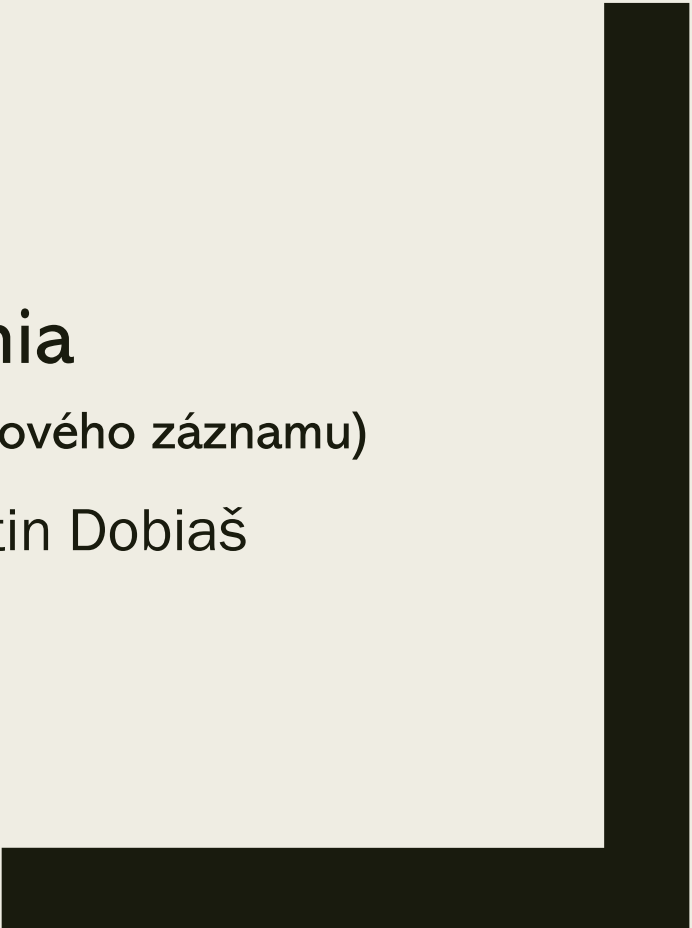


Forenzná analýza USB zariadenia

(v prípade manipulácie kamerového záznamu)

Martin Dobiaš



Úvod do prípadu

V spoločnosti X bol zaznamenaný výpadok kamerového záznamu a po jeho obnovení sa zistil chýbajúci kamerový záznam

Počas kontroly serverovne sa našlo na podlahe USB ktoré sa predalo forenznému tímu ako dôkazový materiál, pre preverenie, či bolo použité pri trestnej činnosti pozmenenia kamerových záznamov a nájdenie vinníka

Cieľ DFA:

Identifikovať, či USB zariadenie použité pri trestnom čine

Preskúmať súbory a metadáta na USB a zistiť ich

Zrekonštruovať udalosti trestného činu

Identifikovať možného páchatel'a

Poskytnúť dôveryhodné dôkazy pre právne kroky

Identifikácia

Kto?

- Predmetom
vyšetrovania (predpoklad
majiteľ USB)

Čo?

- Pozmenenie
kamerového záznamu z
dôvodu skrytia inej
trestnej činnosti

Kedy?

- Pri výpadku kamerového
záznamu v nočných
hodinách (okolo 2-4
rannej hodiny)

Where?

- V serverovni danej
spoločnosti X

Prečo?

- Skrytie inej nelegálnej
(trestnej) činnosti alebo
export záznamu z
neznámeho dôvodu

Ako?

- Predmetom
vyšetrovania (predpoklad
lokálne pomocou USB
alebo cez sieť)

Zaistenie dôkazy



Hypotézy

Hypotéza 1: Export kamerových záznamov na USB

Hypotéza 2: Vymazanie záznamov (na USB sa nachádzal skript na vymazanie logov)

Hypotéza 3: Zapojenie USB a spustenie skriptu na vymazanie záznamu

~~Hypotéza 4: Vymazanie záznamu cez sieť (USB nebolo súčasťou)~~



Analýza USB

Data Sources

ObrazFTK.001_1 Host

File Views

File Types

By Extension

Images (25)

Videos (1)

Audio (1)

Archives (0)

Databases (0)

Documents

HTML (0)

Office (0)

PDF (0)

Plain Text (486)

Rich Text (0)

Executable

.exe (0)

.dll (0)

.bat (0)

.cmd (0)

.com (0)

By MIME Type

application

x-msdownload (1)

json (497)

octet-stream (17)

image

vnd.microsoft.icon (1)

x-portable-floatmap (1)

vnd.zbrush.pcx (1)

x-portable-arbitrarymap (1)

text

x-python (1)

plain (479)

csv (489)

x-ini (2)

x-log (498)

Usage	
OS	
Size	15,48 GB
File Types	
Images	1
Documents	1 963
Executables	1
Unknown	17
Other	6
Not Analyzed	95
Allocated Files	
2 059	
Unallocated Files	
24	
Slack Files	
13	
Directories	
35	

Image

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
commands_backup.txt			0	2025-03-22 08:26:42 SEČ	2025-03-22 08:26:42 SEČ	2025-03-22 08:26:42 SEČ	2025-03-22 06:09:05 SEČ	227	Allocated	Allocated	unknown
file_1015.txt			0	2025-03-19 20:38:46 SEČ	2025-03-20 20:56:56 SEČ	2025-03-22 06:09:06 SEČ	2025-03-22 06:09:06 SEČ	405	Allocated	Allocated	unknown
file_1018.txt			0	2025-03-19 20:38:46 SEČ	2025-03-20 20:57:00 SEČ	2025-03-22 06:09:06 SEČ	2025-03-22 06:09:06 SEČ	410	Allocated	Allocated	unknown
file_102.txt			0	2025-03-19 20:38:46 SEČ	2025-03-20 20:57:19 SEČ	2025-03-22 06:09:06 SEČ	2025-03-22 06:09:06 SEČ	176	Allocated	Allocated	unknown
file_1026.txt			0	2025-03-19 20:38:46 SEČ	2025-03-20 20:56:42 SEČ	2025-03-22 06:09:06 SEČ	2025-03-22 06:09:06 SEČ	410	Allocated	Allocated	unknown

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Strings

Extracted Text

Translation

Page: 1 of 1 Page

Matches on page: - of - Match

100%

Reset

Text Source: File Text

-- Export všetkých záznamov pred vymazaním

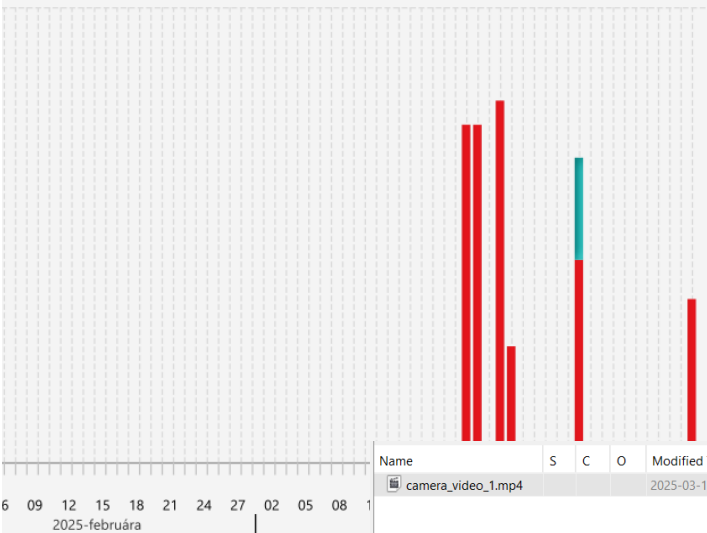
SELECT * FROM recordings INTO OUTFILE '/tmp/extracted_data.csv';

-- Vymazanie logov o prístupe

DELETE FROM access_logs WHERE user='unknown' AND timestamp > '2025-03-18 02:00:00';

-----METADATA-----

Documents; 1 963
94%



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
camera_video_1.mp4				2025-03-19 20:48:46 SEČ	2025-03-20 20:56:30 SEČ	2025-03-22 06:10:12 SEČ	2025-03-22 06:10:12 SEČ	54	Allocated	Allocated	unknown

Číslo:	01	Typ súboru:	.py	Obnovený súbor:	nie	Veľkosť:	1kB
Popis prípadu:		Forenzná analýza USB zariadenia v prípade manipulácie kamerového systému					
Názov súboru:		backup_script.py					
Miesto získania digitálnej stopy:		USB zariadenie					
Poznámky:		USB nájdené na podlahe serverovne, nikto sa k USB nehlásil					
Časové pečiatky							
Access:	[2025-03-25 1:03:58]	Modify:	[2025-03-25 1:58:00]	Change:			
Digitálny odtlačok (heš)	MD5	2074394f08ade3501392f4b9ea8bb873					
	SHA1	562d0bec89e45576592a77c3b92ac2fad3121335					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
28.03.2025 10:24		Kontrola zhody digitálneho odtlačku					
Change Time		Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known

Analýza PC (RAM)

```
249E59000 01 00 00 00 F8 03 00 00 68 74 74 70 73 3A 2F 2F ....f...https://
249E59010 77 77 77 2E 67 6F 6F 67 6C 65 2E 63 6F 6D 2F 73 www.google.com/s
249E59020 65 61 72 63 68 3F 71 3D 75 73 62 2B 73 63 72 69 earch?q=usb+scri
249E59030 70 74 2B 74 6F 2B 64 65 6C 65 74 65 2B 72 65 63 pt+to+delete+rec
249E59040 6F 72 64 2B 66 72 6F 6D 2B 68 69 6B 76 69 73 69 ord+from+hikvisi
249E59050 6F 6E 2B 6E 76 72 26 63 6C 69 65 6E 74 3D 66 69 on+nvr&client=fi
249E59060 72 65 66 6F 78 2D 62 2D 64 26 73 63 61 5F 65 73 refox-b-d&scas
249E59070 76 3D 36 33 66 34 30 31 61 36 65 62 34 35 62 38 v=63f401a6eb45b8
249E59080 32 31 26 65 69 3D 4F 33 58 65 5A 5F 57 61 4E 37 21&ei=O3XeZ_WaN7
249E59090 4B 72 39 75 38 50 38 49 4F 69 6B 41 67 26 76 65 Kr9u8P8IOikAg&ve
249E590A0 64 3D 30 61 68 55 4B 45 77 69 31 70 4F 57 43 6F d=0ahUKEwilpOWCo
249E590B0 35 32 4D 41 78 57 79 6C 66 30 48 48 66 43 42 43 52MaxWylf0HHfCBC
249E590C0 49 49 51 34 64 55 44 43 42 41 26 75 61 63 74 3D IIQ4dUDCBA&uact=
249E590D0 35 26 6F 71 3D 75 73 62 2B 73 63 72 69 70 74 2B 5&oq=usb+script+
249E590E0 74 6F 2B 64 65 6C 65 74 65 2B 72 65 63 6F 72 64 to+delete+record
249E590F0 2B 66 72 6F 6D 2B 68 69 6B 76 69 73 69 6F 6E 2B +from+hikvision+
```

Properties			
Device Name:	Port_#0002.Hub_#0002	Description:	Kingston DataTraveler 2.0 USB Device
Device Type:	Mass Storage	Connected:	No
Safe To Unplug:	Yes	Disabled:	No
USB Hub:	No	Drive Letter:	M:
Serial Number:	C860008863CFB0804A16A977	Registry Time 1:	25. 3. 2025 1:58:00
Registry Time 2:	12. 2. 2025 16:59:36	VendorID:	0930
ProductID:	6545	Firmware Revision:	1.10
WCID:		USB Class:	08
USB SubClass:	06	USB Protocol:	50
Hub / Port:		Computer Name:	LAPTOP-16A977
Vendor Name:		Product Name:	
ParentID Prefix:		Service Name:	USBSTOR
Service Description:	@usbstor.inf,%USBSTOR.SvcDesc%;USB Mass	Driver Filename:	USBSTOR.SYS
Device Class:		Device Mfg:	Compatible USB storage device
Friendly Name:		Power:	
USB Version:	2.00	Driver Description:	USB Mass Storage Device
Driver Version:	10.0.19041.4355	Driver InfSection:	USBSTOR_BULK.NT
Driver InfPath:	usbstor.inf	Instance ID:	USBVID_0930&PID_6545\C860008863C
Capabilities:	Removable, UniqueID, SurpriseRemovalOK	Install Time:	
First Install Time:		Connect Time:	
Disconnect Time:			

Číslo:	03	Typ súboru:		Obnovený súbor:	nie	Veľkosť:	8GB
Popis prípadu:	Forenzná analýza USB zariadenia v prípade manipulácie kamerového systému						
Názov súboru:	sys						
Miesto získania digitálnej stopy:	PC v kancelárii X						
Poznámky:	PC podozrivého zamestnanca firmy , PC zapnutý – urobený image RAM						
Časové pečiatky							
Access:		Modify:		Change:			
Digitálny odtlačok (heš)	MD5	f5d2b3a0ac467f7fa1ff3b428d8d7f4b					
	SHA1	ce2e4d97fd76efed6fcb8275e8f8f24f3c9f7c9a					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
26.03.2025 8:24		Vytvorenie image pamäte RAM z PC					
28.03.2025 15:36		Analýza image v AutoPsy					

OK

Analýza NVR

1	2025-3-25 2:15:00
Hlavný typ: Informácie Vedľajší typ: USB zariadenie pripojené Lokálne prihlásenie užívateľa: admin IP adresa hosta: N/A Parameter: USB_DISK_1 Port: USB-Front	
2	2025-3-25 2:15:35
Hlavný typ: Operácia Vedľajší typ: Export záznamu Lokálne prihlásenie užívateľa: admin IP adresa hosta: N/A Parameter: 2025-03-25 02:15:00 - 2025-03-25 03:00:00 Kanál č.: A1	
3	2025-3-25 2:16:00
Hlavný typ: Informácie Vedľajší typ: USB zariadenie odpojené Lokálne prihlásenie užívateľa: admin IP adresa hosta: N/A Parameter: USB_DISK_1 Port: USB-Front	

Číslo:	02	Typ súboru:	.txt	Obnovený súbor:	nie	Veľkosť:	9kB
Popis prípadu:		Forenzná analýza USB zariadenia v prípade manipulácie kamerového systému					
Názov súboru:		20250410140051logBack.txt					
Miesto získania digitálnej stopy:		NVR Hikvision					
Poznámky:		NVR značky Hikvision nájdené v serverovni z ktorého bol pravdepodobne vymazaný record					
Časové pečiatky							
Access:	[2025-04-10 9:00:00]	Modify:	[2025-04-10 9:00:00]	Change:			
Digitálny odtlačok (heš)	MD5	2074394f08ade3512592f4b9eb8ab122					
	SHA1	2074394f08ade3512592f4b9eb8abd3121335					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
28.03.2025 11:24		Export logov z NVR					

Záver vyšetrovania

- Na základe výpisu z NVR vieme dokázať, že naozaj bola manipulácia zo záznamom a taktiež že nájdené USB bolo naozaj pripojené a využité na tento útok.
- Na PC ktorého RAM pamäť prešla analýzou sa taktiež vyhl'adával podozrivý obsah (po otvorení webovej adresy sme našli použité príkazy, ktoré sa zhodovali s tými na USB). Taktiež po analýze PC dvoch zamestnancov firmy sa potvrdilo že v jednom z ich PC bolo dané USB zapojené cca 15 minút pred incidentom. Po pokročilom preskúmaní sa na USB objavili aj stiahnuté záznamy na ktorých sa majiteľ PC taktiež nachádza.
- Potvrdili sa hypotézy 1-3, 4 hypotéza že išlo o sieťový útok sa vyvrátila.



ĎAKUJEM ZA POZORNOST

Martin Dobiaš 2024/2025

