliť ako náhodné sťahovanie – ide o extrémne citlivé dáta, ktoré bežný používateľ nemá dôvod vlastniť.

Záver: Táto hypotéza je **málo pravdepodobná**. Dôkazy ukazujú na úmyselné konanie.

- **Hypotéza 3:** *Účet zamestnanca bol kompromitovaný a využitý inou osobou na neoprávnené aktivity.*

Čiastočne podporené:

- **SID 1004** pri unixphreak.txt sa líši od bežného SID zamestnanca AlbertE (1000), čo by mohlo naznačovať, že dokument bol vytvorený alebo otvorený iným účtom.
- Tento fakt naznačuje možnosť využitia iného účtu (alebo kompromitácie systému).
- Zmazané súbory a nealokované dáta môžu byť výsledkom činnosti niekoho, kto sa snažil zahľadiť stopy po použití účtu.

Avšak:

- Väčšina aktivít a súborov bola zaznamenaná v profilovej štruktúre používateľa AlbertE, čo naznačuje aspoň fyzický prístup k jeho účtu/zariadeniu.
- Zatiaľ nie sú priame dôkazy o vzdialenom prístupe.

Záver: Táto hypotéza **nie je vylúčená** a je **možná ako alternatívne vysvetlenie**, no momentálne chýbajú kľúčové technické dôkazy (logy, sieťové záznamy, indikácie vzdialeného prístupu), ktoré by ju podporili ako hlavný scenár.

Forenzné rozšírenie vyšetrovania – odôvodnenie zabavenia zariadenia Iamana

Počas analýzy dôkazového materiálu č. 02, konkrétne pri skúmaní metadát podozrivého súboru jet.mpg:unixphreak.txt, bol identifikovaný SID s koncovkou -1004. Tento SID sa nezhodoval so známym SID používateľa AlbertE (...-1000), a teda naznačoval, že k súboru mohol mať prístup iný používateľ.

Zistenie odlišného SID vyvolalo hypotézu, že k manipulácii s podozrivým obsahom mohlo dôjsť zo strany iného lokálneho účtu – prípadne prostredníctvom dočasného prihlásenia správcu alebo technika z oddelenia IT. Vzhľadom na túto možnosť, a na fakt, že k dokumentu bol prístup z účtu mimo bežného používateľa systému, sa forenzní analytici zamerali na overenie, či sa nejedná o internú infiltráciu.

Na základe tejto hypotézy bol identifikovaný technik Iaman z interného IT oddelenia ako možný vlastník účtu so SID ...-1004. Jeho zariadenie (notebook), ktoré dovtedy nebolo predmetom analýzy, bolo preto následne zaistené.

4. Analýza dôkazového materiálu č. 04

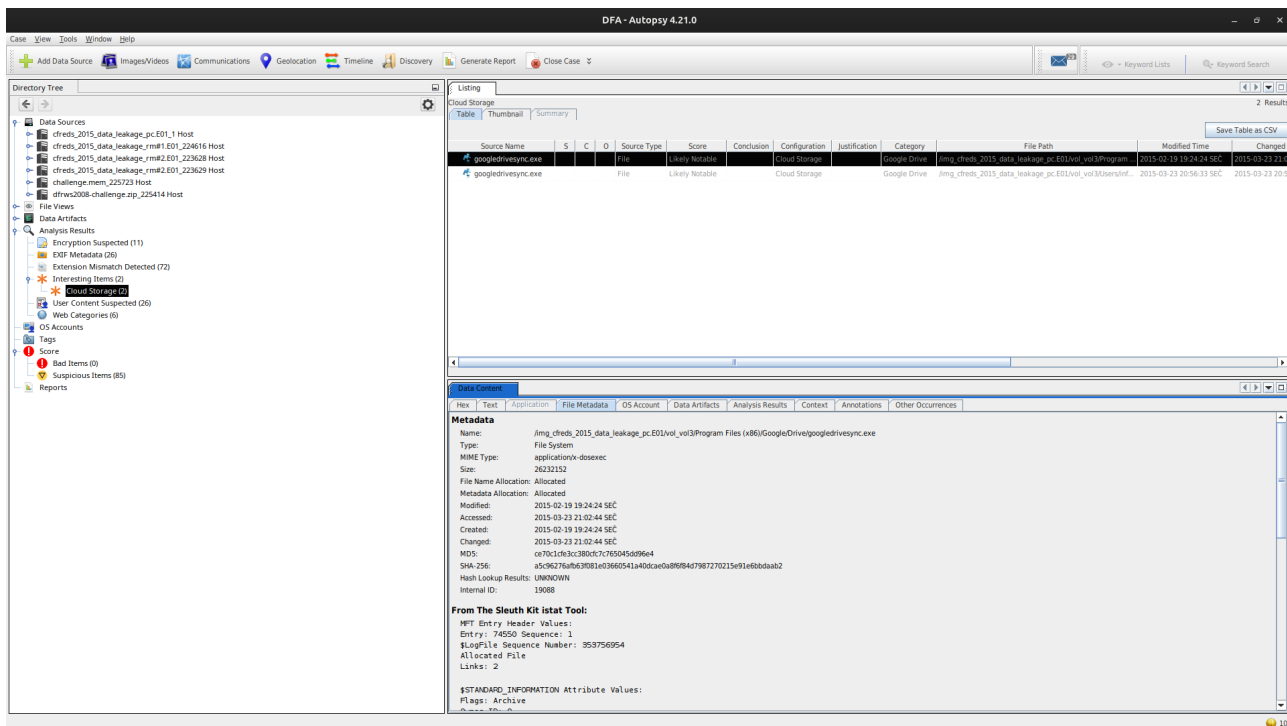
- Exfiltrácia dát cez Google Drive:

Používateľ „informant“ stiahol súbor **googledrivesync.exe** do priečinka Downloads.

Časové známky:

- **Vytvorené:** 2015-03-23 20:56:30
- **Modifikované:** 2015-03-23 20:56:31-33
- **Prístup:** 2015-03-23 20:56:30

Všetky časové značky sú veľmi blízko pri sebe, čo je typické pre novo stiahnutý súbor, ktorý ešte nebol aktívne spúšťaný ani modifikovaný.



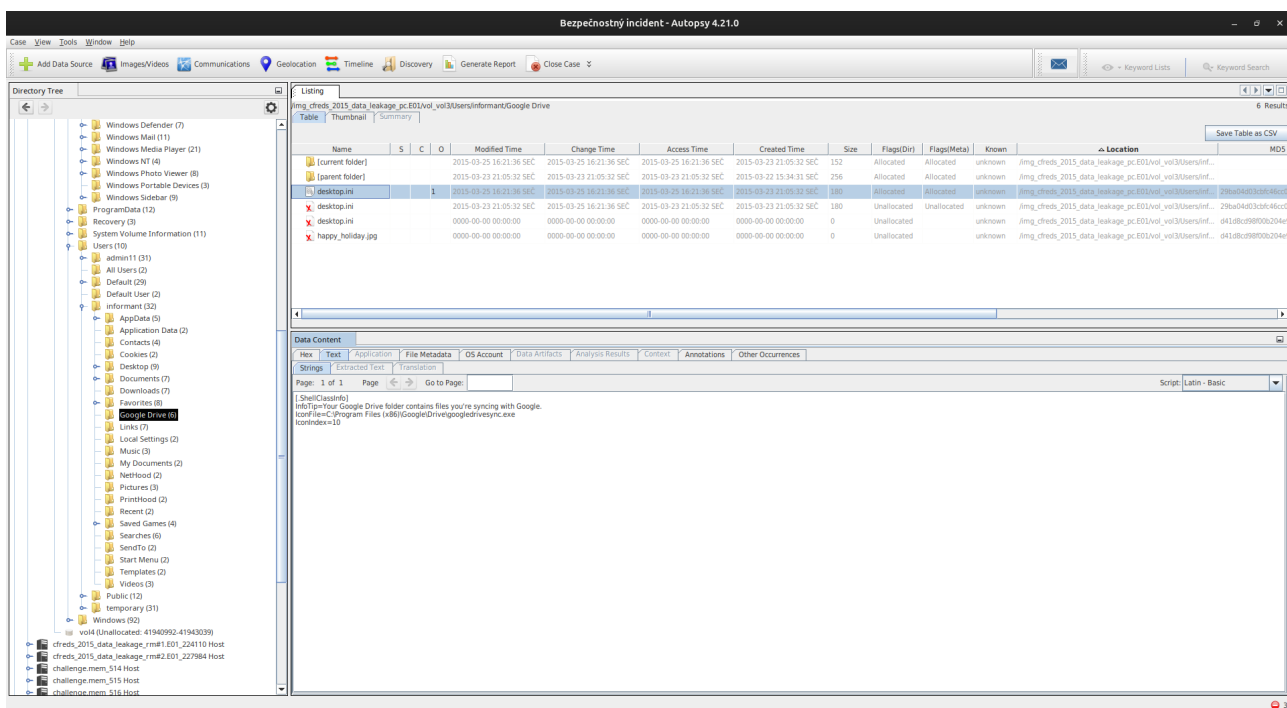
Obrázok 6: googledrivesync.exe

Tento nástroj môže slúžiť na prístup k externému úložisku, synchronizáciu lokálnych dokumentov s cloudom alebo prenášanie súborov mimo organizácie.

V kontexte vyšetrovania je tento nástroj potenciálne rizikový kanál.

Súbor **desktop.ini** konfiguruje vzhľad a chovanie priečinka vo Windows. V tomto prípade ide o priečinok synchronizovaný s Google Drive:

C:\Program Files (x86)\Google\Drive\googledrivesync.exe

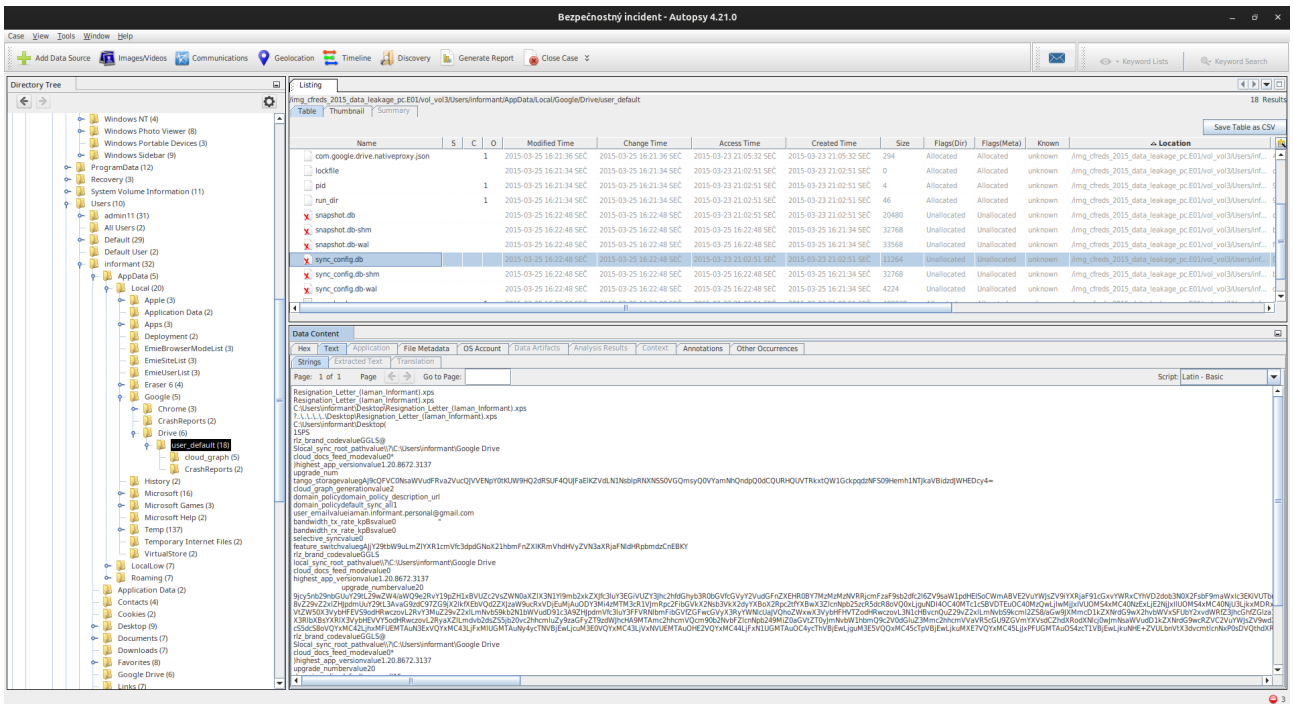


Obrázok 7: desktop.ini

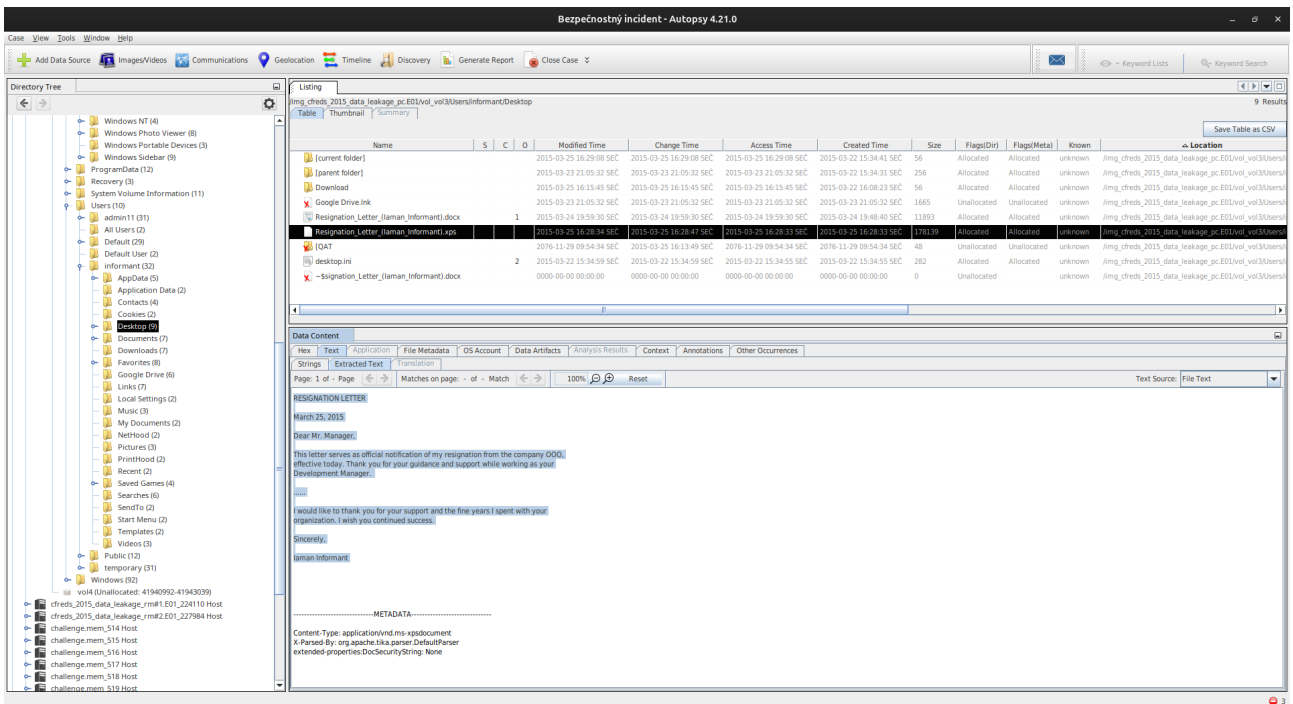
Znamená to, že Google Drive bol nie len stiahnutý, ale aj nainštalovaný. Používateľ pravdepodobne nastavil synchronizáciu s konkrétnym cloudovým účtom.

Súbory umiestnené v tomto priečinku sa automaticky nahrávali do Google Drive účtu, s ktorým bol klient spárovaný. Ak tam boli napr. interné dokumenty, mohli byť odovzdané na externý účet, ktorý nemusí byť pod správou firmy.

Analýza súboru **sync_config.db** viedla k súboru **Resignation_Letter_(Iaman_Informant).xps**.



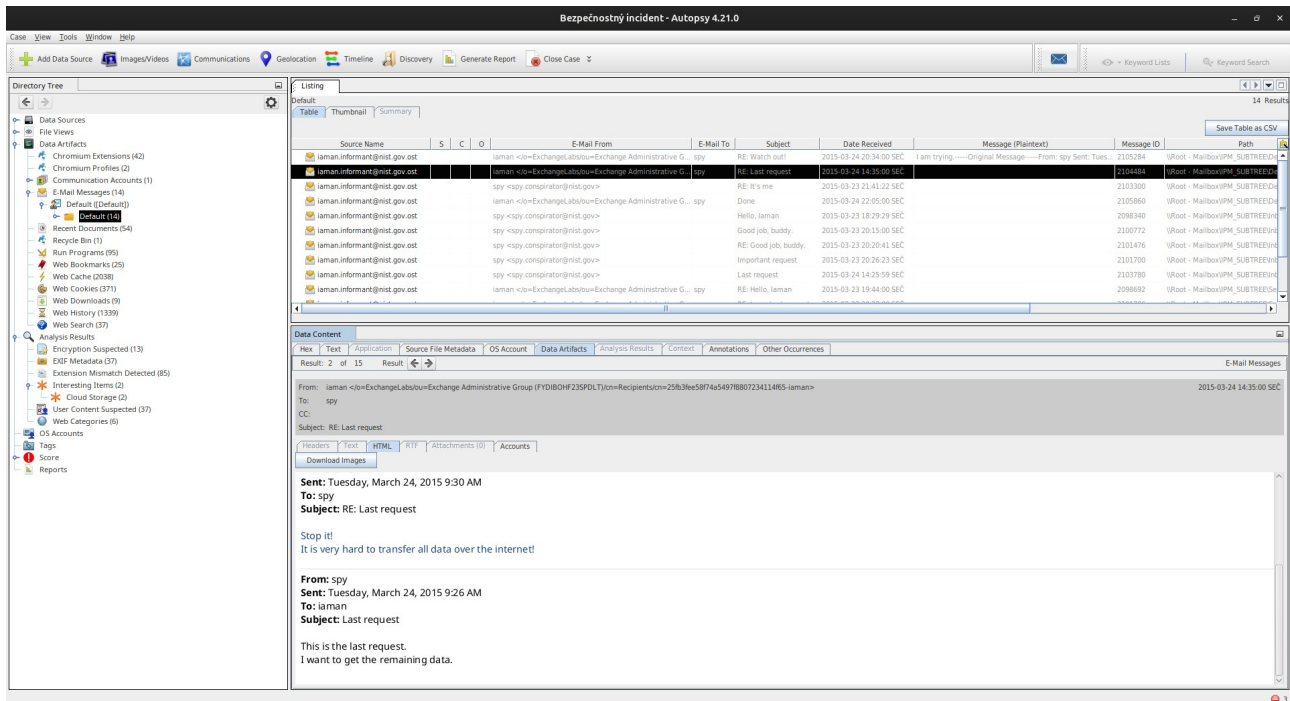
Obrázok 8: sync_config.db



Obrázok 9: Resignation_Letter_(Iaman_Informant).xps

Aj keď to v liste nie je explicitne vyjadrené, mohlo by sa jednať o doznanie v prípade, že by bol únik dát odhalený.

- Mailová komunikácia medzi iaman.informant@nist.gov.ost a spy.conspirator@nist.gov.ost



Obrázok 10: Mailová komunikácia medzi iaman.informant@nist.gov.ost a spy.conspirator@nist.gov.ost

Časový sled udalostí – utorok, 24. marec 2015:

9:26 AM – **"Last request" od spy:** *"I want to get the remaining data."*

Spy sa jasne domáha zvyšných dát → to nie je bežná komunikácia, ale priama požiadavka na odovzdanie.

9:30 AM – **Odpoveď od iaman:** *"Stop it! It is very hard to transfer all data over the internet!"*

Silne emocionálna reakcia: „**Stop it!**“, potvrdenie, že časť dát už bola poskytnutá a zvyšok sa ťažko prenáša – pravdepodobne kvôli veľkosti / citlivosti.

9:34 AM – **spy odpovedá:** *"No problem. U can directly deliver storage devices that stored it."*

Návrh na fyzický prenos dát (cez úložné zariadenie) - veľmi nenápadný spôsob ako obísť sieťové monitorovanie, čo je jasný znak obchádzania bezpečnostných protokolov.

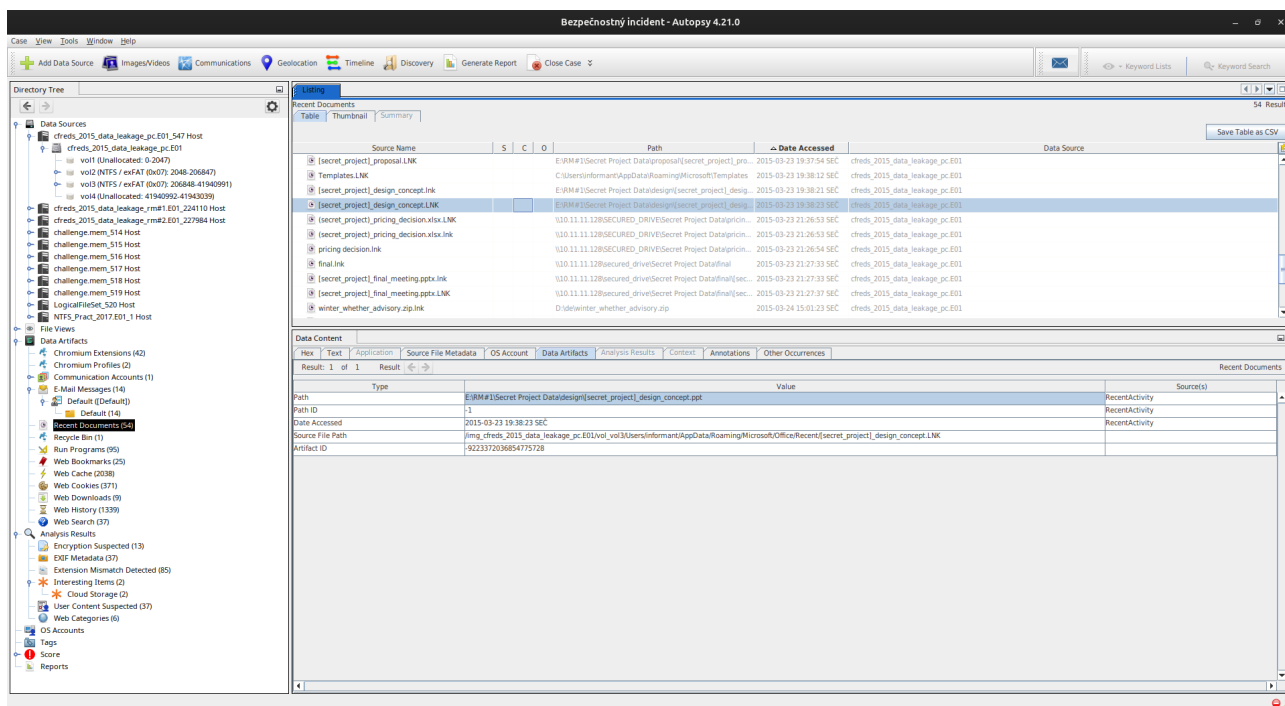
Mailová komunikácia v kontexte nadväzuje na súbor `Resignation_Letter_(Iaman_Informant).xps`, ktorý vznikol 25. marca 2015. Vyzerá to tak, že Iaman Informant je insider, ktorý sa dostal do situácie, kde bol donútený alebo presvedčený zdieľať dáta. Na konci však už nechcel spolupracovať, čo môže vysvetľovať „priznanie“ vo forme listu. V roku 2015 však jeho ilegálna činnosť nebola odhalená, preto sa ani jeho priznanie neobjavilo.

5. Analýza dôkazového materiálu č. 05

- Záznam o utajovaných dokumentoch v Recent Documents

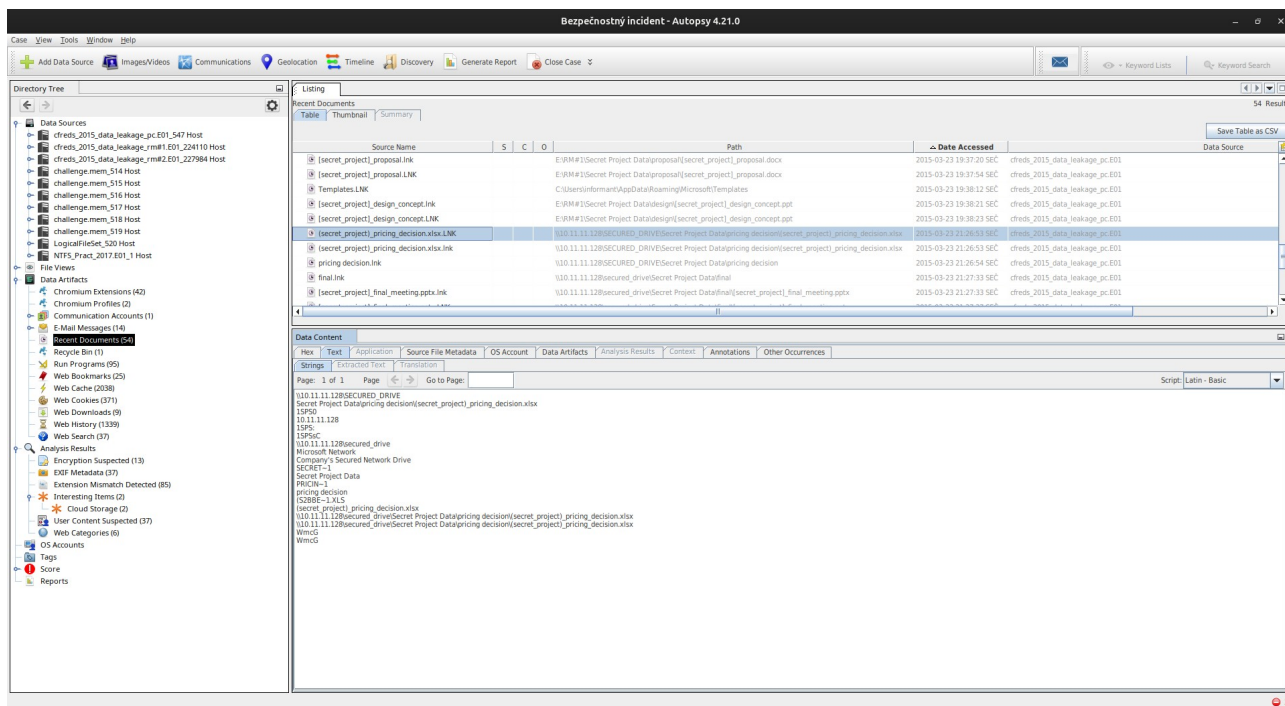
V zložke Recent Documents, sa našiel dôkaz o prístupe a exfiltrácii citlivých dát.

23.5.2015 v čase približne o 19:38 boli tajné súbory otvárané na USB zariadení zamestnanca Iaman (E:\RM#1).



Obrázok 11: Záznam o utajovaných dokumentoch v Recent Documents

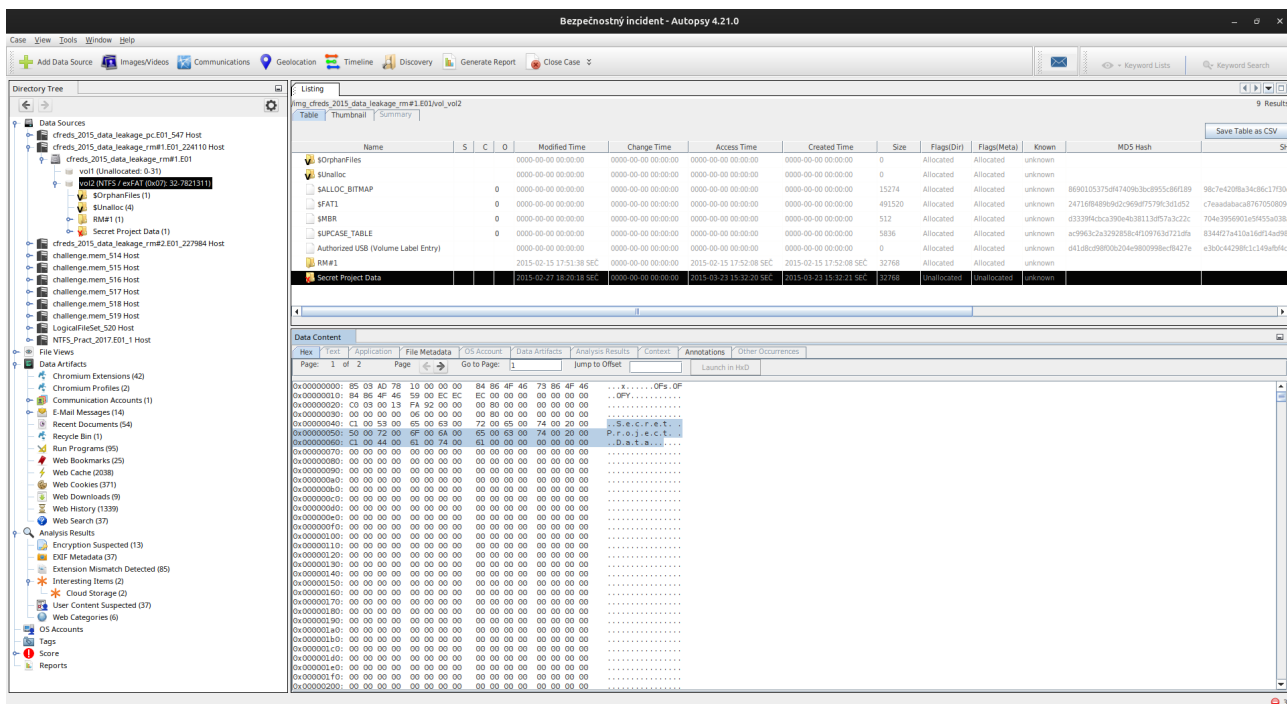
Následne v čase približne o 21:26 prenesené na sieťový disk (\\10.11.11.128\secured_drive)



Obrázok 12: Záznam o utajovaných dokumentoch v Recent Documents

Zo sieťového úložiska secured_drive v internej sieti 10.11.11.128 boli stiahnuté utajené dáta k projektu a následne skopírované na externé úložisko RM#1 pripojené na disk E:\.

- Citlivé dáta nájdené na osobnom USB flash drive

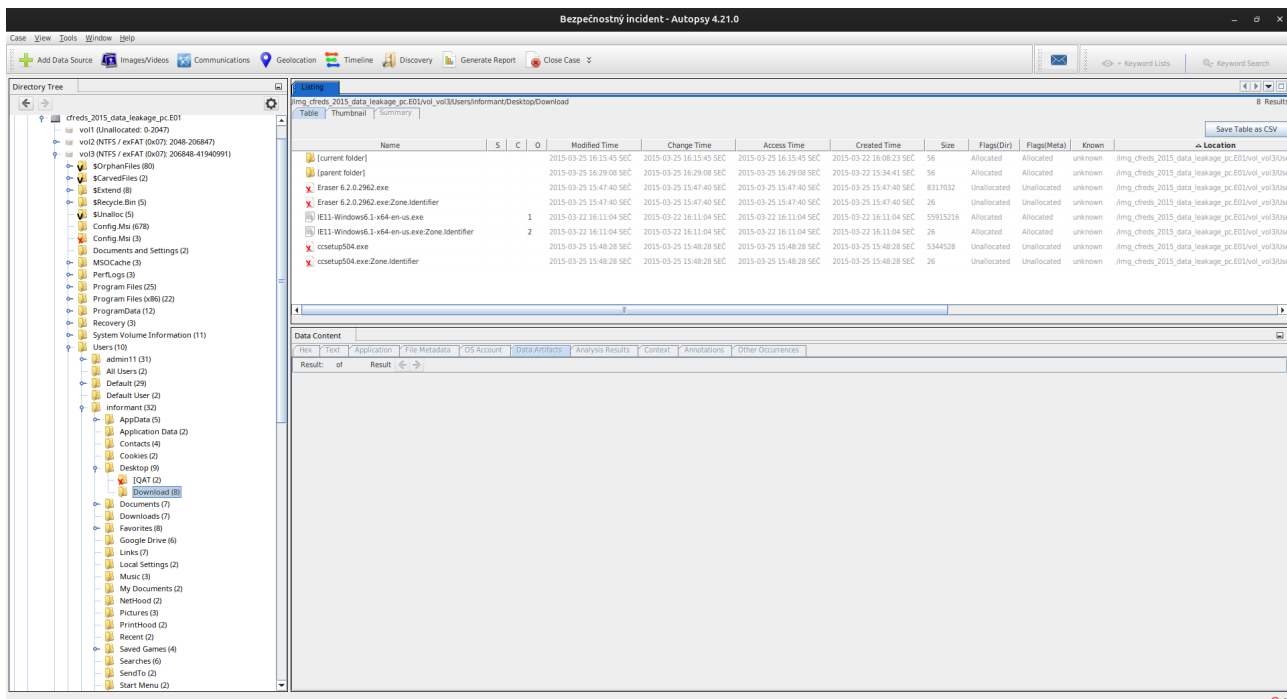


Obrázok 13: Analýza dát na USB flash drive zamestnanca Iamana

Piečinkok Secret Project Data je na zariadení unallocated, čo znamená, že bol zmazaný. Môže ísť o pokus o zmazanie stôp po úniku dát.

6. Pokus o zahľadenie stôp po úniku dát.

Na notebooku Iamana sa našiel inštalčný súbor **Eraser 6.2.0.2962.exe**. Jedná sa o nástroj na bezpečné mazanie súborov. Súbor bol stiahnutý a použitý 25.3.2015, len pár hodín pred vytvorením rezignačného listu a pravdepodobne aj pred samotným odovzdaním dát. V kontexte ostatných dôkazov to podporuje hypotézu o vedomom a úmyselnom odstránení dôkazov o úniku citlivých dát.



Obrázok 14: Eraser 6.2.0.2962.exe

8. Záver od forenzného analytika

Na základe vykonanej digitálnej forenzej analýzy a korelácie dostupných údajov som dospela k záveru, že zamestnanec AlbertE nebol priamym pôvodcom kompromitujúcich súborov nachádzajúcich sa na jeho pracovnom počítači. Analýzou metadát a systémových záznamov bolo zistené, že súbor *jet.mpg:unixphreak.txt* bol vytvorený a uložený používateľským účtom so SID končiacim na 1004, zatiaľ čo účet AlbertaE mal pridelený SID 1000.

Autorom dokumentu *cyberbullying_by_proxy.doc* je podľa metadát používateľ s aliasom *buckyball*, čo je meno, ktoré sa neobjavuje medzi známymi aliasmi AlbertaE. V rámci ďalšieho vyšetrovania bol zabezpečený obraz disku notebooku IT technika, Iamana. Na tomto počítači boli identifikované stopy po používaní nástrojov *Eraser* a *CCleaner*, čo sú aplikácie používané na trvalé odstránenie digitálnych stôp.

Zásadným dôkazom je však archivovaná e-mailová komunikácia Iamana z obdobia pred dvoch rokov, ktorá obsahuje jasné náznaky neautorizovaného zdieľania interných dokumentov s konkurenčnou firmou. Vzhľadom na načasovanie (plánované uvedenie produktov konkurencie na trh) je vysoko pravdepodobné, že Iaman sa pokúsil zakryť svoje predchádzajúce konanie tým, že úmyselne podstrčil dôkazy na zariadenie kolegu AlbertaE a tým sa ho pokúsil falošne označiť za vinníka.

V ďalšej fáze analýzy bol preskúmaný pracovný počítač podozrivý z predchádzajúcej účasti na úniku dát (*img_cfreds_2015_data_leakage_pc.E01*). Medzi inštalovanými aplikáciami bol identifikovaný súbor *googledrivesync.exe* – oficiálny klient služby Google Drive. Tento program umožňuje automatickú synchronizáciu súborov medzi lokálnym zariadením a cloudovým úložiskom. Analýza metadát ukázala, že inštalácia bola vykonaná používateľom s oprávneniami systémového účtu, pričom čas posledného prístupu sa zhoduje s časovým rámcom, v ktorom pravdepodobne došlo k úniku dát.

Hoci samotný súbor *googledrivesync.exe* nebol identifikovaný ako škodlivý softvér, jeho prítomnosť v kombinácii s ostatnými nálezmi (časové pečiatky, absencia politiky povoľujúcej používanie cloudových služieb) naznačuje, že mohol byť použitý ako kanál na exfiltráciu citlivých firemných údajov mimo kontrolované prostredie organizácie. Tento zistený fakt posilňuje závery vyplývajúce z komunikácie a digitálnych stôp Iamana a zapadá do časovej osi, ktorá predpokladá, že informácie boli odovzdané konkurencii práve cez túto infraštruktúru.

Získané dôkazy jednoznačne svedčia o manipulácii s digitálnym prostredím, falšovaní dôkazov a cielenej snahe odviesť pozornosť od skutočného páchatela. Na základe týchto zistení odporúčam prípad uzavrieť ako interný incident s podozrením na úmyselný čin zo strany zamestnanca Iamana, s návrhom na ďalšie disciplinárne alebo právne kroky voči nemu. Použitie nástrojov na zahľadanie stôp, ako aj dôsledná príprava falšovania dôkazov naznačujú premyslený zámer a sofistikovanú snahu zmariť vyšetrovanie.

Zdroje

<https://github.com/dfrws/dfrws2008-challenge/tree/master/details>

https://cfreds-archive.nist.gov/data_leakage_case/data-leakage-case.html

Vypracovala: Martina Petřková