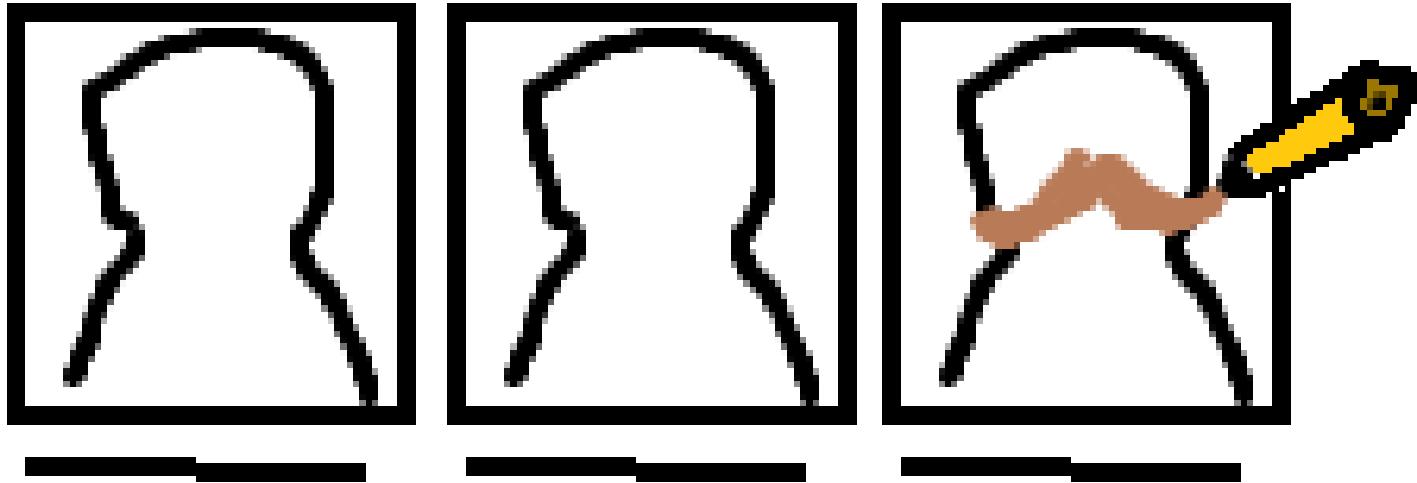


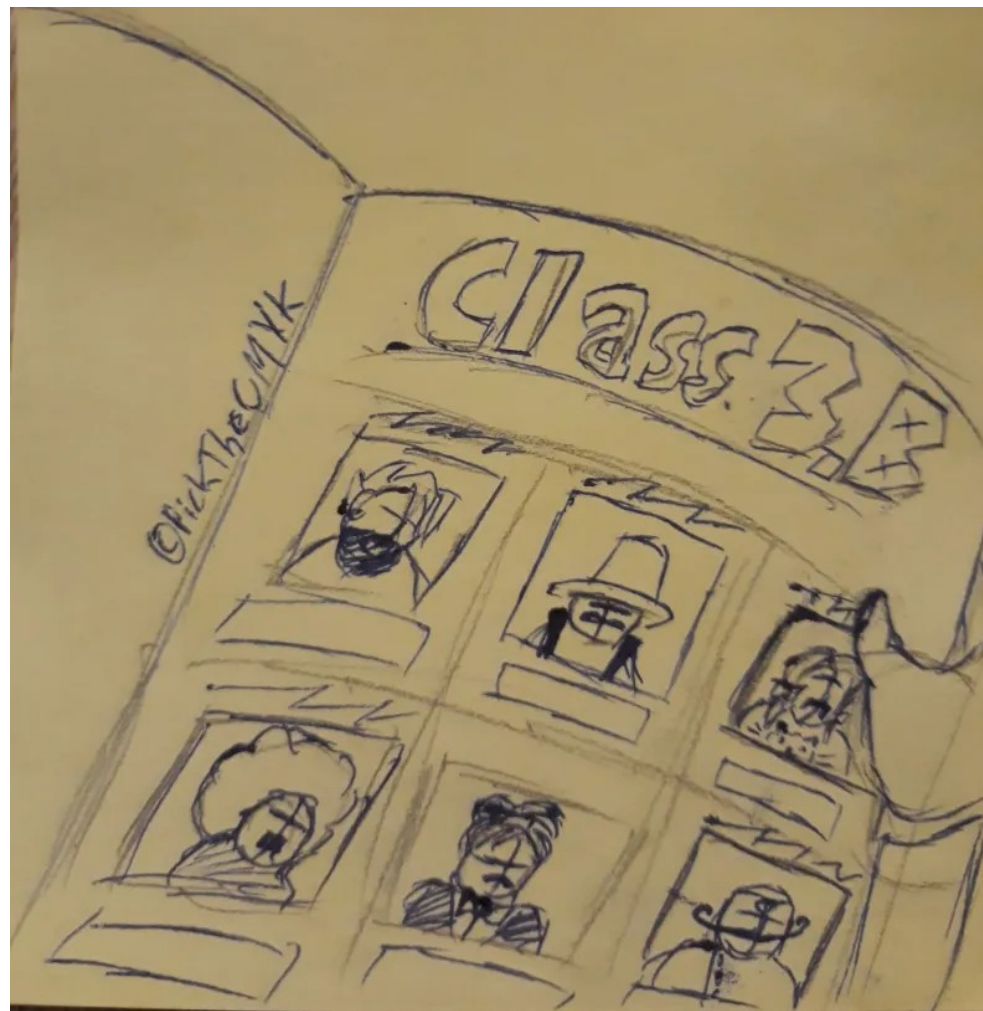


Fúzatý prípad

Marek Miškolci

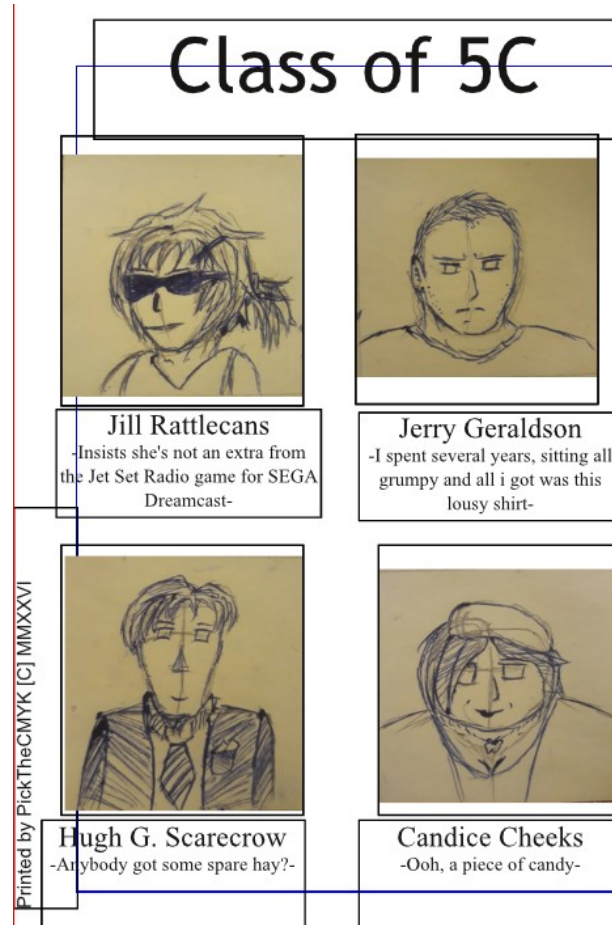
Popis prípadu

- Vandalizácia digitálnej publikácie – ročenky pridáním fúzov do jednotlivých obrázkových súborov.
- Deň pred tlačou po tlačovej kontrole
- Súbory na tlač boli na notebooku, našiel sa pri ňom USB kľúč.
- Je možné, že sa na USB nachádza ešte niečo



Predmet a cieľ vyšetrovania

- Zaistiť všetky potenciálne zdroje dôkazov, spraviť image operačnej pamäte, úložiskových médií, analyzovať ich
- Na základe vyšetrovania zoceliť bezpečnosť tlačiarenskej firmy
- Zistiť presne kto a prečo to spravil donútiť ho pokryť náklady spojené s pokazenou tlačou



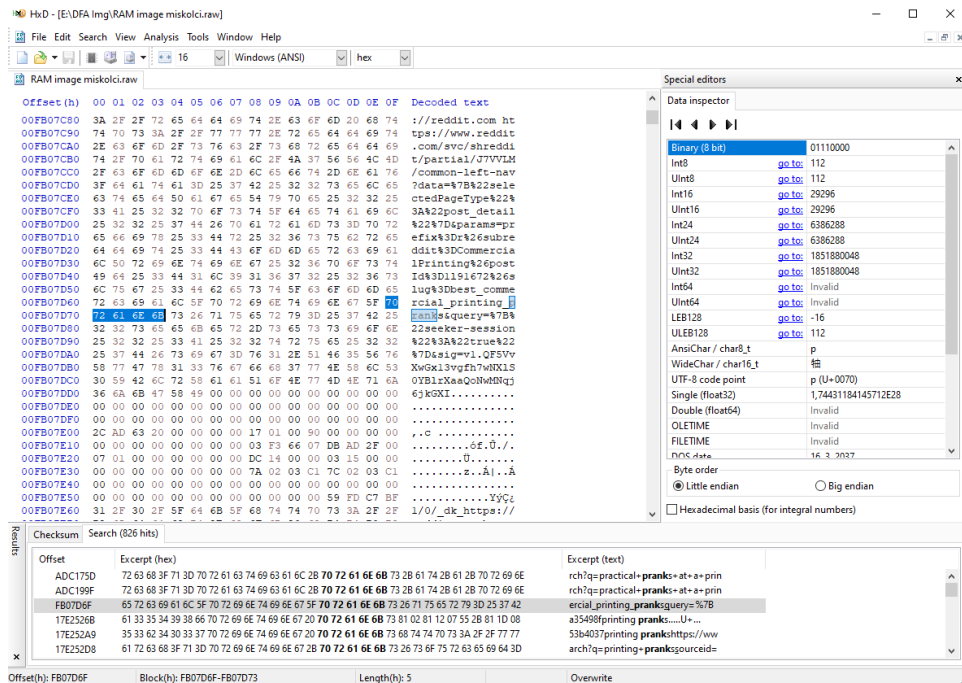
5WH

- What?
Znehodnotenie tlačovej publikácie
- Who?
Pravdepodobne niekto z personálu tlačovej firmy
- Where?
Oddelenie tlačovej firmy
- When?
Deň pred tlačou.
- Why?
Je viacero možných motívov(sabotáž, žartík,iné...)
- How?
Pravdepodobne prostredníctvom softvéru na USB

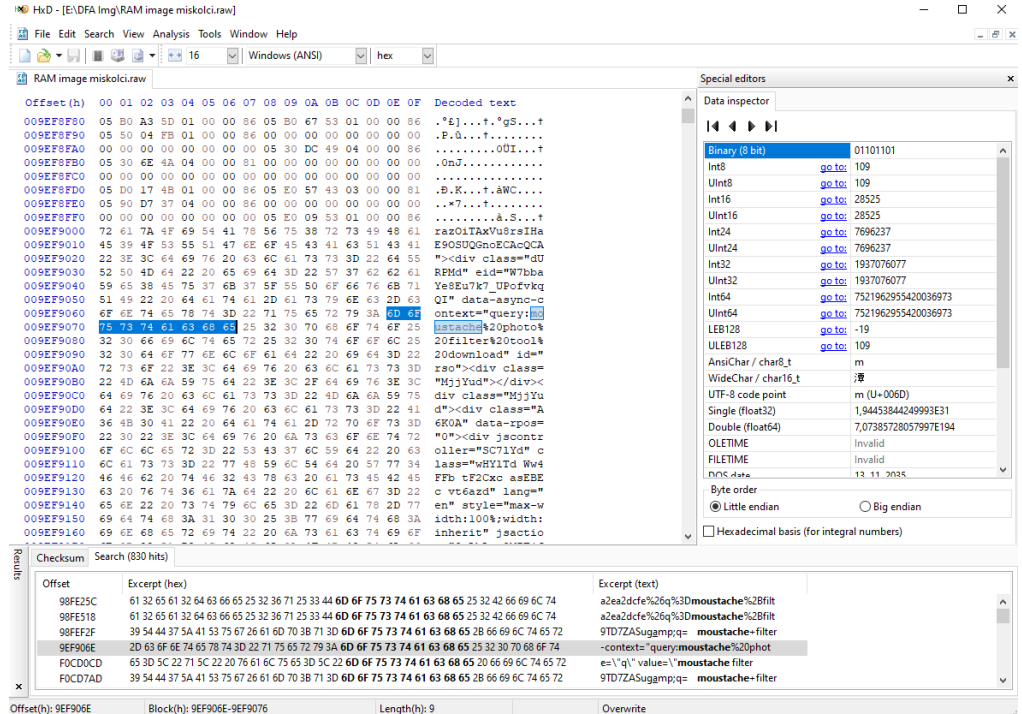
Hypotézy

- A: Motívom bolo spravenie žartíku, na USB popri programe na pridanie fúzov boli ďalšie
- B: Išlo o úmyselnú sabotáž, vandalizmus fotiek mal od toho odlákať pozornosť
- C: USB/Notebook skompromitované treťou stranou
- D: Na USB bol len program na vandalizáciu, možný motív z hypotéz A-C

- Páchateľ zanechal stopy na základe ktorých bolo zrejmé, že chce vyparatiť nejaký žartík, no druhá časť hypotézy bola zamietnutá, nakoľko sa na USB našiel len softvér na znehodnotenie tlačovej publikácie
- Čiastočne potvrdená

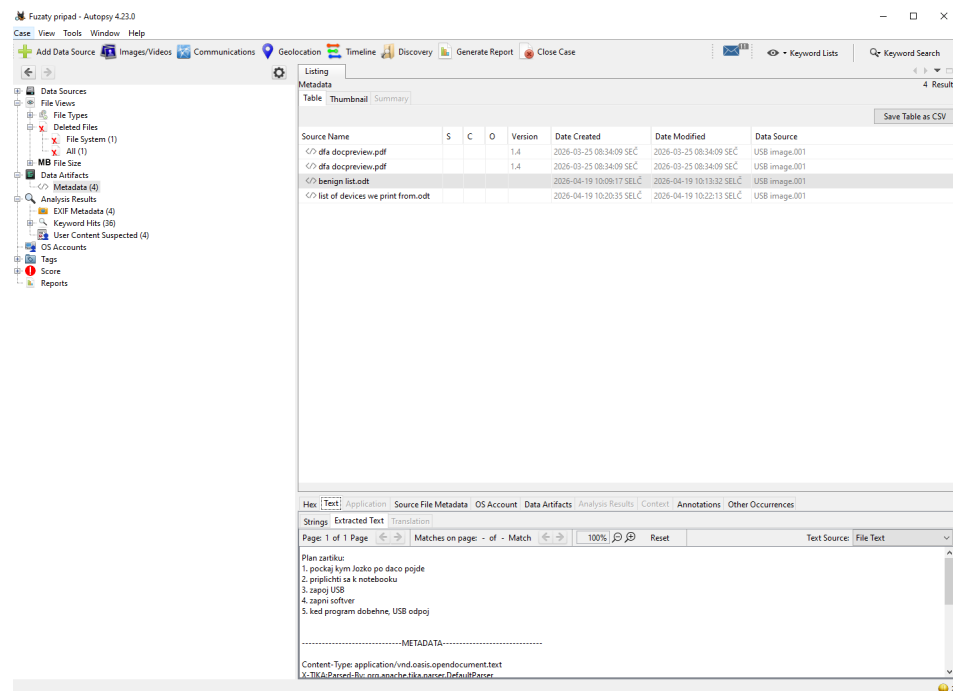
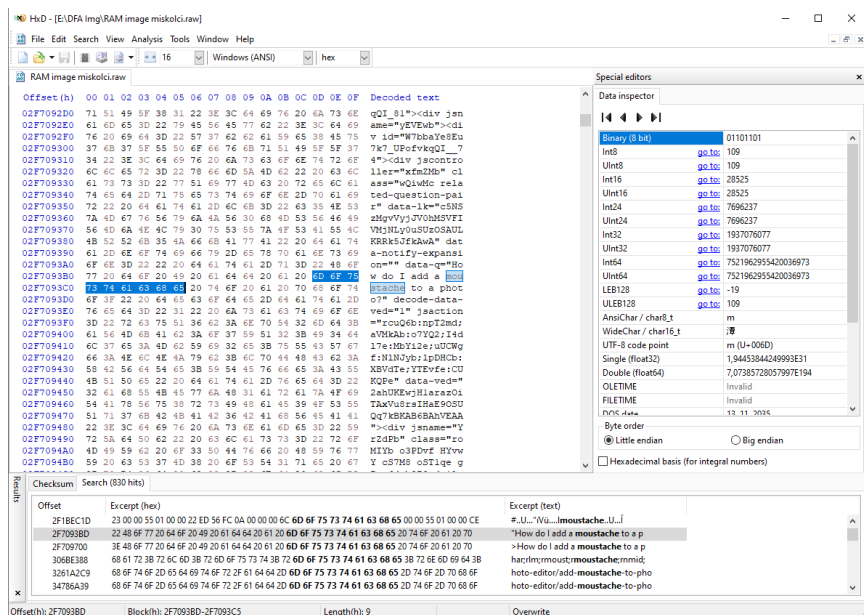


- Na základe stôp nie je možné podložiť túto hypotézu, práveže naopak – dôkazy nás vedú do opačného smeru
- Zamietnutá



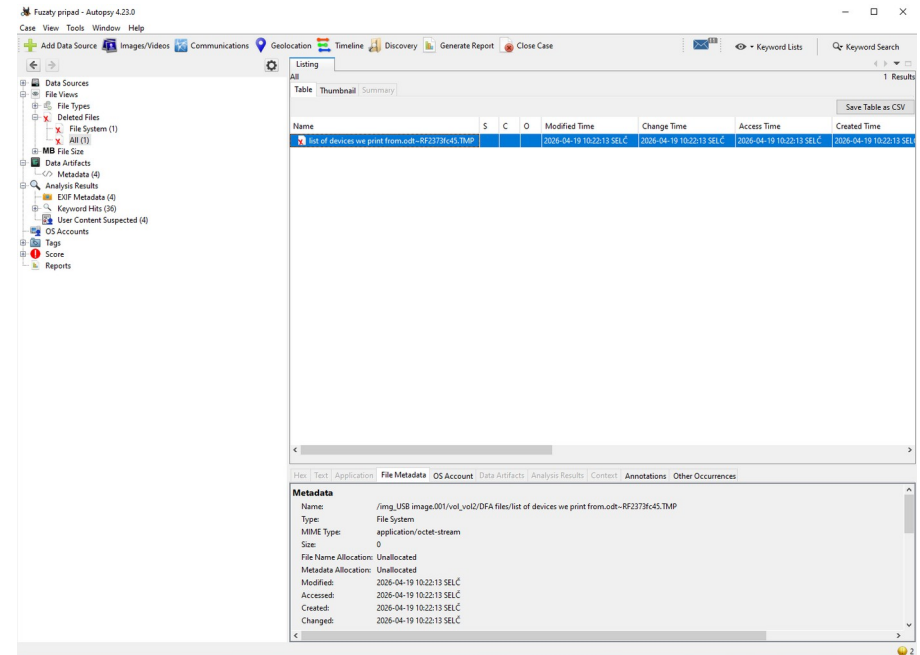
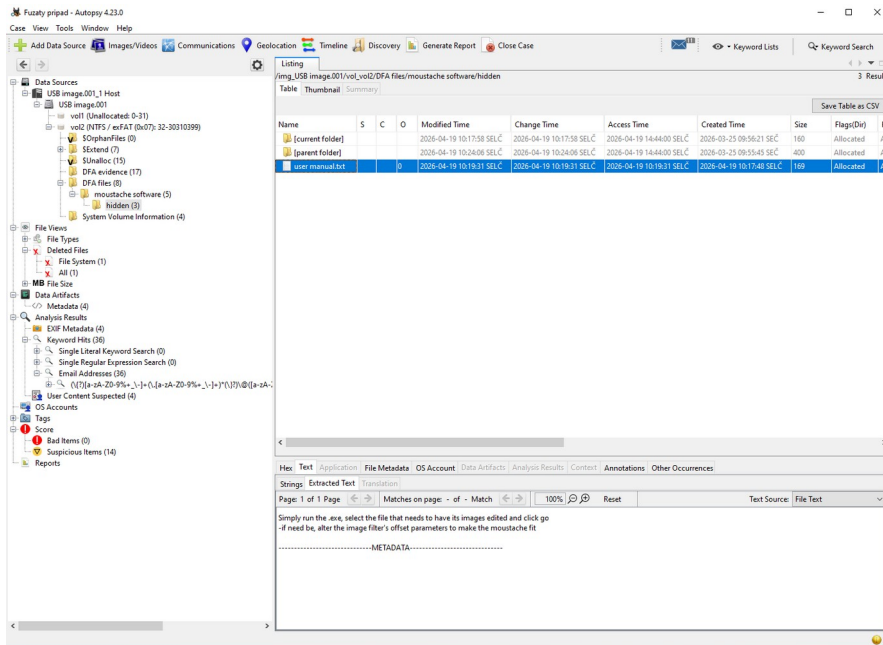
Overechné Hypotézy C

- Analýza USB a jej výsledky potvrdili, že išlo o niečo vopred plánované a zámerné, bez zásahu tretej strany
- Zamietnutá



Overenie Hypotézy D

- Na (image) USB sa (ani vo vymazaných súboroch) nenašlo nič okrem softvéru na znehodnotenie tlačovej publikácie a s tým spojenými súbormi
- Motív je viac než pravdepodobne identický s hypotézou A
- Potvrdená



Zariadenia

Notebook: DELL Latitude E7270

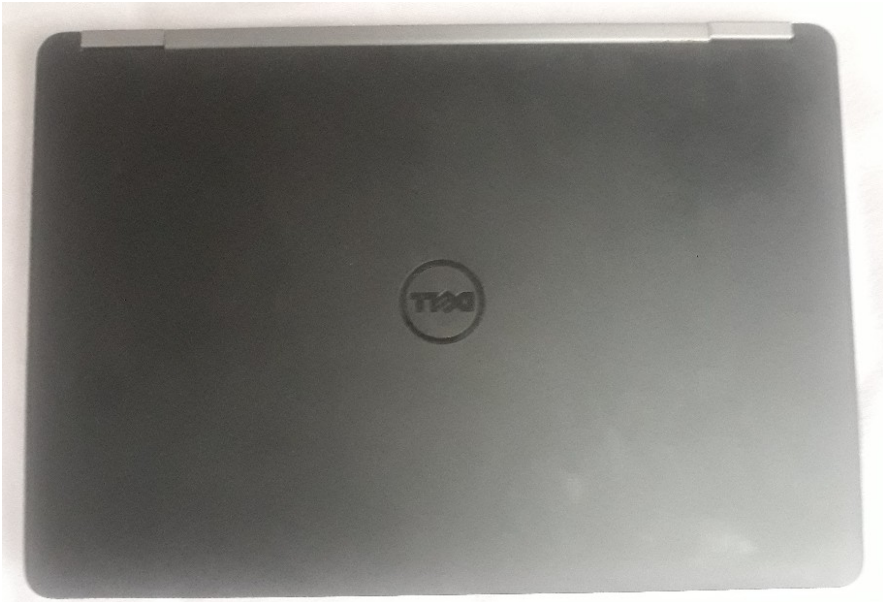
-Úložisko: 252 GB

-OS: Windows 10 Pro

-Procesor: Intel Core i5(2-core, 2.40GHz)

-RAM: 8GB

-GPU: Integrovaný Intel HD Graphics 520(300MHz, 345.6 GFLOPS)



Zariadenia

USB: Verbatim Slider

-tzv. DFA_usb

-USB 2.0

-16 GB



Zoznam použitých softvérových nástrojov a ich použitie

- Exterro FTK Imager-Vytvorenie a čítanie image zariadenia spojeného s prípadom
- HxD-Prístup ku a prehliadanie image súboru pre RAM
- Magnet RAM Capture-Získanie image RAM-ky
- Autopsy-nástroj na analýzu dôkazov a ďalšie vyšetrovanie

Zabezpečenie dôkazov a reťazec úschovy

- Image súbory získané z operačnej pamäte a USB s použitím writeblockera
- Zálohy
- Fyzické zabezpečenie USB a pamäťového média, ktoré uskladňuje jednotlivé image súbory
- Založený chain-of-custody

Číslo:	1	Typ súboru:	Image USB, RAM	Obnovený súbor:		Veľkosť:	31GB
Popis prípadu:	Interná vandalizácia tlačovej publikácie, podozrenie, že na npadnutom hardvéri sú potenciálne škodlivé súbory						
Názov súboru:	USB kľúč „DFA_USB“(USB_image.raw), dáta z RAM (RAM_image.raw)						
Miesto získania digitálnej stopy:	Na pravdepodobnom mieste činu, v oddelení tlačovej firmy, z ktorého bola znehodnotená publikácia finalizovaná a posielaná do tlače						
Poznámky:	Image z USB, čo bol Marek kúpiť v nedeľu(8.3.) večer v Alze, zabezpečené v pôvodnom obale, pri notebooku(z ktorého pochádza RAM image)						
Časové pečiatky							
Access:	17:27(9.3.2026)		Modify:	13:20(12.4.2026)		Change:	N/A
Digitáln y odtlačok (heš)	MD5	8a23fa77df5549bd894f0e71d91336f3					
	SHA1	61a2b2879833a68d485c0fccddf234c622f1fc37					
Časová pečiatka	Akcia vykonaná s digitálnou stopou						
10:51(11.3.2026)	Spravený image USB kľúča(cez FTK Imager)						
13:20(12.4.2026)	Spravenie image-u RAM pamäte (cez Magnet Forensics RAM Capture)						



Ďakujem za pozornosť