

Neoprávnená manipulácia s dátami na USB kľúči

Autor: Barbora Horváthová

Prezentácia:

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

Obsah

Neoprávnená manipulácia s dátami na USB kľúči	1
5WH analýza pre prípad neoprávnenej manipulácie s USB kľúčom: ..	2
Predmet vyšetrovania:	3
Cieľ vyšetrovania:.....	3
Opis prípadu:.....	4
Informácie, ktoré hľadáme:	4
Očakávaný výsledok:.....	4
Hypotézy:.....	4
Typ analyzovanej digitálnej stopy:	5
Digitálne zariadenie súvisiace s prípadom:	5
Zariadenie:	5
Testovanie rýchlosti USB kľúča:.....	6
Zaujímavé dáta nájdené v obraze RAM:	6
Použité nástroje:.....	7
Bitové kópie:.....	7
Výsledky overenia obrazu:	8
Informácie z FTK Imager:	8
Hypotéza 1 - USB nebolo manipulované	10

Hypotéza 2/3 - USB bolo pripojené, ale súbory neboli zmenené / USB bolo pripojené a súbory boli otvorené	12
Hypotéza 4 - Súbory boli upravené alebo vymazané	13
Hypotéza 5 - USB obsahovalo škodlivý softvér	14
Umiestnenie súborov + súborový systém:	16
Reťazec starostlivosti:	16
Bezpečnostné opatrenia:	17
Odborné články z DFRWS:	17
Literatúra a prípadové štúdie:	18
Záver	19

5WH analýza pre prípad neoprávnenej manipulácie s USB kľúčom:

- Who? (Kto?)**
 Neznáma osoba, ktorá mohla manipulovať so súbormi na USB kľúči. Môže to byť zamestnanec firmy alebo iná osoba, ktorá USB našla.
- What? (Čo?)**
 USB kľúč obsahujúci citlivé firemné dokumenty bol stratený a následne nájdený. Cieľom vyšetrovania je zistiť, či boli súbory otvorené, upravené alebo vymazané.
- When? (Kedy?)**
 USB bolo stratené a po niekoľkých dňoch nájdené. Analýza metadát pomôže určiť presný čas interakcie s USB.
 - Strata: 2.3.2025, 20:15
 - Nález: 3.3.2025, 10:15

- **Where?** (Kde?)
USB bolo nájdené na firemnom parkovisku.
- **Why?** (Prečo?)
Cieľom je zabezpečiť firemné dáta, zistiť, či došlo k úniku informácií.
- **How?** (Ako?)
Vyšetrovanie sa vykoná pomocou forenzných metód, ako sú analýza metadát, kontrola systémových logov, a prípadné obnovenie vymazaných súborov.

Predmet vyšetrovania:

- Analýza metadát súborov (čas poslednej úpravy, prístupové časy, autor úprav).
- Kontrola systémových logov operačných systémov, ku ktorým bolo USB pripojené.
- Obnovenie vymazaných súborov pomocou forenzných nástrojov (napr. Autopsy, FTK Imager, TestDisk).
- Identifikácia zmenených súborov.

Cieľ vyšetrovania:

Cieľom vyšetrovania je určiť, či došlo k neoprávnenej manipulácii s dátami na USB kľúči, ktorý bol dočasne stratený a neskôr nájdený. Konkrétne sa vyšetrovanie zameria na:

1. **Analýzu časových značiek súborov** – kontrola metadát súborov (čas poslednej úpravy, prístupové časy) na odhalenie neautorizovanej aktivity.
2. **Možnú identifikáciu podozrivého zariadenia** – skúmanie digitálnych stôp a logov, ktoré by mohli pomôcť identifikovať konkrétne zariadenie, ktorý s USB kľúčom pracoval.

3. Prípadné obnovenie vymazaných dát – využitie forenzných nástrojov na obnovu odstránených súborov a analýzu ich obsahu.

Opis prípadu:

Zamestnanec firmy nahlásil stratu USB kľúča, ktorý obsahoval citlivé firemné dokumenty. Po niekoľkých dňoch sa USB kľúč našiel na firemnom parkovisku. Firma chce zistiť, či boli súbory skopírované, vymazané alebo inak manipulované.

Informácie, ktoré hľadáme:

Dôkazy o manipulácii so súbormi, ich možnej úprave alebo odstránení. Budeme sa zameriavať na obsah dokumentov a multimediálnych súborov, ktoré by mohli obsahovať citlivé alebo kompromitujúce informácie, ako aj na metadáta odhaľujúce históriu prístupu, úprav a zdieľania súborov.

Očakávaný výsledok:

- Zistenie, či boli súbory otvorené alebo vymazané.
- Obnovenie prípadných vymazaných dokumentov a analýza ich obsahu.
- Možná identifikácia zariadenia, ktoré s USB kľúčom pracovalo (napr. cez systémové logy).
- Možná identifikácia osoby, ktorá manipulovala s USB kľúčom.

Hypotézy:

1. USB nebolo manipulované
2. USB bolo pripojené, ale súbory neboli zmenené
3. USB bolo pripojené a súbory boli otvorené
4. Súbory boli upravené alebo vymazané

5. USB obsahovalo škodlivý softvér

Typ analyzovanej digitálnej stopy:

Budeme hľadať informácie uložené na USB kľúči, pričom sa zameriame na súbory typu: HTML, PDF, TXT, DOC, PPT, JPG, XLS, GIF. Analyzujeme históriu úprav, časové pečiatky a možné digitálne stopy, ktoré by mohli odhaliť, kto s USB pracoval a aké dáta boli manipulované. Cieľom je určiť, či došlo k neoprávnenej úprave alebo prenosu citlivých informácií.

(4,457 súborov, 1.9GB dát (1.2GB compressed), zdroj datasetu: <http://roussev.net/t5/t5.html>)

Budeme taktiež analyzovať metadáta určitých súborov.

Digitálne zariadenie súvisiace s prípadom:

USB kľúč Patriot Supersonic Rage XT 32GB, ktorý mohol byť použitý na prenos, úpravu alebo mazanie dôležitých dokumentov.

Zariadenie:



- Značka: Patriot
- Model: Supersonic Rage XT 32GB

- Sériové číslo: 097C011440A0
- Kapacita úložiska: 32 GB
- Rozhranie: USB 3.2 Gen 1 (USB 3.0), kompatibilné aj s USB 2.0
- Konektor: USB-A
- Rýchlosť čítania: 180 MB/s
- Rýchlosť zápisu: 50 MB/s
- Materiál: Guma
- Vyhotovenie: Vysúvací mechanizmus chrániaci konektor
- Rozmery: 53 mm (dĺžka) x 21,8 mm (šírka) x 11 mm (výška)
- Hmotnosť: 11 g
- Farba: Čierna

Testovanie rýchlosti USB kľúča:

Speed Test

Device description: Patriot Memory USB Device

Drive Letter: D:\

Write Speed: 27.17 MB/Sec

Read Speed: 174.42 MB/Sec

Publish Test Result Start Test Close

Zaujímavé dáta nájdené v obraze RAM:

3625018C0	26 DF 09 DF 05 D8 66 61 69 6C 65 64 5F 74 6F 61	4B.B.Řfailed to a
3625018D0	73 00 00 00 C2 B8 05 79 0B D2 83 79 1E F9 22 56	s...Ā,.y.Ň.y.ů"
3625018E0	79 6D 61 7A 61 6E 69 65 20 73 61 20 6E 65 70 6F	ymazanie sa nepo
3625018F0	64 61 72 69 6C 6F 2E 20 04 04 01 00 53 6B FA 73	darilo.Skús
362501900	74 65 20 74 6F 20 7A 6E 6F 76 61 99 01 2A D8 52	te to znova™.*ŘR

Nástroj HxD bol použitý na analýzu dátových zvyškov, kde bol identifikovaný text naznačujúci pokus o vymazanie súborov.

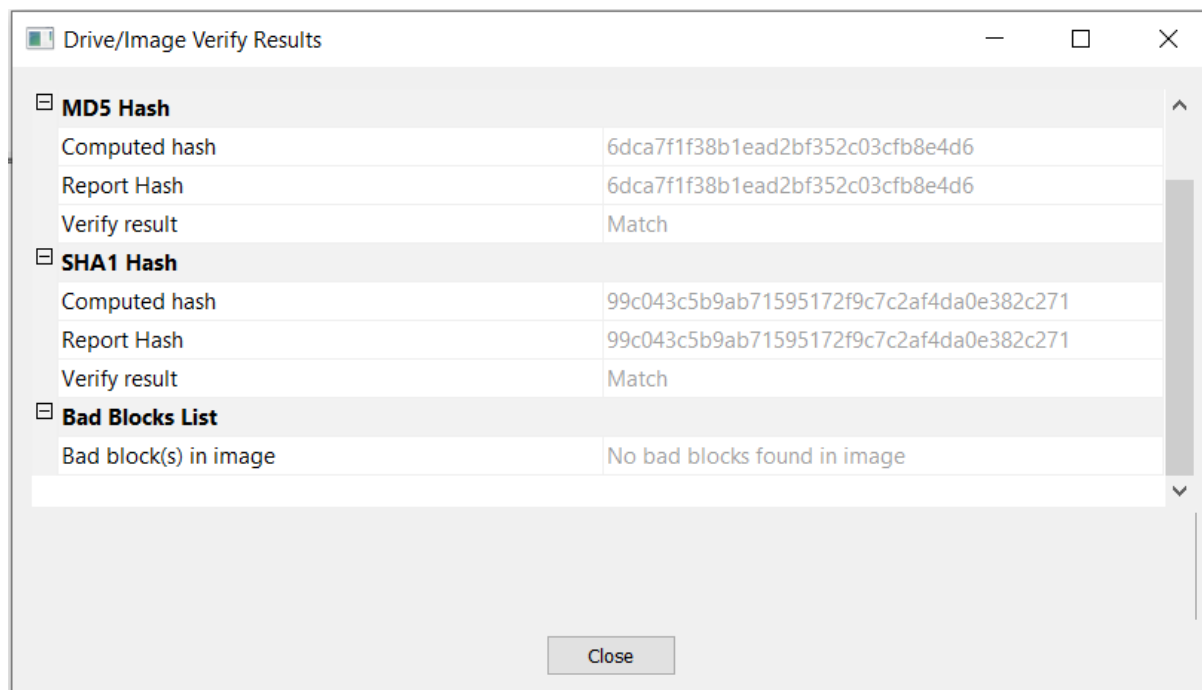
Použité nástroje:

- FTK Imager – softvér na tvorbu forenzných obrazov USB zariadenia.
- Autopsy – forenzný nástroj na prehliadanie a analýzu obrazov USB diskov.
- HxD Hex Editor – nástroj na analýzu pamäte a USB na úrovni hexadecimálnych hodnôt.
- USBDeview – nástroj na testovanie rýchlosti USB kľúča.

Bitové kópie:

- Prvá bitová kópia (BK1):
 - Umiestnenie: Uložená na laptope s Windows 10, ktorý slúži ako pracovné prostredie na forenznú analýzu.
 - Použitie: Notebook je v mojom vlastníctve a využíva sa na prácu s digitálnymi dôkazmi a analýzu dát z USB kľúča.
- Druhá bitová kópia (BK2):
 - Umiestnenie: Uložená na externom HDD vo forenznom laboratóriu.
 - Použitie: HDD je zabezpečené a uzamknuté v laboratóriu, ktoré slúži ako špecializované pracovné prostredie na digitálnu forenznú analýzu.

Výsledky overenia obrazu:



Informácie z FTK Imager:

Created By Exterro® FTK® Imager 4.7.3.81

Case Information:

Acquired using: ADI4.7.3.81

Case Number: 1

Evidence Number: 1

Unique Description:

Examiner: Horváthová

Notes: USB Patriot Rage blue 32GB

Information for D:\Skola\DFA\USB Patriot Rage blue 32GB:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 3 846

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 61 800 448

[Physical Drive Information]

Drive Model: Patriot Memory USB Device

Drive Serial Number: 097C011440A0

Drive Interface Type: USB

Removable drive: True

Source data size: 30176 MB

Sector count: 61800448

[Computed Hashes]

MD5 checksum: 6dca7f1f38b1ead2bf352c03cfb8e4d6

SHA1 checksum: 99c043c5b9ab71595172f9c7c2af4da0e382c271

Image Information:

Name		Login Name	Host
S-1-5-21-917722829-4245695347-2639746596-1001			USB Patriot Rage blue 32GB.001_1 Host

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Basic Properties

Login:

Full Name:

Address: S-1-5-21-917722829-4245695347-2639746596-1001

Type:

Creation Date:

Object ID: 8

Realm Properties

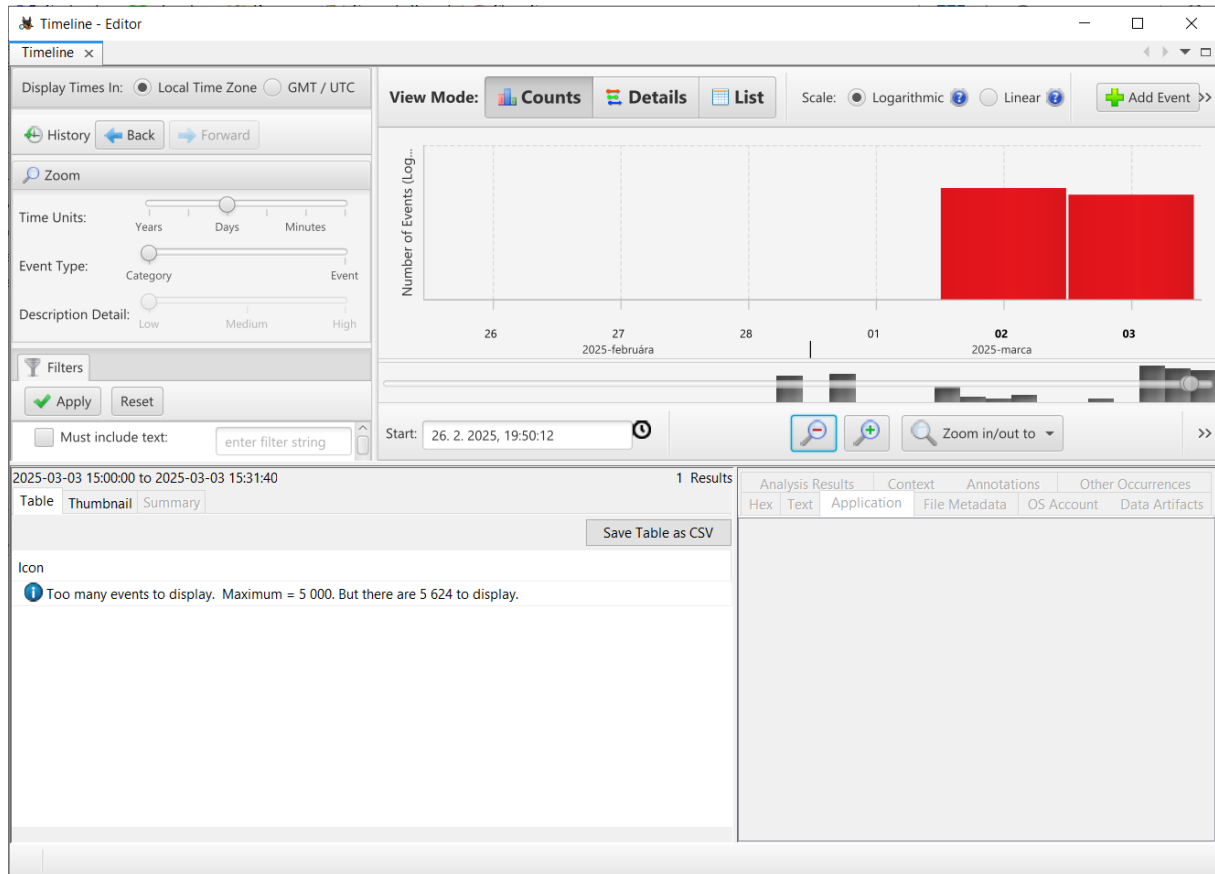
Name: Unknown

Address: S-1-5-21-917722829-4245695347-2639746596

Scope: Domain

Confidence: Known

Identifikovaný systémový účet naznačuje, že analyzované USB zariadenie bolo pripojené k systému s konkrétnym používateľským účtom, ktorý nepatrí zamestnancovi.



Pomocou Timeline v Autopsy môžeme vidieť, že s USB bolo manipulované v čase, kedy bolo USB stratené/ukradnuté.

Hypotéza **nie je potvrdená**.

Hypotéza 2/3 - USB bolo pripojené, ale súbory neboli zmenené / USB bolo pripojené a súbory boli otvorené

Name	△ S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	
000071.html				2011-02-09 01:37:51 SEČ	2025-03-02 18:14:54 SEČ	2025-03-03 15:30:46 SEČ	2025-03-02 18:14:54 SEČ	47111	Allocated	Allocated	unknown	/img_USB Patriot	^
000065.html				2011-02-09 01:37:51 SEČ	2025-03-02 18:14:54 SEČ	2025-03-03 15:30:46 SEČ	2025-03-02 18:14:54 SEČ	5883	Allocated	Allocated	unknown	/img_USB Patriot	
000206.html				2011-02-09 01:38:01 SEČ	2025-03-02 18:14:59 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:59 SEČ	27836	Allocated	Allocated	unknown	/img_USB Patriot	
000208.html				2011-02-09 01:38:01 SEČ	2025-03-02 18:14:59 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:59 SEČ	7211	Allocated	Allocated	unknown	/img_USB Patriot	
000209.html				2011-02-09 01:38:01 SEČ	2025-03-02 18:14:59 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:59 SEČ	66135	Allocated	Allocated	unknown	/img_USB Patriot	
000196.html				2011-02-09 01:38:01 SEČ	2025-03-02 18:14:59 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:59 SEČ	43407	Allocated	Allocated	unknown	/img_USB Patriot	
000197.html				2011-02-09 01:38:01 SEČ	2025-03-02 18:14:59 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:59 SEČ	25594	Allocated	Allocated	unknown	/img_USB Patriot	
000198.html				2011-02-09 01:38:01 SEČ	2025-03-02 18:14:59 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:59 SEČ	36088	Allocated	Allocated	unknown	/img_USB Patriot	
000199.html				2011-02-09 01:38:01 SEČ	2025-03-02 18:14:59 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:59 SEČ	58983	Allocated	Allocated	unknown	/img_USB Patriot	
000201.html				2011-02-09 01:38:01 SEČ	2025-03-02 18:14:59 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:59 SEČ	19570	Allocated	Allocated	unknown	/img_USB Patriot	▼

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	
000009.pdf				2011-02-09 01:37:40 SEČ	2025-03-02 18:14:57 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:57 SEČ	39586	Allocated	Allocated	unknown	/img_USB Patriot R	^
000010.pdf				2011-02-09 01:37:40 SEČ	2025-03-02 18:14:57 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:57 SEČ	120441	Allocated	Allocated	unknown	/img_USB Patriot R	
000011.pdf				2011-02-09 01:37:40 SEČ	2025-03-02 18:14:57 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:57 SEČ	31367	Allocated	Allocated	unknown	/img_USB Patriot R	
000012.pdf				2011-02-09 01:37:40 SEČ	2025-03-02 18:14:57 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:57 SEČ	22857	Allocated	Allocated	unknown	/img_USB Patriot R	
000013.pdf				2011-02-09 01:37:40 SEČ	2025-03-02 18:14:57 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:57 SEČ	38638	Allocated	Allocated	unknown	/img_USB Patriot R	
000014.pdf				2011-02-09 01:37:41 SEČ	2025-03-02 18:14:57 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:57 SEČ	3779383	Allocated	Allocated	unknown	/img_USB Patriot R	
000015.pdf				2011-02-09 01:37:41 SEČ	2025-03-02 18:14:57 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:56 SEČ	55964	Allocated	Allocated	unknown	/img_USB Patriot R	
000016.pdf				2011-02-09 01:37:41 SEČ	2025-03-02 18:14:56 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:56 SEČ	150586	Allocated	Allocated	unknown	/img_USB Patriot R	
000017.pdf				2011-02-09 01:37:41 SEČ	2025-03-02 18:14:56 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:56 SEČ	1081343	Allocated	Allocated	unknown	/img_USB Patriot R	
000018.pdf				2011-02-09 01:37:41 SEČ	2025-03-02 18:14:56 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:56 SEČ	94424	Allocated	Allocated	unknown	/img_USB Patriot R	▼

Name	△ S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	
000001.doc				2011-02-09 01:37:40 SEČ	2025-03-02 18:14:57 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:57 SEČ	40960	Allocated	Allocated	unknown	/img_USB Patriot	^
000002.doc				2011-02-09 01:37:40 SEČ	2025-03-02 18:14:57 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:57 SEČ	57856	Allocated	Allocated	unknown	/img_USB Patriot	
000003.doc				2011-02-09 01:37:40 SEČ	2025-03-02 18:14:57 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:57 SEČ	55808	Allocated	Allocated	unknown	/img_USB Patriot	
000004.doc				2011-02-09 01:37:40 SEČ	2025-03-02 18:14:57 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:57 SEČ	175616	Allocated	Allocated	unknown	/img_USB Patriot	
000005.doc				2011-02-09 01:37:40 SEČ	2025-03-02 18:14:57 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:57 SEČ	180736	Allocated	Allocated	unknown	/img_USB Patriot	
000006.doc				2011-02-09 01:37:40 SEČ	2025-03-02 18:14:57 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:57 SEČ	67584	Allocated	Allocated	unknown	/img_USB Patriot	
000007.doc				2011-02-09 01:37:40 SEČ	2025-03-02 18:14:57 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:57 SEČ	179200	Allocated	Allocated	unknown	/img_USB Patriot	
000127.doc				2011-02-09 01:37:55 SEČ	2025-03-02 18:14:52 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:52 SEČ	32768	Allocated	Allocated	unknown	/img_USB Patriot	
000130.doc				2011-02-09 01:37:55 SEČ	2025-03-02 18:14:51 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:51 SEČ	39936	Allocated	Allocated	unknown	/img_USB Patriot	
000111.doc				2011-02-09 01:37:52 SEČ	2025-03-02 18:14:53 SEČ	2025-03-03 15:30:45 SEČ	2025-03-02 18:14:53 SEČ	376832	Allocated	Allocated	unknown	/img_USB Patriot	▼

Získané údaje obsahujú dokumenty rôznych formátov (HTML, PDF, textové súbory). Boli analyzované časové atribúty súborov (modified, change, access, created).

Keďže change time sa zhoduje s časom, kedy zamestnanec pracoval s USB, môžeme povedať, že súbory neboli zmenené.

Táto analýza odhalila manipuláciu so súbormi – access time zaznamenal dátum, kedy bolo USB stratené/ukradnuté. Tým vieme povedať, že súbory boli otvorené.

Vyvrátili sme hypotézu 1 – „USB nebolo manipulované“, čím vieme povedať, že USB bolo pripojené k inému zariadeniu.

Hypotéza 2 je potvrdená.

Hypotéza 3 je potvrdená.

Hypotéza 4 - Súbory boli upravené alebo vymazané

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
 clientcommon.en.txt				2023-09-13 02:48:10 SELČ	2023-11-10 10:32:30 SEČ	2024-01-04 10:19:23 SEČ	2023-11-24 19:26:21 SEČ	36425
 clientcommon.es.txt				2023-09-13 02:48:10 SELČ	2023-11-10 10:32:30 SEČ	2024-01-04 10:19:23 SEČ	2023-11-24 19:26:21 SEČ	40091
 clientcommon.ja.txt				2023-09-13 02:48:10 SELČ	2023-11-10 10:32:30 SEČ	2024-01-04 10:19:23 SEČ	2023-11-24 19:26:21 SEČ	45171
 clientcommon.ko.txt				2023-09-13 02:48:10 SELČ	2023-11-10 10:32:30 SEČ	2024-01-04 10:19:23 SEČ	2023-11-24 19:26:21 SEČ	41490
 clientcommon.zh-Hans.txt				2023-09-13 02:48:10 SELČ	2023-11-10 10:32:30 SEČ	2024-01-04 10:19:23 SEČ	2023-11-24 19:26:21 SEČ	30896
 clientcommon.zh-Hant.txt				2023-09-13 02:48:10 SELČ	2023-11-10 10:32:30 SEČ	2024-01-04 10:19:23 SEČ	2023-11-24 19:26:21 SEČ	31631

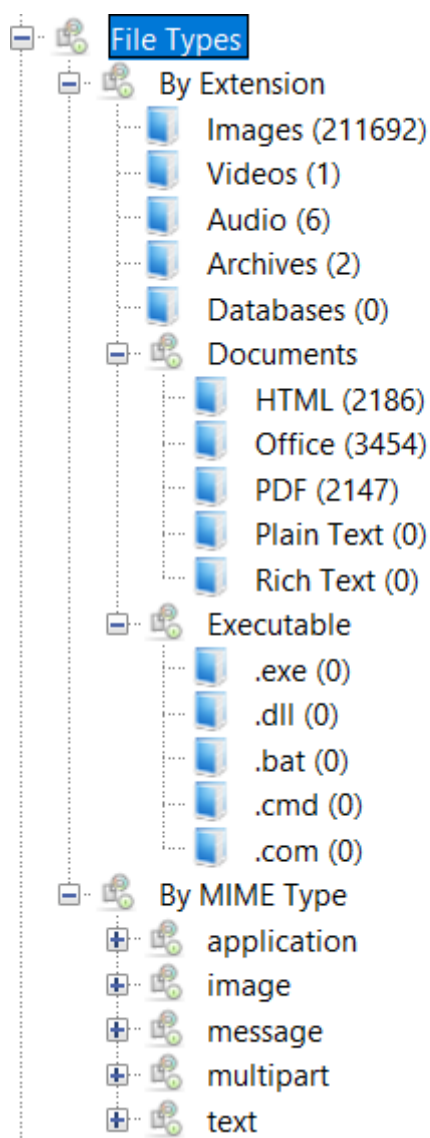
Pomocou analýzy sme našli niekoľko vymazaných súborov, ale podľa dátumov a časov vidíme, že boli vymazané pred stratou USB.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
 000610.html				2011-02-09 01:38:26 SEC	2025-03-02 18:15:16 SEC	2025-03-03 15:30:47 SEC	2025-03-02 18:15:16 SEC
 000611.html				2011-02-09 01:38:26 SEČ	2025-03-02 18:15:16 SEČ	2025-03-03 15:30:47 SEČ	2025-03-02 18:15:16 SEČ
 000612.html				2011-02-09 01:38:26 SEČ	2025-03-02 18:15:16 SEČ	2025-03-03 15:30:47 SEČ	2025-03-02 18:15:16 SEČ
 000613.html				2011-02-09 01:38:26 SEČ	2025-03-02 18:15:16 SEČ	2025-03-03 15:30:47 SEČ	2025-03-02 18:15:16 SEČ
 000620.text				2011-02-09 01:38:26 SEČ	2025-03-02 18:15:16 SEČ	2025-03-03 15:30:47 SEČ	2025-03-02 18:15:16 SEČ
 000624.text				2011-02-09 01:38:26 SEČ	2025-03-02 18:15:16 SEČ	2025-03-03 15:30:47 SEČ	2025-03-02 18:15:16 SEČ
 000625.text				2011-02-09 01:38:26 SEČ	2025-03-02 18:15:16 SEČ	2025-03-03 15:30:47 SEČ	2025-03-02 18:15:16 SEČ
 000627.jpg				2011-02-09 01:38:26 SEČ	2025-03-02 18:15:16 SEČ	2025-03-03 15:30:47 SEČ	2025-03-02 18:15:16 SEČ
 000628.pdf				2011-02-09 01:38:26 SEČ	2025-03-02 18:15:16 SEČ	2025-03-03 15:30:47 SEČ	2025-03-02 18:15:16 SEČ
 000629.pdf				2011-02-09 01:38:26 SEČ	2025-03-02 18:15:16 SEČ	2025-03-03 15:30:47 SEČ	2025-03-02 18:15:16 SEČ
 000630.pdf				2011-02-09 01:38:26 SEČ	2025-03-02 18:15:16 SEČ	2025-03-03 15:30:47 SEČ	2025-03-02 18:15:16 SEČ
 000631.pdf				2011-02-09 01:38:26 SEČ	2025-03-02 18:15:16 SEČ	2025-03-03 15:30:48 SEČ	2025-03-02 18:15:16 SEČ
 000632.pdf				2011-02-09 01:38:26 SEČ	2025-03-02 18:15:16 SEČ	2025-03-03 15:30:48 SEČ	2025-03-02 18:15:16 SEČ
 000633.xls				2011-02-09 01:38:27 SEČ	2025-03-02 18:15:16 SEČ	2025-03-03 15:30:48 SEČ	2025-03-02 18:15:16 SEČ
 000633.xls:Zone.Identifier				2011-02-09 01:38:27 SEČ	2025-03-02 18:15:16 SEČ	2025-03-03 15:30:48 SEČ	2025-03-02 18:15:16 SEČ
 000634.html				2011-02-09 01:38:27 SEČ	2025-03-02 18:15:16 SEČ	2025-03-03 15:30:48 SEČ	2025-03-02 18:15:16 SEČ
 000635.html				2011-02-09 01:38:27 SEČ	2025-03-02 18:15:16 SEČ	2025-03-03 15:30:48 SEČ	2025-03-02 18:15:16 SEČ

Zmeny v údajoch vieme overiť podľa change time, ale keďže sa zhoduje s created time, vieme povedať, že dáta neboli upravené.

Hypotéza **nie je potvrdená**.

Hypotéza 5 - USB obsahovalo škodlivý softvér



V zozname analyzovaných údajov neboli nájdené žiadne spustiteľné súbory (.exe, .dll, .bat), čo môže naznačiť, že v tomto prípade sa nejedná o malvérovú infekciu.

List Name	Files with Hits
 base64 (13)	13
 cmd.exe (5)	5
 download (505)	505
 exec (150)	150
 powershell (6)	6
 run (1685)	1685

Source Name	S	C	O	Keyword Preview	Keyword	Modified Time	Access Time	Change Time
001164.text				-transfer-encoding: «base64»content-type: image	base64	2011-02-09 01:38:57 SEČ	0000-00-00 00:00:00	0000-00-00 00:00:00
001164.text				-transfer-encoding: «base64»content-type: image	base64	2011-02-09 01:38:57 SEČ	2025-03-03 15:30:50 SEČ	2025-03-02 18:15:41 SEČ
001174.text				-transfer-encoding: «base64»content-type: image	base64	2011-02-09 01:38:57 SEČ	2025-03-03 15:30:50 SEČ	2025-03-02 18:15:40 SEČ
001174.text				-transfer-encoding: «base64»content-type: image	base64	2011-02-09 01:38:57 SEČ	0000-00-00 00:00:00	0000-00-00 00:00:00
001175.text				-transfer-encoding: «base64»content-type: image	base64	2011-02-09 01:38:57 SEČ	2025-03-03 15:30:50 SEČ	2025-03-02 18:15:40 SEČ
001175.text				-transfer-encoding: «base64»content-type: image	base64	2011-02-09 01:38:57 SEČ	0000-00-00 00:00:00	0000-00-00 00:00:00
002353.text				-transfer-encoding: «base64»>ej8+igkpaqqaacae	base64	2009-03-06 01:59:19 SEČ	2025-03-03 15:30:55 SEČ	2025-03-02 18:16:26 SEČ

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Strings

Extracted Text

Translation

Page: 61 of 77 Page
Matches on page: 1 of 2 Match
100%
Reset
Text Source: Search Results

```

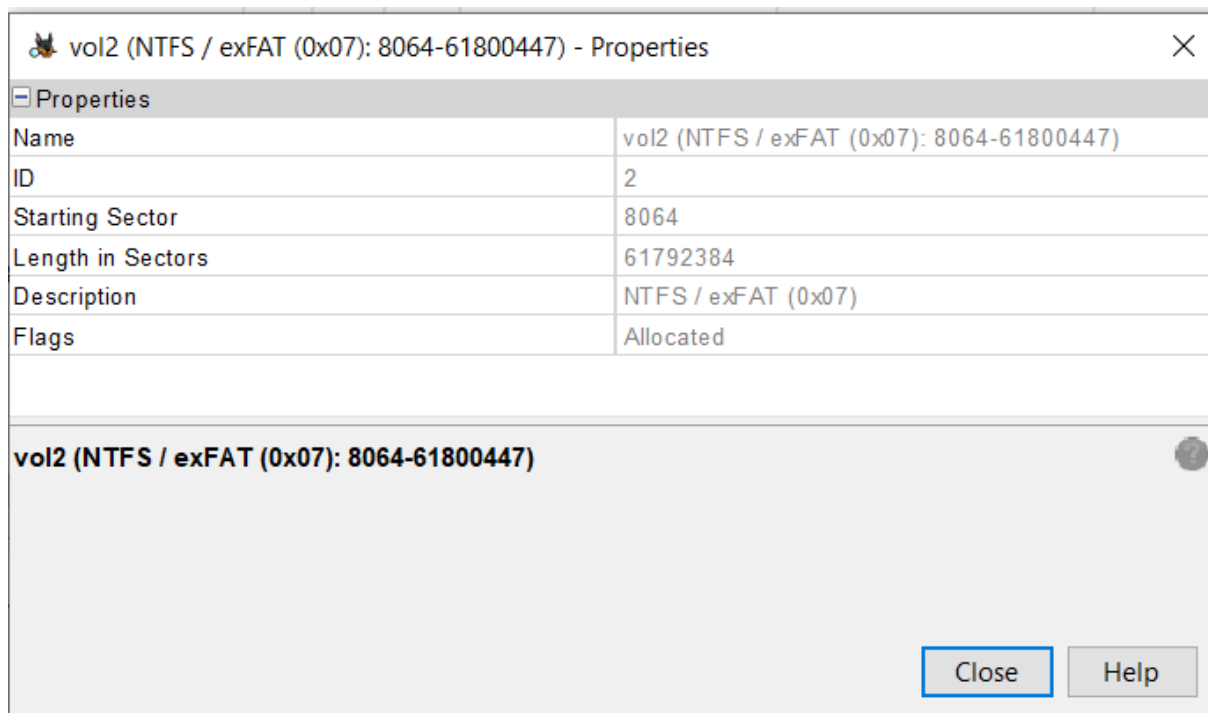
</div>
</div>
</body>
</html>
-----=NextPart_01C61113.FE222820
Content-Location: file:///C:/9E79BCBE/TownPlan_files/image001.gif
Content-Transfer-Encoding: base64
Content-Type: image/gif
R0IGODihNAFaAXcAMSH+GINvZnR3YXJlOiBNaWNyb3NvZnQgT2ZmaWNlACH5BAEAAAAALAEAAw
AVUBGQAAAAAAP///wECawl/jl+py+0Po5y02ouz3jyID4biSjbmiaqbrybuC8fyTNeYef6zvf+
DwyScMKi8YhMkoXEpFMjUqBzan1is1aq9qu9wumcZMl0/hWRvc8ubOubQ6xsS63Osu2ofn5p73
Y5NndBfV8gHgjhCdx4+Aa51NgnORhzaHMZ1Agz+Am5SsapRCdQGVqYdipXtWqoGvwoeKAoG8tq
y96q2vHvSvYh5O2Soybm6ug6yTKS2rMGKYw/FtNK828lzmMfc2LxgveDR4N6+o9rH1M3R3tvAZN
mEc/7X7dnrgej99//18OYAlj6byFK8jPX7Im8vTlurRM4LdpzCZuo1UMoUJ+/8s2xtE4y6Nedk/g
xUOxaaTGcg6BdonEmGnfnESqrQJcuGkhtOVVQFk5xHoO8M2suZL6BMpOao4YvitNbNcFFM7uill
juVRW9wQvelKjKLrQd9t5yYqai0sTR/XQx6luezMCfpOrXrUG5PvDqsQvHL15PevVEFDY5UuCfg
q4cTO34MGVPjyJQrW/55ObPmzY3se/6MpTPo0aRLTS6NoJWTO6pbu9bE+rXs25xEO76Nm2ju3bxx
x+4NvLx4MRHDy+OXPPx5Mwpl2BOPHz6NTtTq+OHO9PY0g6htkuLDzd35AhGrrRXTwY8Lqy+yD/
2Lwi9fTRozu9SibuXfbT0f/k4o5xHDIzDIABgfUdPl68BACoFn3QNNUJfGNVUOFl+GNLnyHzq
qGNgpxy24+FdCZ4Yon8pcthhfySuWEeFrqVxz4Yr3tiCd6rICON89vlo4Y473igkkD+2woiN5x5FZ
oo1FjiibSSO0SeVXKgx5UltAlrkhlgNCGWQZWB5ZloRbXkmi1JtmSWTUU64pJZy8uiCV0by+GSP
Tqo3Z4hKltkniT4Kug5bbPopHjYDOjnlNvCwSuiCulo6ahcoloo2LueWGNKBqKqZyZbldjfsIS
+IKGggoYYSeHPojmlb3EISGXxoaKa59m8bphYdf1mh1KwaL0UAdwzGFsssr/LsusBG8OC61yweZL

```

Pomocou Autopsy Keyword Search boli vyhľadávané kľúčové slová, ktoré sa objavili v niektorých súboroch. Hoci samotné súbory pôsobia podozrivo, ich kontext nevyzerá byť škodlivý.

Hypotéza **nie je potvrdená**.

Umiestnenie súborov + súborový systém:



Zariadenie obsahuje partíciu vo formáte NTFS/exFAT, čo umožňuje uchovávanie metadát a logov.

Reťazec starostlivosti:

Číslo:	1	Typ súboru :	.mem	Obnovený súbor:	Nie	Veľkosť :	17,2 GB
Popis prípadu:	Neoprávnená manipulácia s dátami na USB kľúči						
Názov súboru:	memdump.mem						
Miesto získania digitálnej stopy:	Patriot Supersonic Rage XT 32GB						
Poznámky :							
	MD5	6dca7f1f38b1ead2bf352c03cfb8e4d6					

Digitálny odtlačok (hash):	SHA 1	99c043c5b9ab71595172f9c7c2af4da0e382c271
Časová pečiatka:	Akcia vykonaná s digitálnou stopou:	
Mon Mar 3 15:35:22 2025	Akvizícia sa začala	
Mon Mar 3 15:38:28 2025	Akvizícia ukončená	

Bezpečnostné opatrenia:

1. Fyzická ochrana

- Zariadenie bolo uložené do antistatického obalu a bezpečnostného puzdra.
 - Chránené pred teplotou, vlhkosťou a magnetickými poľami.

2. Digitálna ochrana

- USB kľúč nebol pripájaný k bežnému počítaču, aby sa predišlo zmene dát.
- Bol použitý write-blocker na ochranu pred zápisom.
- Čo najskôr vytvorený forenzný obraz (pomocou FTK Imager).

3. Dokumentácia a skladovanie

- Bol evidovaný dátum, čas, miesto nálezu a manipulácia.
- USB kľúč bol uchovávaný v trezore a analyzovaný v izolovanom prostredí.

Odborné články z DFRWS:

1. DFRWS 2021 Challenge – Časť 4: QNAP NAS

Táto forenzná výzva zahŕňa analýzu NAS zariadenia, čo je relevantné pre prípady, kde je potrebné rekonštruovať RAID pole a analyzovať systémové dáta. Hoci sa priamo nezameriava na USB kľúče, poskytuje cenné poznatky o analýze úložných

zariadení.

<https://dfrws.org/dfrws-2021-challenge/>

2. FirmUSB: Vetting USB Device Firmware using Domain Informed Symbolic Execution

Tento článok predstavuje FirmUSB, ktorý využíva symbolickú analýzu na preverovanie firmvéru USB zariadení. Cieľom je identifikovať potenciálne škodlivé aktivity v embedded USB zariadeniach bez potreby zdrojového kódu.

<https://arxiv.org/abs/1708.09114>

Literatúra a prípadové štúdie:

1. MAGNETO: Fingerprinting USB Flash Drives via Unintentional Magnetic Emissions

Tento článok predstavuje metódu identifikácie USB flash diskov prostredníctvom analýzy ich neúmyselných magnetických emisií. Štúdia ukazuje, že tieto emisie sú jedinečné pre každý USB disk, čo umožňuje ich presnú identifikáciu. Táto technika môže byť užitočná pri forenzných analýzách na overenie autenticity USB zariadení.

<https://arxiv.org/abs/2002.05905>

2. Teardown and Feasibility Study of IronKey -- The Most Secure USB Flash Drive

Tento článok sa zaoberá analýzou hardvéru a bezpečnostných mechanizmov USB flash disku IronKey, ktorý je považovaný za jeden z najbezpečnejších na trhu. Štúdia poskytuje podrobný pohľad na vnútornú architektúru zariadenia a hodnotí jeho odolnosť voči rôznym typom útokov. Tieto informácie môžu byť cenné pri posudzovaní bezpečnosti USB zariadení v rámci forenzných vyšetrení.

<https://arxiv.org/abs/2110.14090>

Záver

Vyšetrovanie neoprávnenej manipulácie s dátami na USB kľúči prinieslo niekoľko dôležitých zistení. Analýza metadát, časových pečiatok a systémových logov pomocou forenzných nástrojov (Autopsy, FTK Imager, HxD) potvrdila, že USB kľúč bol v čase jeho straty a neskoršieho nálezu pripojený k systému, ktorý nepatril zamestnancovi, ktorý nahlásil stratu. Zistenia poukazujú na to, že súbory na USB boli otvorené, avšak nedošlo k ich úprave alebo vymazaniu v období po strate – vymazané súbory boli identifikované ako operácie vykonané pred stratou kľúča, kvôli tomuto faktu nebolo potrebné obnovovať vymazané údaje.

Ďalej bola overená integrita dát, pričom sa nezistili žiadne stopy škodlivého softvéru ani spustiteľných súborov, čo svedčí o tom, že hoci došlo k neoprávnenému prístupu, neboli vykonané aktívne škodlivé zmeny. Celková analýza teda potvrdzuje, že USB kľúč bol manipulovaný neoprávnene, pričom sa najviac prejavil neoprávnený prístup k citlivým firemným dátam. Tieto zistenia podčiarkujú potrebu prísnejších bezpečnostných opatrení, aby sa predišlo podobným incidentom v budúcnosti.