

Napadnutý neznámou osobou:

Autor: Filip Libutka

Prípad

Dňa 30.10.2024 bol poškodený napadnutý neznámou osobou na parkovisku. K útoku došlo bez akéhokoľvek pokusu o krádež, čo naznačuje, že mohlo ísť o útok motivovaný osobnými dôvodmi.

Poškodený neutrpel fatálne zranenia, avšak incident si vyžiadal vážne zranenia a lekárske ošetrovanie.

K dispozícii sú kamerové záznamy z dvoch rôznych uhlov:

Prvá kamera nachádza sa bližšie k miestu útoku a môže poskytnúť detailnejšie zábery na tvár alebo postavu páchatel'a.

Druhá kamera je umiestnená ďalej, ale môže poskytnúť širší pohľad na situáciu a odhaliť spôsob príchodu a úniku útočníka.

Cieľ vyšetrovania:

Zistiť motiváciu útočníka a identifikovať ho na základe dostupných dôkazov, aby bolo možné podniknúť ďalšie právne kroky.

Ďalší postup:

Zaistenie a analýza miesta činu

Analýza kamerových záznamov

Hľadanie

Vyhodnotenie možných motívov svedkov

Identifikácia a dolapenie páchatel'a

Hypotézy

Úmyselný fyzický útok bez krádeže

Páchateľ mal osobný alebo iný dôvod na napadnutie poškodeného, ale jeho cieľom nebola krádež.

Mohlo ísť o pomstu, vyhrážanie alebo nezhody medzi páchatel'om a poškodeným.

Ak sa nepoznali, mohol byť útok vyvolaný napr. slovným konfliktom alebo nejakým nedorozumením.

Zistím ci poškodeny ma nejakych nepriatelov co by mu chceli ublizit poprípade analyzujem jeho telefon pre potencialnych pachatelov

Náhodný útok zo strany agresívnej osoby

Páchateľ mohol byť pod vplyvom alkoholu, drog alebo trpieť psychickými problémami.

Útok nemusel mať žiadny konkrétny dôvod, poškodený bol len náhodnou obeťou.

Z kamerových záznamov budem pozorovat ci pachatel isiel priamo za poškodnenym alebo stretnutie bolo nahodne. Popripade ci nebola chvozda nepravidelna ako pri omamenej osobe.

Pokus o lúpež, ktorý páchatel' prerušil

Možno mal páchatel' pôvodne v úmysle okradnúť poškodeného, ale bol vyrušený alebo sa zl'akol kamier. Mohol si všimnúť, že poškodený nemá pri sebe cenné veci, a preto od krádeže upustil.

Budeme pozorovat ci pachatel bol preruseny tretov osobou alebo niecim inym.

5W1H analýza prípadu napadnutia na parkovisku

Who (Kto) – Poškodený bol fyzicky napadnutý neznámou osobou. Páchateľ zatiaľ nebol identifikovaný, ale existujú dôkazy z kamerových záznamov, ktoré môžu pomôcť s jeho identifikáciou.

What (Čo) – Fyzický útok na poškodeného bez pokusu o krádež, čo naznačuje osobnú motiváciu páchatel'a. Poškodený utrpel vážne zranenia a musel byť ošetrovaný lekármi.

When (Kedy) – Incident sa stal 30. októbra 2024. Presný čas je možné určiť z kamerových záznamov.

Where (Kde) – K útoku došlo na parkovisku, kde boli umiestnené dve bezpečnostné kamery, ktoré zaznamenali incident z rôznych uhlov.

Why (Prečo) – Útok nemal znaky lúpeže, čo naznačuje, že mohol byť osobne motivovaný – mohol byť výsledkom konfliktu, pomsty alebo iného osobného motívu.

How (Ako) – Páchateľ pristúpil k poškodenému na parkovisku a fyzicky ho napadol. Prvá kamera, umiestnená bližšie, mohla zachytiť jeho tvár alebo postavu, zatiaľ čo druhá kamera mohla zaznamenať spôsob, akým sa páchateľ dostal na miesto činu a ako z neho unikol.

Boli vytvorené 3 kópie pomocou FTK imager každá je na vlastnom USB kľuči Kingston DataTraveler 3.0 USB Device o veľkosti 64 GB a majú priradené každé svoj chain of custody.

Digitálna stopa:

Created By AccessData® FTK® Imager 4.7.1.2

Case Information:

Acquired using: ADI4.7.1.2

Case Number: 1

Evidence Number: 1

Unique description: image

Examiner: filip

Notes: KINGSTONE_64_GB

Information for C:\Users\student\Documents\Libutka\USB64GB:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 7 526

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 120 907 776

[Physical Drive Information]

Drive Model: Kingston DataTraveler 3.0 USB Device

Drive Serial Number: EE08DB5154E8

Drive Interface Type: USB

Removable drive: True

Source data size: 59037 MB

Sector count: 120907776

[Computed Hashes]

MD5 checksum: 93929ec99074216d04926b958f6e7779

SHA1 checksum: 25b30e88d594bffb96eca69fa13c1e72b379cfb

Image Information:

Acquisition started: Mon Mar 10 09:57:03 2025 Acquisition finished: Mon Mar 10 10:07:56 2025 Segment list:

C:\Users\student\Documents\Libutka\USB64GB.001

Image Verification Results:

Verification started: Mon Mar 10 10:07:56 2025

Verification finished: Mon Mar 10 10:10:09 2025

MD5 checksum: 93929ec99074216d04926b958f6e7779 : verified

SHA1 checksum: 25b30e88d594bffb96eca69fa13c1e72b379cfb : verified

Fotografia zariadenia bližšej kamery:



Technické parametre

Vonkajšia celokovová kamera

IR nočný prísvit 850 nm 12× IR LED

Dosvit IR 15 - 20 m

1/2,9" 2Mp CMOS snímač

Objektív šošovka 4mm f=2,4, pevný, horizontálny uhol 84°, vertikálny uhol 45°

Full HD 1080p 30fps záznam

Kompresia záznamu H.265

LAN RJ45 konektor 10/100M (Podporuje POE 48V napájanie)

DC Jack - napájací konektor

Pracovná teplota -15°C/+50°C

Spotreba max. 12W

Seriové číslo 30000D556

Fotografia zariadenia vzdialenejšej kamery:



Technické parametre

Vonkajšia celokovová kamera

IR nočný prísvit 850 nm 12× IR LED

Dosvit IR 15 - 20 m

1/2,9" 2Mp CMOS snímač

Objektív šošovka 4mm f=2,4, pevný, horizontálny uhol 84°, vertikálny uhol 45°

Full HD 1080p 30fps záznam

Kompresia záznamu H.265

LAN RJ45 konektor 10/100M (Podporuje POE 48V napájanie)

DC Jack - napájací konektor

Pracovná teplota-15°C/+50°C

Spotreba max. 12W

Seriové číslo B00085A88

Pomocou programu HxD editor sa podarilo v obraze RAM pamäti nájsť:

44 72 69 76 65 20 4D 6F 64 65 6C 3A 20 4B 69 6E 67 73 74 6F 6E 20 44 61 74 61 54 72 61 76 65 6C

65 72 20 33 2E 30 20 55 53 42 20 44 65 76 69 63 65 0D 0A 20 44 72 69 76 65 20 53 65 72 69 61 6C

20 4E 75 6D 62 65 72 3A 20 45 45 30 38 44 42 35 31 35 34 45 38 = Drive Model: Kingston DataTraveler 3.0 USB Device

Pomocou programu autopsy sa podarilo nájsť niekoľko vymazaných snímok ktoré by mohli byť relevantné k prípadu:

Case View Tools Window Help

Add Data Source

Images/Videos

Communications

Geolocation

Timeline

Discovery

Generate Report

Close Case

44 Results

Save State as CSV

Listing

File System

Table Thumbnail Summary

Data Sources

File Views

File Types

File Extensions

Images (262)

Indexes (0)

Audio (0)

Archives (42)

Databases (0)

Documents

Executable

By MIME Type

Default View

By File Extension

All (44)

MB File Size

Data & Events

Analysis Results

OS Accounts

Tags

Reports

Name

S

C

O

Modified Time

Change Time

Access Time

Created Time

Size

Flags(Dx)

Flags(Hex)

Known

Location

Nový prečítok

0000-00-00 00:00:00

2025-03-02 14:29:39 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:29:39 CET

8

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

MSI_EP_2Mpx.gz

0000-00-00 00:00:00

2025-03-02 14:29:56 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:29:56 CET

1258037112

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

skvo_off.7z

0000-00-00 00:00:00

2025-03-02 14:29:32 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:29:32 CET

9422917

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

ED_2Mpx.gz

0000-00-00 00:00:00

2025-03-02 14:29:58 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:29:58 CET

90491727

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

bridge-close_off.7z

0000-00-00 00:00:00

2025-03-02 14:29:50 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:29:50 CET

39652349

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

bridge-close_off.7z

0000-00-00 00:00:00

2025-03-02 14:29:48 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:29:48 CET

152991604

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

bridge-far_off.7z

0000-00-00 00:00:00

2025-03-02 14:29:48 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:29:48 CET

19466205

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

bridge-far_off.7z

0000-00-00 00:00:00

2025-03-02 14:29:38 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:29:38 CET

39497070

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

contagion_off.7z

0000-00-00 00:00:00

2025-03-02 14:29:34 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:29:34 CET

6028434

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

isa_off.7z

0000-00-00 00:00:00

2025-03-02 14:29:32 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:29:32 CET

13769567

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

carphone_off.7z

0000-00-00 00:00:00

2025-03-02 14:29:32 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:29:32 CET

7832740

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

claw_off.7z

0000-00-00 00:00:00

2025-03-02 14:29:32 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:29:32 CET

5915359

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

contagion_off.7z

0000-00-00 00:00:00

2025-03-02 14:29:39 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:29:39 CET

2028989

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

container_off.7z

0000-00-00 00:00:00

2025-03-02 14:29:26 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:29:26 CET

4326205

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

container_off.7z

0000-00-00 00:00:00

2025-03-02 14:29:26 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:29:26 CET

2118907

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

foreman_off.7z

0000-00-00 00:00:00

2025-03-02 14:18:36 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:18:36 CET

24786315

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

foreman_off.7z

0000-00-00 00:00:00

2025-03-02 14:18:34 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:18:34 CET

6172049

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

hdmv_off.7z

0000-00-00 00:00:00

2025-03-02 14:18:32 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:18:32 CET

141421362

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

hdmv_off.7z

0000-00-00 00:00:00

2025-03-02 14:18:29 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:18:29 CET

14601719

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

hdmv_off.7z

0000-00-00 00:00:00

2025-03-02 14:18:24 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:18:24 CET

21291418

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

hdmv_off.7z

0000-00-00 00:00:00

2025-03-02 14:18:24 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:18:24 CET

24603842

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

hdmv_off.7z

0000-00-00 00:00:00

2025-03-02 14:18:16 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:18:16 CET

680328

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

hdmv_off.7z

0000-00-00 00:00:00

2025-03-02 14:18:16 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:17:54 CET

77784280

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

hdmv_off.7z

0000-00-00 00:00:00

2025-03-02 14:18:16 CET

0000-00-00 00:00:00

2025-03-02 00:00:00 CET

2025-03-02 14:18:09 CET

38070951

Unallocated

Unallocated

unknown

Img_D:\Bart\pnc

File Metadata

OS Accounts

Data & Events

Analysis Results

Context

Annotations

Other Occurrences

Uschovanie dôkazov:

Ku všetkým dôkazovým materiálom má prístup iba pár ľudí nutných pre vyšetrovanie prípadu každá položka ma priložený papier chain of custody ktorý musí byť vyplnený pred manipuláciu s dátami.

Číslo:	01	Typ súboru:	.jpg	Obnovený súbor:	Áno	Veľkosť:	10195
Popis prípadu:	Kamerove zaznamy z parkoviska						
Názov súboru:	80085.jpg						
Miesto získania digitálnej stopy:	Obraz kamery						
Poznámky:	Blizsia kamera						
Časové pečiatky							
Access:	Modify:	Change:					
[2024-	02-04	[2024-02-	04	[0000-00-00			
20:01:00] 00:01:00] 00:00:00]							
Digitálny odtlačok (heš)	MD5	f587bb744e9fe6256ce7d1214fee9197					
	SHA1	b36ed259acc0f0bed40a7e53fe90b6620c8ad2de7ef504bc92b0ad4494472c32					

Číslo:	02	Typ súboru:	.jpg	Obnovený súbor:	Áno	Veľkosť:	20055
Popis prípadu:		Kamerove zaznamy z parkoviska					
Názov súboru:		8008.jpg					
Miesto získania digitálnej stopy:		Obraz kamery					
Poznámky:		Vzdialena kamera					
Časové pečiatky							
Access:	Modify:	Change:					
[2024-10:01:00]	02-04 [2024-02-00:01:00]	04	[0000-00-00]				
Digitálny odtlačok (heš)	MD5	f587bb744e9fe6256ce7d1214fee9197					
	SHA1	b36ed259acc0f0bed40a7e53fe90b6620c8ad2de7ef504bc92b0ad4494472c32					

Odborné články

Secure Digital Camera

<https://dfrws.org/presentation/secure-digital-camera/>

Navrhujeme biometrické riešenie na vyriešenie niektorých významných problémov spojených s používaním digitálnych kamerových snímok ako dôkazov na súde. Predstavujeme bezstratové vodoznakovanie ako riešenie problémov spojených s integritou digitálnych snímok a ich vzťahom k reťazcu dôkazov. Integrita digitálnych snímok ako dôkazov spočíva v presnom zodpovedaní jednoduchej otázky: Kto čo kedy urobil? Ukazujeme, ako použiť bezstratové vkladanie dát na identifikáciu fotografa, fotoaparátu, času zhotovenia snímky a na overenie integrity obrazu. Fotoaparát s touto schopnosťou nazývame „Secure Digital Camera“. Navrhovaný koncept poskytne forenzným

vyšetrovateľom nástroj, ktorý im pomôže preukázať integritu digitálnej kamerovej snímky predloženej súdu a dokázať, že ide o pravdivé a presné zobrazenie reality.

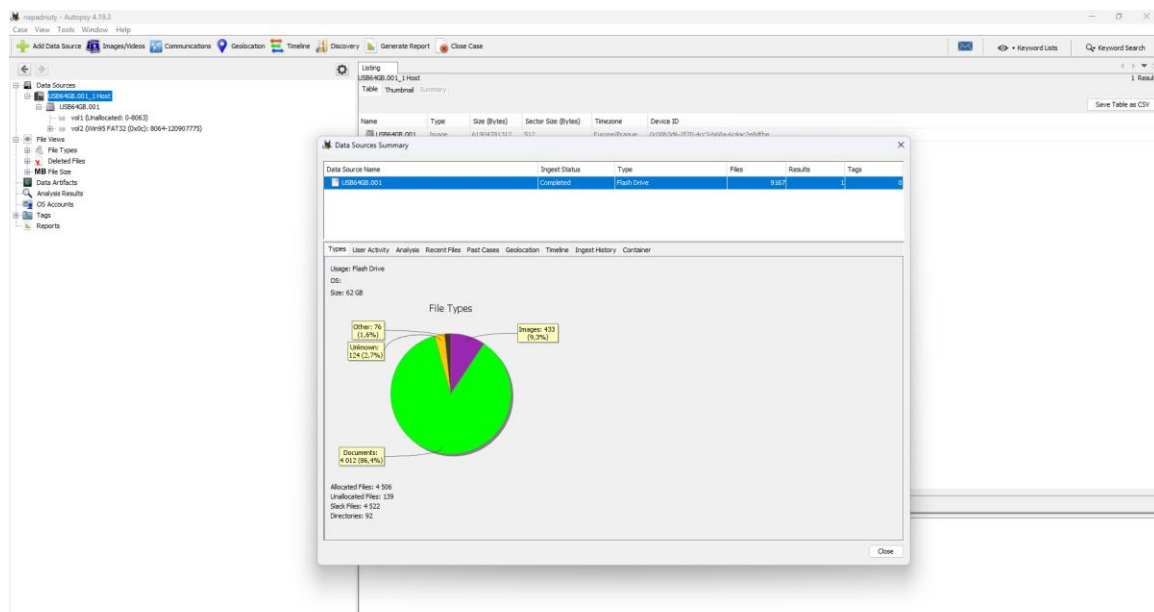
Forensic Analysis of Video File Formats

<https://dfrws.org/presentation/forensic-analysis-of-video-file-formats/>

Štandardy formátov video súborov definujú iba obmedzený počet povinných funkcií a ponechávajú priestor na interpretáciu. Dizajnové rozhodnutia výrobcov zariadení a softvérových dodávateľov sú preto cenným zdrojom pre forenznú autentifikáciu videa. Tento článok podrobne skúma video prúdy vo formátoch AVI a MP4 pochádzajúce z mobilných telefónov a digitálnych kamier. Používame prispôsobené analyzátory na extrakciu všetkých štruktúr formátu súborov z videí pochádzajúcich celkovo z 19 modelov digitálnych kamier, 14 modelov mobilných telefónov a 6 nástrojov na úpravu videa. Hlásime značné rozdiely vo výbere kontajnerových formátov, algoritmov kompresie zvuku a videa, parametrov snímania a vnútornej štruktúry súborov. V kombinácii môžu tieto charakteristiky pomôcť pri forenznej autentifikácii digitálnych video súborov tým, že umožňujú rozlišovať medzi originálnymi a post-procesovanými videami, overovať deklarovaný zdroj súboru alebo identifikovať skutočný model záznamového zariadenia či softvér použitý na spracovanie videa.

Budem pracovať s datasetom

<https://cfreds.nist.gov/all/ArizonaStateUniversity/MediaSamples10Video>



Kde sa nachádza 4 506 súborov . (Veľkovť 26,1 GB)

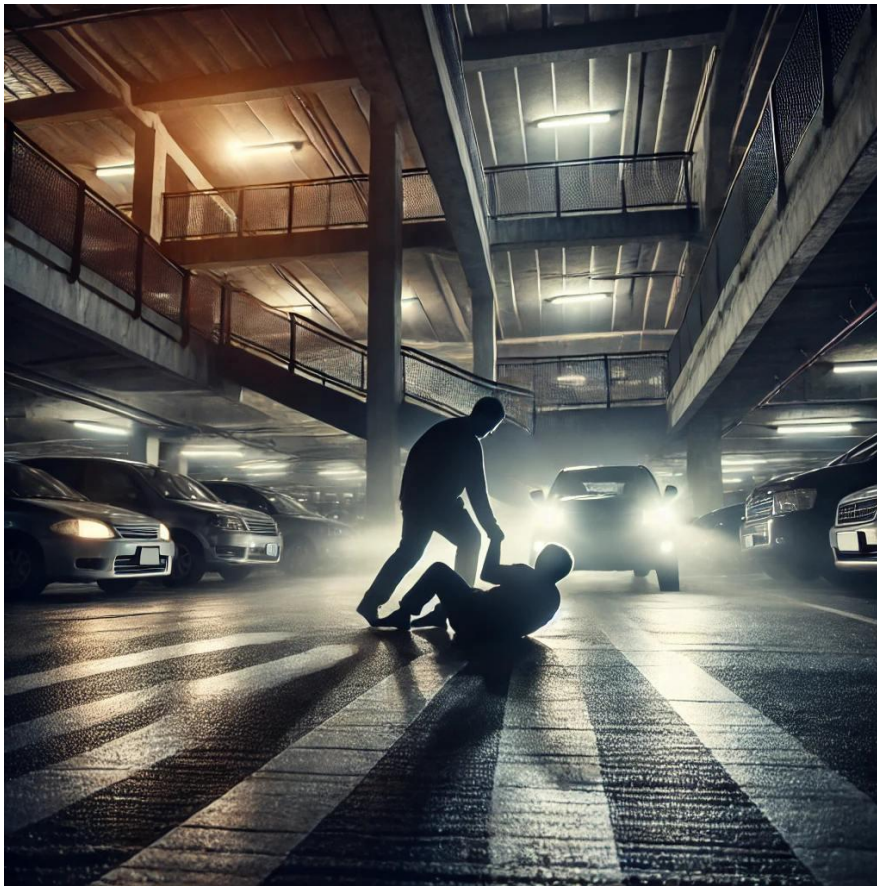
získané dôkazy

po zaistení dokazov sme analyzovali zavery s kamier a zistili sme

Zo záznamu bližšej kamery bola postava páchatel'a zachytená z profilu a zozadu, no tvár bola zakrytá kapucňou.

Záznam jasne dokazuje úmyselnosť útoku – páchatel' neblúdil, šiel priamo k poškodeniu, čo vylučuje náhodnosť.

Kamera zachytila, ako páchatel' odchádza vozidlom typu Škoda Kodiaq čiernej farby, pričom je viditeľná EČV.



Na analýzu boli použité nasledujúce nástroje:

- FTK Imager aby sme overili spravnosť dát či sa s nimi nemanipulovalo
- Autopsy na kontrolu vymazaných záznamov
- HxD editor

Overovanie Hypotéz

1. Úmyselný fyzický útok bez krádeže

Z kamerového záznamu z vzdialenejšej kamery jasne vyplýva, že útočník kráčal priamo k poškodeniu, bez váhania alebo blúdenia.

Kamera zachytila, ako páchatel' odchádza vozidlom typu Škoda Octavia čiernej farby, pričom je viditeľná EČV.

2. Náhodný útok zo strany agresívnej osoby

Z kamerového záznamu z vzdialenejšej kamery jasne vyplýva, že útočník kráčal priamo k poškodeniu, bez váhania alebo blúdenia.

Neexistujú žiadne znaky dezorientácie, nekoordinovanosti či podozrivého správania, ktoré by poukazovali na omámený stav

K útoku došlo bez slovného konfliktu, provokácie alebo impulzívnej reakcie – páchatel' nebol vyprovokovaný, ale konal priamo, čo je typické pre plánovaný čin.

3. Pokus o lúpež, ktorý páchatel' prerušil

Poškodený vypovedal, že pri sebe niesol len mobilný telefón a kľúče – žiadna hotovosť, žiadna luxusná taška či predmet, ktorý by mohol byť cieľom zlodca.

Páchatel' neprezrel ani neprehľadal vrecká alebo veci poškodeného – po útoku hneď odišiel, bez pokusu čokoľvek získať.

Miesto činu bolo relatívne opustené, neobjavila sa žiadna tretia osoba ani vozidlo, ktoré by ho mohlo vystrašiť.

Hľadanie pachatela

Zo záznamu bližšej kamery bola postava páchatel'a zachytená z profilu a zozadu, no tvár bola zakrytá kapucňou a maskou.

Na základe že Kamera zachytila, ako páchatel' odchádza vozidlom typu Škoda Octavia čiernej farby, pričom je viditeľná EČV (evidenčné číslo vozidla).

Evidenčné číslo bolo analyzované cez databázu polície, kde sa zistilo, že je registrované na osobu Marek H., ktorý je bývalým manželom manželky poškodeného.

Po prehľadaní telefónu a emailov manželky sa našli staršie správy a emaily od Mareka H. s výhražným obsahom, ktoré poukazujú na žiarlivosť a nevyriešené spory.