

Online vydieranie

Samuel K.

Link na prezentáciu:

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

Prípad vyšetrovania:

V rámci tohto prípadu došlo k vytvoreniu falošného profilu na sociálnej sieti Instagram, kde boli zverejnené fotografie jednej študentky. Tieto fotografie mohli byť získané rôznymi spôsobmi, napríklad tajným fotografovaním obete alebo zneužitím jej zariadenia alebo účtu na sociálnych sieťach. Osoba, ktorá vytvorila tento falošný profil, sa následne vydávala za obeť a začala s ňou komunikovať, pričom tvrdila, že má prístup k ďalším súkromným materiálom. Po nadviazaní kontaktu začala táto osoba obeť vydierať, požadujúc od nej finančnú sumu výmenou za nezverejnenie ďalších údajne kompromitujúcich fotografií. Obeť si všimla falošný profil, keď jej prišla žiadosť o sledovanie, a ihneď si uvedomila, že jej fotografie boli použité bez jej súhlasu. Začala s páchateľom komunikovať a neskôr pochopila, že ide o vydieranie. Rozhodla sa prípad nahlásiť na políciu a poskytla všetky dostupné informácie, vrátane komunikácie s páchateľom, názvu falošného profilu a časových údajov o interakciách. Niektoré správy boli však zo strany páchateľa odstránené. Okoloidúci svedok taktiež poskytol svoj mobilný telefón ako prostriedok dôkazov. Forenzní analytici následne začali vyšetrovanie s cieľom identifikovať a usvedčiť páchateľa.

5WH:

Who (Kto):

- **Páchateľ:** Osoba, ktorá získala fotografie obete a vytvorila falošný profil na sociálnej sieti.
- **Obeť:** Osoba, ktorej fotografie boli zverejnené bez jej súhlasu a ktorá čelila vydieraniu.
- **Svedok:** Osoba, ktorá mohla byť prítomná v okolí, napríklad študent, ktorý mohol mať prístup k relevantným informáciám alebo videozáznamu.
- **Vyšetrovatelia:** Polícia a forenzní analytici, ktorí sa zaoberajú vyšetrovaním prípadu.

What (Čo):

- Páchateľ vytvoril falošný profil na Instagrame, kde zverejnil fotografie študentky bez jej súhlasu. Následne ju kontaktoval a začal ju vydierať s tvrdením, že má ďalšie kompromitujúce materiály a požadoval peniaze za ich nezverejnenie.

When (Kedy):

- Incident sa stal počas letného semestra školského obdobia, kedy fotografie obete boli získané a zverejnené.

Where (Kde):

- **Fyzicky:** Miesto, kde boli fotografie obete tajne zhotovené (pred školou).
- **Digitálne:** Sociálna sieť, kde bol vytvorený falošný profil a prebiehala komunikácia.

Why (Prečo):

- Páchateľ mohol mať osobné alebo finančné motívy na využitie anonymného prostredia internetu za účelom vydierania. Čas útoku mohol byť ovplyvnený aj tým, že obeť mohla byť v zraniteľnej situácii, otočená chrbtom a podobne.

How (Ako):

- Páchateľ pravdepodobne získal fotografie stiahnutím z verejných zdrojov, neoprávneným prístupom k účtu alebo tajným fotografovaním. Potom vytvoril falošný profil, predstieral, že je obeť, nadviazal s ňou kontakt a začal psychologickú manipuláciu a vydieranie.

Predmet vyšetrovania:

Cieľom vyšetrovania je identifikovať a usvedčiť páchatela online vydierania prostredníctvom dôkazov získaných digitálnou forenznou analýzou.

Ciele vyšetrovania:

1. **Identifikácia páchatela** – Zistiť, kto vytvoril falošný profil a komunikoval s obeťou cez analýzu digitálnych stôp.
2. **Preukázanie manipulácie a vydierania** – Pomocou analýzy komunikácie dokázať manipuláciu a vydieranie na strane páchatela.
3. **Stanovenie časovej osi** – Určiť čas a miesto interakcií medzi páchatelom a obeťou pomocou bezpečnostných kamier a mobilného zariadenia svedka.

Očakávaný výsledok:

Cieľom vyšetrovania je zhromaždiť dostatočné dôkazy na identifikáciu a usvedčenie páchatela online vydierania.

Hypotézy:

Hypotéza 1

Študent získal fotografie obete, ktoré tajne odfotil, a následne ich použil na vytvorenie falošného profilu na Instagrame. Po vytvorení profilu začal komunikovať s obeťou, predstierajúc, že má prístup k ďalším súkromným materiálom, a začal ju vydierať.

Hypotéza 2

Fotografie obete sa mohli dostať na internet prostredníctvom inej osoby, ktorá mala prístup k jej mobilnému zariadeniu alebo účtom na sociálnych sieťach. Táto druhá osoba mohla fotografie zneužiť na vytvorenie falošného profilu a následnú komunikáciu s obeťou.

Hypotéza 3

Fotografie obete mohli byť z jej zariadenia stiahnuté prostredníctvom vírusu (malvéru). Útočník, ktorý mal prístup k jej zariadeniu, mohol tieto fotografie zverejniť na internete cez falošný profil, pričom sa vydával za obeť.

Dáta využité v prípade:

V prípade sú využité dáta z datasetov, ktoré sú voľne dostupné a stiahnuteľné z internetu.

Linky na datasety:

<https://web.archive.org/web/20160528133423/http://www.dfrws.org/2008/rodeo.shtml>

<https://web.archive.org/web/20111012154048/http://www.dfrws.org:80/2011/challenge/>

Velkosť datasetu:

Prvý dataset - 635MB

Druhý dataset – 369.86MB

Digitálne zariadenia súvisiace s prípadom:

Mobilné zariadenie obete – Mobilné zariadenie obete mohlo byť použité na komunikáciu s páchateľom, pričom sa môžu nachádzať podozrivé správy, ktoré dokazujú manipulatívne rozhovory alebo vydieranie.

Školské bezpečnostné kamery – Mohli by overiť, uhol zhotovenej fotografie, kedy a kde boli fotografie obete zhotovené a identifikovať páchateľa.

Mobilné zariadenie študenta (svedka) – Video, ktoré možno zachytáva páchateľa pri fotení obete pred školou. Tento záznam môže pomôcť potvrdiť prítomnosť páchateľa v okolí školy, určiť čas a miesto jeho činnosti.

Typ analyzovanej digitálnej stopy:

Vyšetrovanie sa zameria na rôzne digitálne stopy, ktoré pomôžu identifikovať páchateľa a preukázať jeho činnosť. Medzi hlavné analyzované údaje patria:

- **Metadáta fotografií** (.jpg, .png) – Dátum, čas
- **Komunikačné záznamy** (.log) – Obsah správ medzi páchateľom a obeťou, ktoré dokazujú pokus o vydieranie.
- **Záznamy zo školských bezpečnostných kamier** (.mp4, .AVI) – Porovnanie časov snímania fotografií s pohybom podozrivého v škole.
- **Videozáznam z mobilného zariadenia študenta** (.mp4) – Video, ktoré zachytáva páchateľa v pozadí pri fotení obete pred školou.

Fotografia skúmaného zariadenia:



Samsung Galaxy S2 - patriaci obeti

Vlastnosti skúmaného zariadenia:

Funkcia	Podrobnosti
Model	Samsung Galaxy S2
Vydanie	2011
Operačný systém	Android 2.3 (Gingerbread), aktualizácia na 4.1.2 (Jelly Bean)
Úložisko	16 GB, 32 GB, 64 GB (expandovateľné microSD)
Displej	4.3 palca Super AMOLED Plus
Rozlíšenie displeja	480 x 800 px
Procesor	Dual-core 1.2 GHz Cortex-A9
Pamäť RAM	1 GB
Fotoaparát	8 MP, autofokus, LED blesk
Predná kamera	2 MP
Batéria	1650 mAh
Senzory	Akcelerometer, gyroskop, kompas, proximita, GPS
Rozmery	125.3 x 66.1 x 8.49 mm
Hmotnosť	116 g
Životnosť batérie	1650 mAh (až 8 hodín hovoru, 18 hodín v pohotovostnom režime)
Rýchlosť procesora	1.2 GHz dual-core Cortex-A9
Rýchlosť čítania/zápisu	Čítanie: 20 MB/s, Zápis: 10 MB/s
Prístupová doba	Rýchlosť prístupu k pamäti RAM: 6-8 GB/s
Čas nabíjania	1.5 až 2 hodiny na plné nabitie
Architektúra procesora	ARM Cortex-A9 (32-bit), dual-core

Chain of custody:

Číslo:	01	Typ súboru:	001	Obnovený súbor:	Áno	Veľkosť:	6GB
Popis prípadu:		Online vydieranie					
Názov súboru:		Mobil_obet001					
Miesto získania digitálnej stopy:		Samsung Galaxy S2, kópia zabezpečená v laboratóriu					
Poznámky:		Obraz zariadenia robený cez FTK Imager					
Časové pečiatky							
Access:	8.3.2025 14:07:25		Modify:	8.3.2025 14:07:25		Change:	-
Digitálny odtlačok (heš)	MD5	95c395695db081a80d86970ae0eacbf1					
	SHA1	8995eedfa4478ab0a18773eb933b6c911f73562d					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
8.3.2025 08:24:37		Obraz mobil. zariadenia					
8.3.2025 08:28:11		Dokončenie obrazu mobil. zariadenia					
8.3.2025 08:50:07		Overovanie Hashov					

Obráz mobilného zariadenia obete:

Creating Image...

Image Source:

Destination:

Status:

Progress



Elapsed time:

Estimated time left:

Hash:

Drive/Image Verify Results

Name	Mobile_Device - 01.001
Sector count	15728640
MD5 Hash	
Computed hash	95c395695db081a80d86970ae0eacbf1
Report Hash	95c395695db081a80d86970ae0eacbf1
Verify result	Match
SHA1 Hash	
Computed hash	8995eedfa4478ab0a18773eb933b6c911f
Report Hash	8995eedfa4478ab0a18773eb933b6c911f
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Created By Exterro® FTK® Imager 4.7.3.81

Case Information:

Acquired using: ADI4.7.3.81

Case Number: 01

Evidence Number: 01

Unique description: Samsung Galaxy S2

Examiner: Kovac Samuel

Notes: mobile_image

Information for C:\Programy\FTK_imager\Obraz Mobil\Mobile_Device - 01:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 979

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 15 728 640

[Physical Drive Information]

Drive Model: VendorCo ProductCode USB Device

Drive Serial Number: 8038501235840601924

Drive Interface Type: USB

Removable drive: True

Source data size: 7680 MB

Sector count: 15728640

[Computed Hashes]

MD5 checksum: 95c395695db081a80d86970ae0eacbf1

SHA1 checksum: 8995eedfa4478ab0a18773eb933b6c911f73562d

Image Information:

Acquisition started: Sat Mar 15 16:47:36 2025

Acquisition finished: Sat Mar 15 16:54:32 2025

Segment list:

C:\Programy\FTK_imager\Obraz Mobil\Mobile_Device - 01.001

C:\Programy\FTK_imager\Obraz Mobil\Mobile_Device - 01.002

C:\Programy\FTK_imager\Obraz Mobil\Mobile_Device - 01.003

C:\Programy\FTK_imager\Obraz Mobil\Mobile_Device - 01.004

C:\Programy\FTK_imager\Obraz Mobil\Mobile_Device - 01.005

C:\Programy\FTK_imager\Obraz Mobil\Mobile_Device - 01.006

COMPUTED HASH : 95c395695db081a80d86970ae0eacbf1

COMPUTED HASH : 8995eedfa4478ab0a18773eb933b6c911f73562d

Image Verification Results:

Verification started: Sat Mar 15 16:54:32 2025

Verification finished: Sat Mar 15 16:54:59 2025

MD5 checksum: 95c395695db081a80d86970ae0eacbf1 : verified

SHA1 checksum: 8995eedfa4478ab0a18773eb933b6c911f73562d : verified

Kópie obrazu RAM mobilného zariadenia:

Kópie vytvorené v programe **FTK Imager**

Počet: 2ks

Kedy boli vytvorené kópie: 8.3.2025

Uložené na: forenzných čistých harddiskoch, ktoré sú uložené v plastových nádobách

Fotografia skúmaného zariadenia:



Dahua HAC-HFW1200TLP

Parameter	Hodnota
Výrobca	Dahua Technology
Model	HAC-HFW1200TLP
Typ kamery	Analógová CCTV kamera
Rozlíšenie	2 MP (1920 × 1080)
Snímací senzor	1/2.7" CMOS
Infračervené nočné videnie	Áno, do 40 m
Ohnisková vzdialenosť	3.6 mm (fixný objektív)
Uhol záberu	Približne 87° (horizontálne)
Video formát	HDCVI / CVBS / AHD / TVI
Maximálna snímková frekvencia	30 snímok za sekundu pri 1080p
Kompresia videa	H.265 / H.264
Odolnosť voči poveternostným vplyvom	IP67 (odolná voči prachu a vode)
Napájanie	12V DC ± 30%
Spotreba energie	Max. 3.7 W
Materiál tela	Kov
Životnosť	Približne 5 – 7 rokov (v závislosti od podmienok)
Prístupová doba k záznamom	Závisí od rýchlosti DVR/NVR systému
Architektúra systému	Koaxiálne pripojenie k DVR alebo hybridnému záznamníku

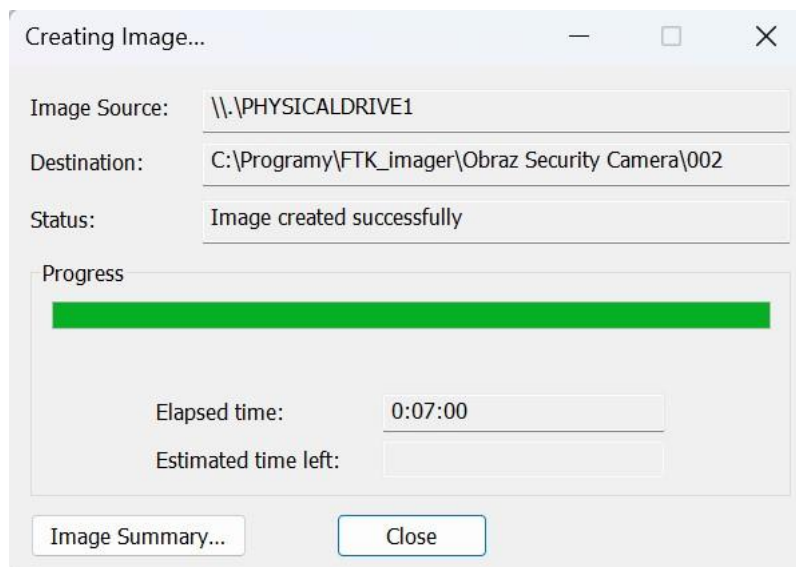
Úložisko záznamov	Externé DVR/NVR zariadenie
-------------------	----------------------------

Vlastnosti skúmaného zariadenia:

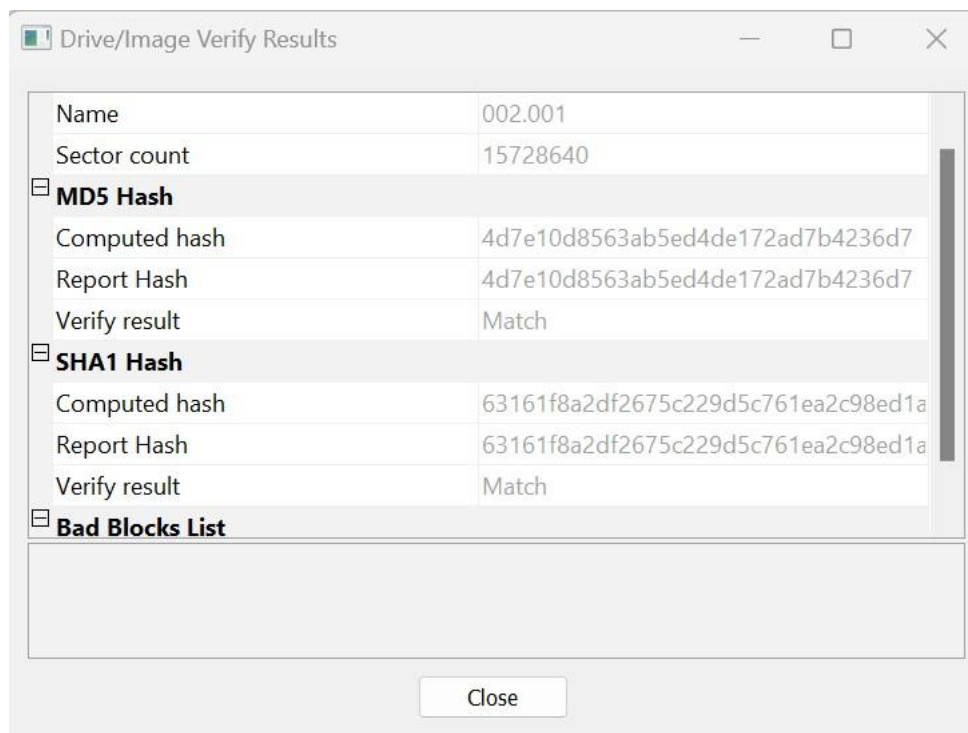
Chain of custody:

Číslo:	02	Typ súboru:	.002	Obnovený súbor:	Nie	Veľkosť:	25GB
Popis prípadu:		Online vydieranie					
Názov súboru:		sec_camera.002					
Miesto získania digitálnej stopy:		Dahua HAC-HFW1200TLP					
Poznámky:		Obraz zariadenia robený cez FTK Imager					
Časové pečiatky							
Access:	8.3.2025 16:59:14		Modify:	8.3.2025 16:59:14		Change:	-
Digitálny odtlačok (heš)	MD5	4d7e10d8563ab5ed4de172ad7b4236d7					
	SHA1	63161f8a2df2675c229d5c761ea2c98ed1ae318d					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
8.3.2025 17:28:14		Obraz mobil. zariadenia					
8.3.2025 17:32:25		Dokončenie obrazu mobil. zariadenia					
8.3.2025 17:35:10		Overovanie Hashov					

Obraz bezpečnostnej kamery:



Hash:



Created By Exterro® FTK® Imager 4.7.3.81

Case Information:

Acquired using: ADI4.7.3.81

Case Number: 02

Evidence Number: 02

Unique description: Dahua HAC-HFW1200TLP

Examiner: Kovac Samuel

Notes: security_camera_image

Information for C:\Programy\FTK_imager\Obraz Security Camera\002:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 979

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 15 728 640

[Physical Drive Information]

Drive Model: VendorCo ProductCode USB Device

Drive Serial Number: 8038501235840601924

Drive Interface Type: USB

Removable drive: True

Source data size: 7680 MB

Sector count: 15728640

[Computed Hashes]

MD5 checksum: 4d7e10d8563ab5ed4de172ad7b4236d7

SHA1 checksum: 63161f8a2df2675c229d5c761ea2c98ed1ae318d

Image Information:

Acquisition started: Sun Mar 16 12:11:41 2025

Acquisition finished: Sun Mar 16 12:18:41 2025

Segment list:

C:\Programy\FTK_imager\Obraz Security Camera\002.001

C:\Programy\FTK_imager\Obraz Security Camera\002.002

C:\Programy\FTK_imager\Obraz Security Camera\002.003

C:\Programy\FTK_imager\Obraz Security Camera\002.004

C:\Programy\FTK_imager\Obraz Security Camera\002.005

C:\Programy\FTK_imager\Obraz Security Camera\002.006

COMPUTED HASH : 4d7e10d8563ab5ed4de172ad7b4236d7

COMPUTED HASH : 63161f8a2df2675c229d5c761ea2c98ed1ae318d

Image Verification Results:

Verification started: Sun Mar 16 12:18:41 2025

Verification finished: Sun Mar 16 12:19:18 2025

MD5 checksum: 4d7e10d8563ab5ed4de172ad7b4236d7 : verified

SHA1 checksum: 63161f8a2df2675c229d5c761ea2c98ed1ae318d : verified

Kópie obrazu RAM bezpečnostnej kamery:

Kópie vytvorené v programe **FTK Imager**

Počet: 2ks

Kedy boli vytvorené kópie: 9.3.2025

Uložené na: forenzných čistých harddiskoch, ktoré sú uložené v plastových nádobách

Fotografia skúmaného zariadenia:



Huawei P30 - patriaci svedkovi

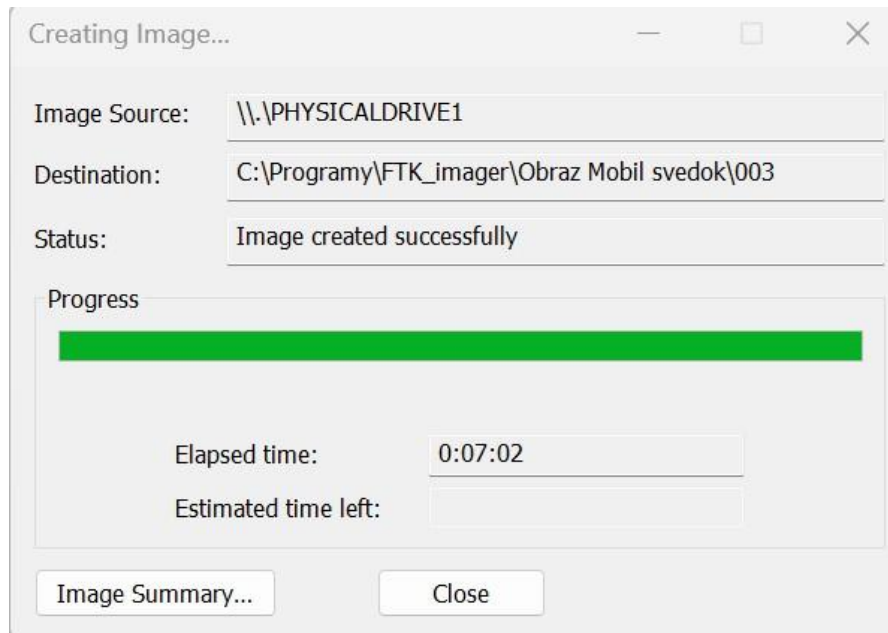
Funkcia	Podrobnosti
Model	Huawei P30
Vydanie	2019
Operačný systém	Android 9.0 (Pie), EMUI 9.1, aktualizácia na 10.0
Úložisko	128 GB, 256 GB (neexpandovateľné)
Displej	6.1 palca OLED, Full HD+
Rozlíšenie displeja	2340 x 1080 px
Procesor	Octa-core (4x2.6 GHz Cortex-A76 & 4x1.8 GHz Cortex-A55)
Architektúra procesora	ARM Cortex-A76 (4x 2.6 GHz), ARM Cortex-A55 (4x 1.8 GHz)
Pamäť RAM	6 GB, 8 GB
Fotoaparát	40 MP (širokouhlý), 16 MP (ultrawide), 8 MP (telefoto), OIS
Predná kamera	32 MP
Batéria	3650 mAh, rýchle nabíjanie (22.5W)
Senzory	Akcelerometer, gyroskop, kompas, proximita, snímač odtlačkov prstov, GPS
Rozmery	149.1 x 71.4 x 7.6 mm
Hmotnosť	165 g
Životnosť batérie	Až 23 hodín v pohotovostnom režime, až 8 hodín hovoru
Rýchlosť procesora	2.6 GHz (Cortex-A76), 1.8 GHz (Cortex-A55)
Rýchlosť čítania/zápisu	Čítanie: 20 MB/s, Zápis: 10 MB/s
Prístupová doba	6-8 GB/s (rýchlosť prístupu k pamäti RAM)
Čas nabíjania	1.5 až 2 hodiny na plné nabitie

**Vlastnosti
skúmaného
zariadenia:**

Chain of custody:

Číslo:	03	Typ súboru:	.003	Obnovený súbor:	Nie	Veľkosť:	7GB
Popis prípadu:		Online vydieranie					
Názov súboru:		Mobil_svedok.003					
Miesto získania digitálnej stopy:		Huawei P30					
Poznámky:		Obraz zariadenia robený cez FTK Imager					
Časové pečiatky							
Access:	9.3.2025 09:29:13		Modify:	9.3.2025 09:29:13		Change:	-
Digitálny odtlačok (heš)	MD5	4d7e10d8563ab5ed4de172ad7b4236d7					
	SHA1	63161f8a2df2675c229d5c761ea2c98ed1ae318d					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
9.3.2025 07:14:47		Obraz mobil. zariadenia					
9.3.2025 07:19:11		Dokončenie obrazu mobil. zariadenia					
9.3.2025 07:50:24		Overovanie Hashov					

Obraz mobilného zariadenia svedka:



Hash:

Created By Exterro® FTK® Imager 4.7.3.81

Case Information:

Acquired using: ADI4.7.3.81

Case Number: 03

Evidence Number: 03

Unique description: Huawei P30

Examiner: Kovac Samuel

Notes: witness_mobile_device

Information for C:\Programy\FTK_imager\Obraz Mobil svedok\003:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 979

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 15 728 640

[Physical Drive Information]

Drive Model: VendorCo ProductCode USB Device

Drive Serial Number: 8038501235840601924

Drive Interface Type: USB

Removable drive: True

Source data size: 7680 MB

Sector count: 15728640

[Computed Hashes]

MD5 checksum: 4d7e10d8563ab5ed4de172ad7b4236d7

SHA1 checksum: 63161f8a2df2675c229d5c761ea2c98ed1ae318d

Image Information:

Acquisition started: Sun Mar 16 13:43:12 2025

Acquisition finished: Sun Mar 16 13:50:15 2025

Segment list:

C:\Programy\FTK_imager\Obraz Mobil svedok\003.001

C:\Programy\FTK_imager\Obraz Mobil svedok\003.002

C:\Programy\FTK_imager\Obraz Mobil svedok\003.003

C:\Programy\FTK_imager\Obraz Mobil svedok\003.004

C:\Programy\FTK_imager\Obraz Mobil svedok\003.005

C:\Programy\FTK_imager\Obraz Mobil svedok\003.006

COMPUTED HASH : 4d7e10d8563ab5ed4de172ad7b4236d7

COMPUTED HASH : 63161f8a2df2675c229d5c761ea2c98ed1ae318d

Image Verification Results:

Verification started: Sun Mar 16 13:50:15 2025

Verification finished: Sun Mar 16 13:51:01 2025

MD5 checksum: 4d7e10d8563ab5ed4de172ad7b4236d7 : verified

SHA1 checksum: 63161f8a2df2675c229d5c761ea2c98ed1ae318d : verified

Kópie obrazu RAM mobilného zariadenia svedka:

Kópie vytvorené v programe **FTK Imager**

Počet: 2ks

Kedy boli vytvorené kópie: 10.3.2025

Uložené na: forenzných čistých harddiskoch, ktoré sú uložené v plastových nádobách

Použité nástroje DFA:

FTK Imager – RAM obraz, kópie zariadení

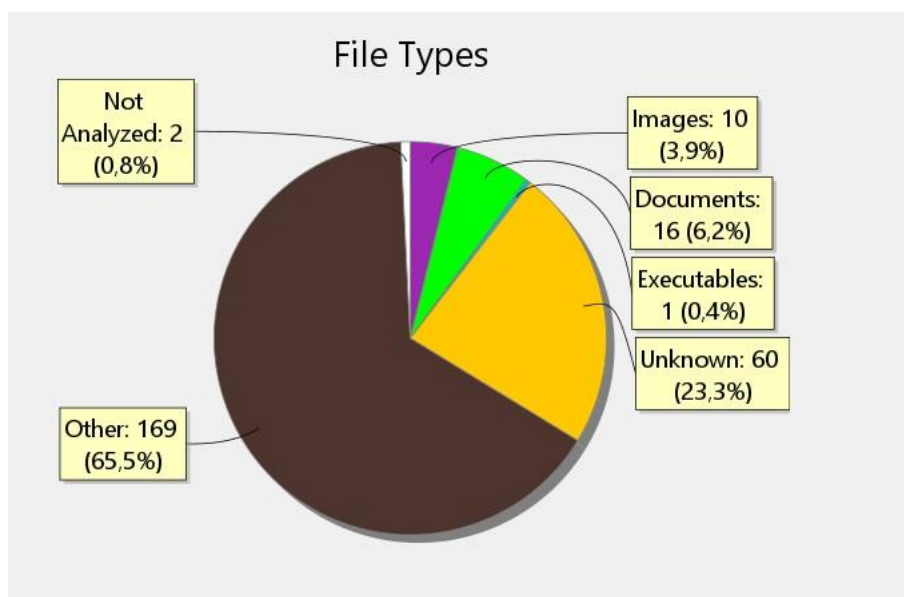
HxD editor – Prieskum obrazu RAM

AutoPsy – Analýza údajov a súborov

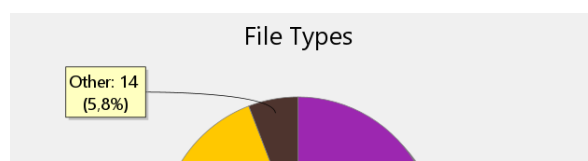
Použitý súborový systém:

- Obraz mobil. zariadenia svedka – **FAT**
- Obraz mobil. Zariadenia obete – **FAT**
- Obraz bezp. Kamery - **exFAT**

Vytažovanie:



Súbory z obrazu mobilného zariadenia svedka



Vyvrátenie/potvrdenie hypotéz:

Hypotéza 1

Študent získal fotografie obete, ktoré tajne odfoťil, a následne ich použil na vytvorenie falošného profilu na Instagrame. Po vytvorení profilu začal komunikovať s obeťou, predstierajúc, že má prístup k ďalším súkromným materiálom, a začal ju vydierať.

Potvrdená

Nájdene dôkazy na mobilnom zariadení obete (HxD):

Súbor: insta_chat.log

62fd420	73 6D 73 3A 2F 2F 6D 65-73 73 61 67 65 2F 4D 61	sms://message/Ma
62fd430	79 20 35 2C 20 32 30 31-31 20 31 31 3A 34 31 3A	y 5, 2011 11:41:
62fd440	32 32 20 50 4D 20 45 44-54 00 4A 28 0F 00 01 21	22 PM EDT -J(....!

V tejto konverzácii sa našla správa, ktorá obsahuje dôkaz o vydieraní obete. Páchateľ v nej píše:

"Ak mi nezaplatíš do večera, všetky tvoje súkromné fotky sa objavia na internete. Vieš, že hovorím pravdu, videla si, čo som už zverejnil. Nehraj sa so mnou!"

Odoslaná bola od osoby s menom Terry Johnson.

Terry Johnson wrote:

Táto správa jasne naznačuje úmysel páchatela manipulovať obeť a donútiť ju k platbe pod hrozbou.

Súbor: IMG_1334.png

02A6D93A0	6D 79 6D 75 73 69 63 5C 2A 2E 2A 22 64 65 6C 2F	mymusic*.*"del/
02A6D93B0	66 2F 71 22 63 3A 5C 75 73 65 72 73 5C 63 3A 5C	f/q"c:\users\c:\
02A6D93C0	75 73 65 72 73 5C 70 65 74 65 72 5C 6D 79 64 6F	users\peter\mydo
02A6D93D0	63 75 6D 65 6E 74 73 5C 6D 79 70 69 63 74 75 72	cuments\mypictur
02A6D93E0	65 73 5C 2A 2E 2A 22 6E 65 74 73 74 6F 70 22 6D	es*.*"netstop"m

V HxD editore bola identifikovaná sekvencia bajtov naznačujúca existenciu odstránenej fotografie v komunikácii medzi páchatelom a obeťou.

Táto zistená fotografia je dôkazom, že páchatel skutočne zdieľal a následne odstránil kompromitujúci obsah v konverzácii s obeťou.

Nájdene dôkazy na bezpečnostnej kamere (HxD):

Súbor: sec_camera_214.mp4

02ACA2C00	04 C3 07 38 24 01 80 FF FF FF FF 01 80 01 80 01	.Ä.8\$.€'...'€.€.
02ACA2C10	80 2C 01 19 04 C3 05 59 47 FF 01 80 2D 73 75 6E	€,...Ä.YG'.€-sun
02ACA2C20	2F 73 65 63 75 72 69 74 79 2F 6B 72 62 35 2F 4E	/security/krb5/K
02ACA2C30	72 62 53 65 72 76 69 63 65 4C 6F 63 61 74 6F 72	rbServiceLocator
02ACA2C40	24 53 72 76 52 65 63 6F 72 64 02 C1 02 11 32 31	\$SrvRecord.Ä..21

Po podrobnej analýze dát obnovovaných z pamäťového úložiska sme v hexadecimálnom editore HxD identifikovali fragmenty videozáznamu (.mp4) pochádzajúceho z bezpečnostnej kamery Dahua HAC-HFW1200TLP, ktorá monitorovala priestor pred školou. Na videu je jasne viditeľná postava muža, ktorý drží mobilný telefón na rovnakom mieste z akého boli neskôr použité fotografie na falošnom účte na Instagrame. Neskôr na zázname obeť fotografuje. Celková dĺžka záznamu: **05:17:23**.



Nájdene dôkazy na mobilnom zariadení svedka:

Súbor: skolsky_vlog.mp4

033AEA960	64 65 63 6F 64 65 2D 62 70 70 3D 38 2C 64 65 63	decode-bpp=8,dec
033AEA970	6F 64 65 2D 72 65 73 2D 78 3D 31 39 32 30 2C 64	ode-res-x=1920,d
033AEA980	65 63 6F 64 65 2D 72 65 73 2D 79 3D 31 30 38 30	ecode-res-y=1080
033AEA990	2C 64 65 63 6F 64 65 2D 62 69 74 72 61 74 65 3D	,decode-bitrate=
033AEA9A0	31 30 30 30 30 30 30 30 2C 64 65 63 6F 64 65 2D	10000000,decode-
033AEA9B0	66 70 73 3D 33 30 00 76 69 64 65 6F 2F 6D 70 34	fps=30.video/mp4
033AEA9C0	3E 63 6F 64 65 63 73 3D 22 24 31 22 3B 66 65 61	;codecs="\$1";fea

V hexadecimálnom editore HxD sme identifikovali fragmenty videozáznamu, ktorý zachytáva páchatela v oblasti, kde bol neskôr zaznamenaný aj bezpečnostnými kamerami. Na videu je jasne viditeľná postava muža, ktorý sa nachádza na rovnakom mieste, kde ho neskôr zachytili bezpečnostné kamery. Tento fakt potvrdzuje, že páchatel bol v daný čas na mieste činu. Celková dĺžka záznamu: **00:03:17**.



Dôkazy, ktoré potvrdzujú hypotézu

- Záznam z bezpečnostnej kamery (HFW1200TLP) zachytáva muža držiaceho mobilný telefón, z ktorého boli neskôr použité fotografie na falošnom profile.
- Video z mobilného zariadenia svedka (Huawei P30) taktiež zachytáva páchateľa pri fotografovaní obeť pred školou.
- Obnova odstránenej fotografie (IMG_1334.png) v HxD z mobilného zariadenia potvrdzuje, že fotografia bola odoslaná v komunikácii s obeťou a následne odstránená.

Hypotéza 2

Fotografie obeť sa mohli dostať na internet prostredníctvom inej osoby, ktorá mala prístup k jej mobilnému zariadeniu alebo účtom na sociálnych sieťach. Táto druhá osoba

mohla fotografie zneužiť na vytvorenie falošného profilu a následnú komunikáciu s obeťou.

Zamietnutá

```
CHARLI~4.TXTtxt!6
FILE0
CHARLI~4.TXT-120
Charlie_2009-12-07_1142_Sent.txt
( H
@<Charlie_2009-12-07_1142_Sent.txt
( H
(@h@
(8`8
( H
]]+7
@<Charlie_2009-12-07_1142_Sent.txt
( H
(@h@
(8`8
(8`8
( H
@<Charlie_2009-12-07_1142_Sent.txt
( H
]]RCRD(
( H
```



Po preskúmaní log súboru zariadenia obete neboli zistené žiadne náznaky o neoprávnenom prístupe. Všetky prístupy k zariadeniu boli autorizované, a neexistovali žiadne neznáme prihlásenia alebo pokusy o pripojenie zo zariadení

Dôkazy, ktoré zamietajú hypotézu:

- Neexistujú žiadne dôkazy o neoprávnenom prístupe do mobilného zariadenia obete alebo jej účtu na sociálnych sieťach.
- Fotografie boli zachytené **priamo** páchateľom, čo potvrdzujú bezpečnostné kamery aj mobilný záznam svedka.

Hypotéza 3

Fotografie obete mohli byť z jej zariadenia stiahnuté prostredníctvom vírusu (malvéru). Útočník, ktorý mal prístup k jej zariadeniu, mohol tieto fotografie zverejniť na internete cez falošný profil, pričom sa vydával za obeť.

Zamietnutá

```
!This program cannot be run in DOS mode.  
.text  
.rdata  
@.data  
.idata  
.rsrc  
@.reloc  
SVWh  
hhPAQ  
%Cf=  
hhPAQ  
r`hdPA  
#C;]  
%Cj]h  
%C_^]  
%Cf=  
5\PA  
5`PA  
|%C_^]  
v$hlPAS  
5XZAJ0
```

Nájdený súbor R54402.EXE

Pri analýze mobilného zariadenia obete som prešiel všetky súbory v získanom obraze zariadenia a hľadal podozrivé prípony, ktoré by mohli indikovať prítomnosť malvéru. Zistil som, že v zariadení sa nachádzal len jeden súbor s príponou .exe, ktorý sa však ukázal ako neškodný a neobsahoval žiadne známky malvéru. Ostatné prípony, ako .apk, .bat, .js, .jar a ďalšie potenciálne hrozby, sa v zariadení nenachádzali. Na základe tejto analýzy nebol nájdený žiadny malvér v podozrivých súboroch zariadenia.

Nájdený súbor **R54402.EXE** je inštalačný alebo konfiguračný súbor, ktorý patrí k legítimnej aplikácii používané v rámci určitého softvérového prostredia alebo zariadenia. Tento súbor obsahuje skompilovaný kód a je navrhnutý na spustenie v operačnom systéme Windows, ako naznačuje jeho hlavička, ktorá vylučuje spustenie v DOS režime. Analýza tohto súboru neukázala žiadne známky škodlivého správania. Po prehľadaní kódu a sekcií súboru neboli zistené žiadne indicie naznačujúce, že by bol tento súbor malvérom. Súbor obsahuje štandardné sekcie používané v bežných Windows aplikáciách, ako sú .text, .rdata, .data, .idata, .rsrc, a .reloc, ktoré sú typické pre legítimné programy.

Dôkazy, ktoré zamietajú hypotézu:

- Analýza digitálnych stôp neukázala žiadne znaky škodlivého softvéru alebo malvéru, ktorý by mohol stiahnuť fotografie z jej zariadenia.
- Fotografie boli jednoznačne zhotovené páchatelom fyzicky, čo potvrdzujú videozáznamy aj obnovené súbory.

Literatúra:

<https://dfrws.org/presentation/database-image-content-explorer-carving-data-thatdoes-not-officially-exist/>

Tento príspevok sa zaoberá analýzou obsahu databázových obrazov (Database Image Content Explorer) a metódami obnovy dát, ktoré „oficiálne neexistujú.“ Zameriava sa na carving dát, čo je technika digitálnej forenznej analýzy umožňujúca získavanie informácií zo zmazaných alebo skrytých oblastí úložiska.

<https://dfrws.org/presentation/comprehending-the-iot-cyber-threat-landscape-a-datadimensionality-reduction-technique-to-infer-and-characterize-internet-scale-iotprobing-campaigns-2/>

Tento príspevok sa zaoberá analýzou obsahu databázových obrazov a obnovou dát, ktoré oficiálne neexistujú. Predstavuje nástroj Database Image Content Explorer, ktorý umožňuje vyhľadávať a extrahovať informácie zo zmazaných alebo skrytých dát v databázových súboroch. Hlavným cieľom je identifikovať a obnoviť dáta, ktoré neboli správne vymazané alebo sú stále uložené v systéme, aj keď nie sú bežne prístupné. Táto technika je dôležitá pri digitálnej forenznej analýze, najmä pri vyšetrovaní kybernetických zločinov.

Záver:

Na základe hypotézy č. 1 sa nám podarilo identifikovať páchatela – osobu vystupujúcu pod falošnou identitou s menom Terry Johnson. Analýzou komunikácie a digitálnych stôp sa potvrdilo, že práve on stál za prípadom catfishingu.