

UNIVERZITA SV. CYRILA A METODA V TRNAVE
FAKULTA PRÍRODNÝCH VIED

HODINKY V TME

Semestrálna práca

PREZENTÁCIA

OBSAH

ZOZNAM OBRÁZKOV A TABULIEK	3
1 Opis prípadu.....	4
2 Ciele digitálnej forenznej analýzy	4
3 5WH.....	5
3.1 Who? (Kto?)	5
3.2 What? (Čo?).....	5
3.3 When? (Kedy?)	5
3.4 Where? (Kde?).....	5
3.5 Why? (Prečo?)	5
3.6 How? (Ako?).....	5
4 Hypotézy.....	6
5 Zaisťovanie a zber.....	7
5.1 Údaje o zaistenom zariadení – digitálne smart hodinky	7
5.2 Údaje o zaistenom zariadení – USB	8
6 Použitý dataset	9
6.1 Dataset z hodínok.....	9
6.2 Dataset z USB.....	9
7 Vyťažovanie dôkazov	10
7.1 Digitálne hodinky	10
7.2 USB.....	16
8 Použité nástroje.....	18
8.1 FTK Imager.....	18
8.2 Autopsy.....	18
8.3 Microsoft Excel.....	18
9 Bezpečnostné opatrenia	19

ZOZNAM OBRÁZKOV A TABULIEK

Obrázok 1 Huawei Fit digitálne hodinky	7
Obrázok 2 Pretec i-Disk BulletProof USB	8
Obrázok 3 Image csv súboru	11
Obrázok 4 Autopsy - súbory	12
Obrázok 5 Náhľad .csv súboru	12
Obrázok 6 Metadáta súboru	12
Obrázok 7 HEX	13
Obrázok 8 Graf biometrických hodnôt z hodínok	14
Obrázok 9 Čas kľudu	15
Obrázok 10 Čas incidentu	15
Obrázok 11 Obraz USB cez FTK imager	16
Obrázok 12 Zistené súbory v Autopsy	17
Obrázok 13 Podozrivý .bat súbor (Autopsy)	17
Obrázok 14 Chain of custody - CSV	19
Obrázok 15 Chain of custody - USB	20

1 Opis prípadu

Ráno pri príchode do priestorov firmy X v Trnave zamestnanci zistili, že v kancelárii panuje výrazný neporiadok. V miestnosti sa nachádzala rozbitá sklenená vitrína a veľká časť dokumentov a materiálov bola rozhádzaná po podlahe. Počas obhliadky miesta činu boli na podlahe pri vitríne nájdené smart hodinky, ku ktorým sa nikto zo zamestnancov neprihlásil. Zároveň bolo v miestnosti objavené USB zariadenie.

Keďže smart hodinky sú schopné zaznamenávať biometrické a lokalizačné údaje a USB zariadenie môže byť nosičom dôkazov alebo zdrojom napadnutia technického zariadenia, vzniklo podozrenie, že obe zariadenia môžu patriť osobe, ktorá sa v čase incidentu nachádzala na mieste činu. Z tohto dôvodu boli hodinky aj USB zariadenie zaistené a podrobené digitálnej forenznej analýze s cieľom zistiť, či obsahujú údaje využiteľné pri objasnení prípadu a identifikácii možného páchatel'a.

2 Ciele digitálnej forenznej analýzy

- Zistiť, či nájdené smart hodinky obsahujú údaje relevantné pre vyšetrovanie krádeže.
- Analyzovať zaznamenané dáta zo zariadenia, najmä časové údaje, tepovú frekvenciu, pohybovú aktivitu a lokalizačné informácie.
- Preskúmať nájdené USB zariadenie a zistiť, aký obsah na ňom bol uložený.
- Identifikovať podozrivé odchýlky v zaznamenaných údajoch, ktoré by mohli súvisieť s pohybom alebo aktivitou osoby na mieste činu.
- Zistiť, či je možné na základe údajov zo smart hodínok určiť pravdepodobný čas incidentu.

3 5WH

3.1 Who? (Kto?)

Cieľom je identifikovať osobu, ktorej nájdené smart hodinky patrili, a zistiť, či táto osoba mohla byť prítomná v kancelárii v čase incidentu.

3.2 What? (Čo?)

Predmetom vyšetrovania je krádež v kancelárii a zároveň preskúmanie toho, či smart hodinky a USB obsahujú údaje dôležité pre objasnenie prípadu.

3.3 When? (Kedy?)

Presný čas incidentu zatiaľ nie je známy. Jednou z úloh analýzy je preto určiť pravdepodobný čas udalosti na základe časových pečiatok a zmien v zaznamenanej aktivite zariadenia.

3.4 Where? (Kde?)

Incident sa odohral v kancelárii firmy v Trnave, kde boli hodinky nájdené počas obhliadky miesta činu.

3.5 Why? (Prečo?)

Dôvodom vyšetrovania je objasnenie incidentu a zistenie, či smart hodinky aj USB zariadenie obsahujú digitálne stopy s objasnením dôvodu vlámania.

3.6 How? (Ako?)

Vyšetrovanie bude vykonané digitálnou forenznou analýzou exportovaných dát zo smart hodínok, najmä časových údajov, tepovej frekvencie, pohybovej aktivity a ďalších technických identifikátorov zariadenia. Súčasťou analýzy bude aj forenzný obraz USB zariadenia, vytvorený v nástroji FTK Imager a analyzovaný v Autopsy, s cieľom zistiť jeho obsah a význam pre vyšetrovanie.

4 Hypotézy

1. **Hypotéza 1:** Nájdené smart hodinky patrili osobe, ktorá sa v čase incidentu nachádzala na mieste činu. Táto hypotéza vychádza zo skutočnosti, že zariadenie bolo nájdené priamo v kancelárii pri poškodenom mieste, a preto je možné predpokladať, že mohlo patriť osobe súvisiacej s incidentom.
2. **Hypotéza 2:** Dáta uložené v smart hodinkách obsahujú záznamy o aktivite, ktoré môžu pomôcť určiť pravdepodobný čas incidentu. Predpokladá sa, že analýzou časových pečiatok, tepovej frekvencie, pohybovej aktivity a ďalších údajov bude možné identifikovať neobvyklé zmeny správania zariadenia, ktoré môžu časovo súvisieť s vyšetrovanou udalosťou.
3. **Hypotéza 3:** V údajoch zo zariadenia sa nachádzajú odchýlky od bežnej aktivity, ktoré môžu naznačovať zvýšený stres alebo pohyb osoby počas incidentu. Ak zariadenie zaznamenáva biometrické údaje a pohybové dáta, je možné predpokladať, že v čase incidentu mohlo dôjsť k ich výraznej zmene oproti bežnému stavu.
4. **Hypotéza 4:** Technické identifikátory zariadenia môžu pomôcť prepojiť hodinky s konkrétnou osobou alebo ďalším zariadením. Ide najmä o možnosť využitia identifikátorov ako MAC adresa, párované zariadenie alebo iné technické údaje, ktoré by mohli podporiť identifikáciu používateľa hodínok.
5. **Hypotéza 5:** USB zariadenie, nájdené v miestnosti, mohlo byť použité na prenos dát alebo na uchovanie súborov spojených s incidentom, pričom v čase zaistenia nebol jeho obsah známy. Predpokladá sa, že analýza obrazu USB v Autopsy odhalí podozrivé alebo relevantné súbory, ktoré môžu poskytnúť ďalšie dôkazy pre objasnenie prípadu.

5 Zaist'ovanie a zber

Počas obhliadky miesta činu boli zaistené smart hodinky a USB zariadenie, ktoré mohli obsahovať digitálne stopy pre vyšetrovanie. Pri ich zaistení bolo nevyhnutné zabezpečiť zachovanie integrity dát a zabrániť ich zmene alebo poškodeniu.

Analýza prebiehala na kópiách dát. Zo smart hodínok bol vytvorený export do formátu CSV a z USB zariadenia bol pomocou nástroja FTK Imager vytvorený forenzný obraz, ktorý bol následne analyzovaný.

5.1 Údaje o zaistenom zariadení – digitálne smart hodinky

- **Model:** Huawei Watch Fit
- **MAC adresa zariadenia:** AA:BB:CC:DD:EE:FF
- **Bezdrôtová konektivita:** Bluetooth 5.0
- **Veľkosť úložiska:** 4GB
- **Typ displeja:** AMOLED
- **Funkcie:** GPS, gyroskop, akcelerometer, snímač tepovej frekvencie, krokomer, pulzný oxymeter.



Obrázok 1 Huawei Fit digitálne hodinky

5.2 Údaje o zaistenom zariadení – USB

- **Model:** Pretec i-Disk BulletProof
- **Podpora:** USB 2.0
- **Kapacita:** 4GB
- **Rýchlosť prenosu dát pri čítaní:** 72 Mb/s (9MB/s)
- **Rýchlosť prenosu dát zápise:** 56 Mb/s (7 MB/s)



Obrázok 2 Pretec i-Disk BulletProof USB

6 Použitý dataset

Použitý dataset v tejto práci pozostáva z dvoch hlavných častí a to: dát zo smart hodínok a dát z USB zariadenia.

6.1 Dataset z hodínok

Dataset bol získaný exportom dát zo zariadenia vo formáte CSV. Obsahuje časovo usporiadané záznamy o aktivite zariadenia, najmä:

- časové pečiatky (timestamp),
- hodnoty tepovej frekvencie (bpm),
- údaje o pohybovej aktivite (počet krokov),
- lokalizačné údaje (GPS súradnice),
- technické identifikátory zariadenia (napr. MAC adresa párovaného zariadenia).

Tieto dáta boli analyzované pomocou nástrojov Autopsy a Microsoft Excel.

6.2 Dataset z USB

Druhú časť datasetu tvorí forenzný obraz USB zariadenia vytvorený pomocou nástroja FTK Imager. Tento obraz obsahoval súborový systém s viacerými súbormi rôznych typov.

Počas analýzy v nástroji Autopsy bol identifikovaný podozrivý súbor s príponou .bat, ktorý bol vyhodnotený ako potenciálny malvér a predstavuje významný dôkaz pre vyšetrovanie.

7 Vyt'azovanie dôkazov

Cieľom vyt'azovanie bolo analyzovať všetky dôkazy zo zaistených zariadení. Analýza sa zameriava na dve hlavné kategórie: smart hodinky, ktoré obsahujú časovo a priestorovo usporiadané biometrické dáta a USB zariadenie, ktoré môže obsahovať dáta spojené s incidentom.

7.1 Digitálne hodinky

Na vyt'azovanie dôkazových dát bol použitý nástroj Autopsy, v ktorom bol otvorený, zaevidovaný a preskúmaný exportovaný CSV súbor zo smart hodínok. V prostredí Autopsy bolo možné identifikovať samotný dôkazový súbor, zobrazit' jeho textový obsah, overit' metadáta a zároveň získať hexadecimálny náhľad súboru.

V prvej fáze analýzy bol v nástroji Autopsy lokalizovaný dôkazový súbor vo formáte CSV, ktorý obsahoval export časovo usporiadaných záznamov zo smart hodínok. Následne bol preskúmaný jeho textový náhľad, metadáta a hexadecimálny obsah, čím bola potvrdená existencia relevantného dátového súboru použiteľného na ďalšiu analytickú interpretáciu.

Created By Exterro® FTK® Imager 4.7.3.81

Case Information:

Acquired using: ADI4.7.3.81

Case Number: 001

Evidence Number:

Unique Description: smart_watches_on_scene

Examiner: stefkova

Notes:

Information for D:\VŠ\3. ročník - 2. semester\Digitálna forenzná analýza\image\image_watches.ad1:

[Computed Hashes]

MD5 checksum: 034b74f3e7c0c65d7b57fdce1f5b3ff4

SHA1 checksum: 9267702e71ed964b6642ade7830ae2d990c97557

Image information:

Acquisition started: Sat Mar 7 19:11:45 2026

Acquisition finished: Sat Mar 7 19:11:45 2026

Segment list:

D:\VŠ\3. ročník - 2. semester\Digitálna forenzná analýza\image\image_watches.ad1

COMPUTED HASH : 034b74f3e7c0c65d7b57fdce1f5b3ff4

COMPUTED HASH : 9267702e71ed964b6642ade7830ae2d990c97557

Image Verification Results:

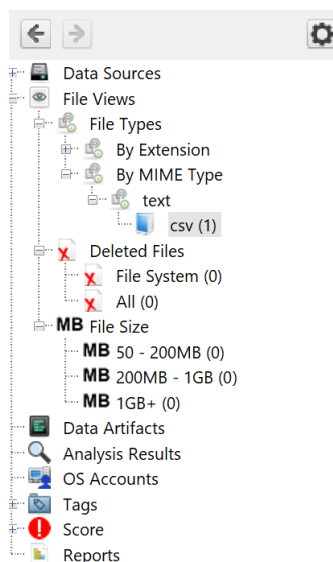
Verification started: Sat Mar 7 19:11:45 2026

Verification finished: Sat Mar 7 19:11:45 2026

MD5 checksum: 034b74f3e7c0c65d7b57fdce1f5b3ff4 : verified

SHA1 checksum: 9267702e71ed964b6642ade7830ae2d990c97557 : verified

Obrázok 3 Image csv súboru



Obrázok 4 Autopsy - súbory

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences		
Strings: Extracted Text Translation											
Page: 1 of 8 Page Matches on page: - of - Match 100% Reset Text Source: File Text											
Timestamp	Heart_Rate	Steps	Sleep_Stage	GPS_Lat	GPS_Lon	User_ID	Bluetooth_MAC	Nearby_Devices	Device_Model	Paired_Phone_MAC	Period
22:33:44:55:66	6.3.2026 0:00 67	Full_Calm_Day	0	1	48.37215055556772	17.58727664165434	HW_Fit_007	AA:BB:CC:DD:EE:FF	77:88:99:AA:BB:CC	Huawei Watch Fit 007	11:
22:33:44:55:66	6.3.2026 0:01 64	Full_Calm_Day	0	2	48.37399993338452	17.58390515574326	HW_Fit_007	AA:BB:CC:DD:EE:FF	11:22:33:44:55:66	Huawei Watch Fit 007	11:
22:33:44:55:66	6.3.2026 0:02 68	Full_Calm_Day	0	1	48.37340202996141	17.585924846117997	HW_Fit_007	AA:BB:CC:DD:EE:FF	11:22:33:44:55:66	Huawei Watch Fit 007	11:
22:33:44:55:66	6.3.2026 0:03 72	Full_Calm_Day	0	2	48.37215457108061	17.589246078595263	HW_Fit_007	AA:BB:CC:DD:EE:FF	77:88:99:AA:BB:CC	Huawei Watch Fit 007	11:
22:33:44:55:66	6.3.2026 0:04 63	Full_Calm_Day	0	1	48.37449916348661	17.584434741136146	HW_Fit_007	AA:BB:CC:DD:EE:FF		Huawei Watch Fit 007	11:22:33:44:55:66
22:33:44:55:66	6.3.2026 0:05 63	Full_Calm_Day	0	1	48.372652107155325	17.58843415807399	HW_Fit_007	AA:BB:CC:DD:EE:FF	77:88:99:AA:BB:CC	Huawei Watch Fit 007	11:
22:33:44:55:66	6.3.2026 0:06 72	Full_Calm_Day	0	2	48.37161337850882	17.58735555627717	HW_Fit_007	AA:BB:CC:DD:EE:FF	11:22:33:44:55:66	Huawei Watch Fit 007	11:
22:33:44:55:66	6.3.2026 0:07 68	Full_Calm_Day	0	1	48.37350868301859	17.586528089027954	HW_Fit_007	AA:BB:CC:DD:EE:FF	77:88:99:AA:BB:CC	Huawei Watch Fit 007	11:
22:33:44:55:66	6.3.2026 0:08 62	Full_Calm_Day	0	1	48.370973940976754	17.586440150915355	HW_Fit_007	AA:BB:CC:DD:EE:FF		Huawei Watch Fit 007	11:22:33:44:55:66
22:33:44:55:66	6.3.2026 0:09 67	Full_Calm_Day	0	1	48.369625552500125	17.586017940603845	HW_Fit_007	AA:BB:CC:DD:EE:FF	77:88:99:AA:BB:CC	Huawei Watch Fit 007	11:
22:33:44:55:66	6.3.2026 0:10 63	Full_Calm_Day	0	2	48.37308070084887	17.58610605805586	HW_Fit_007	AA:BB:CC:DD:EE:FF	77:88:99:AA:BB:CC	Huawei Watch Fit 007	11:

Obrázok 5 Náhľad .csv súboru

Metadata	
Name:	/LogicalFileSet1/complete_watch_data_calm_vs_crime.csv
Type:	Local
MIME Type:	text/csv
Size:	232070
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	0000-00-00 00:00:00
Accessed:	0000-00-00 00:00:00
Created:	0000-00-00 00:00:00
Changed:	0000-00-00 00:00:00
MD5:	75e3d5a11f81645dd6607e8081fd6d9d
SHA-256:	4734c44041fd6661fb40d0248b6ede68c02676de70b3e585b4f14f1b4038dec0
Hash Lookup Results:	UNKNOWN
Internal ID:	2
Local Path:	D:\VŠ3. ročník - 2. semester\Digitálna forenzná analýza\data\complete_watch_data_calm_vs_crime.csv

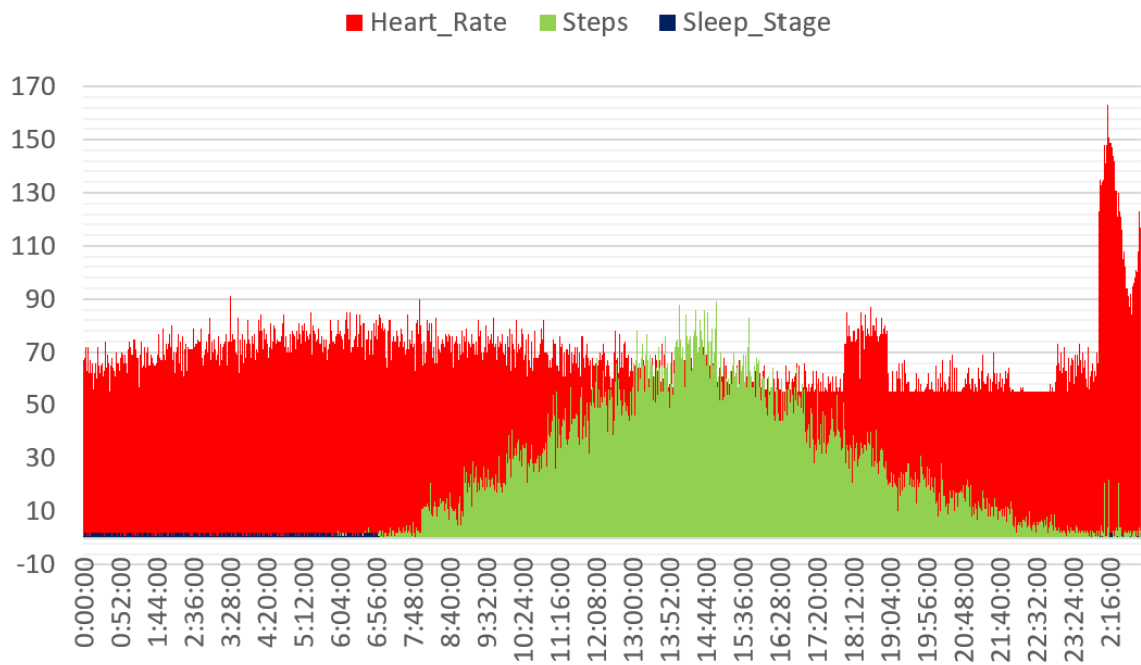
Obrázok 6 Metadáta súboru

0x00000000:	54 69 6D 65	73 74 61 6D	70 3B 3B 48	65 61 72 74	Timestamp;;Heart
0x00000010:	5F 52 61 74	65 3B 53 74	65 70 73 3B	53 6C 65 65	_Rate;Steps;Slee
0x00000020:	70 5F 53 74	61 67 65 3B	47 50 53 5F	4C 61 74 3B	p_Stage;GPS_Lat;
0x00000030:	47 50 53 5F	4C 6F 6E 3B	55 73 65 72	5F 49 44 3B	GPS_Lon;User_ID;
0x00000040:	42 6C 75 65	74 6F 6F 74	68 5F 4D 41	43 3B 4E 65	Bluetooth_MAC;Ne
0x00000050:	61 72 62 79	5F 44 65 76	69 63 65 73	3B 44 65 76	arby_Devices;Dev
0x00000060:	69 63 65 5F	4D 6F 64 65	6C 3B 50 61	69 72 65 64	ice_Model;Paired
0x00000070:	5F 50 68 6F	6E 65 5F 4D	41 43 3B 50	65 72 69 6F	_Phone_MAC;Perio
0x00000080:	64 0D 0A 36	2E 33 2E 32	30 32 36 20	30 3A 30 30	d..6.3.2026 0:00
0x00000090:	3B 30 3A 30	30 3A 30 30	3B 36 37 3B	30 3B 31 3B	;0:00:00;67;0;1;
0x000000a0:	34 38 2E 33	37 32 31 35	30 35 35 35	35 36 37 37	48.3721505555677
0x000000b0:	32 3B 31 37	2E 35 38 37	32 37 37 36	36 34 31 36	2;17.58727766416
0x000000c0:	35 34 33 34	3B 48 57 5F	46 69 74 5F	30 30 37 3B	5434;HW_Fit_007;
0x000000d0:	41 41 3A 42	42 3A 43 43	3A 44 44 3A	45 45 3A 46	AA:BB:CC:DD:EE:F
0x000000e0:	46 3B 37 37	3A 38 38 3A	39 39 3A 41	41 3A 42 42	F;77:88:99:AA:BB
0x000000f0:	3A 43 43 3B	48 75 61 77	65 69 20 57	61 74 63 68	:CC;Huawei Watch
0x00000100:	20 46 69 74	20 30 30 37	3B 31 31 3A	32 32 3A 33	Fit 007;11:22:3
0x00000110:	33 3A 34 34	3A 35 35 3A	36 36 3B 46	75 6C 6C 5F	3:44:55:66;Full_
0x00000120:	43 61 6C 6D	5F 44 61 79	0D 0A 36 2E	33 2E 32 30	Calm_Day..6.3.20
0x00000130:	32 36 20 30	3A 30 30 3B	30 3A 30 31	3A 30 30 3B	26 0:00;0:01:00;
0x00000140:	36 34 3B 30	3B 32 3B 34	38 2E 33 37	33 39 39 39	64;0;2;48.373999
0x00000150:	39 33 33 33	38 34 35 32	3B 31 37 2E	35 38 33 39	93338452;17.5839
0x00000160:	30 35 31 35	35 37 34 33	32 36 3B 48	57 5F 46 69	0515574326;HW_Fi

Obrázok 7 HEX

Po overení dôkazového súboru v Autopsy bola vykonaná jeho obsahová analýza v programe Excel, kde boli vizualizované hodnoty srdcovej frekvencie a počtu krokov. Cieľom bolo porovnať bežný pokojový interval s intervalom, ktorý časovo zodpovedal predpokladanému incidentu.

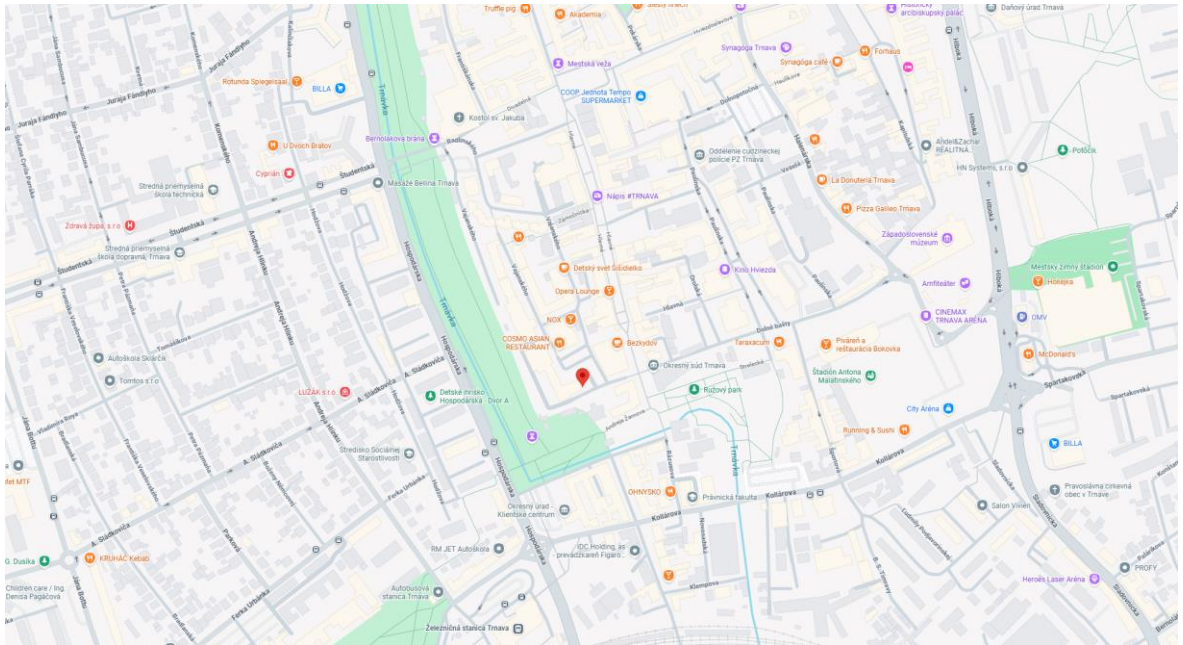
Analýza ukázala, že dňa 6. 3. 2026 o 02:00:00 bola zaznamenaná pokojová hodnota srdcovej frekvencie 73 bpm pri 0 krokoch. Naopak dňa 7. 3. 2026 o 02:00:00 bola zaznamenaná hodnota 123 bpm pri 1 kroku, pričom v nasledujúcich minútach srdcová frekvencia vzrástla až na 163 bpm spolu so zvýšenou pohybovou aktivitou. Tieto zistenia poukazujú na výraznú odlišnosť medzi pokojovým a incidentným nočným intervalom a naznačujú, že osoba používajúca zariadenie sa v sledovanom čase nachádzala v neštandardnej situácii.



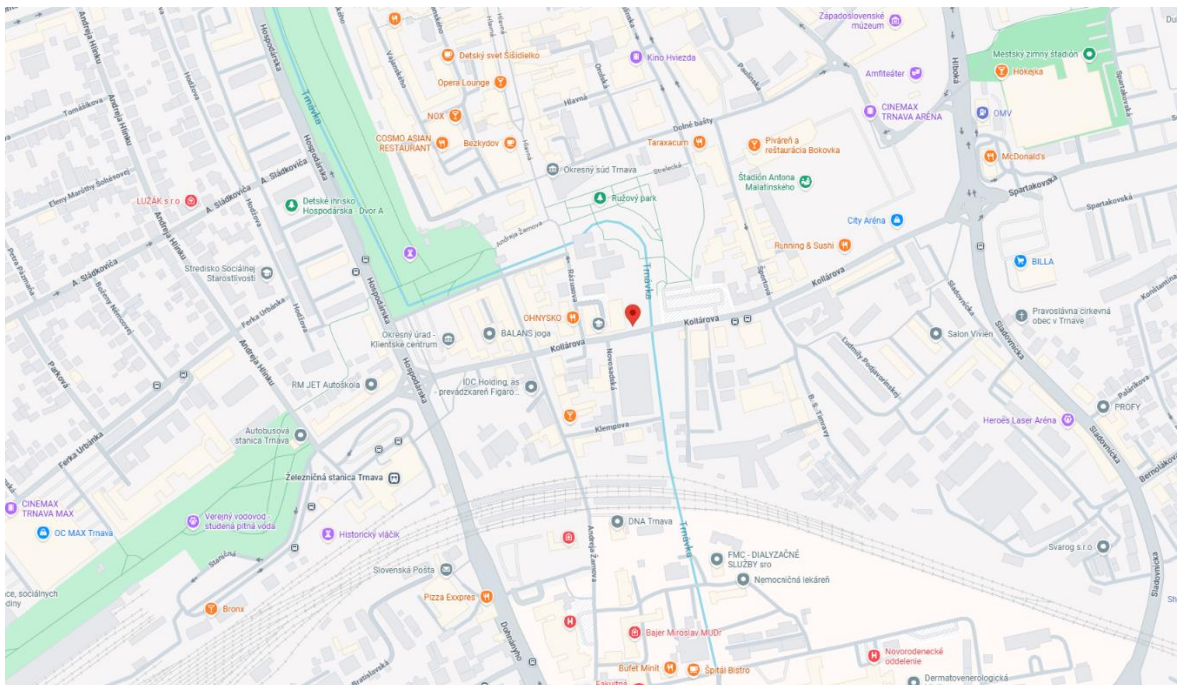
Obrázok 8 Graf biometrických hodnôt z hodínok

Analyzovaný dataset okrem fyziologických údajov obsahoval aj lokalizačné a identifikačné informácie, konkrétne GPS súradnice (GPS_Lat, GPS_Lon) a MAC adresu párovaného telefónu (Paired_Phone_MAC). Tieto údaje rozšírili analýzu o priestorový a technický kontext a umožnili sledovať pohyb zariadenia v analyzovanom období.

Na základe vyhodnotenia GPS záznamov bolo možné rekonštruovať orientačný pohyb zariadenia a určiť lokality, v ktorých sa nachádzalo pred incidentom a počas incidentného intervalu. Takto získané údaje pomohli zúžiť okruh preverovaných miest a podporili predpoklad, že zariadenie sa v rozhodujúcom čase pohybovalo v priestore relevantnom pre vyšetrovaný skutok. MAC adresa párovaného telefónu zároveň predstavovala technický identifikátor, ktorý by v nadväzujúcom vyšetrovaní mohol slúžiť na prepojenie zariadenia s konkrétnym používateľom alebo mobilným telefónom.



Obrázok 9 Čas kl'udu



Obrázok 10 Čas incidentu

Pri porovnaní pokojového intervalu a incidentného intervalu bolo možné pozorovať nielen rozdiel v srdcovej frekvencii, ale aj zmenu pohybovej aktivity a priestorového kontextu zariadenia. Kombinácia týchto údajov zvyšuje dôkaznú hodnotu smart hodínok, pretože umožňuje posudzovať incident nielen z pohľadu jedného biometrického ukazovateľa, ale aj v širších súvislostiach správania zariadenia.

7.2 USB

Pri analýze USB zariadenia bol najskôr vytvorený jeho forenzný obraz pomocou nástroja FTK Imager. Následne bol tento obraz importovaný do nástroja Autopsy, kde prebehla detailná analýza jeho obsahu.

Počas analýzy bol identifikovaný súbor s príponou .bat, ktorý predstavuje skript určený na spúšťanie príkazu. Tento súbor bol vyhodnotený ako podozrivý, keďže môže slúžiť na vykonávanie automatizovaných operácií bez vedomia používateľa.

Analýzou obsahu súboru bolo zistené, že skript môže byť využitý na spúšťanie škodlivých príkazov, manipuláciu so systémom alebo šírenie malvéru. Na základe týchto zistení bol súbor označený ako potenciálny malvér.

```
Created By Exterro® FTK® Imager 4.7.3.81

Case Information:
Acquired using: ADI4.7.3.81
Case Number: 001
Evidence Number: 002
Unique description: usb_evid
Examiner:
Notes:

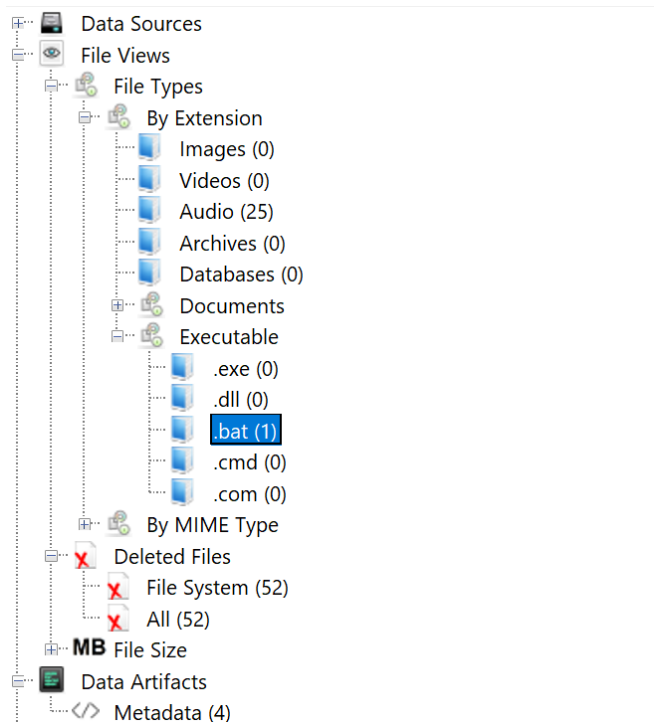
-----
Information for D:\img_usb\ev-usb:

Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 491
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 7 892 040
[Physical Drive Information]
Drive Model: Pretec UltimatGuard USB Device
Drive Serial Number: 1e80083526363f
Drive Interface Type: USB
Removable drive: True
Source data size: 3853 MB
Sector count: 7892040
[Computed Hashes]
MD5 checksum: 39b8629deeb0638ce9b4d8e6a70e8e6b
SHA1 checksum: 6eff5094523c78278304700f3558a0b25a127f1f

Image Information:
Acquisition started: Thu Mar 5 16:36:05 2026
Acquisition finished: Thu Mar 5 16:38:51 2026
Segment list:
D:\img_usb\ev-usb.E01
D:\img_usb\ev-usb.E02
D:\img_usb\ev-usb.E03
COMPUTED HASH : 39b8629deeb0638ce9b4d8e6a70e8e6b
COMPUTED HASH : 6eff5094523c78278304700f3558a0b25a127f1f

Image Verification Results:
Verification started: Thu Mar 5 16:38:51 2026
Verification finished: Thu Mar 5 16:39:09 2026
MD5 checksum: 39b8629deeb0638ce9b4d8e6a70e8e6b : verified
SHA1 checksum: 6eff5094523c78278304700f3558a0b25a127f1f : verified
```

Obrázok 11 Obraz USB cez FTK imager



Obrázok 12 Zistené súbory v Autopsy

.bat 1 Results

Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
Invoice_2026-01-02.bat			0	2026-03-05 12:47:34 SEC	0000-00-00 00:00:00	2026-03-05 01:00:00 SEC	2026-03-05

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

```
@echo off
color 4f
title WARNING: VIRUS DETECTED
echo =====
echo !! VIRUS DETECTED: SYSTEM COMPROMISED !!
echo =====
echo.
echo Name: Trnava_Malware.Module_01.exe
echo Status: Infected
```

Obrázok 13 Podozrivý .bat súbor (Autopsy)

8 Použité nástroje

Na spracovanie a analýzu zaistených zariadení boli použité špecializované softvérové nástroje určené pre digitálnu forenznú prácu.

8.1 FTK Imager

Bol použitý na vytvorenie forenzného obrazu USB zariadenia. Tento nástroj umožňuje vytvoriť bitovú kópiu pôvodného média, čím sa zabezpečí, že originálny dôkaz nie je poškodený alebo upravený. Obraz USB bol následne analyzovaný v nástroji Autopsy.

8.2 Autopsy

Autopsy slúžil na detailnú digitálnu forenznú analýzu dát zo smart hodínok a USB zariadenia. V prostredí Autopsy bolo možné identifikovať a prezrieť CSV súbor z hodínok, overiť jeho metadáta, zobrazit' obsah v textovej forme a získať hexadecimálny náhľad súborov. Nástroj zároveň umožnil lokalizovať podozrivé súbory na USB zariadení, vrátane skriptu (.bat), ktorý bol vyhodnotený ako potenciálny malvér.

8.3 Microsoft Excel

Microsoft Excel bol využitý na obsahovú analýzu a vizualizáciu biometrických údajov zo smart hodínok, najmä tepovej frekvencie a pohybovej aktivity. Grafické spracovanie dát umožnilo porovnanie pokojového a incidentného intervalu a podporilo interpretáciu dát.

9 Bezpečnostné opatrenia

Pri analýze zariadení boli pôvodné hodinky a USB skopírované do bitových kópií pomocou FTK Imager, aby sa zachovala integrita dát. Pre každú kópiu boli vypočítané hash hodnoty (MD5 a SHA-256) a uchovávané na šifrovanom úložisku s obmedzeným prístupom. Originálne zariadenia boli fyzicky zabezpečené, uložené v uzamknutej bezpečnostnej skrini a prístup k nim mali len poverené osoby.

Číslo:	01	Typ súboru:	Binárny obraz	Obnovený súbor:	nie	Veľkosť:	41,9 kB
Popis prípadu:		Hodinky v tme					
Názov súboru:		image_watches.ad1					
Miesto získania digitálnej stopy:		Kancelária spoločnosti					
Poznámky:		CSV z digitálnych hodín					
Časové pečiatky							
Access:	00.00.0000 0:00:00		Modify:	00.00.0000 0:00:00		Change:	00.00.0000 0:00:00
Digitálny odtlačok (heš)	MD5	034b74f3e7c0c65d7b57fdce1f5b3ff4					
	SHA1	9267702e71ed964b6642ade7830ae2d990c97557					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
7.3.2026 6:50		Zaistenie a vloženie do tieniaceho obalu.					
7.3.2026 10:30		Vytvorenie forenznej kópie.					
8.3.2026 9:30		Odovzdanie dôkazov na forenznu analýzu.					

Obrázok 14 Chain of custody - CSV

Číslo:	02	Typ súboru:	Binárny obraz	Obnovený súbor:	nie	Veľkosť:	4GB
Popis prípadu:		Hodinky v tme					
Názov súboru:		ev-usb.E01, ev-usb.E02, ev-usb.E03					
Miesto získania digitálnej stopy:		Kancelária spoločnosti					
Poznámky:		USB Pretec i-Disk BulletProof					
Časové pečiatky							
Access:	05.03.2026 1:00:00		Modify:	05.03.2026 12:47:34		Change:	05.03.2026 17:34:45
Digitálny odtlačok (heš)	MD5	39b8629deeb0638ce9b4d8e6a70e8e6b					
	SHA1	6eff5094523c78278304700f3558a0b25a127f1f					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
7.3.2026 7:00		Zaistenie a vloženie do tieniaceho obalu.					
7.3.2026 11:15		Vytvorenie forenznjej kópie.					
8.3.2026 9:30		Odovzdanie dôkazov na forenznú analýzu.					

Obrázok 15 Chain of custody - USB

ZÁVER

Cieľom práce bolo overiť, či nájdené smart hodinky môžu slúžiť ako relevantný digitálny dôkaz pri objasňovaní krádeže v kancelárii. Analýza ukázala výrazný rozdiel medzi pokojovým a incidentným intervalom, najmä v hodnotách srdcovej frekvencie a pohybovej aktivity, čím sa potvrdili hypotézy 2 a 3.

Hypotézu 1 nebolo možné jednoznačne potvrdiť, keďže zo samotných údajov hodínok nemožno s istotou určiť konkrétneho používateľa. Hypotéza 4 bola potvrdená len čiastočne, pretože lokalizačné údaje a MAC adresa párovaného telefónu pomohli zúžiť okruh podozrivých, no samy osebe nepostačujú na úplnú identifikáciu osoby.

Hypotéza 5, týkajúca sa USB zariadenia, bola potvrdená čiastočne: analýza odhalila súbor .bat, ktorý je potenciálne škodlivý a môže súvisieť s incidentom, čím sa potvrdila jeho relevancia ako digitálneho dôkazu.

Práca ukázala, že smart hodinky aj USB zariadenie môžu významne prispieť k rekonštrukcii priebehu udalosti, poskytujú časové, priestorové a technické údaje, ktoré podporujú vyšetrovanie a hodnotenie incidentu.