

Prípado: Neoprávnená manipulácia s USB kľúčom v internátnej študovni

Výetrovateľ: Jakub Juliš

Prezentácia: <https://bcstudent.fpvucm.sk/~julisjakub/dfa/prezentacia.pdf>

Opis prípadu:

Študent, ubytovaný na vysokoškolskom internáte, nahlásil, že jeho USB kľúč s osobnými projektmi a citlivými dokumentmi zmizol z internátnej študovne. O niekoľko dní neskôr USB kľúč znovu našiel v študovni. Avšak vzhľadom ku tomu, že bol dostatočne edukovaný ohľadom bezpečnosti zariadení, v zmysle že nie je dobrý nápad zapájať USB zariadenia, ktoré nájdeme len tak niekde pohodené, rozhodol sa, že svoje vlastné USB najprv zverí forenznému analytikovi, ktorý skontroluje, či bolo s kľúčom manipulované, resp. či je bezpečné kľúč používať. Existuje totiž podozrenie, že kľúč niekto použil, prípadne manipuloval s jeho obsahom a mohol prezerat' či kopírovať súkromné dáta.

Predmet výetrovania:

- Analýza metadát súborov (časy posledného prístupu, úpravy, vytvorenia).
- Kontrola systémových logov na počítačoch v internátnej miestnosti (Windows Event Logs, resp. v prípade macOS „Unified Logs“).
- Obnovenie prípadne vymazaných súborov pomocou forenzných nástrojov (FTK Imager, resp. Autopsy).
- Porovnanie hashov pôvodných súborov so súčasnými verziami (MD5/SHA-256).
- Identifikácia zariadenia či používateľa, ktorý s USB mohol neoprávnene pracovať (na základe logov či iných digitálnych stôp).

Očakávaný výsledok:

- Zistiť, či boli súbory otvorené, skopírované alebo pozmenené.
- Obnoviť prípadne vymazané dokumenty a preskúmať ich obsah.
- Prípadne identifikovať používateľa alebo konkrétny počítač v internátnej študovni, ktorý mohol byť so zariadením prepojený.

5WH analýza pre prípad neoprávnenej manipulácie s USB kľúčom:

Who? – Kto?

Neznáma osoba (alebo viac osôb) využívajúca miestnosť internátnej študovne. Môže ísť o iných študentov alebo pracovníkov internátu.

What? – Čo?

USB kľúč s osobnými a citlivými dokumentmi bol stratený a znovu nájdený.

When? – Kedy?

Kľúč sa stratil v priebehu jedného dňa a o pár dní bol nájdený v tej istej miestnosti. Logy môžu presne určiť okamih možného pripojenia USB k počítačom.

Where? – Kde?

Miestnosť študovne v priestoroch vysokoškolského internátu, kde majú prístup viacerí študenti.

Why? – Prečo?

Existuje podozrenie, že sa niekto mohol dostať k citlivým dokumentom a mohol ich zneužiť.

How? – Ako?

Teoreticky neoprávnený používateľ mohol pripojiť USB kľúč do jedného z počítačov a prezrieť či upraviť obsah, následne kľúč vrátiť.

Hypotézy:

- 1. USB kľúč bol počas doby straty pripojený k neznámemu zariadeniu a došlo k neoprávnenému prístupu k súborom**
Možné overenie: Analýza časovej osi udalostí skrz „Autopsy Timeline“, kontrola relevantných metadát súborov (napr. časy posledného prístupu) v obraze USB.
- 2. Na USB kľúči sa nachádza škodlivý alebo podozrivý obsah, ktorý tam mohol byť umiestnený počas doby straty**
Možné overenie: Analýza obsahu existujúcich aj obnovených súborov (napr. pomocou Autopsy Ingest Modules a následná manuálna kontrola súborov), obnova dát z voľného priestoru (my sme použili Autopsy, no možné vykonať aj cez FTK Imager).
- 3. Pripojenie alebo manipulácia s USB kľúčom zanechala stopy v operačnej pamäti počítača v študovni a/alebo sa na USB zariadení vyskytujú podozrivé kľúčové slová**
Možné overenie: Analýza obrazu operačnej pamäte (vytvoríme memdump.mem cez Belkasoft RAM Capturer a prezeráme napr. skrz ImHex), a vyhľadávanie kľúčových slov v obraze USB (cez Autopsy Keyword Search).

Fotodokumentácia zariadenia:



Základné parametre zariadenia:

Názov zariadenia: Flash Drive DUO

Značka zariadenia: Samsung

Kapacita úložiska: 64 GB

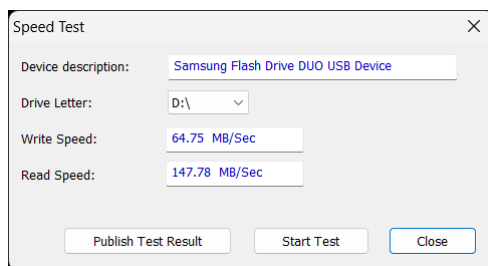
Rozhranie: USB 3.0

Konektor: USB-A & microUSB

Rýchlosť čítania: 147,78 MB/s

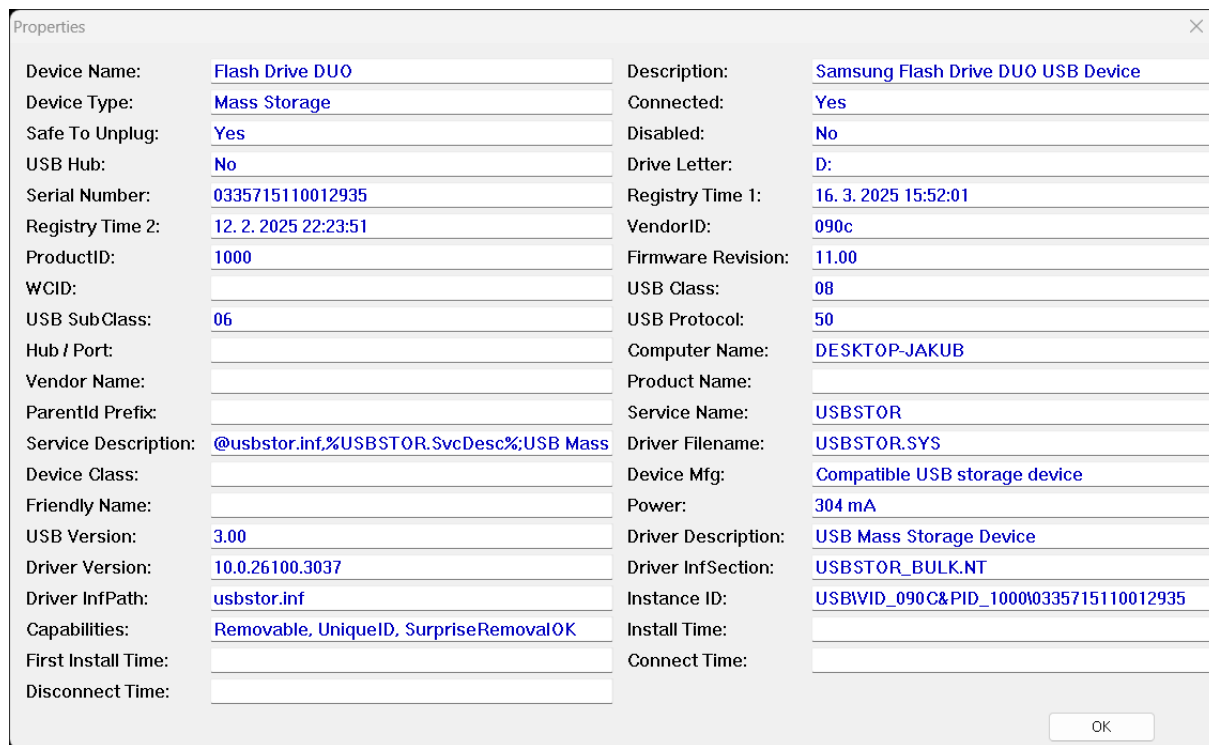
Rýchlosť zápisu: 64,75 MB/s

Sériové číslo: 0335715110012935



Obrázok 1 Výsledok testovania rýchlosti zápisu a čítania cez softvér USBDeview

Rozšírené parametre zariadenia:

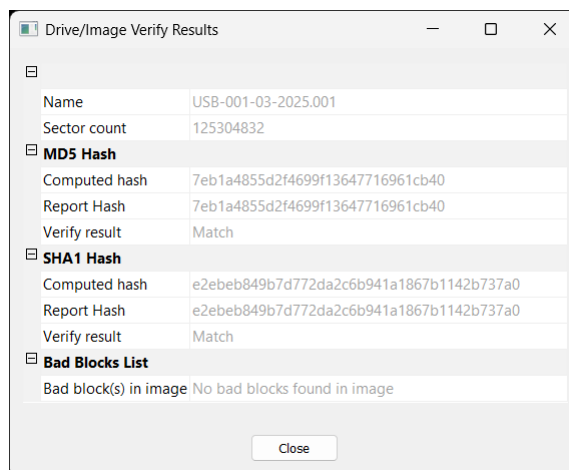


Obrázok 2 Vlastnosti zariadenia získané cez softvér USBDeview

Použité nástroje:

- **FTK Imager 4.7.3.81** – nástroj využitý na vytvorenie forenzného obrazu zariadenia
- **USBDeview 3.07** – využitý na testovanie rýchlosti a zobrazenie vlastností zariadenia
- **ImHex Hex Editor 1.37.4** – využitý na analýzu RAM a USB na úrovni hexadecimálnych hodnôt, resp. priame čítanie stringov, vďaka konvertovaniu na ASCII (rovnako dobre by poslúžil aj softvér **HxD editor**, jedná sa len o osobnú preferenciu)
- **Autopsy 4.22.0** – využitý na kompletnú forenznú analýzu USB a keyword search

Výsledok overenia obrazu:



Zhrnutie obrazu:

Created By Exterro® FTK® Imager 4.7.3.81

Case Information:

Acquired using: ADI4.7.3.81

Case Number: 001

Evidence Number: 001-03-2025

Unique description: Obraz USB zariadenia

Examiner: Jakub Juliš

Notes: Na účely DFA

Information for C:\Users\Jakub\Documents\USB\USB-001-03-2025:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 7 799

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 125 304 832

[Physical Drive Information]

Drive Model: Samsung Flash Drive DUO USB Device

Drive Serial Number: AA00000000000489

Drive Interface Type: USB

Removable drive: True

Source data size: 61184 MB

Sector count: 125304832

[Computed Hashes]

MD5 checksum: 7eb1a4855d2f4699f13647716961cb40
SHA1 checksum: e2eb849b7d772da2c6b941a1867b1142b737a0

Image Information:

Acquisition started: Sun Mar 16 16:11:48 2025

Acquisition finished: Sun Mar 16 16:42:13 2025

Segment list:

C:\Users\Jakub\Documents\USB\USB-001-03-2025.001

COMPUTED HASH : 7eb1a4855d2f4699f13647716961cb40

COMPUTED HASH : e2eb849b7d772da2c6b941a1867b1142b737a0

Image Verification Results:

Verification started: Sun Mar 16 16:42:13 2025

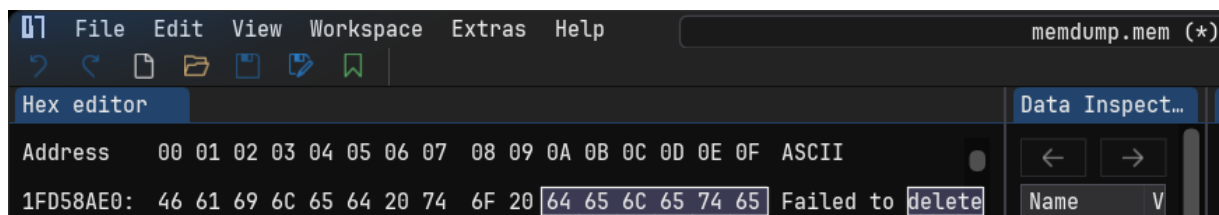
Verification finished: Sun Mar 16 16:44:33 2025

MD5 checksum: 7eb1a4855d2f4699f13647716961cb40 : verified

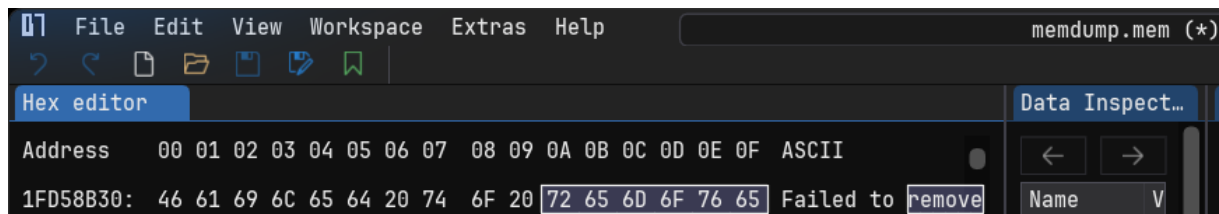
SHA1 checksum: e2eb849b7d772da2c6b941a1867b1142b737a0 : verified

Nájdené dôkazy v obraze RAM:

Pri analýze obrazu RAM na počítači v študovni sa vykonalo hľadanie reťazcov, ktoré by mohli mať niečo spojené s modifikovaním, či vymazaním údajov. Pri hľadaní stringov „delete“ a „remove“ sme našli dve dôležité informácie, no spoločne pred kľúčovým hľadaným reťazcom bolo napísané „Failed to“, čo indikuje, že pokus o vymazanie či odstránenie údajov od útočníka bol neúspešný. Existujúce podozrenie, že mohlo byť USB zneužitá sa teda priamo nepotvrdilo, no ani nevyvrátilo.



Obrázok 3 Dôkaz #1 naznačuje, že došlo k pokusu o vymazanie



Obrázok 4 Dôkaz #2 naznačuje, že došlo k pokusu o odstránenie

V pamäti RAM sa teda našli isté dôkazy, ktoré naznačujú, že by sa potenciálne niekto mohol snažiť o 1) vymazanie a 2) odstránenie dát.

Použitý dataset:

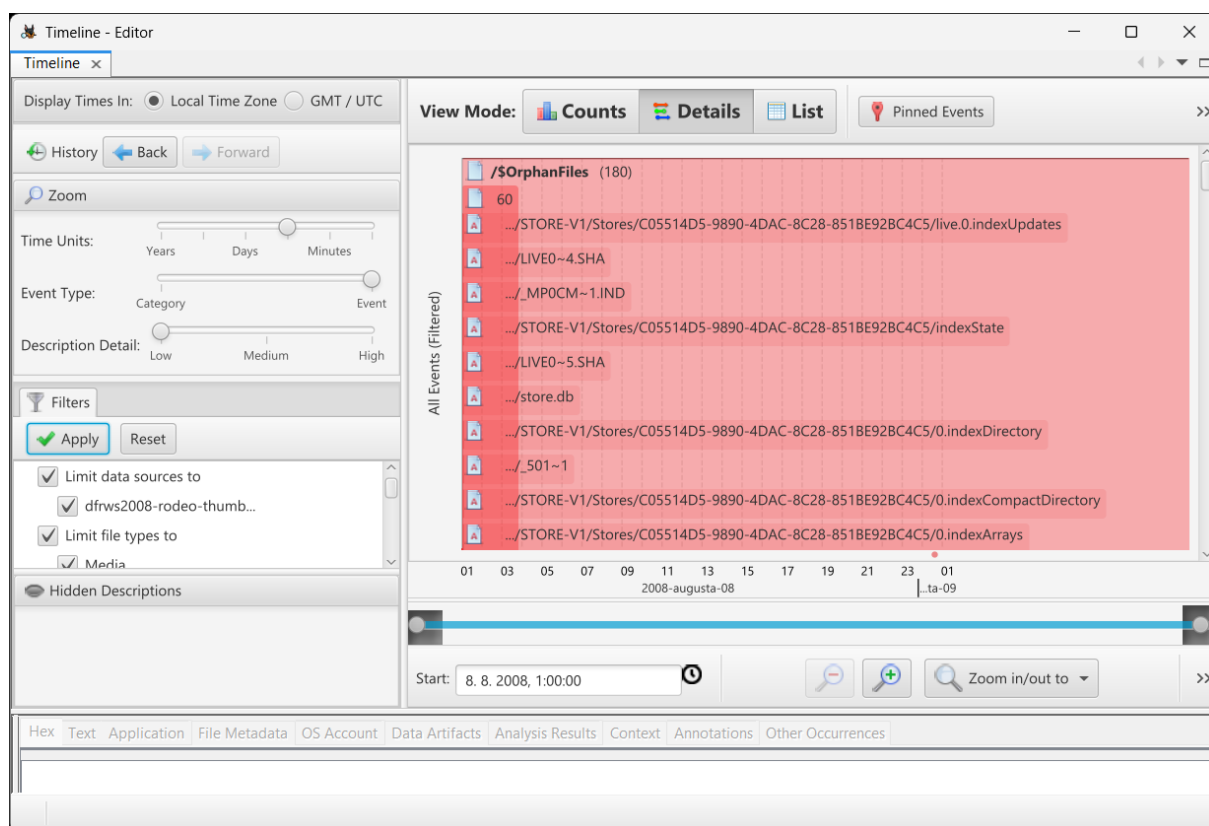
V práci sme použili dataset veľký 182 MB, ktorý sme našli na webe <https://cfreds.nist.gov/all> a konkrétne sa jedná o <https://cfreds.nist.gov/all/DFRWS2008Rodeo/DFRWS2008USBFlashDriveImages> (DFRWS 2008 - USB Flash Drive Images)

Hypotéza 1

Pomocou funkcie Timeline v nástroji Autopsy sme analyzovali aktivity v USB zariadení. Dňa 8. augusta 2008 bolo zaznamenaných viac ako 100 udalostí, ktoré indikujú prístup k súborom a adresárom. Inú aktivitu ako tú z roku 2008 sa nám nepodarilo nájsť a prípad vyšetrujeme v roku 2025.

Na základe toho možno konštatovať, že zariadenie pravdepodobne nikto iný v študovni po jeho údajnej strate nepoužíval.

Na základe analýzy časovej osi v poskytnutom obraze USB neboli nájdené žiadne dôkazy o aktivite, ktorá by zodpovedala časovému rámcu popisovanému v scenári (rok 2025). Hypotézu 1 o nedávnom prístupe k súborom táto analýza **nepotvrdila**.



Obrázok 5 Aktivita v USB zariadení (Timeline funkcia v Autopsy)

Hypotéza 2

USB neobsahovalo priamy škodlivý softvér, ale obsahovalo podozrivý obsah.

Aj keď nástroj Autopsy nenašiel na USB žiadne známe škodlivé .exe, .dll alebo .bat súbory, identifikoval viacero podozrivých súborov – konkrétne 9. Najpodstatnejším z týchto súborov bol HTML dokument **Billing_and_delivery_information.html**. Obsahuje detailné informácie o plánovanej ceste z Washingtonu DC do Libérie pre troch pasažierov (konkrétne Steve Vagon, Catherine Lagarde, Matthew Geiger) s cenou presahujúcou 2 tisíc dolárov.

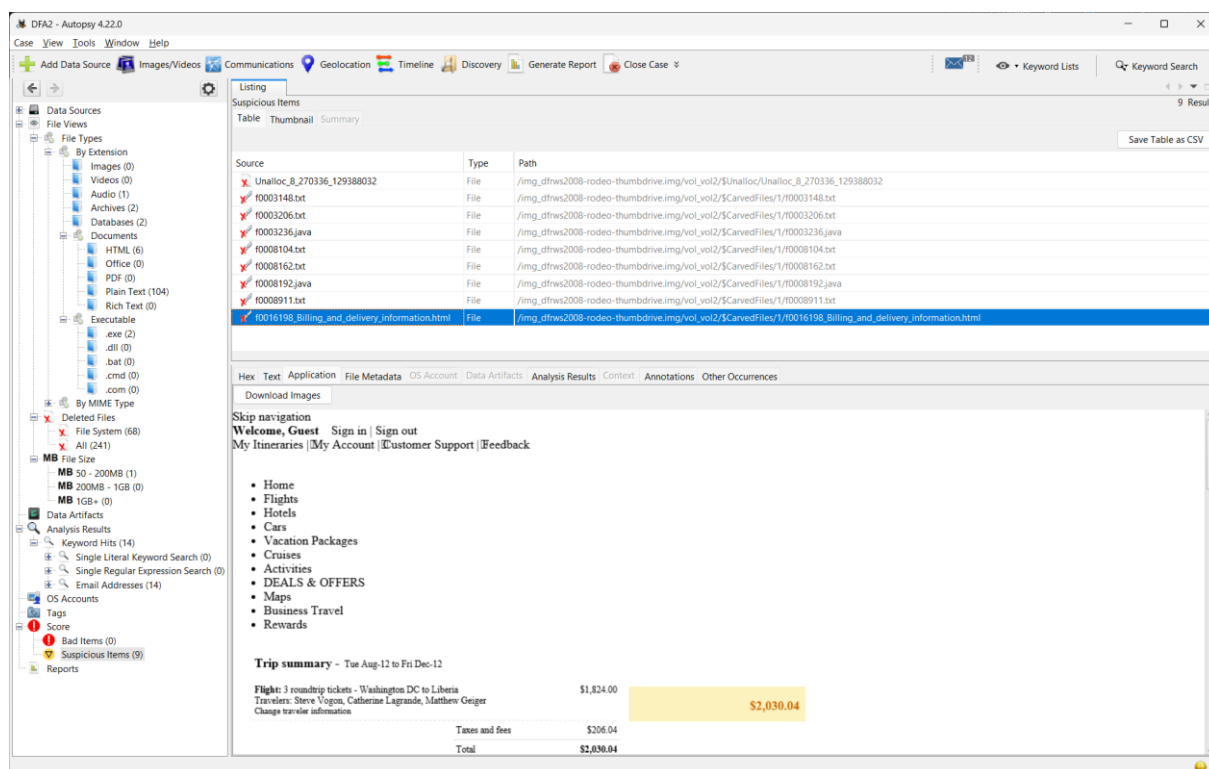
Tieto údaje boli extrahované z časti disku, ktorá naznačuje, že súbor bol získaný z voľného (unallocated) priestoru, čo môže znamenať, že ho niekto predtým zmazal.

Vzhľadom na obsah – ktorý pôsobí ako vytvorený alebo získaný phishingový e-mail či web stránka na simulovanie faktúry – nie je možné vylúčiť, že USB zariadenie bolo použité v minulosti na prenos alebo uchovávanie potenciálne klamlivého obsahu.

Nie je vylúčené, že osoba, ktorá vlastní USB, mohla byť súčasťou podvodu, alebo že súbor bol stiahnutý z kompromitovanej stránky. V každom prípade, čo sa týka momentálneho obsahu USB, sa nenašiel žiaden iný podozrivý obsah, ktorý by bol aktuálny pre rok 2025.

Nájdenný HTML súbor bol síce podozrivý, ale nachádzal sa vo voľnom (unallocated) priestore, čo naznačuje, že ide o starší, predtým zmazaný súbor. V kontexte analyzovaného obrazu tento nález nepotvrdzuje hypotézu 2 o aktívnom škodlivom kóde alebo nedávno umiestnenom podozrivom obsahu relevantnom pre rok 2025, resp. náš prípad straty v študovni.

Hypotéza 2 – je síce **potvrdená, no bezpredmetná** pre rok 2025.



Obrázok 6 Podozrivý súbor identifikovaný vďaka Autopsy: billing_and_delivery_information.html s údajmi o cestovnej rezervácii v hodnote presahujúcej dve tisíc dolárov

Hypotéza 3:

Pripojenie alebo manipulácia s USB kľúčom zanechala stopy v operačnej pamäti počítača v študovni + na zariadení sa vyskytujú podozrivé výrazy (Keyword Search)

Na overenie tejto hypotézy bol najprv vytvorený obraz operačnej pamäte (súbor memdump.mem) z počítača v internátnej študovni, kde mohlo dôjsť k neoprávnenému pripojeniu USB kľúča. Na zachytenie obrazu RAM by sme použili nástroj Belkasoft RAM Capturer. Následná analýza tohto obrazu bola vykonaná pomocou hex editora ImHex na vyhľadanie relevantných textových reťazcov.

Pri manuálnej analýze obrazu RAM pomocou ImHex sme sa zamerali na hľadanie kľúčových slov súvisiacich s možnou manipuláciou dát, ako napríklad delete (vymazať) a remove (odstrániť). Podarilo sa identifikovať dva kľúčové nálezy:

- Reťazec Failed to delete
- Reťazec Failed to remove

Tieto reťazce, nájdené priamo v surových dátach operačnej pamäte, indikujú, že na analyzovanom počítači došlo k pokusu o vymazanie alebo odstránenie nejakých dát. Systém tieto operácie zaznamenal ako neúspešné („Failed to“). Aj keď tieto stopy priamo nepotvrdzujú, že išlo o manipuláciu s dátami konkrétne z USB kľúča študenta, dokazujú prítomnosť podozrivej aktivity (neúspešné mazanie) na počítači v študovni v čase vytvorenia obrazu RAM. V kontexte nášho scenára (rok 2025) tento nález podporuje obavy študenta, že sa niekto mohol pokúsiť o neoprávnenú manipuláciu.

V rámci digitálnej forenzej analýzy sme ďalej využili funkciu Keyword Search nástroja Autopsy na overenie prítomnosti výrazov, ktoré by mohli indikovať bezpečnostný incident, škodlivý kód alebo pokus o manipuláciu so súbormi.

Zamerali sme sa na tieto tri kľúčové výrazy:

- password – indikátor únikov prihlasovacích údajov
- cmd – potenciálny náznak spustenia príkazového riadku alebo skriptu
- delete – snaha o mazanie súborov alebo dát

Výsledky boli nasledovné:

- password → 2 relevantné výskyty, avšak nič zaujímavé pre prípad
- cmd → niekoľko výskytov v bežnom HTML kóde, nič podozrivé
- delete → **51 výskytov** vo viacerých .java, .txt a .dll súboroch

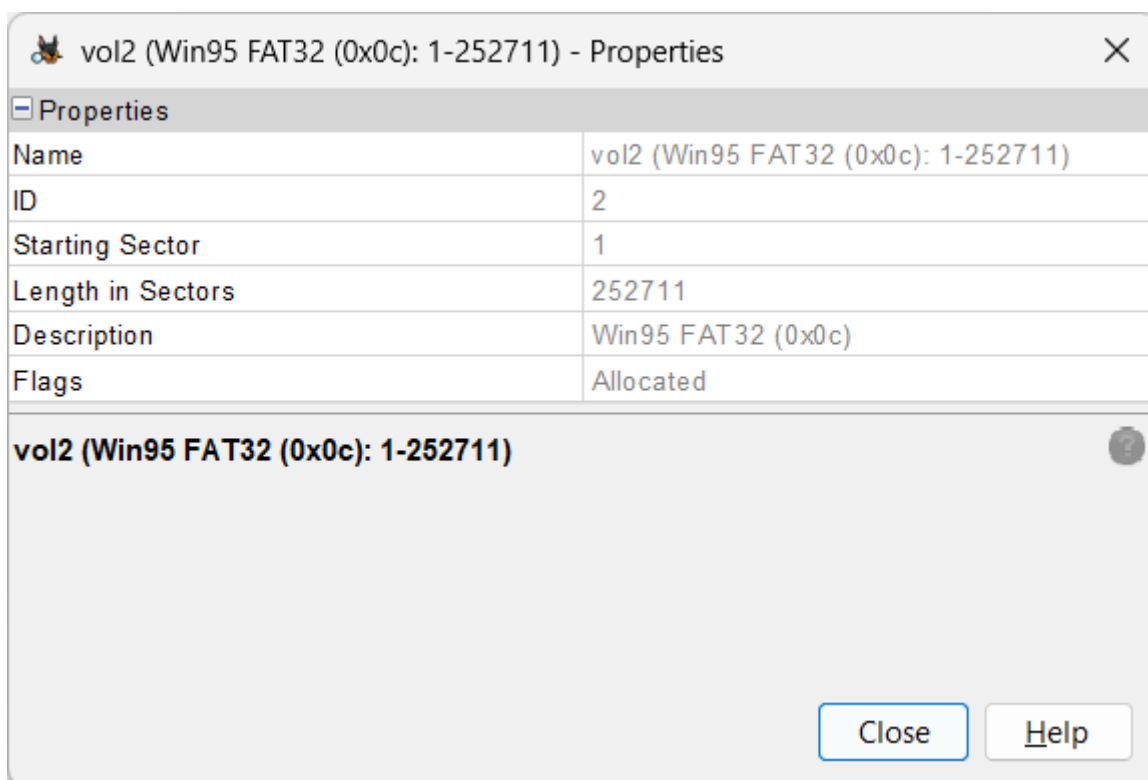
Nakoľko kľúčové slovo *delete* pôsobí podozrivo, bolo všetkých 51 výskytov ručne preverených brigádnikmi (viď obrázok nižšie). Výskyt tohto slova bol vo väčšine prípadov súčasťou obyčajných skriptov v jazyku Java – bez známkov škodlivej činnosti.

Hypotéza 3 – analýza operačnej pamäte potvrdila prítomnosť stôp („Failed to delete/remove“), ktoré naznačujú pokus o manipuláciu s dátami na počítači v študovni. Hypotéza, že manipulácia zanechala stopy v RAM, bola teda **potvrdená**. Čo sa týka vyhľadávania podozrivých kľúčových slov – na základe ručnej analýzy obsahu všetkých nálezov neboli identifikované žiadne škodlivé skripty ani iné dôkazy a teda hypotéza o tom, že by sa na zariadení vyskytovali podozrivé výrazy **nebola potvrdená**. Dokopy teda označujeme hypotézu ako **nepotvrdenú**, pretože nemáme jednoznačný dôkaz.

The screenshot shows the Autopsy 4.22.0 interface. The 'Keyword search' window is open, displaying a table of search results for the keyword 'delete'. The table has columns for Name, Keyword Preview, Location, Modified Time, Change Time, Access Time, and Created Time. The results list several files, including 'f0009049.java', 'f000375.txt', 'f0009098.html', 'f0003400.txt', 'f0003427.java', 'f0003459.java', 'Unaloc_8_270336_129388032', 'f0003511.java', 'f0011628_libeay32.dll', and 'f0003514.java'. The 'Strings' tab is selected, showing extracted text from the selected file, which includes code snippets like 'delete \$libCache(\$par);', 'delete \$file (sort keys %\$inc_ref) {', 'delete \$inc(\$file);', 'require \$file;', '}', 'sub read_file {', 'my \$file = pop;', 'foreach my \$zip ((@LibCache) {', 'my \$member = _first_member(\$zip, \$file) or next;', 'return scalar \$member->contents;', '}', 'return;', '}', 'sub par_handle {', 'my \$par = pop;', 'return \$libCache(\$par);', '}', 'my %escapes;', '}'.

Obrázok 7 Výsledok vyhľadávania kľúčového slova „delete“ s ukážkou časti nejakého java skriptu.

Umiestnenie súborov a súborový systém



Obrázok 8 Vlastnosti analyzovanej partície zariadenia vo formáte FAT32 (typ: Win95 FAT32, sektor 1–252711)

Zariadenie obsahuje partíciu vo formáte FAT32, čo umožňuje uchovávanie základných informácií o súboroch – metadáta.

Reťazec starostlivosti (Chain of Custody):

Číslo:	001	Typ súboru:	Obraz disku	Obnovený súbor:	Nie	Veľkosť:	61184 MB
Popis prípadu:							
Názov súboru:		USB-001-03-2025					
Miesto získania digitálnej stopy:		Internátna študovňa					
Poznámky:		Na účely DFA					
Časové pečiatky							
Access:	16.03.2025 16:11:48		Modify:	16.03.2025 16:42:13		Change:	16.03.2025 16:44:33
Digitáln y odtlačok (heš)	MD5	7eb1a4855d2f4699f13647716961cb40					
	SHA1	e2ebeb849b7d772da2c6b941a1867b1142b737a0					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
16.03.2025 16:11:48		Začiatok akvizície obrazu USB					
16.03.2025 16:42:13		Ukončenie akvizície obrazu USB					
16.03.2025 16:44:33		Overenie integrity obrazu (MD5 a SHA1)					

Bezpečnostné opatrenia:

- **Fyzická ochrana** – zariadenie bolo umiestnené v antistatickom obale a bezpečnostnom puzdre, ktoré ho chránilo pred vplyvom vlhkosti, teploty a magnetických polí.
- **Digitálna ochrana** – zariadenie nebolo pripájané k bežnému počítaču, aby sa zabránilo nežiaducim zmenám dát. Ihneď po nahlásení bol vytvorený forenzný obraz zariadenia s využitím softvéru Exterro FTK Imager verzie 4.7.3.81.
- **Dokumentácia a skladovanie** – zaevidované boli miesto nálezu zariadenia, spoločne s dátumom a časom manipulácie.

Odborné články z DFRWS:

1. **Duck Hunt: Memory Forensics of USB Attack Platforms** (<https://dfrws.org/presentation/duck-hunt-memory-forensics-of-usb-attack-platforms/>)

Tento článok sa zameriava na forenznú analýzu pamäte pri USB útokoch a skúma digitálne stopy generované škodlivými USB zariadeniami, ako sú USB Rubber Ducky a Bash Bunny. Predstavuje dva open-source plugíny, ktoré umožňujú extrakciu dôkazov z pamäťových dumpov systému Windows 10, vrátane identifikátorov zariadení, diagnostických udalostí a DHCP logov. Tieto nástroje môžu byť užitočné pri vyšetrovaní neoprávneného použitia USB zariadení a detekcii známkov kompromitácie systému.

2. **DiagAnalyzer : User Behavior Analysis and Visualization Using Windows Diagnostics Logs** (<https://dfrws.org/presentation/diagalyzer-user-behavior-analysis-and-visualization-using-windows-diagnostics-logs/>)

Tento článok sa zaoberá analýzou a vizualizáciou používateľského správania pomocou Windows Diagnostics logov, ktoré zaznamenávajú rôzne aktivity v systémoch Windows 10 a 11. Predstavuje nástroj DiagAnalyzer, ktorý automaticky analyzuje diagnostické udalosti, ako sú pripojenie a odpojenie USB zariadení, aktivity webového prehliadača a sieťové pripojenia. Táto metóda môže byť užitočná v digitálnej forenznej analýze na sledovanie interakcií používateľa so systémom a identifikáciu podozrivých aktivít.

Literatúra a prípadové štúdie:

1. **An automated timeline reconstruction approach for digital forensic investigations** (<https://doi.org/10.1016/j.diin.2012.05.006>)

Tento článok sa zaoberá automatizovanou rekonštrukciou časovej osi digitálnych forenzných vyšetrovaní, pričom sa zameriava na identifikáciu udalostí, ako je napr. pripojenie USB kľúča. Predstavuje metódu, ktorá analyzuje systémové udalosti a transformuje ich do prehľadnej časovej osi. Táto technika môže byť užitočná pri skúmaní neoprávnenej manipulácie s USB zariadením a sledovaní zmien súborov.

2. **Digital Evidence Cabinets: A Proposed Framework for Handling Digital Chain of Custody** (<http://dx.doi.org/10.5120/18781-0106>)

Tento článok sa zameriava na problematiku reťazca dôkazov pri digitálnych dôkazoch a navrhuje framework „Digital Evidence Cabinets“ na zlepšenie ich správy. Predstavuje model, ktorý kombinuje systémy správy dôkazov, bezpečné označovanie a kontrolu prístupu s cieľom zabezpečiť integritu a dôveryhodnosť digitálnych dôkazov. Tento koncept môže byť užitočný pri forenznej analýze USB zariadení, aby sa zachovala spoľahlivosť a neporušenosť zhromaždených dôkazov.

Záver

Táto práca forenzne analyzovala USB kľúč na základe podozrení študenta z neoprávnenej manipulácie počas jeho straty v roku 2025. Analýza dostupného obrazu USB a obrazu RAM však nepreukázala nedávny neoprávnený prístup, aktuálny škodlivý obsah, ani relevantné podozrivé kľúčové slová priamo na USB.

Jediným, aspoň trochu relevantným nálezom, boli stopy neúspešného pokusu o mazanie dát v analyzovanej RAM pamäti počítača, čo naznačuje možnú podozrivú aktivitu v študovni, avšak bez priameho dôkazu o spojitosti s USB kľúčom.

Celkovo teda vykonaná analýza poskytnutých dát nepotvrdila obavy študenta z kompromitácie jeho USB kľúča v rámci popisovaného scenára a študent môže ďalej pokojne spať.