Zajišťování důkazních materiálů v kybernetických systémech

Bc. František Sedláček

Diplomová práce

2021

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2020/2021

ZADÁNÍ DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. František Sedláček**
Osobní číslo:	**A19497**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Zajišťování důkazních materiálů v kybernetických systémech**
Téma práce anglicky:	**Providing evidence in cybernetic systems**

Zásady pro vypracování

1. Analyzujte existující doporučení pro akvizici digitálních důkazu, včetně legislativních požadavků.
2. Specifikujte problematické oblasti z hlediska dodržení legislativních požadavků při technických opatřeních
3. Navrhněte postupy pro řešení vybraných scénářů.
4. Ověřte navržené postupy prostřednictvím řízeného experimentu včetně vypracování znalecké zprávy.
5. Sestavte kompletní metodiku pro řešení problematických oblastí z bodu 2.

Forma zpracování diplomové práce: **Tištěná/elektronická**

Seznam doporučené literatury:

1. SCHEIDT, Nancy a Mo ADDA. Identification of IoT Devices for Forensic Investigation. 2020 IEEE 10th International Conference on Intelligent Systems (IS), Intelligent Systems (IS), 2020 IEEE 10th International Conference on [online]. 2020, , 165-170 [cit. 2020-10-23]. ISBN 9781728154565. ISSN edseee.IEEEConferenc. Dostupné z: doi:10.1109/IS48319.2020.9200150
2. BECIROVIC, Seila a Sasa MRDOVIC. Manual IoT Forensics of a Samsung Gear S3 Frontier Smartwatch. 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Software, Telecommunications and Computer Networks (SoftCOM), 2019 International Conference on [online]. 2019, , 1-5 [cit. 2020-10-23]. ISBN 9789532900880. ISSN 1847358X. Dostupné z: doi:10.23919/SOFTCOM.2019.8903845
3. KRUGER, Jaco-louis a Hein VENTER. Requirements for IoT Forensics. 2019 Conference on Next Generation Computing Applications (NextComp), Next Generation Computing Applications (NextComp), 2019 Conference on [online]. 2019, , 1-7 [cit. 2020-10-23]. ISBN 9781728114606. ISSN edseee.IEEEConferenc. Dostupné z: doi:10.1109/NEXTCOMP.2019.8883615
4. VYSKOČIL, Ladislav. Zajišťování a analýza digitálních důkazů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 105 s. Dostupné také z: http://hdl.handle.net/10563/24882. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav informatiky a umělé inteligence. Vedoucí práce Malaník, David.
5. KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016, 522 s. CZ.NIC. ISBN 9788088168157. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf
6. MIDDLETON, Bruce. Cyber crime investigator's field guide. 2nd ed. Boca Raton: Auerbach Publications, c2005, xiv, 279 s. ISBN 0849327687.

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **15. ledna 2021**
Termín odevzdání diplomové práce: **17. května 2021**

L.S.

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 15. ledna 2021

Jméno, příjmení: Bc. František Sedláček

Název bakalářské/diplomové práce: Zajišťování důkazních materiálů v kybernetických systémech

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 11. 5. 2021

František Sedláček, v.r.
podpis diplomanta

ABSTRAKT

Práce zkoumá problémy vznikající při terénní práci kriminalistických expertů v moderních systémech s ohledem na rozvoj kybernetické složky společenského života ve formě IoT a inteligentních zařízení. Ty přináší nové požadavky a výzvy při získávání dat pro účely vyšetřování trestných činů na místě činu po zajištění těchto zařízení.

V teoretické části se práce zabývá metodami a postupy, které je nutné dodržet, aby bylo možné získat data s dostatečnou mírou důvěryhodnosti pro jejich použití v důkazním šetření. Takto teoreticky navržené postupy dále ověřuje pomocí praktických scénářů, které se soustředí na získání dat z konkrétních zařízení tříd *smart technology* nebo *IoT* s důrazem na zajištění všech právních a technických požadavků stanovených předběžně z teoretického hlediska.

Klíčová slova: IoT, důkazní materiál, kriminalistika, kybernetika, metodika, IoT důkazy

ABSTRACT

The present thesis inspects issues arising during preliminary work of forensic experts in contemporary systems, mainly due to increasing impact of cybernetical components of everyday affairs in the form of IoT and intelligent systems, bringing forth new requirements and challenges when obtaining raw data for crime scene investigators.

Theoretical part describes methods and procedures that need to be upheld to obtain data of sufficient quality for forensic investigations. Those theoretical designs are then applied to practical scenarios, focusing on obtaining data from chosen pieces of IoT or Smart devices with emphasis on maintaining all legal and technical requirements, as set in preliminary theoretical analysis.

Keywords: IoT, evidence, forensics, criminalistics, cybernetics, methodology, IoT evidence

Za umožnění zpracování práce bych chtěl poděkovat Magistrátu města Brna a dále:

- Policii České republiky, jmenovitě Ing. kpt. Ladislavu Vyskočilovi, za praktické konzultace a poznatky;
- společnosti Brněnské komunikace, a. s., za poskytnutí vozidla vybaveného C-ITS systémem a konzultací při analýze C-ITS platformy;
- společnosti Minalox, s. r. o., za ochotu poskytnout laboratoře k analýze technologií chytré stavby (nerealizováno kvůli pandemii);
- mým rodičům Ing. Vladimíru Sedláčkovi a Ing. Miriam Sedláčkové za pomoc při analýze a realizaci praktických experimentů.

A v neposlední řadě děkuji své ženě Lence Sedláčkové, svému školiteli Ing. Davidu Malaníkovi, Ph.D., korektorce Mgr. Alžbětě Vintrové a všem, kteří mi pomohli s přípravou a realizací diplomové práce.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Využívání inteligentních technologií, které sbírají data a posílají je ke zpracování do různých informačních systémů, zažilo v poslední době velký boom. Objevuje se nositelná elektronika, naprostá většina lidí používá mobilní telefon[1].

Zároveň s tím se také rozšiřuje množství informací, které mají lidé o sobě samých k dispozici. Chytré hodinky, auta i mobilní telefony obvykle mají GPS tracker nebo alespoň jsou schopné sledovat pohyb nositele, chytré zámky a poplachové systémy umí zaznamenávat průchody dveřmi a podobně.

Tato práce sleduje, nakolik by údaje reálně získatelné z těchto zařízení při ohledání zájmového místa mohly zůstat neporušeny a poskytovat dostatek relevantních dat, aby je bylo možné v případě potřeby využít pro důkazní řízení před soudem.

Abychom toho dosáhli, musíme mít jistotu, že jsme schopni získat data, která mají vypovídací hodnotu, ale také plní příslušné legislativní i technické normy, které jsou kladeny na data, jež se mají použít v soudních líčeních. Práce je rozdělena na dva okruhy – v prvním analyzuje existující doporučení pro získávání digitálních důkazů a porovnává je s technickými možnostmi a údaji, které jsou v dispozici v různých IoT zařízeních, ať už teoreticky, nebo podle deklarace výrobce. Soustředí se přitom na údaje, které je možné získat již v první fázi vyšetřování, tedy před samotným soudním procesem, a které mohou pomoci stanovit základní kriminalistickou hypotézu.

V další části tohoto prvního okruhu jsou tyto poznatky obohaceny o možné využití takových dat pro doplnění fyzických důkazů v typovém šetření fiktivních případů různé povahy. Cílem je, aby bylo jasné, jaká data musíme primárně ze zařízení být schopni získat, než může opustit místo činu. Práce se snaží zajistit metodou, která umožňuje bezpečné ověření těchto dat, replikaci celého postupu a další podmínky pro použitelnost důkazního materiálu před soudem.

[1] Podle šetření Českého statistického úřadu z roku 2020 je v české populaci ve věkovém rozmezí 16–74 let podíl osob využívajících chytrý telefon 75,8 % a tento podíl každým rokem roste.

Druhý okruh se potom bude soustředit na praktickou ukázku. Vybrané scénáře, navržené jako výstup prvního okruhu, budou následně ověřeny v laboratorních podmínkách, a to s důrazem na zachování procesní čistoty a všech podmínek pro využití získaných dat ve forenzním šetření.

Poslední část práce navrhuje metodiku, kterou by do budoucna bylo možné využít pro forenzně prokazatelné získávání dat z těchto zařízení. Práce tak poskytuje návrh jakési kuchařky shrnující metody zajištění důkazů pro různé skupiny IoT zařízení. Vzhledem k místu vzniku práce bude pro tyto účely posuzováno právní prostředí České republiky, které je součástí evropského kontinentálního právního prostoru. Všechna relevantní pravidla pro zajišťování důkazů budou tedy prováděna v souladu s českými předpisy a porovnávána s českými požadavky na evidenci a zpracování důkazních materiálů.

LEGISLATIVNĚ-TECHNICKÉ ASPEKTY ZAJIŠŤOVÁNÍ DŮKAZŮ V IOT ZAŘÍZENÍCH

1 PRÁVNÍ STRÁNKA ZAJIŠTOVÁNÍ DŮKAZNÍHO MATERIÁLU

Abychom se v práci mohli zabývat problematikou zajišťování důkazního materiálu, musíme se nejprve podívat na to, co se vlastně důkazním materiálem rozumí.

V obecné rovině českého trestního práva jsou důkazy prostředkem, kterým se realizuje proces dokazování. Ten Polčák, Púry a Harašta popisují takto [1]: „…Dokazování v trestním řízení je vedle rozhodování nejdůležitější procesní činností orgánů činných v trestním řízení, protože umožňuje zjistit skutkový základ pro jejich rozhodování a pro další postup tak, aby mohl být splněn účel trestního řízení vymezený v ustanovení § 1 odst. 1 trestního řádu (dále také TŘ). Jím je takový postup orgánů činných v trestním řízení, který zaručí, aby trestné činy byly náležitě zjištěny a jejich pachatelé byli podle zákona spravedlivě potrestáni. Řízení přitom musí působit k upevňování zákonnosti, k předcházení a zamezování trestné činnosti, k výchově občanů v duchu důsledného zachovávání zákonů a pravidel občanského soužití i čestného plnění povinností ke státu a společnosti.“

Z uvedeného vyplývá, že důkazní řízení je důležitý proces, bez kterého se trestní řízení neobejde. Jeho cílem je zjistit skutkovou podstatu dané události a vyvodit, zda daná událost je skutečně protizákonným konáním a v jakém smyslu, tedy zda jde o zločin, trestný čin, nebo přestupek.

Forenzní disciplínou, která dokazování provádí tím, že vypracovává postupy k odhalování, předcházení a vyšetřování trestné činnosti, je kriminalistika. Proto postupy, které vedou ke správnému zajištění důkazního materiálu, nazýváme *kriminalistickými postupy*.

1.1 Digitální důkazy v soudním řízení

Výše uvedené principy se nezabývají detailněji povahou získaného důkazního materiálu. Pro účely obecného stanovení důkazních principů jsou si všechny důkazy rovny. Trestní řád poskytuje demonstrativní výčet důkazních prostředků, které se mohou pro dokazování skutečností v trestním řízení použít. Tento výčet ovšem ze své podstaty nemůže nikdy být kompletním autoritativním výčtem všech důkazních forem. Poskytuje pouze nezbytnou oporu pro provádění základních druhů

kriminalistické analýzy. Podrobněji se potom trestní řád z důkazních postupů, které se přímo netýkají kybernetického prostředí, věnuje zejména: výpovědi obviněného, výpovědi svědků a vybraným zvláštním způsobům dokazování. Mezi ně řadí: konfrontaci, rekognici, vyšetřovací pokus, rekonstrukci a prověrku na místě, znaleckou činnost, ohledání těla a vyšetření duševního stavu. Jak je z tohoto výčtu patrné, s výjimkou vypracování znaleckého posudku se žádný z těchto postupů nedá aplikovat na důkazy, které potřebujeme zajistit v kybernetickém prostředí.

Z tohoto hlediska jsou zajímavější zbývající dva oddíly. Jedním je výslech obviněného prostřednictvím videokonferenčního zařízení a posuzování věcných a listinných důkazů.

1.2 Postupy k zajištění digitálních důkazů v rámci přípravného řízení

Všechny výše uvedené důkazní postupy se týkají důkazů využitelných v dokazování před soudem, což je pozdější fáze trestního řízení. Tomu ještě obvykle předchází přípravné řízení, které se dělí na fázi prověřování a fázi vyšetřování. Zde je k dispozici širší paleta důkazních postupů a institutů. Kromě výše zmíněných zde ještě přichází v úvahu institut povinnosti k předložení nebo vydání věci a institut *odnětí věci* (§ 78, případně § 79 zákona 141/1961 Sb., trestního řád – dále také „TŘ“), institut domovní a osobní prohlídky, *prohlídky jiných prostor a pozemků* (oddíl pátý TŘ), *odposlech a záznam telekomunikačního provozu* (§ 88 TŘ) případně *vyžádání údajů o telekomunikačním provozu* (§ 88a TŘ) a některé z již výše uvedených postupů, jako je ohledání, prohlídka místa činu nebo využití posudku znalce.

Řada výše uvedených institutů přitom slouží k získání datových nosičů, tedy hmotných prostředků, které slouží k ukládání nebo zpracování dat. Důkazem potom jsou samotná data uložená na těchto datových nosičích. Při zajišťování důkazů v IoT systémech se zde ovšem projevují určitá specifika. Například zařízení ze třídy nositelné elektroniky, tzv. *wearable device*, jako například chytré hodinky nebo náramek, je možné již na místě činu použít k vyčtení vybraných biometrických údajů oběti, stejně jako informací o jejích schůzkách, komunikaci, telefonních kontaktech, případně dalších dat z volitelných aplikací, které mohou být v zařízení přítomny.

Dále můžeme zjistit například telefonní číslo oběti, což může být užitečné při lokalizaci mobilního telefonu, došlo-li k jeho odcizení, nebo její jméno či další údaje. Při všech těchto krocích ovšem musíme vést v patrnosti podmínky pro získávání odpovídajícího typu důkazního materiálu, respektive dodržení odpovídajícího důkazního postupu, jak je stanovuje právě trestní zákoník.

1.3 Specifika zajištění důkazů v podobě digitálních dat

V případě elektronických důkazů představuje hardwarové zařízení pouze prostředek, který skutečně drží daný důkaz. Tato situace se dá přirovnat k zajištění listinného důkazu. Také v tomto případě není skutečným důkazem samotná listina, ale vyjádření, které poskytuje. Nicméně listinné a digitální důkazy mají několik podstatných rozdílů. Zatímco postupy zajištění autenticity listinných důkazů jsou dobře známé a listiny je snadné verifikovat proti případné manipulaci, tato samá důvěryhodnost není automatická u digitálních důkazů. Pojem ***digitální důkaz*** už ovšem nepochází z trestního zákoníku ani jiných ustanovení právního řádu ČR. Jeho definici poskytuje například Kolouch [2], který navrhuje následující znění: „Digitálním důkazem jsou jakákoliv data či informace, jež byly přeneseny, vytvořeny, uloženy či modifikovány za použití počítačového systému a které prokazují nebo vyvracejí dokazovanou skutečnost a mohou být prostředkem k odhalení a zjištění trestného činu a jeho pachatele, jakož i stopy trestného činu."

Z této definice je jasné, že digitálním důkazem není samotné zajištěné zařízení, ale až data či informace v něm uložené. Je z ní také patrné, že zmíněná data mohou být v průběhu životního cyklu modifikována, aniž by toto ohrozilo jejich důkazní hodnotu před samotným zajištěním.

Jiná situace ovšem nastává po zajištění digitálních dat. Zde již za jejich autentičnost, tedy nezměněnost oproti původnímu stavu, odpovídá osoba, která důkaz v dané chvíli zpracovává. Tok důkazů se dokumentuje proti podpisu – výsledný manipulační protokol je součástí vyšetřovacího spisu. Opět je možné chápat tento požadavek jako ekvivalentní k požadavku nutnosti neznehodnotit důkazní materiál během

kriminalistické analýzy, abychom dodrželi jistotu, že byly ze získaného materiálu vyvozeny správné závěry.

Pro účely zajištění dat z IoT zařízení v terénu pak může být nutné data ze zařízení získat za omezených podmínek pro manipulaci s ním. Musíme tedy uvažovat, že může být nezbytné mít k dispozici nejen technický počítač, který umí bezpečně pořídit kopii dat, ale také mnohem méně obvyklý technický mobilní telefon nebo technický mikropočítač, který je schopný data získat bez využití obvyklé aplikace. Místo aplikace dostupné pro tyto účely na OS Android je třeba využít specifického technického nebo odposlechového software. Z povahy IoT zařízení pak vyplývá, že data v tomto zařízení není možné snadno modifikovat a velká část z nich umožňuje jen jednosměrný pohyb uživatelských dat, což nám umožňuje verifikovat data až ve spárovaném technickém zařízení. Ani v tomto případě není ovšem možné uvažovat autenticitu dat automaticky, naopak pokud se dokážeme dostat přímo k datům v zařízení, je dobré předpokládat, zejména nevyžaduje-li proces nějaký extrémně komplexní technický prostředek, že se k nim mohl dostat také případný pachatel.

2 TECHNICKÉ ASPEKTY ZÍSKÁVÁNÍ DŮKAZŮ

Pro účely technického zajišťování důkazů a manipulace s nimi je nezbytné zajistit celou řadu podmínek. Jejich cílem je dodržení právní hodnoty důkazních materiálů a jejich využitelnosti. Jak již bylo výše uvedeno, hlavním problémem je fenomén datové volatility. Data se v systémech průběžně mění, a pokud chceme soud skutečně přesvědčit, že určitá data dokazují určitou skutečnost, musíme doložit, že nedošlo k manipulaci s nimi.

Této požadované vlastnosti digitálních důkazů říkáme autenticita a je možné ji definovat různě. Nejjednodušší definici nabízí Výkladový slovník Kybernetické bezpečnosti, který ji popisuje jako „vlastnost, že entita je tím, za co se prohlašuje“ [3]. Procesem, který vede k zajištění autenticity, je autentizace. Ve stejném zdroji najdeme autentizaci dat definovanou jako „proces používaný k ověření integrity dat (např. ověření, že přijatá data jsou identická s odeslanými daty, ověření, že program není infikován virem)“. Pro účely důkazního řízení jde o proces, kterým zajišťujeme, že data předkládaná soudu jsou stejná data, která byla získána některým z procesních postupů trestního práva, jež byly definovány v předchozí kapitole.

2.1 Zajištění autenticity důkazních stop

K zajištění autenticity důkazních stop existuje více postupů, například je možné data uložit na médium, které neumožňuje po vytvoření zapsaná data modifikovat (CD-R disk). Alternativním a běžněji doporučovaným postupem je ovšem využití matematických funkcí známých jako hash. Tím vzniká takzvaný kontrolní otisk, „který je pak nedílnou součástí zajištěných dat nebo pořízených bitových kopií digitálních stop a primárně je určen k autentizaci těchto stop. Hodnota tohoto kontrolního otisku se pak ukládá do textového souboru na stejném paměťovém médiu, kde jsou uložena i zajištěná data. V praxi to znamená vypočíst kontrolní otisk pro každý zajištěný soubor nebo vytvořenou bitovou kopii paměťového média. Kdykoliv později je pak možné provedení výpočtu kontrolního otisku opakovat za účelem ověření, že data nebyla žádným způsobem modifikována“ [4].

Tento postup ovšem potenciálně nese jedno riziko – pokud máme hashe jen a výhradně na stejném zařízení, na kterém jsou samotné důkazy, může potenciálně dojít k tomu, že kdokoliv, kdo by měl zájem s důkazy manipulovat, přepíše i tyto otisky, a tedy znehodnotí celou práci na získaném důkazu. V policejní praxi se proto hash kromě uložení na stejném médiu vedle platného obrazu ještě přepisuje do protokolu, který je součástí vyšetřovacího spisu. Tento hash existuje v listinné podobě, a protože celý protokol je následně ještě verifikován podpisem jak elektronicky před vytištěním, tak fyzicky následně ihned po něm, slouží sekundární záznam hashe na něm jako pojistka proti ztrátě integrity.

Výše zmíněné principy jsou dobře aplikovatelné pro jakákoliv zařízení, která mají povahu datových nosičů. Předpokládají ovšem mimo jiné možnost původní datový nosič přímo bezpečně okopírovat nebo z něj vytvořit bitový obraz, který se použije v analytickém stroji. Tato situace je v praxi dobře proveditelná u většiny obvyklých počítačů nebo mobilních telefonů, které obsahují operační systém se známou strukturou. Ten je vesměs možné zachytit v podobě bitové kopie, tedy obrazu, který je naprosto totožný se zajištěným originálem, a toto ověření je dále dokladováno některým z matematických postupů, například pomocí kryptograficky bezpečného hashe. V praxi se pro kontrolu kopírování dat nepoužívají vždy nezbytně kryptografické funkce. Místo nich se používají CRC algoritmy, které mají oproti kryptograficky bezpečným hashům určité výhody. Například jde o rychlost, kterou jednotlivé implementace poskytují, ale také o možnost ověření výstupů z CRC kódu pomocí kontrolního Hammingova kódování, kterým je možné zajistit opravu chyb až na úroveň detekce a opravy chyb jednotlivých bytů, což je pro kopie klíčové [5].

Kryptograficky bezpečné algoritmy totiž sice umožňují ověřit, že získaná data jsou navzájem stejná, ale už ne najít nebo opravit chyby v případě, že se něco stane při přenosu. Jinými slovy, pokud takto zajišťujeme důkazní materiál, ke kterému není možné udělat předem z jakéhokoliv důvodu samostatný kryptografický otisk, pak CRC kód poskytne nejen možnost ověření, ale také možnost korekce chyb, které při přenosu mohly vzniknout. CRC jako mechanismus pro zajištění autenticity dat ovšem není možné akceptovat, protože bylo dokázáno, že stávající CRC implementace

nejsou dostatečně kryptograficky bezpečné kvůli nutné znalosti použitého generátorového polynomu, díky čemuž je následně možné invertovat celý proces získávání otisku zprávy [6].

Tento proces ovšem opět naráží na specifickou povahu většiny IoT zařízení. Ta totiž kromě technicky náročnější operace přehrání firmware novou verzí nabízí jen možnost data ze zařízení vyčítat, nikoliv na něj nová data ukládat. S výjimkou některých kamer, které mají jako formu úložiště externí SD kartu, tak můžeme data ve chvíli jejich zaslání do technického zařízení[2] považovat za autentická a ověřovat pouze autenticitu získaných souborů. U nich již ovšem musíme využít některý z výše popsaných postupů. Ideálním případem pak je, pokud technické zařízení má příslušné forenzní subrutiny a otisk přijatého datového souboru vytvoří a uloží ihned po ukončení přenosu zprávy.

2.2 Problematika zajištění datových důkazů v kontextu IoT zařízení

Jelikož se má tato práce zabývat zajišťováním důkazů v IoT zařízeních, je nezbytné si také určit, co přesně chápeme pod pojmem IoT zařízení. Jednou z možných definic v tomto ohledu je, že jde o zařízení schopná v rámci vykonávání své běžné funkce získávat, zpracovávat a dále předávat údaje ze svého okolí. Zejména je důležitá podmínka schopnosti data předávat – ta odlišuje IoT či „chytrá“ zařízení od jejich běžných protějšků [7]. V Česku se potom potkáváme s českým překladem „internet věcí“, nicméně v této diplomové práci se budeme snažit držet původního anglického názvosloví, tedy IoT nebo internet of things.

Z českého termínu nicméně vychází definice, která pochází od inženýra Sichrovského, ředitele společnosti České radiokomunikace. Ve své diplomové práci ji uvádí Weissmannová [8]. Podle této definice se „jedná o svět věcí, které jsou

[2] Pojmem „technické zařízení“ v kriminalistice rozumíme zařízení, které využívá vyšetřovatel a jehož obsah je dostatečně známý a zdokumentovaný, aby bylo možné rozlišit, jaká data na něm byla původně a jaká se na něj dostala jako součást získávání důkazních materiálů.

propojené primárně, nikoli však nutně, bezdrátově, které umí komunikovat prostřednictvím sdílení dat. A tato komunikace nesměřuje pouze k tomu, aby data získaná z těchto věcí byla centralizována v místě, kde budou dále zpracovávána a využívána, ale ideálně aby zúčastněné věci komunikovaly obousměrně, spolupracovaly a data využívaly pro své autonomní fungování a řízení svého vnějšího prostředí“. Společným prvkem obou definic je tedy požadavek na umožnění vzájemné komunikace mezi jednotlivými zařízeními, který je doplňkem jejich běžné funkce. V tomto smyslu budeme IoT zařízení chápat i v kontextu této práce.

Nevýhodou IoT zařízení v tomto smyslu nicméně je, že ne všechna tato zařízení mají vhodný operační systém, který umožňuje vytváření kopií nebo vůbec přístup k datům na úrovni jednotlivých souborů. Za tímto účelem je nutné odlišit dva možné scénáře – analýzu přímo zapojených zařízení a dat, která z nich přichází (analýzu „živého“ zařízení), a analýzu dat, která se v zařízení uchovala po jeho zajištění.

Model pro umožnění zajištění analýzy živých zařízení předkládají ve své práci například Kruger a Venter [9], kteří uvádí nutnost existence centrálního úložiště IoT dat, které funguje ideálně jako read-only sběrné místo. Analýze jsou potom podrobována data z tohoto úložiště, místo dat proudících z jednotlivých zařízení.

V běžné praxi by takové sekundární úložiště záleželo na konkrétní povaze zařízení. U IoT kamer napojených na domovní instalace by jím mohlo být dozorové centrum nebo ústředna PZTS, u nositelných zařízení například mobilní telefon vlastníka a podobně.

Vzhledem k povaze tohoto centrálního úložiště se pak dá čekat, že by na něj byla aplikovatelná některá ze známých metodik pro akvizici digitálních důkazů, například z běžných operačních systémů nebo mobilních telefonů. Jak uvádí Kruger a Venter (*tamtéž*), pokud dodržíme read-only vlastnost spojení mezi analytikem a centrálním repozitářem, měli bychom být schopni dosáhnout dostatečné úrovně důvěrnosti. Vychází přitom z předpokladu, že data zasílaná jednotlivými zařízeními do centrálního repozitáře nebudou žádným způsobem modifikována, respektive že mají standardizovanou ochranu proti modifikaci. Centrálním repozitářem v tomto smyslu

pak může podle nich být i cloudové úložiště, pokud jsme schopni zajistit jeho read-only vlastnost a pokud jej považujeme za dostatečně důvěryhodné.

Za hlavní nevýhodu pak autoři považují neexistenci jednotných datových formátů pro různá zařízení i pro jednotlivé programové platformy pro digitální forenzní analýzu. Jinými slovy, pokud bychom výše popsaný systém implementovali ve formě preventivního opatření, může se stát, že jím zachycená data bude stále nutné konvertovat do jiných datových formátů, případně z nich vytvořit odpovídající datové sady. To je ovšem již předmětem další fáze, tedy digitální forenzní analýzy, jejíž postupy, možností a cíle jsou mimo rozsah této diplomové práce a byly opakovaně popsány.[3]

Dalším problematickým faktorem je poměrně široká škála existujících zařízení, která do této třídy řadíme. Obecně se sice mluví o IoT zařízeních, ale ve skutečnosti do této obecné kategorie patří větší množství zařízení. Jak totiž vyplývá z definice IoT zařízení výše v této kapitole, může jím být v podstatě jakékoliv zařízení, které obsahuje senzory, nebo alespoň slouží jako centrální komunikační sběrnice pro senzorová data, přičemž umožňuje získaná data sdělit dále, případně přijmout zprávu z dalších systémů.

2.3 Klasifikace IoT zařízení pro účely přístupů k analýze

Abychom tedy zúžili škálu IoT zařízení, využijeme pomocné třídění, podle kterého dělí Blinowski a Piotrowski [10] IoT zařízení na následujících šest tříd:

„• H – Home and SOHO[4] devices; routers, on-line cameras and monitoring, other customer grade-appliances.

[3] V českém prostředí například v rámci bakalářské práce Ivo Šulce, obhájené v roce 2016 na právnické fakultě Masarykovy univerzity v Brně, práce je dostupná na https://is.muni.cz/th/u9ozv/?fakulta=1433.

[4] SOHO – Small Office / Home Office.

• S – SCADA and industrial systems, automation, sensor systems, non-home IoT appliances, car and vehicles (subsystems), medical devices, industrial video recorders and surveillance systems.

• E – Enterprise, Service Provider (SP) hardware (routers, switches, enterprise Wi-Fi and networking) – this constitutes mainly the network level of IoT infrastructure.

• M – mobile phones, tablets, smart watches, and portable devices – this constitutes the "controllers" of IoT systems.

• P – PCs, laptops, PC-like computing appliances and PC servers (enterprise) – this constitutes the "controllers" of IoT systems.

• A – other, non-home appliances: enterprise printers and printing systems, copy machines, non-customer storage and multimedia appliances. "

Zdrojový článek uvádí, že kategorií je sedm, ovšem neuvádí žádné podrobnosti ke kategorii označené písmenem „C". Na přímý dotaz odpověděl autor článku, že se jedná o třídu průmyslových ovladačů (z anglického „C" – Controller), tedy čipů a jednočipových hradel používaných pro řízení jednotlivých IoT zařízení, jelikož prováděli klasifikaci pomocí strojového učení. Pro naše účely je tedy tato třída nezajímavá a nebudeme ji dále uvažovat, jelikož taková zařízení se téměř nevyskytují samostatně bez další elektroniky, s níž dohromady tvoří komplexní stroj. Autoři sami k této kategorii nepodávají ve svém článku žádné vysvětlení.

Jak vidíme, v této práci se autoři do jisté míry drží širšího chápání pojmu IoT, než se objevuje obecně v literatuře, a sice jako obecně jakéhokoliv zařízení, které umožňuje přístup na internet a sdílení dat.

V této práci nicméně není cílem zabývat se opakovaně analýzou již popsaných systémů, u kterých lze pořídit bitovou kopii a analyzovat až tu, jelikož akvizice i analýza bitových kopií je poměrně dobře známým fenoménem.

Z tohoto důvodu se budeme soustředit primárně na zařízení v méně typických třídách. Jde o třídy, kde buď nemůžeme zařízení z místa činu „odnést", nebo kde manipulace s tímto zařízením může způsobit ovlivnění nebo ztrátu dat nebo jiných důkazů,

například proto, že zaznamenává údaje neustále nebo že se dotýká jiného objektu, a musíme tedy být schopní rozlišit data zajištěná na místě činu od dat modifikovaných v rámci potenciálního přenosu a akvizice.

Z výše popsaných tříd se z těchto důvodů budeme zabývat zejména třídami H, S, E a A. Dále jako páté zařízení pro úplnost doplníme zařízení z třídy M, konkrétně chytré hodinky, jako jeden z velmi obvyklých zástupců IoT zařízení.

Pro každou z těchto tříd nyní zkusíme definovat pravděpodobný scénář útoku. Za scénář útoku přitom nebudeme považovat zneužití konkrétní zranitelnosti, ale komplexní scénář, ve kterém určitý motivovaný útočník zařízení napadne za účelem vlastního obohacení.

Cílem těchto scénářů není technologicky popsat možné vektory útoku proti daným zařízením, ale spíše z hlediska kriminalisticko-technické expertízy popsat, zda či jak lze data uložená v těchto zařízeních využít v první fázi vyšetřování trestné činnosti. Pomineme přitom fakt, že již samotné napadení elektronického zařízení je podle českého právního řádu trestným činem, a zaměříme se skutečně jen na scénáře, kdy zařízení obsahuje nemodifikovaná data použitelná pro kriminalisticko-technickou expertízu.

Scénáře budeme následně analyzovat z hlediska možných zajistitelných důkazů s ohledem na zachování jejich důvěrnosti, integrity a dostupnosti, jak je definuje teorie bezpečnosti informačních systémů, a dále s ohledem na principy jejich zajišťování, jak jsou popsány v literatuře [1] a jak byly zmíněny v předchozích kapitolách.

2.4 Jednotlivé scénáře napadení IoT zařízení

Nyní se tedy pokusíme stanovit jednotlivé scénáře pro výše definované skupiny zařízení tak, aby bylo jasné, jakým způsobem lze data v těchto zařízeních obsažená použít ke stanovení kriminalistické hypotézy a případně zařadit mezi důkazní materiál.

Tyto scénáře mají dvojí využití – na jejich bázi stanovíme obecnou metodiku pro zajišťování IoT zařízení a tuto dále konkretizujeme pro zajištění zařízení v jednotlivých kategoriích. Dále budeme s využitím těchto scénářů navrženou metodiku v praktické části práce testovat.

Při jejich stanovení se nebudeme zaměřovat na útoky na tato zařízení jako jediný cíl páchané trestné činnosti, ale na scénáře, kdy může být IoT zařízení využito jako prostředek, kterým objasníme spáchaný skutek a jeho kontext.

2.4.1 Scénář pro skupinu H – domácí zařízení a zařízení pro drobné podnikatele

Do této kategorie patří typická zařízení, s kterými se setkáváme i v našich domovech. Nabízí se analýza dat z připojené Wi-Fi kamery, která nenahrává pravidelně údaje na žádné další zařízení, tedy je ukládá jen na vnitřním úložišti nebo cloudu výrobce, případně analýza chytrého termostatu řízeného přes mobilní aplikaci.

Právě druhý scénář budeme uvažovat v této diplomové práci. A to následujícím způsobem – mějme opuštěný objekt, u kterého majitel nahlásí rozbité okno. Na místo přijede místně příslušná hlídka, která prvotní obhlídkou a rozhovorem s majitelem zjistí, že se v objektu ani jeho okolí již 10 dní nepohyboval, protože jej trvale neobývá. Při dalším příjezdu majitel zjistil, že je rozbité okno, a do objektu zatím nevstoupil, protože se domnívá, že okno mohl rozbít vandal, jenž může případně být stále uvnitř. Přivolá tedy na místo technika-vyšetřovatele, který provede technickou prohlídku.

Po provedení prohlídky objektu technik zaznamená, že je na zdi mimo jiné IoT termostat bez řídicího panelu a od majitele se dozví, že termostat je řízen aplikací v jeho telefonu a v budově se jeho pomocí udržuje konstantní teplota. Aplikace ovšem umí jen nastavovat parametry vytápěcího cyklu, ostatní údaje, jako například

změna teploty za posledních deset dní, jsou v termostatu a dostat se k nim dokáže jen technik řešící případné závady na zařízení.

Přitom data z termostatu mohou ukazovat na zvýšenou míru otevření vytápěcích ventilů, což by značilo narušení tepelné izolace objektu v důsledku právě zjištěného rozbití okna. Jinými slovy, pokud se je podaří získat, je možné odhadnout před jakou dobou k tomu došlo. Díky údajům z termostatu tedy bude dále možné zúžit časový okruh dalších zájmových skutečností z deseti dní na desítky hodin.

2.4.2 Scénář pro skupinu S – SCADA a průmyslové systémy

Jde o velmi širokou skupinu zařízení, která zahrnuje systémy monitorování průmyslových provozů, letišť, věznic a dalších zařízení. Do skupiny S jsou dále zařazeny systémy pro korporátní účely, včetně medicinských systémů, systémů pro ostrahu a systémů pro chytrá vozidla.

Právě poslední skupinu využijeme pro účely této práce. A to v podobě aktuálně vznikající infrastruktury pro systém inteligentního řízení dopravy C-ITS. Například v Brně nyní probíhá pilotní běh tohoto projektu. V jeho rámci má po roce 2023 dojít v Evropě k vytvoření IoT infrastruktury, která bude spojovat vozidla, prvky dopravní infrastruktury a mapové podklady města pro řízení semaforové signalizace, evidenci vjezdu do označených zón („modré zóny“), řízení hustoty provozu a další. Jednotka C-ITS v sobě uchovává údaje o pohybu vozidla a má unikátní identifikační číslo, které se hlásí okolním C-ITS jednotkám infrastruktury.

Scénář by pak mohl zahrnovat využití C-ITS jednotky pro trasování zájmového vozidla. Může přitom jít například o odstavené vozidlo, u kterého potřebujeme zjistit jeho předchozí trasu, protože se domníváme, že jde o únikové vozidlo po přepadení nebo vozidlo, ve kterém se nacházela pohřešovaná osoba. Potřebujeme tedy zjistit ID C-ITS jednotky, které potom můžeme porovnat postupně s C-ITS jednotkami v okolí, a získat tak pravděpodobnou poslední trasu vozidla před jeho zajištěním.

2.4.3 Scénář pro skupinu E – enterprise systémy a infrastruktura

Jde o skupinu, která slouží k zajišťování samotné konektivity a připojení do sítě. Jelikož jednou z podmínek IoT zařízení, která se objevuje v odborné literatuře, bývá, že jde o zařízení, která by existovala i bez internetu, mohlo by se zdát, že do této skupiny „skutečná“ IoT zařízení nepatří.

Budeme ovšem vycházet z Blinkowského klasifikace a považovat zařízení třídy E rovněž za součást IoT. Rozhodujícím faktem v tomto případě je, že právě infrastrukturní prvky často umožňují komunikaci mezi typickými IoT connected zařízeními a vnějším internetovým prostředím a z hlediska zajišťování digitálních stop tedy mohou poskytovat unikátní údaje například o zařízeních připojených v určitou chvíli nebo o komunikaci v uplynulé době. Tyto údaje mohou nahradit přímo logování určitého IoT prvku, který by sám o sobě nedisponoval vhodným nástrojem pro zjištění, že nebo jak k němu bylo přistupováno.

Pro účely analýzy zařízení ve skupině E se tedy podíváme na takovýto kombinovaný scénář, například na IoT Wi-Fi kameru, která přenáší svůj záznam na cloud, ale která vykazuje podivné chování – například byla v době vloupání do objektu natočena „do zdi“, neaktivní, nebo byl záznam jiným způsobem znehodnocen a přímo z kamery nelze získat odpovídající logy nebo jiné relevantní údaje, které by její chování mohly vysvětlit.

2.4.4 Scénář pro skupinu A – různá zařízení chytré kanceláře

U této skupiny jde o zařízení, která rovněž tradičně mají nějakou formu konektivity, podobně jako zařízení ve skupině M nebo E, ale zároveň jsou nově připojována k internetové síti, aby se posílily jejich možnosti a funkce.

V návaznosti na naši podmínku, že samotný útok proti daným zařízením nepovažujeme za vhodný scénář, stojíme před úkolem definovat takový trestný čin, který je proveditelný prostřednictvím tiskárny. V případě IoT zařízení, která jsou napojena na internet nebo minimálně centrální tiskový server, se ale nabízí následující – uvažme, že ovládací jednotka, která zpracovává jednotlivé tiskové úlohy, byla napadena a její firmware modifikován tak, aby se kopie každého

dokumentu, zpracovávaného daným zařízením, odesílala ještě na útočníkův server. Jde tedy o trestný čin průmyslové špionáže a cílem zajišťování důkazních materiálů bude dokázat, že došlo k manipulaci s příslušným firmware a že dochází ke komunikaci s útočníkovým C&C strojem.

2.4.5 Scénář pro skupinu M – mobilní telefony, tablety a další přenosná zařízení

Jelikož mobilní telefony, tablety, notebooky a další výpočetní technika spadají do známých a dobře popsaných forenzních případů, zvolíme pro tuto skupinu jako reprezentativní zařízení chytré hodinky, tzv. „smartwatch“. Jde o IoT variantu klasických náramkových hodinek, které kromě času poskytují také možnost měření tepu včetně historie, dále přehled o poslední aktivitě, kterou oběť vykonávala, a některé modely obsahují také vestavěný čip GPS, který umožňuje přenést údaje o poloze přístroje do mobilního telefonu.

Nabízí se scénář, kdy hlídka při rutinní obchůzce nalezla oběť v šoku neschopnou interakce a potřebuje do příjezdu záchranné služby zjistit co nejvíc informací. Může tedy za tímto účelem zkusit oběť vytěžit a jako digitální důkaz stáhnout údaje z chytrých hodinek, na základě kterých získá základní informace o intenzitě, délce trvání a povaze útoku. Navíc získá možný přehled o místě, kde se mohl pohybovat pachatel, a to korelací údajů o míře stresu či fyzické aktivity a poloze uživatele hodinek.

Z technického hlediska dále rozlišujeme chytré hodinky do čtyř tříd. Hodinky s operačním systémem (Android/Tizen), autonomní nositelná zařízení, hodinky s chytrými funkcemi bez operačního systému a hodinky s krokoměrem, ale bez dalších chytrých funkcí. V této kategorii tedy budeme mít více technických metodik vzhledem k povaze zajišťovaného zařízení.

Jelikož je z popisu scénářů patrné, že některé kategorie se logicky dále dělí, zavedeme pro jemnější rozlišení techniky v jednotlivých kategoriích ještě podskupiny, ke kterým stáhneme jednotlivé konkrétní scénáře.

2.5 Obecná charakteristika zařízení skupiny H – domácí smart elektronika

V této kategorii se nacházejí zařízení, která je možné najít v běžné domácnosti a která řadíme do takzvané spotřební elektroniky. Z hlediska důkazního zajišťování zde nacházíme dva druhy zařízení. Těmi tradičnějšími jsou různé domácí routery, webkamery, dozorové kamery nebo třeba chytré spotřebiče jako IoT lednice, televize či meteostanice. Druhou skupinu tvoří inteligentní domovní instalace – termostaty, videozvonky a ústředny k nim, chytré zámky a obecně „chytré“ varianty zařízení, které jsou obvykle pevnou součástí domovní elektroinstalace.

2.5.1 Podskupina H1 – přenositelná domácí elektronika

2.5.1.1 Obecná charakteristika skupiny

Tato podskupina je poměrně rozsáhlá a obsahuje velkou část běžných zařízení, která mají chytré funkce. Typickým představitelem jsou chytré televize, dále například chytré lednice, chytré termostaty, inteligentní samočinné vysavače („Roomba“) a také síťové prvky, které zajišťují komunikaci mezi těmito zařízeními.

Společným definičním znakem zařízení v této podskupině je, že nejsou pevně konstrukčně spojená s prostředím, ve kterém se nacházejí, a tedy je možné je přenést či převézt do laboratoře na bližší prozkoumání. Zajištění digitálních důkazů lze u nich nechat až na laboratorní prostředí, ovšem pouze za předpokladu, že zajistíme kontinuální nebo téměř kontinuální napájení, aby nedošlo k odstranění dat z volatilních pamětí. Některá zařízení, například chytré vysavače, lze programovat dálkovým ovládáním a je dobré zajistit s nimi také toto ovládání, případně mohou mít napájecí doky, které je také žádoucí lokalizovat, případně zajistit.

2.5.1.2 Možný scénář zahrnující tuto podskupinu

Příkladem scénáře, v kterém může tato podskupina figurovat, je například bytová loupež. Některé inteligentní televize nebo domácí asistenti[5] totiž začínají zaznamenávat zvuk v místnosti již při překročení určité hladiny. To znamená, že pokud došlo k jejich aktivaci, i když nebyl vykonán žádný povel, můžeme z časové značky této aktivace odhadnout, kdy naposledy se v bytě pohybovala nějaká osoba, což může být vodítkem ke zjištění času, kdy došlo k události, kvůli které majitel upozornil policii, že je něco v nepořádku. Někteří tito asistenti umí také alarmovat policii nebo jednotky IZS. Zmíněná varianta je ovšem nad rámec této diplomové práce.

2.5.2 Podskupina H2 – nepřenositelná domácí elektronika

2.5.2.1 Obecná charakteristika podskupiny

Do této podskupiny řadíme prvky domovní elektroinstalace, které zároveň vykazují znaky inteligentní elektroniky. Obecně jde o taková zařízení, která jsou se stavebním objektem pevně spojená, a tedy je není možné bez porušení kabeláže nebo jiné části zařízení odnést. Může jít například o domovní videotelefon, který může a nemusí mít k sobě ještě ústřednu zaznamenávající video, pokud někdo zazvoní, dále třeba inteligentní domovní kamery, termostaty, nebo třeba inteligentní klimatizaci.

2.5.2.2 Možný scénář zahrnující tuto podskupinu

Viz předchozí scénář pro skupinu H zahrnující nutnost analýzy chytrého termostatu.

2.6 Obecná charakteristika zařízení skupiny S – zařízení výrobních podniků

V této podskupině najdeme v jistém slova smyslu opačná zařízení než ve skupině první. Jde o taková zařízení, která sbírají, vyhodnocují, reportují data a pracují s nimi

[5] Jde o řídicí prvky inteligentních bytových systémů obvykle umožňující hlasové ovládání, například systémy Amazon Echo, Apple Home, Google Alexa a podobné.

v průmyslovém nebo chráněném prostředí. Celkově jde tedy o širokou množinu systémů, které plní různé funkce od analytických přes řídicí až po informativní.

Jde o systémy podporující automatizaci ve výrobních a průmyslových procesech, systémy řízení přístupu, systémy pro automotive a přenosná zařízení monitorující stav ve výrobních nebo skladovacích prostorech.

2.6.1 Podskupina S1 – přenosná zařízení pro průmyslové prostředí

2.6.1.1 Obecná charakteristika podskupiny

Ruční přenosná zařízení umožňující přenos krátkých záznamů typu snímání hodnot z čidel, snímání čárových kódů, čtení identifikačních štítků nebo RFID čipů. Slouží k inventarizaci, logistice a jako rozhraní k senzorovým čidlům v některých typech výroby.

2.6.1.2 Možný scénář zahrnující tuto podskupinu

V tomto případě se jako nejpravděpodobnější jeví scénář nenápadné krádeže, kdy pomocí využití funkce daného zařízení pro změnu kódů může pachatel zaměnit například léky ve skladu lékárny a „odečíst“ z něj například opiáty jako běžná analgetika. Pro vyšetření takovéto činnosti budeme tedy muset zajistit a prozkoumat skener, který onu výměnu umožňoval.

2.6.2 SCADA, senzory a kontroléry průmyslové výroby

2.6.2.1 Obecná charakteristika podskupiny

Tato podskupina v sobě sdružuje zařízení podílející se nepřímo na řízení procesu výroby. Jde o systémy, jejichž softwarové komponenty se souhrnně někdy označují jako SCADA – Supervisory Control And Data Acquisition systémy. V hardware rovině potom můžeme hovořit o různých senzorech, analyzátorech, skenerech nebo dávkovačích materiálů, které řídí nebo korigují výrobní proces.

2.6.2.2 Možný scénář zahrnující tuto podskupinu

U všech těchto systémů se nabízí jednoduchý scénář v rámci konkurenčního boje. Pakliže některá část výroby začne náhodou ukazovat nadměrně vysokou zmetkovost,

kdy ovšem tyto zmetky budou úspěšně procházet kontrolou a nenajde se pro to příčina, může se majitel závodu domnívat, že jde právě o poruchu na kontrolních zařízeních. Cílem vyšetřovatele potom bude získat data ze zařízení a stanovit, zda šlo o náhodnou systémovou chybu, byť většího rozsahu, nebo o cílenou manipulaci s parametry systému tak, aby byly zmetkové výrobky pouštěny do oběhu.

2.6.3 Zařízení přístupových systémů a zabezpečovací techniky

2.6.3.1 Obecná charakteristika podskupiny

Jde o relativně úzkou podskupinu, která sdružuje různé inteligentní turnikety, dveřní zámky, trezory s elektronickým zámkem nebo samočinným ovládáním a další prvky průmyslových areálů, které souvisí s řízením přístupu či fyzickou bezpečností. Řadíme sem také průmyslové kamerové systémy, termokamery a další podobné prvky. Samozřejmě je zapotřebí přihlédnout k podmínkám pro smart systémy – z hlediska metodiky jsou relevantní jen ty systémy, které mají integraci s dalším informačním systémem. Terminál na karty s centrálním přístupovým serverem sem spadá, mechatronické panty s motorkem ovládané zámkem přímo ve dveřích jednoznačně ne.

2.6.3.2 Možný scénář zahrnující tuto podskupinu

Jednoduchým scénářem může být průmyslová špionáž, respektive krádež prototypu fyzicky umístěného v areálu firmy. Pokud nemáme jinou možnost, kterou by mohlo dojít ke vniknutí, a firma používá některý z těchto systémů, je logické zkusit získat a analyzovat data v něm, abychom získali například informaci o průchodu neznámé osoby nebo osoby, která je sice známá, ale přistupovala k systémům v atypickém čase – mimo svou pracovní dobu nebo třeba ve chvíli, kdy měla být na dovolené.

2.6.4 Zařízení pro automotive

2.6.4.1 Obecná charakteristika podskupiny

Jde o zařízení, která se instalují do moderních vozidel pro zajištění jejich konektivity. Již v současnosti se můžeme setkat s tím, že některá nákladní vozidla nebo vozidla hromadné dopravy poskytují tzv. telemetrii – údaje o své poloze, stavu pohonných

hmot nebo napájení, údaje o rychlosti a směru, kterým se pohybují, a další. Součástí těchto údajů může být celá řada provozně zajímavých informací.

Od roku 2023 by se okruh vozidel s telemetrií měl v podobě celoevropského projektu C-ITS rozšířit i na osobní vozidla. Jeho doplňkovým partnerem by měla být chytrá městská infrastruktura, reagující na telemetrické údaje vozidel, která se nazývá C-Roads. Pilotní projekty již probíhají v Brně a postupně by měly být rozšířeny do dalších měst v ČR.

2.6.4.2 Možný scénář zahrnující tuto podskupinu

Abychom se vyhnuli kolizi s podskupinou S3 – Zařízení zabezpečovací techniky, zaměříme se právě na projekt C-ITS. Scénář, který se nabízí, je poté scénářem navrženým výše jako reprezentativní ukázkou pro celou skupinu S a nebudeme jej tedy opakovat.

2.7 Obecná charakteristika zařízení skupiny E – infrastrukturní prvky

2.7.1 Obecná charakteristika skupiny

Jelikož tato skupina je částečně popsána v jiných metodikách a spadají do ní primárně prvky, které samy zajišťují komunikační prostředí, a tedy obvykle sdílí nepřenositelnost (vyjmutím z jejich prostředí vždy ztratíme část informací), přímou analyzovatelnost a další vlastnosti diktující metodická omezení při jejich analýze, nebudeme tuto skupinu dále dělit.

2.7.2 Možný scénář zahrnující tuto skupinu

Vzhledem k tomu, že zařízení typu router a switch se běžně vyskytují ve standardních sítích a nemají své offline předobrazy, nejde o IoT zařízení, a tedy jsou mimo rozsah této práce. Místo toho se zaměříme na zařízení, která mají i své offline varianty. V této kategorii se jednoznačně nabízí výše uvedené VoIP ústředny, budeme se tedy držet již navrženého scénáře, uvedeného v popisu celé skupiny.

2.8 Obecná charakteristika zařízení skupiny A – kancelářská technika

2.8.1 Zařízení s přímo přístupným ovládáním

2.8.1.1 Obecná charakteristika podskupiny

Do této podskupiny spadají zařízení, která přijímají, zpracovávají a reportují informace z určitých sítí, ale přitom mají vlastní přímé ovládací prvky. Jde nejčastěji o zařízení umožňující tisk nebo multifunkční zařízení pro zpracování tiskových, skenovacích a dalších úloh pro zacházení s papírovými dokumenty.

2.8.1.2 Možný scénář zahrnující tuto podskupinu

Jeden ze scénářů pro tuto podskupinu jsme rozebrali v části metodiky pro celou skupinu A výše.

2.8.2 Zařízení ovladatelná pouze prostřednictvím další techniky

2.8.2.1 Obecná charakteristika podskupiny

Jde o zařízení, k jejichž využití je předpokládána další technika. Tedy projektory, inteligentní zámky, rezervační systémy kanceláří nebo chytré jednotky řízení prostředí, jako například klimatizace nebo ventilační jednotky.

2.8.2.2 Možný scénář zahrnující tuto podskupinu

Nabízí se kombinované zneužití chytrého zámku kanceláře a rezervačního systému. Jelikož kancelář zamčená rezervačním systémem jde obvykle otevřít jednou zvenčí a pak již jen zevnitř do vyprchání rezervace, můžeme předpokládat, že se útočník mohl v místnosti schovat před započetím plánované schůzky, schůzku nahrát a po jejím skončení odejít. Zajímavá tak budou data ze zámku, která nám umožní zjistit, kolikrát byly dveře místnosti otevřeny během schůzky, případně nápadně dlouho po jejím konci, což může indikovat přítomnost nezvané osoby na schůzce.

2.8.3 Zařízení ovladatelná pomocí tokenů nebo osobních klíčů

2.8.3.1 Obecná charakteristika podskupiny

Jde o tisková zařízení, jídelní automaty, chytré kávovary a další zařízení využívající například systém SafeQ. Tato zařízení jsou propojena s různými systémy řízení identit. Je tedy možné jejich prostřednictvím například přístupový token okopírovat, a tím se dostat k přístupovým a identifikačním údajům libovolného zaměstnance. Tyto systémy bývají řízené centrální soustavou řídicích serverů, i když token, kterým se ovládají, může být víceúčelový, a přístupové údaje se kromě přístupu k tomuto systému mohou využívat také například k přístupu do budovy. Zdánlivě bezvýznamná krádež údajů z tiskového systému se pak může stát pretextem narušení fyzické bezpečnosti celého objektu.

2.8.3.2 Možný scénář zahrnující tuto podskupinu

Pro tuto podskupinu se nabízí výše popsaný scénář krádeže identity prostřednictvím odečtu údajů z tiskového serveru, případně zkombinovaný i s krádeží vybraného dokumentu nebo dokumentů, které daný zaměstnanec zpracovává. Díky této identitě a sérii zařízení vyžadujících identifikaci (kávovary, automaty s občerstvením a podobně) by také mělo být možné analýzou digitální stopy jednotlivce zjistit jeho pohyb po budově nebo budovách firmy, popřípadě vybočení ze zaběhlé denní rutiny.

2.9 Obecná charakteristika zařízení skupiny M – mobilní zařízení

Tato skupina je poměrně široká. Jde o skupinu zařízení pro oblast mobility – chytré hodinky, mobilní telefony, krokoměry a další sportovní a zdravotní pomůcky. V dnešní době jde o různorodou skupinu zařízení, ze které se postupně vývojem vyčlenily tři hlavní podskupiny – mobilní telefony, chytré hodinky a náramky a inteligentní zdravotnická technika. Poslední podskupinou se nebudeme v této práci zabývat, neboť práce s touto podskupinou zařízení vyžaduje odborné znalosti z oblasti medicíny na úrovni, kterou nelze obecně u techniků předpokládat.

2.9.1 Mobilní telefony

Tato podskupina patří mezi velmi běžnou techniku. Český statistický úřad ve své publikaci Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci – ev. číslo 062004-19 uvádí, že v roce 2019 mělo v nějaké podobě mobilní telefon 96,9 % obyvatelstva ve věkové skupině 16+, přičemž 70 % celkové populace uživatelů vlastnilo tzv. „smartphone“, tedy mobilní telefon s operačním systémem podporujícím běh aplikací třetích stran [11].

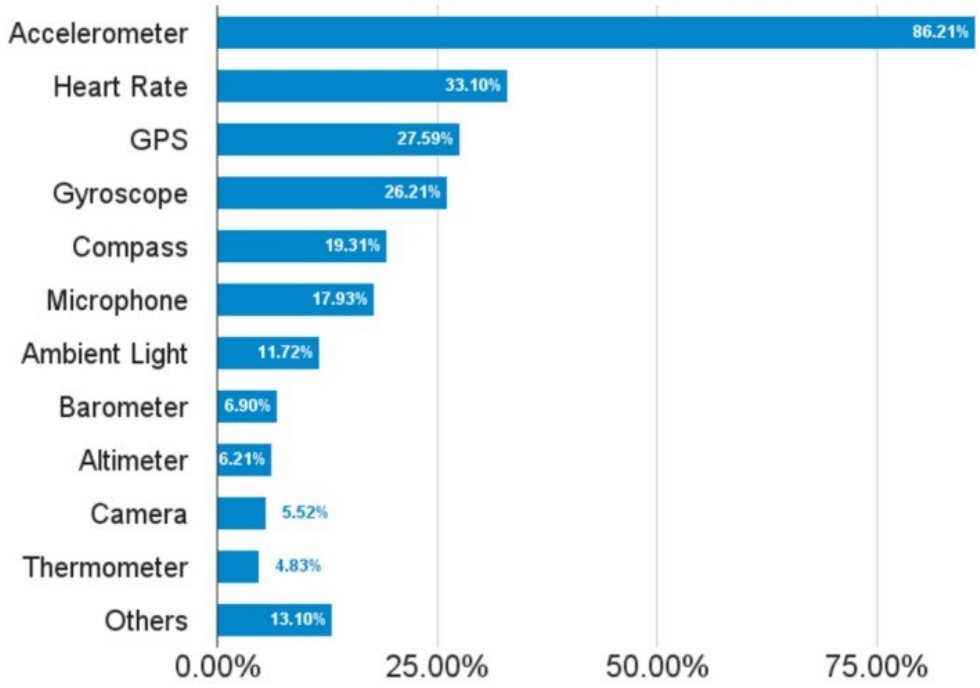
V důsledku této míry rozšíření je problematika forenzní analýzy mobilních telefonů poměrně dobře známou a metodicky zpracovanou oblastí. Mobilní telefony se také obvykle neuvádí jako případ IoT zařízení, ačkoliv naplňují všechny definiční znaky. Blinkowski et al., z jejichž článku vycházíme, je uvádí pouze pro přehlednost a jelikož jsou obsaženy ve zdrojových datech.

Z výše uvedených důvodů se této kategorii nebudeme v metodikách podrobně věnovat. Zájemci mohou využít například bakalářskou práci Ing. Vojtěcha Novotného, Ph.D.[6]

2.9.2 Chytré hodinky a náramky

Jiná situace je ovšem v oblasti chytrých náramků a hodinek. Ačkoliv zde také existují postupy komplexní forenzní analýzy, v práci tyto přístroje zahrneme z hlediska akvizice dat po příjezdu technika přímo v terénu. V některých případech, zejména pokud jsou tato zařízení spojena s čidly tepu, oxymetrem, či dalšími senzory, může totiž být rozdíl v datech získaných přímo v terénu a při následné laboratorní analýze, nebo zařízení dokonce nemusí vůbec být mimo terénní šetření dostupné. Procentuální výskyt senzorů obvyklých ve zařízeních je zachycen například v článku od autorů Arriba-Pérez a kol. [12] – zde v podobě grafu 1.

[6] NOVOTNÝ, Vojtěch. *Forenzní analýza mobilních zařízení s OS Android*. Č. Bud., 2013. Bakalářská práce (Bc.). JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH. Přírodovědecká fakulta.



Graf 1 – Senzory dostupné v nositelných zařízeních podle četnosti.

2.9.2.1 Obecná charakteristika podskupiny

Vzhledem k rozdílnému zastoupení senzorů v této podskupině navrhujeme pro praktické účely ještě rozdělení podskupiny na čtyři kategorie:

a. Zařízení typu „smartwatch“/„smartbracelet“ s minimem funkcí konektivity. Sem patří primárně zařízení, která sdružují jen krokoměr a hodinky. Typickým zástupcem jsou hodinky Garmin VivoMove v první generaci nebo Misfit Phase. V obou případech je jediným aktivním senzorem akcelerometr.

b. Zařízení s pokročilými senzory, ale bez GPS – jde o zařízení určená jako „fitnesstrackery“, která mají vybrané pokročilé funkce, ale nemají plnohodnotný operační systém nebo GPS senzor. Typickým zástupcem je například rodina chytrých náramků MiBand, chytré hodinky Garmin VivoMove HR a další. Akcelerometr u nich doplňuje například tepový senzor, paměť aktivit, nebo některé další senzory uvedené v tabulce 1.

c. Pokročilá zařízení s plnohodnotným operačním systémem. Jde o jednoduchá zařízení, která umožňují dvoucestnou live komunikaci s mobilním telefonem nebo jiným ovládacím zařízením, umožňují například psát SMS, odpovídat na

zprávy z messengerů nebo ovládat vybrané aplikace přímo z chytrých hodinek či náramku. Mají vlastní operační systém, například Tizen, Android nebo jejich ekvivalent, a lze do nich dohrávat aplikace třetích stran. Zástupců je zde mnoho, proto neuvádíme žádný typický model.

d. Specifická zařízení pro samostatný provoz. Tyto chytré hodinky a náramky se používají buď v kombinaci s dalšími zařízeními, nebo samostatně jako podpora různých aktivit. Například společnost Garmin umožňuje doplnit tento typ chytrých hodinek o další zařízení Garmin HRM, která poskytují dodatečné senzorické funkce a vyhodnocení dalších údajů o aktivitě uživatele, nebo doplněk Garmin Approach, který funguje jako senzor pro golfové hole nebo tenisové rakety a umožňuje přenášet získané údaje přímo do chytrých hodinek. Jako příklad hodinek uveďme Garmin Forerunner 945, Apple Watch ve verzi se samostatnou SIM kartou, zařízení TICWRIS a další. Ačkoliv většina z těchto zařízení má plnohodnotný operační systém, není to v tomto případě podmínkou. Definující součástí je přítomnost SIM karty, Wi-Fi modulu nebo jiné komunikační platformy pro přímý přístup k internetu a nezávislost na dalším zařízení typu mobilního telefonu.

2.9.2.2 Možný scénář zahrnující tuto podskupinu

Scénář je k dispozici výše jako reprezentativní pro celou skupinu zařízení M, neuvádíme proto nový scénář. Pro ilustraci tohoto scénáře v praktické části využijeme zařízení z kategorií a, b a c.

3 OBECNÝ METODICKÝ POSTUP ZAJIŠTĚNÍ DAT ZE ZAŘÍZENÍ

Nyní přikročíme ke stanovení obecné metodiky pro akvizici zařízení nebo dat na místě činu. Při tomto stanovování je nezbytné držet neustále na zřeteli požadavky stanovené na zajištění důkazů v kapitolách 1 a 2, tedy legální i technické limitace, které omezí celý proces. Těmito limitacemi jsou:

- zajištění autenticity dat;
- udržení maximálního množství důkazních materiálů, a to i jiné než datové povahy;
- jednoznačně zdokumentovaný proces zajištění zařízení;
- zdokumentovaný, případně opakovatelný postup získání dat z daného zařízení;
- argument korespondencí.

Argument korespondencí odpovídá tradiční korespondenční teorii pravdivosti a je postaven na předpokladu, že pravdivým je tvrzení (výrok) korespondující s materiální pravdou. Praktickou jistotu ohledně pravdivosti na základě uplatnění tohoto argumentu získáváme na základě skutkové informace (důkazu), který skutkové tvrzení přímo spojí s prokazovanou skutečností [1].

3.1 Obecné zásady a podmínky zajišťování

Při zajišťování objektu i samotných zařízení je dále nezbytné mít na paměti zásady, které doporučuje například ENISA ve své publikaci *Electronic evidence – a basic guide for First Responders*, případně jsou obsažené ve veřejně dostupném standardu *Standard Operating Procedures for the collection, analysis and presentation of electronic evidence* a dalších relevantních materiálech. Tyto zásady zde pro přehlednost nerekapitulujeme a budeme pro zjednodušení předpokládáme, že je s nimi technik obeznámen.

Jak je uvedeno také ve výše zmíněných publikacích, konkrétní postup se může lišit v závislosti na okolnostech vyšetřovaného případu, jako je povaha předpokládaného trestného činu, přítomnost a stav obětí, přítomnost svědků a celé řady dalších

okolností. Níže navržený a konzultovaný postup se tedy týká striktně ideálních případů bez komplikací, obdobně jako postupy agentury ENISA a další metodické manuály pro forenzní vyšetřovatele.

Z tohoto důvodu také z jednotlivých postupů vynecháváme v teoretické části místa, kde by měla být pořízena fotodokumentace. Ta může sloužit nejen jako doklad původního místa činu, ale také jako alternativní způsob zaznamenání informací z IoT zařízení formou jeho přirozené prezentace pro uživatele. Pokud v praktické části budeme hovořit o pořízení nebo využití fotografického dokladu či důkazu, obdobně pro jednoduchost předpokládejme, že jsme schopni zajistit a doložit autenticitu fotografie například metodami popsanými v kapitole 2.1 této práce.

3.2 Vlastní metodické postupy

Práce na samotném zajištění musí začít už příchodem hlídky na místo činu před rozhodnutím, že zavolá odpovědného technika.

Pokud je to možné, zeptá se ohlašovatele, oběti, případně majitele objektu, jaká inteligentní zařízení se na místě mohou nacházet a jakým způsobem jsou případně připojena. Soupisku předá jako výchozí bod technikům, jakmile se tito na místo dostaví.

Následně technik přistoupí ke kybernetickému ohledání místa. Pomocí vhodného nástroje zjistí, jestli jsou v okolí detekovatelné bezdrátové sítě, případně zařízení se zapnutou komunikací prostřednictvím technologie Bluetooth.

Celý proces samozřejmě může – případně by mělo – doprovázet získávání odpovídajícího materiálu do protokolu. Nejen v podobě soupisek, ale také jako snímky obrazovky technologických zařízení, případně jako fotky dokladující způsob prezentace dat přímo v zařízení.

Využití fotografické dokumentace se ve všech případech může použít nejen jako součást dokladování fyzického stavu zájmových systémů, ale také přímo jako alternativa k pořizování kopie získávaných dat. Vyfocení panelu, displeje nebo jiného prvku, který data zobrazuje, totiž může sloužit jako důkaz o stavu tohoto prvku, ale

také celého systému. V teoretické části dále nebudeme tento aspekt zmiňovat, avšak návrhy míst na pořízení fotografií se objeví v praktické části a ve výstupním manuálu.

Dále se postup v přípravné fázi bude lišit podle povahy zásahu. Jiný bude u vozidel, u objektů a u jednotlivých osob.

3.2.1 Postup zjištění kybernetického prostoru objektu

Pro první krok postačí vzít mobilní telefon se zapnutým vyhledáváním sítí a zjistit, zda je v okolí nějaká zjistitelná bezdrátová síť, případně provést skenování pomocí aplikace WiFi Analyser[7], která umí zobrazit veškeré sítě a jejich vlastnosti. Zjištěné údaje z aplikace poté technik uloží do svého zařízení. Následně je zapotřebí toto zopakovat pro zjištění zařízení využívajících technologii Bluetooth.

Tímto postupem získáme alespoň představu o stavu rádiového prostoru na daném místě. Z toho můžeme odvodit, jaká je šance, že na místě vůbec existují nějaká IoT zařízení, zaznamenávající údaje v reálném čase. Zajímají nás zejména sítě se skrytým SSID, nebo sítě s atypickým nastavením, případně výskyt více sítí, vysílaných ze stejné vzdálenosti. Tyto všechny indikátory mohou ukazovat na dedikovanou IoT síť, oddělenou od „Běžné“ bezdrátové sítě pro zařízení pro obsluhu lidmi.

Zjištěné informace opět ověříme proti očekávaným zařízením tak, že se zeptáme ohlašovatele, zda seznam zařízení a sítí, který jsme sestavili, odpovídá jeho informacím o sítích a zařízeních, které bylo v objektu možné očekávat. Tento seznam následně uložíme jako důkazní materiál.

Pokud seznáme, že na místě skutečně je bezdrátová síť, zařízení, které komunikuje přes Bluetooth, nebo jiný zjistitelný prvek bezdrátové komunikace, začneme sledovat možná zařízení, která mohou mít aktivní chytré funkce. Každé zařízení, které může tuto definici naplňovat, patřičným způsobem zdokumentujeme, tedy pořídíme jeho fotku jako důkazní materiál ukazující, kde se nacházelo.

[7] Aplikace je ke dni odevzdání práce dostupná v obchodě Google Play, verze pro iOS neexistuje kvůli omezení tohoto operačního systému.

Dále technik u zařízení, u kterých ví, že jde o připojená zařízení, provede zajištění biologických stop a daktyloskopickou analýzu, aby se tyto důkazy zachovaly i při následné manipulaci za účelem získání digitálního důkazu.

Pakliže je technik schopen se na místě připojit na stejnou bezdrátovou síť, na které se nacházejí zajišťovaná zařízení, může tak v tomto kroku učinit a vhodným nástrojem se pokusit zjistit IP adresy a povahu připojených zařízení, například pomocí nástroje Wireless Network Watcher[8] nebo jeho ekvivalentu.

Protokol o sítích a provozu na nich následně uloží jako první digitální důkaz.

3.2.2 Postup pro zajištění kybernetického prostoru vozidel a okolí

V tomto případě můžeme za současných podmínek předpokládat, že součástí vozidla bude přinejlepším systém GPS. Tento systém často zahrnuje obvyklé trasy, případně může ukazovat aktuální trasu, kterou vozidlo urazilo před zastavením nebo jeho nalezením.

Zajímavější je ovšem případná přítomnost několika dalších systémů. Bluetooth sken může odhalit, zda vozidlo nemá například Bluetooth jednotku připojenou k zrcátku, případně integrovanou v palubní desce, a dále může být vozidlo vybaveno prvkem systému ITS. Jde o systém propojených IoT prvků v dopravě, který je v současné době testován v několika zemích EU včetně České republiky a od roku 2023 má tvořit povinnou součást výbavy všech vozidel.

Tento systém je součástí implementace systému ITS, jak jej definuje ve svých standardech ETSI, tedy Evropský ústav pro telekomunikační normy. Systém využívá komunikaci v průmyslové části pásma 5 GHz, tedy stejné části pásma, jako například Wi-Fi sítě. Česká implementace využívá frekvenci 5,9 GHz [13]. Pro adresaci používá kombinaci IPv6 protokolu a pseudonymizace konkrétních zařízení. Celý systém předpokládá několik částí. První, označovaná jako C-Roads, je infrastrukturní

[8] http://www.nirsoft.net/utils/wireless_network_watcher.html

část projektu, která poskytuje infrastrukturní a další propojení, aby mohla inteligentní vozidla získávat informace ze svého okolí.

Druhá část projektu je v Česku označovaná jako C-ITS a týká se samotných vozidel. Jde o zařízení umístěné ve vozidle nebo propojené přímo s palubním počítačem vozidla, které umožňuje interakci s infrastrukturou C-Roads. Jednotlivé systémy C-Roads se dále dělí na:

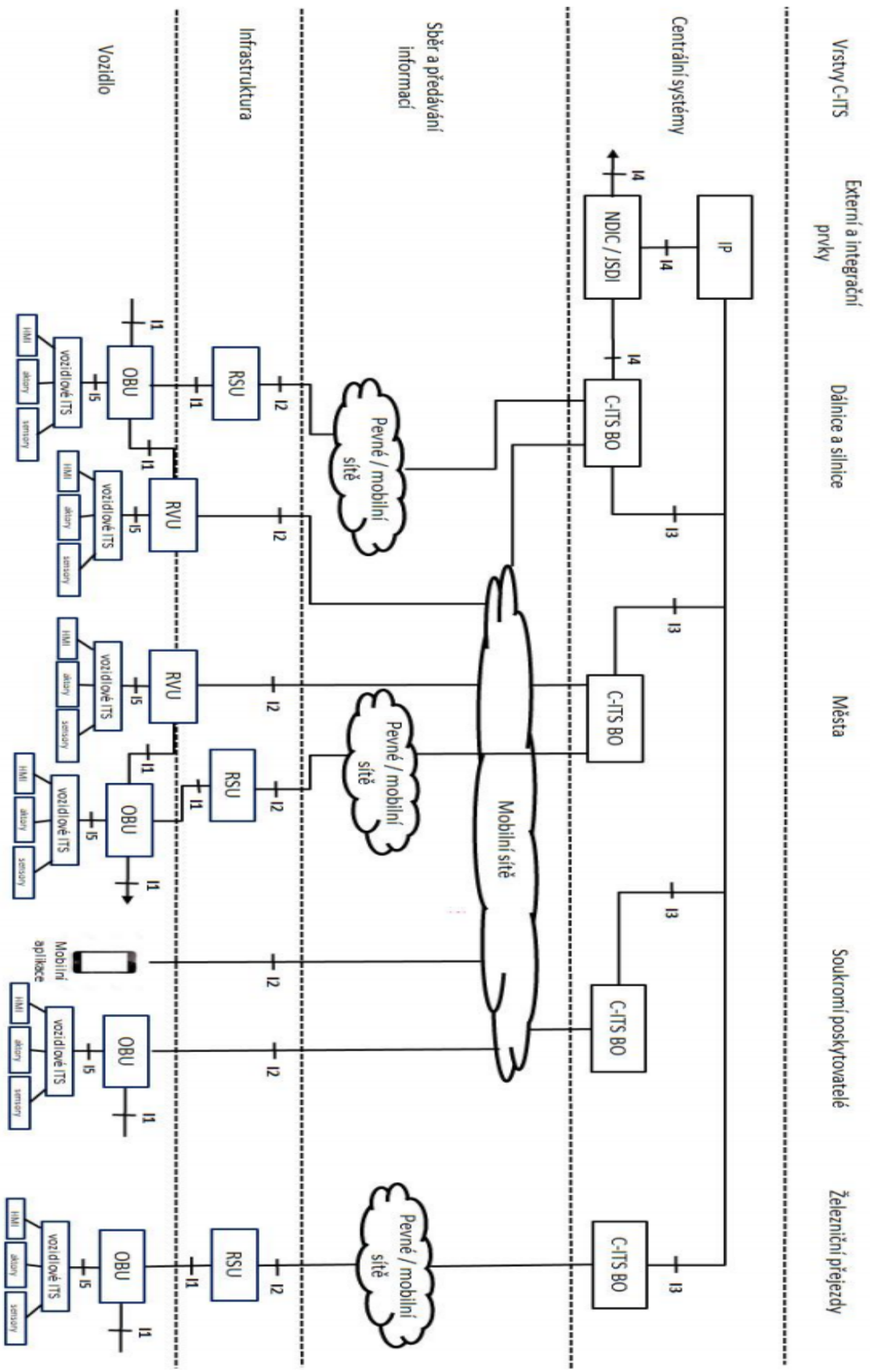
- centrální systémy založené na prvcích umožňujících příjem, zpracování, generování a distribuci ITS zpráv;
- systémy sběru dat a předávání informací, jako jsou LTE sítě či metalické kabely spojující jednotlivé infrastrukturní prvky;
- infrastrukturu, ve smyslu RSU jednotek poskytujících a přebírajících data o jednotlivých vozidlech či situaci na nebezpečných uzlech dopravní sítě;
- vozidla, tedy nosiče C-ITS jednotek, které poskytují telemetrická, lokalizační a provozní data do centrální části C-ITS systému.

Tento systém se tedy skládá z několika různých propojených prvků. Obecná architektura systému C-ITS je vyobrazena na obrázku 1 na následující stránce.

V praxi to znamená, že pokud máme k dispozici C-ITS jednotku, ze které jsme schopní získat její údaje, můžeme oslovit centrální systém, respektive takzvané pracoviště back-office, které by nám mělo být schopno poskytnout informace o pohybu této jednotky v určitém časovém úseku zpětně.

Hlavním úkolem technika u zajištění vozidla tedy bude pomocí Wi-Fi skeneru ověřit, že C-ITS jednotka je aktivní a stále vysílá.

Pokud zůstala aktivní, musí z ní vyčíst identifikační údaje a dále kontaktovat oblastní pracoviště back-office, aby pohyb vozidla vytrasovalo, případně získat telemetrické údaje v jednotce C-ITS uložené.



Obrázek 1 – Schéma C-Roads systému

3.2.3 Postup pro zajištění digitálních stop u osob

Pakliže se digitální stopa získatelná z IoT zařízení nachází u osoby v podobě dat uložených v nositelné technice, jsou dvě možnosti. Pokud nám je osoba schopná techniku sama vydat, můžeme toho využít a data si stáhnout do technického telefonu nebo jiného odpovídajícího zařízení.

V případě, že osoba není spolupráce schopna, třeba proto, že to neumožňuje její fyzický nebo duševní stav, musíme opatrně zkusit data ze zařízení dostat sami. Přitom je důležité, pokud by prodleva nezpůsobila ohrožení života, zařízení z osoby nesnímat, ale pokusit se jej odemknout a spárovat s technickým telefonem již na těle osoby. Nositelnou techniku nesnímáme, protože některá zařízení se po sejmutí zamknou a vyžadují speciální akci nebo kód na opětovné odemčení a dále také proto, že některá zařízení mohou při pokusu o spárování s novým zařízením mimo kontakt s tělem původního majitele data vymazat jako součást převodu do nového vlastnictví.

Tomuto scénáři musíme každopádně předejít, proto je-li to možné, párujeme zařízení ve chvíli, kdy je ještě na těle osoby, jejíž data potřebujeme získat. Zjistíme tedy, zda zařízení detekujeme na svém Bluetooth připojení, a pokud ano a osoba je schopna komunikovat, zeptáme se jí, jakou aplikaci je vhodné k párování použít. Pokud osoba nespolupracuje nebo není-li vzhledem ke svému stavu schopna podat relevantní informace, postupujeme podle odpovídající metodiky pro jednotlivé podskupiny zařízení.

Tímto je společná část pro všechna zařízení dokončena. Dále musíme uvažovat už jednotlivé způsoby pro odpovídající třídu, do které dané zjištěné zařízení spadá. Každá třída totiž bude mít specifický postup, kterým je nutné zařízení zkoumat, abychom neznehodnotili digitální důkazy, které v něm jsou uloženy.

4 METODIKY ZAJIŠTĚNÍ JEDNOTLIVÝCH SKUPIN ZAŘÍZENÍ

V následující části popíšeme jednotlivé výše definované skupiny zařízení a zkusíme stanovit obecné metodické principy pro jejich zajištění.

4.1 Metodika zajištění zařízení skupiny H

Skupina H obsahuje IoT zařízení, která většinou bývají připojena přes vhodnou Wi-Fi nebo ve výjimečných případech drátově. V případě bezdrátového připojení se bavíme o zařízeních, která je velmi často možné odnést do laboratoře a jejich zajištění provést tam. Abychom ovšem předešli ztrátě dat, je vhodné se k zařízení připojit ještě v terénu a stáhnout alespoň základní obraz dat již na místě.

4.1.1 Zařízení, která lze odnést (podskupina H1)

Z hlediska metodiky zpracování jde o snazší skupinu. Tato zařízení důkladně nafotíme, provedeme sběr daktyloskopických a dalších biologických stop a poté se pokusíme zjistit, zda se zařízení objevuje v seznamu bezdrátově připojených zařízení, který jsme získali jako součást technické obhlídky bezdrátového prostoru.

Pokud ano, zkusíme se připojit k Wi-Fi nebo nejbližšímu aktivnímu prvku a pomocí nástroje pro záchyt paketů v síti vyfiltrovat provoz na tomto zařízení. Tímto postupem, který navrhli a ověřili R. M. Alashawi a T. A. Alghamdi [14], ověříme, že je bezpečné zařízení zajistit, protože není zneužíváno žádným útočníkem, kterého by odpojení zařízení mohlo upozornit na problém.

Pokud zařízení není viditelné na připojené Wi-Fi, může být stále připojeno tzv. PoE technologií nebo jiným způsobem, který spojuje datový a napájecí tok, případně pomocí jiné bezdrátové sítě (GSM, LTE, 5G). V takovém případě musíme provést ekvivalent obhlídky popsané výše, avšak toto provedení bude složitější. V případě, že to umožňuje infrastruktura, na kterou je zařízení napojeno, můžeme provést odposlech napojením aktivního prvku do sítě. Toto je běžné například právě u PoE zařízení, která podle specifikace mají zvládnout krátkodobé odpojení bez změny vlastností. Můžeme tedy jako odposlechové zařízení využít vlastní počítač zapojený fyzicky do stejné sítě, například pomocí nástroje WireShark.

Nejsložitější případ je u zařízení řízených datovou SIM kartou. Takovýto modul je nejsnazší odposlechnout tím, že v jeho okolí vytvoříme fiktivní základovou stanici, která je ve skutečnosti v naší plné režii a odposlechneme provoz na ní. Podrobný postup, jak tohoto cíle dosáhnout s vynaložením minimálních prostředků, nabízí třeba Rijsbergen [15], přičemž tento postup lze využít univerzálně pro veškerá připojení až po generaci LTE.

Díky tomuto odposlechu lze zjistit, zda má zařízení vlastní paměť, nebo komunikuje s některou IP adresou pro cloudové úložiště. Pokud ano, uložíme capture soubor s těmito údaji a poznamenáme toto zjištění před odpojením a demontáží zařízení, protože je možné, že odpojením zařízení, a tedy přerušením komunikace s tímto serverem dojde k vymazání komunikačního nastavení, v důsledku čehož se zařízení nemusí v laboratoři pokusit se serverem znovu spojit.

V tuto chvíli můžeme dále fyzicky pokračovat v zajištění samotného zařízení. Odpojíme jej od zdroje napájení a vložíme do elektrostatického sáčku, odpovídajícím způsobem zapečetíme a připravíme na převoz do laboratoře.

4.1.2 Zařízení vestavěná nebo jinak nepřenosná (podskupina H2)

V tomto případě je situace mírně složitější proto, že nemusí být v první chvíli patrné, jakým způsobem je zařízení připojeno, a také proto, že nemůžeme analýzu dokončit v laboratoři, ale musíme ji celou provést na místě.

Neuvažujeme přitom zařízení nepřenositelná například z důvodu objemu nebo váhy, ale hlavně ta, která jsou pevně spojena s podkladem nebo instalací a jejichž odpojení by vyžadovalo zásah do elektroinstalace, případně dalších částí domovních rozvodů, nebo u kterých nemáme jistotu obnovitelnosti funkce v případě odpojení.

Patří sem relativně málo zařízení, například inteligentní termostaty, zabezpečovací systémy, výjimečně sem můžeme řadit také chytré zámky, žaluzie a další inteligentní prvky domovní instalace.

U této skupiny si ovšem musíme uvědomit, že ne každý elektrifikovaný prvek zároveň naplňuje definici IoT. Zajímají nás tedy primárně takové prvky, které jsme v rámci ohledání bezdrátového prostoru určili jako potenciální nositele dat nebo

u kterých vidíme takový způsob připojení, u kterého je pravděpodobné, že jsou přenášena i data (Cat10 kabel, optické vlákno atd.).

Problém může nastat v případě KNX instalací, které přenášejí data – včetně senzorických – prostřednictvím běžné elektrické kabeláže. Z hlediska zajišťování dat můžeme tyto instalace rozdělit do dvou tříd: autonomní instalace a instalace typu Smart Home řízené pomocí chytrého asistenta. V druhém případě jsou data zpracovávána a uchovávána u provozovatele cloudové infrastruktury, na kterou je napojen autonomní asistent. Problém nastává u systému Apple Home, který nevyžaduje nezbytně použití cloudové infrastruktury, ale je možné ho provozovat s využitím úložišť lokálních zařízení typu iPad/iPhone. V takovém případě musíme zajistit příslušné ovládací zařízení. V něm totiž budou uložena nutná data pro identifikaci a analýzu prvků domovního systému.

Součástí zajištění na místě tedy musí být rozpoznání, s jakým cloudovým účtem je propojen příslušný systém, případně zajištění ovládacího prvku smart home instalace. Tam, kde je prvkem vlastní řadič (KNX instalace nebo smart home bezdrátové instalace například od firem Home Connect, Honeywell a dalších), zkusíme zjistit, zda má řadič k dispozici historii údajů, a pokud ano, nafotíme záznamy v něm – data z řadiče není bez poškození možné přímo stáhnout. Alternativně můžeme zkusit metodu bezdrátového odposlechu, uplatněnou ve skupině H1.

V případě chytrých domů s centrálním ovládacím prvkem v podobě počítače Amazon Alexa nebo Google Echo musíme ideálně na místě zjistit, kdo je připojeným uživatelem.

Další zajištění a analýza může postupovat jen se znalostí účtu připojeného k těmto zařízením a s přístupem k tomuto účtu, který poskytne jeho majitel. Postup analýzy dat z těchto systémů je nad možnosti této práce a zpracovává jej například Chung [16].

U autonomních instalací je situace těžší, nicméně stále zde obvykle existuje centrální jednotka fungující jako řídicí prvek. Většinou jde o prvek v podobě buď chytré bezpečnostní stanice (instalace Jablotron SmartHome či obdobné), nebo v podobě

chytré jednotky řízení teploty, tzv. „inteligentního termostatu“ (instalace ecobee, Nest, Honeywell). Rovněž v tomto případě se k datům z celé jednotky dostaneme nejsnáze tak, že požádáme majitele o přístup k ovládacímu účtu. Všechna tato řešení jsou totiž obvykle propojena přes cloudové účty za účelem umožnění IoT funkcionalit. Ověření, zda je termostat v budově inteligentní, provedeme nejsnáze obhlídkou Wi-Fi prostoru (pro dálkově řízené termostaty), případně můžeme použít přímo obhlídku vyhrazeného pásma pro IoT zařízení s protokolem ZigBee s využitím některého z přijímačů schopného komunikovat v tomto pásmu. Návody a popis vysílačů například v článku How to sniff Zigbee traffic[9].

4.2 Metodika zajištění zařízení skupiny S

Základní principy zajištění zařízení v podskupinách u skupiny S se příliš neliší od zajišťování zařízení v předchozí skupině. Hlavními definičními kategoriemi zůstávají podskupiny „zařízení, která lze odnést“ a „zařízení, která odnést nelze“. Ta druhá se ovšem dále dělí na dvě podskupiny – SCADA systémy, tedy systémy řízení výroby, a systémy řízení přístupu. Navíc zde přibývá nová skupina a sice skupina S4 – zařízení pro automotive s nejvýznamnějším zástupcem v podobě systému C-ITS.

4.2.1 Zařízení, která lze odnést (podskupina S1)

Začátek postupu bude stejný, jako u podskupiny H1. Jakmile zařízení fyzicky najdeme a verifikujeme, že je připojeno, pokusíme se odposlechovým softwarem získat jeho provozní údaje, abychom ověřili, zda komunikuje s nějakou serverovou infrastrukturou, nebo ne.

V případě IoT zařízení v podnikovém prostředí zde ovšem může být jedna odchylka, protože podnikové prostředí může mít vlastní uzavřenou síť, která poskytuje dostatečnou část infrastruktury, aby zařízení nemuselo přímo komunikovat s cloudem.

[9] https://www.zigbee2mqtt.io/how_tos/how_to_sniff_zigbee_traffic.html – zobrazeno 20. 2. 2021

Poznáme to tak, že při odposlechu provozu na zařízení nebudou vůbec, nebo téměř vůbec přítomna spojení mimo chráněné rozsahy (10.0.0.0/8, 172.16.0.0/12 nebo 192.168.0.0/16, definované podle RFC-1918). Pokud zjistíme takovýto fakt, je nezbytné uvažovat, že zařízení nemusí samo o sobě obsahovat dostatek dat, případně neobsahuje žádná data, a místo toho jsou data k dispozici na centrálním prvku, jehož adresa se v odposlechu objevuje.

V takovém případě ztrácí koncové zařízení z hlediska digitálního důkazu smysl a je mnohem efektivnější přikročit k zajištění celého serveru jako úložiště, které by mělo obsahovat komunikační historii a další části digitálního důkazu.

Pokud zajištěné zařízení komunikuje přímo s veřejným cloudem nebo odpovídající infrastrukturou, pokračujeme, jako kdyby šlo o zařízení podskupiny H1.

4.2.2 SCADA, senzory a kontroléry pro výrobu (podskupina S2)

Společným znakem těchto kontrolérů je, že pokud nejsou přímo napojeny na logmanagement infrastrukturu, neukládají svoje data do žádných dalších úložišť. Takovéto ukládání totiž není žádoucí vzhledem k objemu a vysoké volatilitě dat.

Přesto existuje několik metod, jak data z těchto zařízení, v anglické literatuře souhrnně označovaných jako ICS[10], forenzně čistým postupem získat.

Vliet et al. [17] v takovém případě upozorňují, že nejsnazším místem, kde získat údaje o proběhlém problému, by měl být dozorový systém sítě, například IDS/IPS podniku. Data v průmyslových sítích se totiž velice rychle mění ve smyslu specifických informací, nemění se ovšem jejich toky.

Tuto informaci musíme mít na paměti, pokud budeme provádět datovou akvizici. Některé systémy monitorování síťového provozu totiž umí „nahlédnout pod pokličku“ SCADA protokolů a v případě potřeby vyčíst i obsah přenášených zpráv. Pokud tedy zjistíme, že potřebujeme vědět, kdy a jaká data byla v rámci těchto přenosů zasílána, je nejsnazší spojit se s příslušným podnikovým úsekem a vyžádat

[10] ICS – Industrial Control Systems, doslova systémy řízení průmyslu.

si přístup k dozorové a monitorovací konzoli, která v ideálním případě bude obsahovat údaje ze sondy či IDS/IPS.

Dále je nutné uvážit, zda jde o analýzu živého, běžícího systému, nebo zda získáváme důkazy tzv. „post-mortem“, tedy ze systému, který byl zasažen havárií, například explozí. V druhém případě ovšem systém již pravděpodobně ztratil svoji IoT povahu a forenzní akvizice digitálních důkazů v něm je nad možnosti této práce.

Pokud ovšem jde o běžící systém, můžeme pro jeho analýzu využít vícero metod. Kromě využití již zmíněného systému detekce síťových anomálií, můžeme využít data nasbíraná v kontrolních jednotkách.

Jde o počítače, do kterých údaje z ICS vstupují. Ty mají v praxi více podob. Může jít o klasické stolní počítače nebo jejich zabudované ekvivalenty, různé řídicí či velicí místnosti nebo přenosné jednotky.

Postup pak vychází z kombinace zjištění na místě a získání dat z těchto řídicích jednotek. Tato data mohou být k dispozici i v případě, že provádíme analýzu post-mortem.

Každopádně zařízení a snímače, které objevíme na zkoumaném místě, musíme zdokumentovat jak po fyzické stránce, tak také podle způsobu připojení. Systémy s některým bezdrátovým připojením jsou totiž náchylnější k výpadkům komunikace, případně jejímu ovlivnění ve srovnání se systémy s připojením drátovým.

V systémech s bezdrátovým připojením může být také zajímavější jeho výpadek. Bezdrátové systémy mají obecně vyšší elektromagnetickou susceptibilitu a dochází u nich častěji k rušení. Ačkoliv v literatuře [17] najdeme návrhy, jak zvýšit imunitu IoT systémů, stále jde o poměrně citlivé součásti.

Toho lze využít, protože elektromagnetické rušení může generovat například požár, výbuch nebo jiný podobný potenciálně zajímavý zdroj. Ve chvíli získávání dat z kontrolních systémů musí tedy technik myslet i na tento fakt a zaznamenat, pokud možno, i prázdná místa, hlášení poruch a další údaje ze systému, které zdánlivě nenesou informaci.

Zvláštní kapitolou jsou v tomto ohledu chybová hlášení systému. Ta nelze při zajišťování opomenout, protože i z nich lze vytěžit data objasňující, co se v zájmové době stalo. Což je další důvod, proč data z této skupiny musí být získávána prostřednictvím externích zařízení, jako jsou monitory síťového provozu nebo alespoň cílové servery.

K zajištění vlastního zařízení bychom měli přistoupit tedy pouze v případech, kdy:

a) zařízení bylo zničeno či značně poškozeno, a kromě digitálního důkazu může obsahovat i důkaz fyzický;

b) digitální důkaz může být přítomný ve chvíli, kdy nefungoval / nebyl dostupný datový kolektor a zařízení má vnitřní paměť.

Ve všech ostatních případech pouze zjišťujeme identifikátor zařízení a zajišťujeme data ze sběrného bodu nebo nejbližšího počítače, který je může obsahovat. Fyzickým důkazem je potom technický disk, na který logy stáhneme a který patřičným způsobem zajistíme.

4.2.3 Zařízení přístupových systémů a zabezpečovací techniky (podskupina S3)

Tato zařízení mají velmi mnoho charakteristik podobných se skupinami H2 a S2. Nejsou přenosná, jsou pevnou součástí instalace, kde se nachází, a v průmyslových podnicích mají primárně bezpečnostní a regulační funkci.

Oproti zařízením v podskupině S2 ovšem mají jinou primární funkci. Jejich cílem není kontrolovat či ovlivňovat výrobní či provozní záležitosti podniku, ale řídit pohyb osob, vozidel nebo aktiv v něm. U zajištění digitálních důkazů v této skupině musíme ovšem rozlišit, kdy jde o IoT zařízení a kdy nikoliv. Brána, kterou na dálku otevírá strážný ze svého působiště, může být bezdrátová, ale není IoT, protože neplní senzorické funkce. Brána, která se otevírá přiblížením odpovídajícího vozidla nebo kódem z něj, už ale IoT je, protože aktivně reaguje na vstup zvenku.

V tomto kontextu si tedy musíme uvědomit, že aby tato zařízení fungovala, je zapotřebí určitý komunikační protokol. Ten může a nemusí být stavový a může a nemusí ukládat přenosová data. V případě nestavového protokolu bez archivace dat

(pouze přijímá zprávu a na jejím základě vykonává příslušný pokyn) může forenzní analýza stále být zajímavá například z hlediska zjištění, zda nedošlo k narušení firmware daného zařízení a zda nebyly pozměněny řídicí toky zpráv. Takovou analýzu ovšem lépe provedeme v laboratoři.

U zařízení, která sice mají stavový protokol, ale nearchivují žádným způsobem provozní údaje, můžeme na místě provést kontrolu protokolu pomocí ověření, že zařízení správně, včas a očekávaným způsobem reaguje na zprávy, které má přijímat. Jde o využití metody vyšetřovacího pokusu podle § 104c zákona 141/1996 Sb., trestní řád, v platném znění. Z hlediska digitálního důkazu nám to ovšem poví jen část a zajištění zařízení pro účely analýzy firmware je také v tomto případě nevyhnutelné.

Jiná situace je u zbývajících dvou kombinací, tedy u zařízení, která využívají bezstavový protokol, ale jednotlivé zprávy logují, a pak u zařízení, která využívají stavový protokol a zároveň logují komunikaci. Zde totiž před přistoupením k analýze samotného zařízení musíme ještě zajistit právě tyto logy.

Vytěžení logů by mělo proběhnout, pokud možno, přímo na místě, protože teprve na základě zjištění z nich (neobvyklý příkaz, neobvyklá kombinace času a příkazu, …) lze stanovit další postup. Tím je buď nutnost zajistit samotné IoT zařízení, pokud uvidíme, že se nechovalo předvídatelně v souladu s logem, nebo jeho ponechání na místě, pokud touto metodou vyloučíme jeho poruchu. V obou případech lze tento postup doplnit také výše popsaným experimentem, kterým ověříme, že se do logu správně zapisuje.

4.2.4 Zařízení pro automotive (podskupina S4)

Zajištění zařízení v této podskupině bude záležet zejména na způsobu jeho zapojení do celkové elektroinstalace vozu. U samostatně stojících zařízení, která jsou z vozidla pouze napájena, můžeme předpokládat, že již k přerušení napájení došlo a zajištění digitálního důkazu přímo na místě řešit nemusíme.

U zařízení, která jsou do vozidla integrována, záleží na více faktorech. Například palubní počítače vozidel mají paměť, do které se dá dostat přes interní konektory.

V takovém případě samozřejmě odtahujeme celé vozidlo a palubní jednotku nezajišťujeme bokem.

Novou variantou, která je v současné době testovaná, ale jejíž nasazení se teprve plánuje, jsou inteligentní jednotky palubních počítačů s Wi-Fi připojením. Mezi ně patří některé jednotky výše zmíněného systému C-ITS. V tomto případě začne jednotka, jakmile je vozidlo nastartováno, vysílat broadcast na speciálním pásmu definovaném ve standardu IEEE 802.11s. Všechny připojené C-ITS jednotky v oblasti pak mohou obdržet zprávu v zásobníku právě připojené jednotky, nebo zprávu, kterou jí zaslal palubní počítač.

Pokud tedy technik přijede na místo, může po dokončení fyzické obhlídky vozidla zkusit projet odpovídajícím nástrojem pásmo, ve kterém operuje C-ITS systém a zjistit, zda palubní jednotka vozidla stále vysílá, případně najít palubní jednotku, připojit ji na místě na zdroj energie a zjistit, zda začne něco vysílat.

C-ITS jednotky, které nejsou napojené jako most do palubního počítače, ovšem z povahy protokolu nedisponují vlastní pamětí. Nedá se tedy spolehnout, že technik vůbec odchytí nějakou vhodnou zprávu.

V případě vozidel firemních nebo využívaných jako vozidla taxislužby, je také nutné do skupiny IoT zařízení uvažovat další systémy tzv. „fleet managementu“. V případě taxislužeb to bývají zařízení taxametrů (ne nezbytně IoT), zařízení pro komunikaci s dispečinkem (IoT ze své povahy – zpracovávají minimálně vstupy od uživatele) a zařízení pro správu zákazníků (mohou být IoT, ale nemusí). Na rozdíl od C-ITS jednotek ovšem tato zařízení nebývají pevně spojena s vozidlem, díky čemuž zajištění digitálních důkazů – pokud jsou v nich přítomny – může probíhat stejně dobře v laboratoři. V tomto případě opět jde o nutnost dodržení obecných pravidel pro zajišťování fyzického materiálu na zkoumaném místě.

4.3 Metodika zajištění zařízení skupiny E

Jde o velmi rozsáhlou skupinu zařízení. Z praktických důvodů je ovšem nebudeme dělit na další podskupiny, jelikož jejich fyzické charakteristiky jsou vesměs stejné. Poskytují tzv. „infrastrukturní podporu“ pro provoz počítačových sítí. Mohli bychom

je teoreticky dělit na přenosná (routery, switche, racky) a nepřenosná (vestavěné rozvodny), ale vzhledem k marginálním výhodám zajištění celých ústředen v porovnání s koncovými prvky se tímto aspektem zabývat nebudeme.

Návrh postupu pro obecnou akvizici dat z těchto systémů včetně případové studie obsahuje například diplomová práce, kterou vypracoval a úspěšně obhájil Giorgos Paraskevas Damiris v roce 2020 na University of Piraeus [18]. V této práci uvažuje dvě možnosti získání dat z routeru – akvizicí běžícího systému a vyvoláním pádu systému s následným sběrem tzv. crash dump, tedy havarijního výpisu paměti.

Práce navíc nepředpokládá, že se nezbytně musí jednat o prvek, ke kterému máme administrační účet. Damiris (*tamtéž*) uvádí, že pro praktické použití získaných dat by nemělo záležet na tom, jestli k zařízení máme oprávněný přístup, nebo jsme na něj zaútočili, pokud dodržíme pravidla pro vedení protokolu a námi provedený útok zaneseme jako známou manipulaci. Každopádně práce poskytuje ukázkový postup, včetně příkazů. Damiris pouze neřeší zásady forenzní práce, svá data považuje automaticky za důvěryhodná. Je tedy zapotřebí si i zde uvědomit, že jakmile získáme crash dump nebo data z živého systému, musíme opět provést jejich zapečetění a ověřovací hash zapsat do protokolu.

4.4 Metodika zajištění zařízení skupiny A

Tato zařízení lze označit souhrnný termínem „smart office“. Jde o zařízení pro tiskovou správu, skenery, kopírky, tiskárny, ale také inteligentní projektory, NAS úložiště a další IoT zaměřená primárně na segment malých kanceláří. Oproti skupině H, která má podobné zaměření, je zde rozdíl v primární funkci, kterou je podpora dokumentového oběhu a s ním spojených procesů. Proto jsou také zařízení skupiny A obvyklejší v kancelářském prostředí.

U všech tiskáren se vyplatí pro začátek zmínit jednu unikátní vlastnost – takzvaný „digitální otisk prstu“. Ten přímo nesouvisí s jejich IoT povahou, ale je podstatným ukazatelem, pokud jde o jejich forenzní analýzu. Každá tiskárna se různým způsobem opotřebovává, což se časem projeví na způsobu, jakým na papír přenáší inkoust nebo jiné tiskové médium. Jelikož je souhrn vlastností působící na konkrétní tiskárnu

v rámci určitého prostředí unikátní, můžeme jednoznačně přiřadit dokument k tiskárně, ze které pochází.

Relevance této vlastnosti k problematice zajištění digitálních důkazních materiálů z konkrétní tiskárny jakožto IoT zařízení je nasnadě – pokud víme, z které tiskárny byl dokument vytištěn, můžeme se zabývat jinými otázkami, než pokud to nevíme. Například pokud tiskárna sice obsahuje údaje o tom, kdo ji obsluhoval, ale ne o dokumentu, který tiskl, můžeme z času tisku a ztotožnění dokumentu s tiskárnou pomocí údajů v ní uložených získat jméno osoby, která dokument zadala k tisku.

4.4.1 Zařízení s přímo přístupným ovládáním (podskupina A1)

Velká část těchto zařízení obsahuje harddisk, na kterém mohou být důležitá data týkající se historie jejich použití, nastavení operačního systému a dalších údajů. V minulosti byl obvyklý způsob forenzní evidence takového zařízení zabavení, převoz do laboratoře a získání harddisku, který se přímo vytěžil. Tento postup je navrhován v několika článcích v odborné literatuře.

V případě IoT tiskáren, tedy takových, jejichž běžné ovládání vyžaduje interakci přímo s daným přístrojem, ale zároveň mají propojení na internet nebo alespoň intranet, se nabízí ještě jedna možnost. Taková tiskárna je prakticky vždy připojena k tiskovému serveru, který zajišťuje její *smart* nebo rovnou *IoT* funkce, přičemž u vybraných tiskáren může být tiskový server reprezentován cloudem výrobce. To umožňuje poskytování automatizovaných funkcionalit jako například doplňování inkoustu. Pokud na místě technik zjistí, že zkoumaná tiskárna skutečně podporuje tento typ připojení a je zapojená do datové sítě, měl by postupovat stejně jako u cloudových zařízení ve skupině H1 – odposlechnout provoz co nejblíže zařízení, aby zjistil, s kterou infrastrukturou nejpravděpodobněji komunikuje, zda jde o lokální adresu, nebo o vzdálený server.

U lokálního serveru je potom vhodné podívat se, zda obsahuje nějaké záznamy o komunikaci nebo činnosti tiskárny, a pokud ano, tyto záznamy obvyklým postupem zajistit.

4.4.2 Zařízení ovladatelná pouze prostřednictvím další techniky (podskupina A2)

V tomto případě jde o zařízení, která jsou ovládaná nepřímo prostřednictvím připojených počítačů. Samy přitom buď nemají ovládání vůbec, nebo mají ovládání závislé pouze na pokynech z řídicího přístroje. U takovýchto zařízení obvykle tiskovou frontu představuje pouze záznam ve volatilní paměti tiskárny.

Jelikož tyto systémy neobsahují často bližší údaje, typickou a jedinou u nich řešenou úlohu představuje ztotožnění tištěného dokumentu s tiskárnou, která jej vytvořila, nebo skenerem, který jej digitalizoval. Za tímto účelem jsou k dispozici dva přístupy – analýza artefaktů z podezřelého zařízení a dále analýza volatilní paměti, abychom věděli, zda zařízení nemělo v době zajištění v tiskové frontě „uvízlý“ nějaký dokument. V tomto případě tedy nesmí dojít k vypnutí zařízení, jelikož tyto paměti vydrží pouze krátký časový úsek, než dojde k jejich vymazání. Oba postupy lze také zkombinovat, čímž dosáhneme vyšší míry jistoty. Tento postup ve svém článku diskutují Fahd a kolektiv [19], kteří docházejí k poznatku, že kombinace obou postupů může být užitečná nejen pro zjištění autentičnosti dokumentu, ale také pro případnou analýzu dokumentů v tiskové frontě.

4.4.3 Zařízení ovladatelná pomocí tokenů nebo osobních klíčů (podskupina A3)

V tomto případě jde o nejkomplexnější podskupinu systémů ve skupině A3. Tyto systémy mají centrální identity management, dále sestavu tiskových databází a cache a také IDM – identity management systém. Pro koncového uživatele jsou tiskárny typické tím, že on jen ze svého počítače zadá povel k tisku centrálnímu managementu a poté na libovolné tiskárně v areálu provede tisk, aniž by musel vybírat, kde bude dokument chtít vytisknout.

Tato zařízení se používají ve středních a větších podnicích, copycentrech a všude tam, kde je žádoucí výše popsaná funkcionalita. Českým představitelem tiskového systému v podskupině A3 je společnost SafeQ, ale popis jejího systému se dá použít i pro další systémy v této skupině.

Akvizice dat v tomto systému probíhá s ohledem na jeho komplexitu poměrně náročně. Například zmíněný SafeQ systém má několik komponent, z nichž

nejpodstatnějšími pro zajištění digitálních důkazů jsou WPS (Workflow Processing System), LDAP replicator, SPOC (Spooler Controller) a systém nazývaný jednoduše Management. Díky své komplexitě funguje SafeQ systém v několika režimech: klasická infrastruktura, deployment na privátní cloud (nejobvyklejší) a veřejný cloudový deployment. Celá infrastruktura přitom poskytuje logy do centrálního log manageru, kde se uchovávají veškeré informace o tiskových úlohách, jako odkud byla zadána, jakým uživatelem a podobně [20]. Právě tyto logy spolu s identifikací zařízení, získanou vyčtením paměti odpovídající tiskárny, mohou přispět k objasnění několika možných skutečností.

K jejich zajištění tedy potřebujeme zkombinovat některý z postupů jednoznačné identifikace tiskárny, popsaných v podskupině A2, případně použít tamtéž popsanou kombinovanou Fadhovu metodu a dále získat údaje o provozu takto identifikovaného zařízení z log managementu celého systému.

Alternativně je možné projít samotný servisní log, který bude obsahovat například informace o tom, kteří uživatelé v daném časovém úseku prováděli některou z úloh dostupnou přes tento federovaný systém (například SafeQ v současné době integruje nejen klasické, ale i 3D tiskárny a do budoucna nevylučují ani zapojení netiskových zařízení), případně může být dobrým sekundárním místem, odkud lze ověřit, zda osoba s daným LDAPovým účtem byla přítomná. Ačkoliv totiž tento systém má LDAP integraci, uchováváním vlastního logu mimo jiné dupluje některé informace z klasického logu LDAPu, a tedy může představovat záchytný bod, pokud bylo s hlavním logem manipulováno.

Zdrojem těchto informací může a nemusí být server typu PC. V některých případech může serverem být IoT jednotka instalovaná uvnitř budovy. Takovou jednotku musíme analyzovat běžnými nástroji pro IoT ovladače, jak bylo popsáno například v podskupině H2, zejména nástroji pro akvizici paměti nebo obsahu disku, protože zařízení nemusí být odpojitelné od podkladu.

4.5 Metodika zajištění zařízení skupiny M

4.5.1 Mobilní telefony (podskupina M1)

Podskupinou M1 se v práci nebudeme příliš zabývat, jde totiž o velmi dobře popsanou množinu zařízení, pro kterou existují specifické nástroje, jejichž použití popisuje celá řada studií a článků. Uvedeme zde například práci autorů Sadiq, Iqbal a kol. [21], kteří srovnávají různé přístupy k forenzní akvizici a analýze dat z mobilních telefonů.

Tento proces je navíc důkladně popsán v materiálech skupiny ENISA a dalších příručkách pro forenzní zpracování. Zde je podskupina uvedena jen pro úplnost v rámci klasifikace, zejména pro dokreslení možných rozdělení skupiny M.

4.5.2 Chytré hodinky a náramky (skupina M2)

Podskupina M2 zahrnuje širokou škálu moderních zařízení, která společně nazýváme *smart wearables* – nositelná zařízení se znaky IoT technologií. Ačkoliv můžeme na trhu najít i chytré prstýnky, zaměříme se zde primárně na běžnější formu těchto pomůcek, což jsou chytré náramky a hodinky.

Hlavní důvod je pragmatický – celá řada chytrých šperků, jako prsteny, brože nebo náhrdelníky, není „always on“ a není snadné ji rozeznat od klasické bižuterie, takže by technický tým musel mít neustále k dispozici aktualizovanou databázi takovýchto výrobků včetně informací o nich. Navíc neexistuje univerzální metodika, jak je posoudit, jelikož každý výrobce řeší připojování, napájení a další IoT funkce specifickým postupem. Hlavně s ohledem na nutnost úspory místa a nenápadnost celého řešení tak vzniká velké množství komplikovaných variant pro zajištění funkcí, což eliminuje snadnou možnost vytvoření typových scénářů.

Z hlediska zajištění můžeme ještě chytré hodinky a náramky rozdělit na čtyři kategorie – chytré hodinky s minimem funkcí (***M2.1***), základní chytré náramky s obvyklými senzory (***M2.2***), běžné hodinky s proprietárním či nerozpoznatelným OS

(***M2.3***), hodinky s komplexním a univerzálním OS na bázi některého komerčního řešení Linux[11], Windows, iOS včetně vlastní SIM karty nebo dalších nástrojů (***M2.3***).

Postup zajištění v rámci těchto kategorií se bude nepatrně lišit, jelikož ne všechna z těchto zařízení poskytují stejné možnosti získání dat a manipulace s nimi. V případě zařízení z kategorií M2.1 a M2.2 je zapotřebí v první řadě zdokumentovat stav, ve kterém se zařízení nacházelo v momentě nálezu. Nemyslíme tím pouze fyzický nález, ale také jestli zařízení například právě nemělo spuštěný systém měření aktivity, jaké ukazovalo aktuální hodnoty a zda mělo aktivní displej.

Jak ve svém článku uvádí Kang a kol. [22], analýza například chytrého náramku MiBand 2 (skupina M2.2) se nejsnáze provádí prostřednictvím artefaktů, které zanechává při synchronizaci se spárovaným telefonem. Článek se ovšem věnuje primárně analýze v laboratorních podmínkách, zatímco metodická podpora pro vyšetřovatele musí zahrnovat i analýzu přímo v terénu. Pak se nabízí dvě možnosti. První je vytěžení dat formou fotografií. Tyto přístroje často nemají vůbec zámek obrazovky, nebo je na úrovni překonatelné přímo v terénu (například pouze dotykem nebo otiskem prstu). V případě, že se podaří hodinky odemknout, můžeme na aktuálních údajích vysledovat některá důležitá fakta bez nutnosti jejich zajištění. Kang a kol. ve svém článku (*tamtéž*) za taková data považují například vývoj stresové hladiny, tepové frekvence, případně i počet uražených kroků, obzvlášť pokud je možné jej vztáhnout ke specifické době.

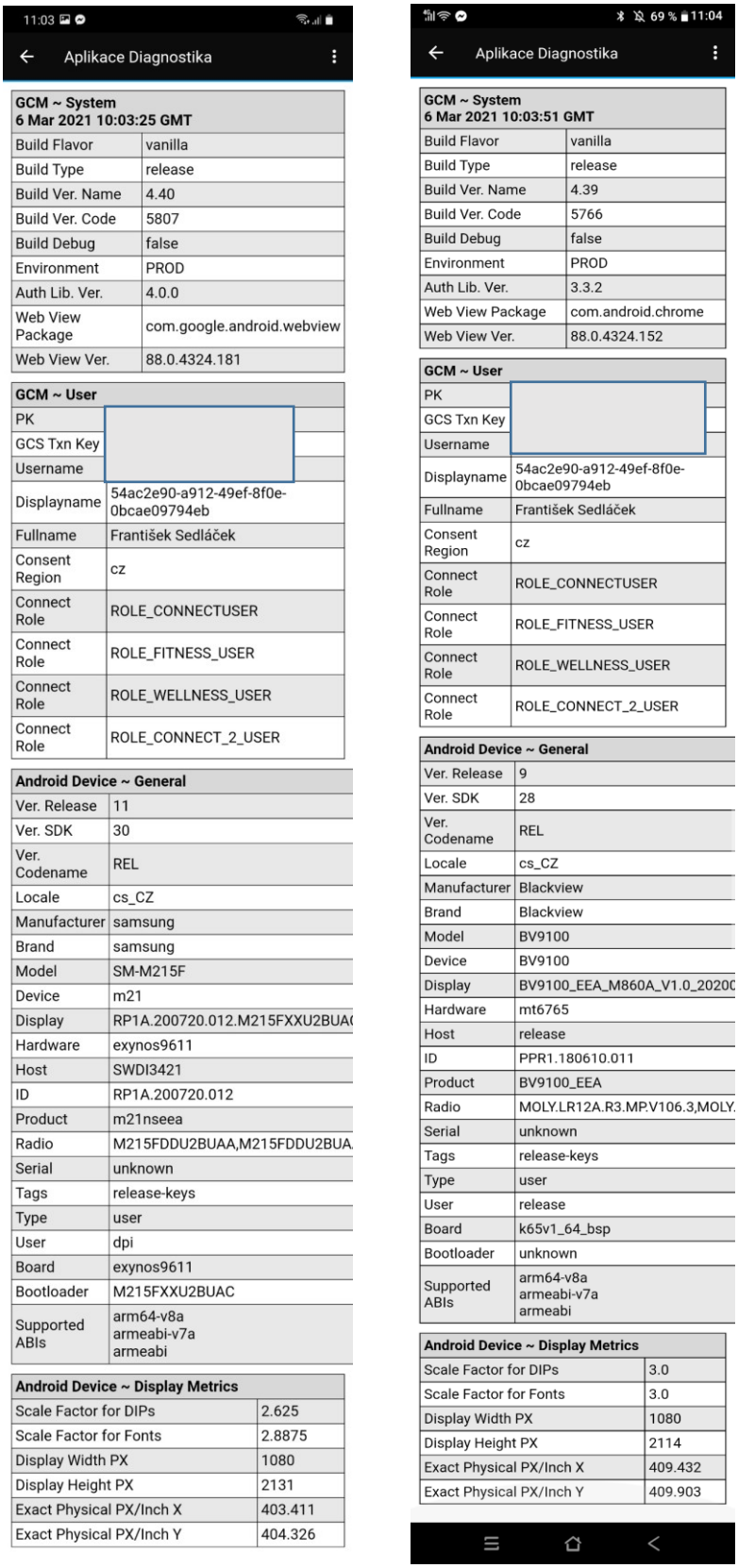
Chytré náramky některých výrobců, například Xiaomi, také mohou fungovat jako fyzický token k odemknutí mobilního telefonu. Pokud je tato funkce aktivní a nastavená, odemkne se telefon oběti pouze přiblížením náramku, není nutné obcházet jeho zabezpečení. V praxí to umožní rychlejší přístup k datům v telefonu, případně možnost přenést data z náramku do telefonu, aniž bychom znali jeho PIN.

To nás přivádí k druhé metodě – pokud je to možné, potřebujeme u skupin M2.1 a M2.2 využít podpůrné zobrazovací funkce, které nabízí propojená mobilní

[11] Včetně platforem Android a Tizen.

aplikace. Pokud máme k dispozici telefon, s kterým je zařízení již spárováno, můžeme z něj data získat obvyklým forenzním postupem, jak jej popsal již zmíněný článek. Bohužel přesun dat mezi mobilními telefony je u těchto zařízení obecně možný jen tím způsobem, že v technickém mobilním telefonu přihlásíme stejný účet cloudové platformy, pod jakým je zařízení registrováno, a data synchronizujeme.

Výstupem takové synchronizace například pro účet Garmin je přihlášení stejného uživatele se všemi zařízeními do více mobilních telefonů, kam se rovněž zkopírují všechny historické údaje z jeho cloudového profilu. Tím pádem je jejich akvizice automatizovaná a zvyšuje se míra autenticity, kterou jim lze přisoudit. Pro srovnání viz obr. 2 na následující straně.



Obrázek 2 – *Ukázka propojení stejného Garmin účtu se dvěma zařízeními*

Pořízením takovéto kopie dat do technického mobilního telefonu a následným uvedením tohoto telefonu do módu bez konektivity před opuštěním zájmového místa zajistíme nezkreslené podklady pro následnou forenzní analýzu.

Popsaný postup tedy řeší situaci, kdy v chytrých hodinkách, které nejsou přímo analyzovatelné, mohou být údaje důležité pro další vyšetřování, případně údaje, které mají povahu digitálního důkazu.

Samozřejmě využití tohoto postupu předpokládá mimo jiné spolupráci oběti nebo získání přihlašovacích údajů od cloudového účtu jiným způsobem. Vzhledem k povaze tohoto digitálního důkazu a relativní anonymitě získávaných údajů (které navíc budou dále zpracovány v rámci analýzy), by nemělo jít o nepřekonatelnou překážku.

Jiná situace je nicméně u zařízení ve třetí a čtvrté skupině. Zde máme totiž k dispozici plnohodnotný počítač s vlastním operačním systémem a pevným diskem nebo jeho ekvivalentem. Pokud navíc systémy čtvrté skupiny obsahují SIM kartu nebo její ekvivalent, dá se říct, že jde o zcela samostatné systémy, u kterých není důvod předpokládat nutnost jiné synchronizace než rovnou s cloudovými službami, a tedy nemusíme hledat ještě „ovládací telefon“, na rozdíl od zařízení ve skupině třetí, která obsahuje chytrá zařízení, jež se při běžném provozu ovšem stále spoléhají na možnost komunikace s ovládacím počítačem pro různé účely.

V tomto případě nezbývá než zařízení nafotit a zajistit jej celé. Ačkoliv bychom mohli zkusit podobnou strategii jako u výše popsaných zařízení, v tomto případě máme k dispozici přímo data, uložená ve stabilní paměti zajišťovaného zařízení. Tím se dostáváme „blíže k senzorům“ do úrovně, kdy je manipulace s nimi velmi obtížná, a tedy se nedá předpokládat, že bychom museli řešit, že získané údaje byly nějakým způsobem změněny.

Ukázkovým zajištěním zařízení třetí kategorie se věnují například Bećirovićová a Mrdović, kteří popisují zajištění chytrých hodinek Samsung Galaxy S3 Frontier [23]. Ve čtvrté kategorii se potom bavíme o zařízeních, která svou komplexitou i možnostmi forenzního zajištění v podstatě odpovídají chytrým telefonům jen

v jiném technologickém provedení, a tedy se jimi nebudeme v práci zabývat extra – fakticky vzato jde totiž o zařízení skupiny M1.

PRAKTICKÁ ČÁST

5 PŘÍPRAVA PRAKTICKÉ ČÁSTI

V praktické části budeme analyzovat vybrané scénáře s využitím konkrétních zařízení, přičemž se pokusíme získat z nich data, udržet během celého zpracování jejich autentičnost a poukázat na jejich možná využití, pokud jde o objasňování skutečností – tedy rozebrat jejich potenciální důkazní hodnotu.

Jelikož výstupem práce má být metodický manuál, budeme si v praktické části všímat obecných, opakujících se kroků společných pro všechna zařízení a v manuálu místo teoretické pomocné klasifikace profesora Blinkowského použijeme spíše praktickou klasifikaci algoritmickou – u jednotlivých postupů budeme vycházet ze společného základu a upozorníme na odlišnosti pouze tam, kde dojde k větvení podle určitých praktických kroků.

Důsledkem tohoto postupu by mělo být, že výsledná metodická pomůcka bude sledovatelná „krok za krokem“, aniž by bylo nutné předem provést klasifikaci zajišťovaného zařízení.

V praktické části budeme proto uvažovat následující scénáře:

- Zajištění dat z domácí chytré kamery (Skupina H1)
- Zajištění dat z C-ITS jednotky osobního vozidla (Skupina S3)
- Zajištění dat z vybraného routeru (Skupina E)
- Zajištění dat z více druhů chytrých hodinek, přičemž zvolíme zařízení:
    - Pro skupinu M2.1 ***Garmin Vívomove Optic*** a ***Garmin Vívomove Sport***
    - Pro skupinu M2.2 ***MiBand 2*** (s technologií SmartUnlock) a ***MiBand 4***
    - Pro skupinu M2.3 ***Samsung Galaxy S4 Frontier***
    - Pro skupinu M2.4/M1 hybridní hodinky ***Lilygo T-Watch-2020***

U každého zařízení se pokusíme popsat, případně nasimulovat scénář zajištění, a to v celém popsaném režimu – od příchodu technika a zajištění virtuálního prostoru až po akvizici a vyhodnocení konkrétních dat.

Praktický experiment práce se tedy rozpadne na sedm scénářů, přičemž sedmý scénář se bude týkat dvou podskupin. S výjimkou skupiny A, jejíž analýzu jsme již ukázali výše, budou v praktickém experimentu zastoupeny všechny jednotlivé skupiny Blinkowského klasifikace.

Shodnou částí designu každého experimentu pro jednotlivou skupinu bude výchozí scénář, ze kterého budeme analýzu provádět, dále samotný experimentální postup zajištění dat včetně fotodokumentace a sepsání výstupní zprávy o ohledání místa činu se všemi náležitostmi podle hlavy třetí, oddílu druhého, § 55 až § 56 zákona 141/1961 Sb., trestního řádu, včetně stanovení dalších znaleckých otázek. Ve vybraném případě bude vypracován i ukázkový znalecký posudek ve smyslu hlavy páté TŘ, a to za účelem demonstrace rozdílu mezi zajištěním materiálu na místě činu a v laboratorním prostředí.

V jednotlivých experimentech praktické části nebudeme pro zjednodušení opakovat úkony ohledání kybernetického prostoru uvedené v předcházející teoretické části. Tyto úkony uvedeme až ve výsledné metodice.

V praxi si při průzkumu digitálního prostoru a zachycování signálů, které mohou IoT zařízení přenášet, zejména pokud se je snažíme detekovat, musíme dát pozor na jejich elektromagnetickou susceptibilitu. Narušení potenciálního elektromagnetického prostoru příliš silnou anténou totiž může mít problematické následky v podobě znepřístupnění, znehodnocení nebo zničení dat či celých zařízení. Toto je obzvlášť patrné v uzavřených nebo malých prostorách s vysokou koncentrací IoT zařízení [24], kde může již v době zajišťování být elektromagnetické pole téměř na limitní kapacitě z hlediska možností jednotlivých systémů. Experimenty proto budou probíhat v kontrolovaných podmínkách s dostatečně nízkou koncentrací elektromagnetického záření, aby nedošlo k poškození zkoumaných systémů, a tím i k znemožnění akvizice.

6 JEDNOTLIVÁ PRAKTICKÁ ZAJIŠTĚNÍ

6.1 Praktický scénář pro skupinu H

Pro skupinu H byla vybrána inteligentní domovní kamera s připojením na cloud. Při zajišťování bylo zjištěno, že kamera nedisponuje vlastní pamětí, která by byla pro naše účely použitelná, a tedy ji z hlediska metodiky pro skupinu H nelze zajistit.

Její zajištění se tedy přesunulo na úroveň nepřímého zajištění SOHO prvku prostřednictvím nejbližšího zařízení s dlouhodobou pamětí, v tomto případě nainstalovaného routeru, na který byla kamera bezdrátově připojena. Popis zajištění kamery připojené k routeru je součástí praktické části této práce v kapitole 6.3 – Praktický scénář pro skupinu E.

6.2 Praktický scénář pro skupinu S

Původní scénář stanovený pro tuto skupinu v teoretické části zněl: *(Máme…) odstavené vozidlo, u kterého potřebujeme zjistit jeho předchozí trasu, protože se domníváme, že jde o únikové vozidlo po přepadení nebo vozidlo, ve kterém se nacházela pohřešovaná osoba. Potřebujeme tedy zjistit ID C-ITS jednotky, které potom můžeme porovnat postupně s C-ITS jednotkami v okolí, a získat tak pravděpodobnou poslední trasu vozidla před jeho zajištěním.*

6.2.1 Výstupy analýzy v terénu

Praktickou analýzou existujících C-ITS jednotek a konzultací s odborníky na C-ITS systémy společnosti Brněnské komunikace, a. s., zejména s Bc. Stratilem, ovšem vyšlo najevo, že tento scénář je velmi nepravděpodobný. Jednotka nejenže neuchovává informace, ale také při každém spuštění motoru vygeneruje nové ID vozidla, přičemž to staré se nedá od nového nijak odvodit. To brání jednak vytěžení okolních C-ITS jednotek a jednak sledování pomocí jednotek infrastrukturních, protože nejsme schopni snadno získat předchozí ID.

Při terénním pokusu nicméně bylo možné demonstrovat sledování jednoho pohybujícího se vozidla z druhého a možnost předávat mezi nimi zprávy. Zpráva

zaslaná vozidlem A byla přijata a zpracována C-ITS jednotkou vozidla B. Ačkoliv se v současné době taková zpráva mezi oficiálními zprávami C-ITS protokolu nevyskytuje, bylo by pravděpodobně možné takto mezi dvěma vozidly předat například výzvu k zastavení nebo informace o sledovaném vozidle v situaci, kdy by hlídky například doprovázely nějaký bankovní transport. Ohledací protokol zde tedy nemá smysl vytvářet, protože žádné šetření na místě není možné.

6.2.2 Výstupy laboratorní analýzy

Zajímavější situace ovšem nastala při analýze záznamu C-ITS komunikace mezi vozidly v rámci experimentu později v laboratoři. Jedno z vozidel totiž nahrávalo veškou komunikaci, probíhající přes C-ITS protokol, tedy zprávy od infrastrukturních jednotek i jednotek vozidel,. Ty byly následně nahrány do nástroje *Wireshark*, který slouží k prohlížení pcap[12] souborů, ve kterém byl zaveden přídavný plugin na dekódování C-ITS zpráv. Díky tomu jsme měli k dispozici praktickou podobu všech typů zpráv, které se v rámci protokolu k datu vypracování experimentu vyskytovaly. Tyto zprávy je možné rozdělit do několika kategorií [25]:

- ***CAM (Cooperative Awarness Message):*** standardizovaný formát zpráv pro šíření základních stavových informací o vozidle (poloha, rychlost, směr, stav vozidlových systémů) Je součástí standardu ITS-G5 definovaného v normách ETSI.
- ***DENM (Decentralized Environmental Notification Message):*** standardizovaný formát zpráv pro šíření informací o vzniklých událostech (dopravní nehoda, kolona, práce na silnici atd.) Je součástí standardu ITS-G5 definovaného v normách ETSI
- ***IVI (In Vehicle Information):*** standardizovaný formát zpráv pro šíření informací, především dopravních značek a symbolů do vozidel. Je součástí standardu ITS-G5 definovaného v normách ETSI.

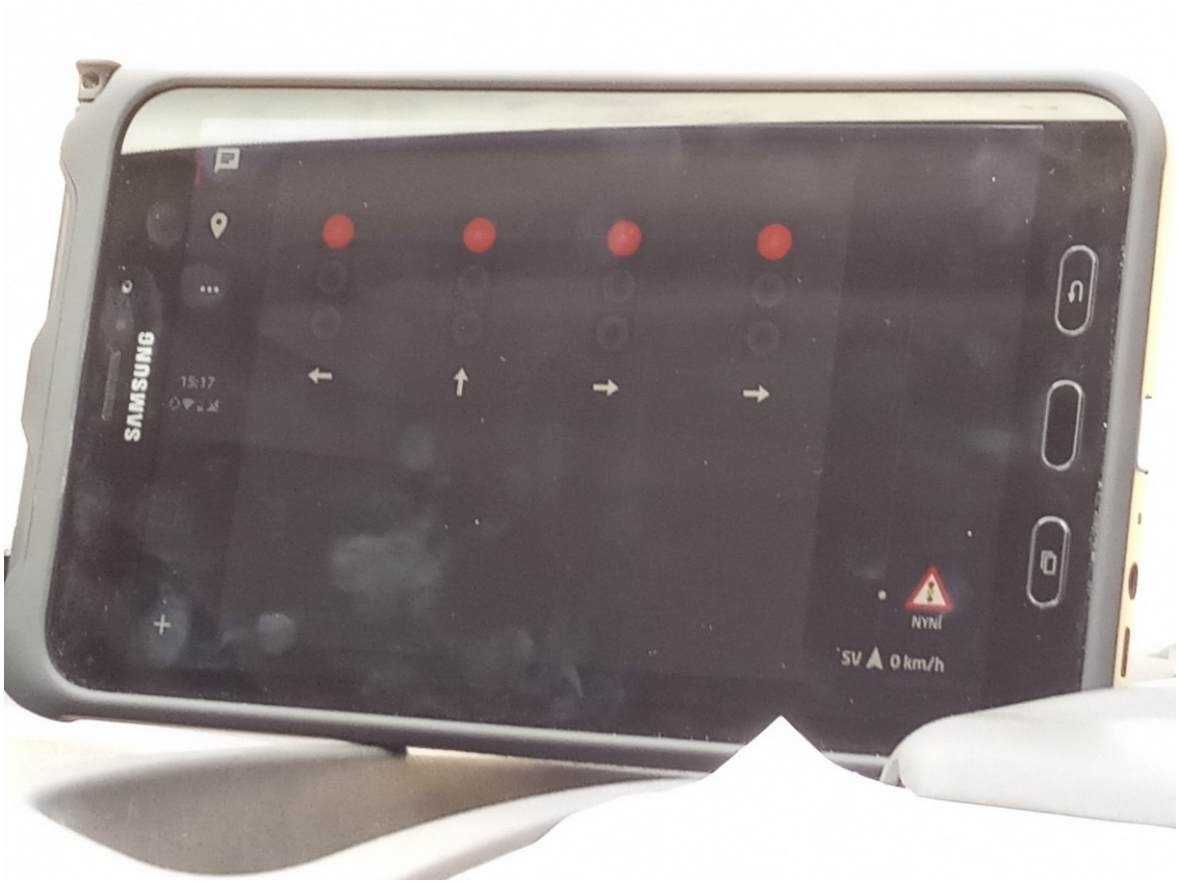
[12] Soubor s obsahem zachycených síťových packetů z komunikace mezi zařízeními, záznam nástroje TCPDUMP (http://www.tcpdump.org/).

Přičemž zachycený provoz obsahoval ještě další dva typy zpráv projektu C-Roads, které nejsou v oficiální dokumentaci. Šlo o zprávy následujících typů:

- ***SPATEM (Signal Phase and Timing Extended Message):*** slouží k poskytování informací o signálním cyklu světelného signalizačního zařízení (SSZ) na křižovatkách. Tento cyklus určuje pořadí a délku jednotlivých signálních dob. SPAT je generována v jednotce RSU v blízkosti SSZ na základě informací z dopravního řadiče. Jedna tato zpráva může obsahovat informace o signálním cyklu jedné nebo i více křižovatek zároveň.
- ***MAPEM (Map Data Extended Message):*** slouží k poskytování informací o topologii a geometrii křižovatkových úseků z jednotek RSU do vozidel nebo do mobilních zařízení. Jedna zpráva MAP může obsahovat informace o geometrii jedné, ale i více křižovatek.

Tyto zprávy navrhl ve své diplomové práci Ing. Jakub Jirák [26] představují prototyp zpráv pro zajištění plynulosti provozu křižovatek. SPAT a MAP zprávy dohromady poskytují přehled o pruzích a světlech na světelných křižovatkách, zatímco MAP zprávy samy poskytují přehled o pruzích a způsobu průjezdu křižovatek nesvětelných. Možnost výsledné podoby dat, jak bude zobrazena řidiči v kabině vozidla, je na obrázku 4 – jde o data z křižovatky spojující informace z CAM zprávy (směr a rychlost), SPATEM a MAPEM zpráv.

Na obrázku je patrné, že jde o průjezd křižovatkou řízenou světly, která umožňuje jízdu rovně do jednoho pruhu, vlevo do jednoho pruhu, nebo vpravo do dvou pruhů a C-ITS jednotka indikuje také stav světelné signalizace pro jednotlivé pruhy, získaný z SPATEM zprávy.



Obrázek 3 – Ukázka možné aplikace pro zobrazení C-ITS dat

Každá jednotka také vysílá jako součást svých zpráv unikátní identifikační řetězec, nazvaný stationID: Tím je možné po dobu, kdy je vozidlo v pohybu, sledovat zprávy z něj pocházející. C-ITS jednotka použitá v testu vygenerovala nové stationID při každém spuštění motoru vozidla, tedy například u vozidel se systémem start-stop by se mohlo vygenerovat při každém zastavení v křižovatce. StationID navíc není známé před vyjetím vozidla, nedá se tedy například použít ke sledování stopy jednoho vozidla napříč více trasami.

K čemu by ovšem bylo možné využít stationID a co demonstrovaly rovněž nasbírané datové údaje z C-ITS systému, které jsme zpracovávali v rámci experimentu, je sledování vozidla v pohybu. Každá CAM zpráva obsahuje informace o pozici, směru a rychlosti vozidla a tyto zprávy odchytává každý C-ITS prvek v okolí, tedy nejen další vozidla, ale také DENM zprávy. Proto by mělo být možné do C-ITS infastruktury přidat zprávu, která by aktivovala vyhodnocování zpráv o konkrétním

vozidle a například umožnila kromě vlastní polohy na GPS mapě zobrazit i jeho polohu průběžně aktualizovanou pomocí jeho CAM zpráv.

Dalším možným využitím C-ITS systému by bylo přidání zpráv, které by napodobovaly zprávy CAM podtypu EVA (Emergency Vehicle Approaching – příjezd vozidla systému IZS) nebo zprávy SPAT se žádostí o prioritu průjezdu křižovatkou, a to za účelem vyžádání zastavení konkrétního vozidla na základě jeho aktuální polohy a směru, případně změny signálního plánu nadcházející křižovatky za účelem pozdržení vozidla. Zprávy se totiž sice vysílají plošně, ale jednotka umožňuje určit okruh vozidel, kterým má zpráva být zobrazena s tím, že ostatní OBU (On-Board Unit, jednotka na palubě vozidla) zprávu „zahodí“ bez zpracování.

6.3 Praktický scénář pro skupinu E

Majitel objektu nahlásil na tísňovou linku vykradení. V objektu se nachází bezdrátová kamera napojená na Wi-Fi, která běžně snímá vchod do objektu, ale má širší provozní rozsah díky otáčivému kloubu. Krátce před vykradením objektu se kamera natočila do zdi a přestala zabírat vstup do objektu dostatečně dlouho na to, aby bylo vidět pouze otevření a opětovné zavření dveří v určitou dobu a poté znovu o pár minut později. Technik, který přijede na místo činu, zjistí, že kamera přenáší záznam na cloudové úložiště, avšak záznam neobsahoval důkaz použitelný pro zjištění, co vyvolalo její náhlý posun, a technik se pokusí ověřit na routeru, zda s kamerou v předmětnou dobu probíhala nějaká komunikace.

Pro tento účel budeme uvažovat typický domácí router využívaný v režimu bezdrátového přístupového bodu. V našem případě konkrétně půjde o Wi-Fi router společnosti Microtic, ke kterému je připojena SOHO kamera (sama o sobě třídy H1) model YCC365 Plus.

6.3.1 Zajištění v terénu

V tomto případě bylo nutné při samotném zajišťování v terénu provést zejména předběžné práce pro analýzu v laboratoři. Nástrojem pro odchycení síťového provozu bylo zjištěno, že kamera komunikuje pravidelně s cloudem na určité IP adrese a dále že při použití ovládací aplikace této kamery dojde k odeslání zprávy nikoliv pouze

z telefonu, na kterém aplikace běží, ale také z tohoto veřejného cloudu. Vycházelo se přitom z toho, že adresa cloudu je pravděpodobně statická, nebo ji bude možné v případě běhu kamery v laboratorních podmínkách získat znovu korelací času poslaného požadavku z kamery a času v komunikaci prostřednictvím aplikace.

Tuto IP adresu je tedy nutné zaznamenat do protokolu, případně i s přihlašovacími údaji k ovládacímu účtu, a to před samotným zajištěním a transportem kamery. Stejně tak je nezbytné před transportem zajistit i IP adresu, která byla kameře přidělena, a veškeré logy, které se mohou nacházet na routeru nebo na jiných zařízeních – například kamery výrobce D-Link umožňují záznam kamer ještě před zasláním na cloud uložit na lokální NAS vybavený příslušným softwarem, který uchovává i provozní záznamy. V systému se kromě samotného záznamu kamery potenciálně mohou nacházet artefakty poskytující informaci o manipulaci s kamerou.

V případě zkoumaného zařízení YCC365 Plus je nicméně veškerá infrastruktura v cloudu, jehož vstupní bod se nachází na adrese esd.icloseli.com. Ověření ovládací aplikací na místě tedy ukáže, že veškerá komunikace by měla probíhat s tímto cloudem. WHOS záznam tohoto cloudu vypadá následovně:

Domain Name: CLOSELI.COM

Registry Domain ID: 1822487085_DOMAIN_COM-VRSN

Registrar WHOIS Server: grs-whois.hichina.com

Registrar URL: http://www.net.cn

Updated Date: 2019-10-16T10:21:26Z

Creation Date: 2013-08-19T16:54:42Z

Registry Expiry Date: 2022-09-10T11:59:59Z

Registrar: Alibaba Cloud Computing (Beijing) Co., Ltd.

Registrar IANA ID: 420

Registrar Abuse Contact Email: DomainAbuse@service.aliyun.com

Registrar Abuse Contact Phone: +86.95187

Domain Status: ok https://icann.org/epp#ok

Name Server: NS-1307.AWSDNS-35.ORG

Name Server: NS-1771.AWSDNS-29.CO.UK

Name Server: NS-442.AWSDNS-55.COM

Name Server: NS-599.AWSDNS-10.NET

DNSSEC: unsigned

URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

>>> Last update of whois database: 2021-04-11T09:33:26Z <<<

(Získáno ze serveru https://whois.paranoia.cz/)

Jde tedy o infrastrukturu čínské společnosti Alibaba Cloud Computing (Beijing) Co., Ltd.

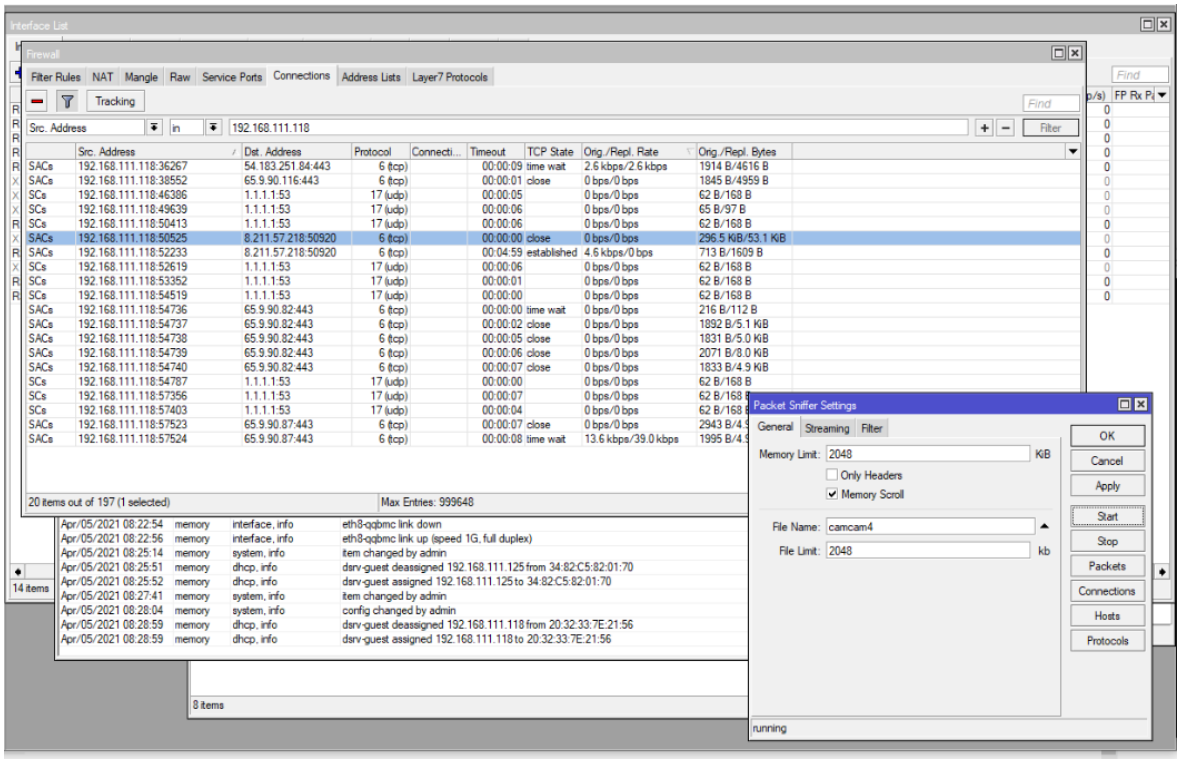
Jelikož kamera podle všech dostupných údajů z předběžného ohledání neobsahuje žádné další informace, které by mohly vést ke stanovení otázek, zaměříme se nyní na laboratorní analýzu routeru.

6.3.2 Laboratorní část analýzy

Pro skupinu E se zaměříme na laboratorní analýzu routeru a jeho logů. Pro tento případ jsme uvažovali, že kamera byla dlouhodobě připojena k routeru společnosti Microtic. Tento router sice neuchovává údaje o provozu, pokud tato funkce není explicitně zapnuta[13], umožňuje ale získat například logy z protokolu DHCP. V případě, že by měl nastavenou statickou adresaci prostoru, je situace ještě snazší, protože na základě MAC adresy přidělí webkameře stejnou IP adresu, jako měla „v provozu“. To znamená, že můžeme rozborem komunikace na cloud ve zkoumané době zjistit, jestli k otočení kamery došlo náhodou, nebo zda útočník zneužil účet či připojení ke kameře jako prostředek, jak ji na dálku otočit odpovídajícím povelem

[13] V kontextu možného kancelářského použití kamery jako součásti bezpečnostního systému se ovšem dá očekávat, že tato funkce použita bude.

z cloudové infrastruktury. Problém může nastat v případě, že by komunikace mezi veřejnou IP adresou a cloudem společnosti Alibaba byly z cílového místa častější, tedy že by se v objektu nacházelo více stejných zařízení, které se spojují s daným cloudem. V takovém případě totiž může ještě být nezbytné zjistit, jak vypadala v danou chvíli tabulka NAT protokolu routeru a zda došlo k přenesení informace přímo k cílové kameře nebo k jinému zařízení. Ukázkový výstup z packet snifferu na obrázku 5 dokládá, že kamera skutečně přes tento router aktuálně komunikuje s cloudovou infrastrukturou, a poskytuje indicie k vyžádání statistických dat pro analýzu síťového provozu.



Obrázek 4 – Ukázka zachycení provozu mezi webkamerou a cloudem Alibaby

6.4 Praktický scénář pro skupinu M

Hlídka při pochůzce přijala ohlášení z operačního střediska tísňové linky, aby zkontrolovala hlášení o ženě sedící bez hnutí na lavičce v potrhaných šatech. Při příchodu si hlídka všimla krve na těle ženy a vyhodnotila, že bude nezbytné přivolat také sanitku a kriminalistického technika, který by posoudil věcné důkazy, které se

mohou na místě nacházet. Všimli si také, že žena má na zápěstí chytré hodinky, a technika o této skutečnosti informovali.

Hlavním cílem ohledání na místě činu by mělo být zjistit, jak se tam žena dostala, co mohlo způsobit její stav a jestli je agresorem, nebo obětí. Za tímto účelem se tedy pokusíme vytěžit údaje z chytrých hodinek.

6.4.1 Návrh experimentu a technické podmínky

Pro snížení možného zkreslení absolvuje figurant před provedením experimentu cestu stejnou trasou se všemi použitými hodinkami. Konkrétně půjde o trasu od obecního úřadu obce Popice u Hustopečí na turistický bod vzdálený 617 metrů s výškovým profilem +37 metrů. Trasu figurant projde jednou se všemi hodinkami a výsledné ohledání bude simulováno v cílovém bodě. Tím je turistický bod „tvrziště Popice" nacházející se v katastru obce Popice u Hustopečí. Pro jednotlivé hodinky bude zaznamenaný počet kroků a další údaje, které bude možné hodinkami zjistit. Zápis kroků proběhne ve výchozím bodě, dále v bodě tvrziště a zpětně v budově obecního úřadu. Celkem bude použito sedm různých hodinek zastupujících všechny podtřídy od mechanických hodinek s IoT krokoměrem, až po počítač na ruku se samostatným komunikačním rozhraním.

6.4.1.1 Garmin Vívomove Sport

Zařízení Garmin Vívomove představuje první generaci v řadě Vívomove. Jde o jedny z prvních hybridních hodinek na trhu. Takto bývají označovány kvůli faktu, že mají zároveň klasický hodinový strojek a zároveň funkce IoT zařízení. Popis z webu výrobce zní: „Na jedinou baterii vydrží bez nabíjení fungovat až 1 rok a poté se baterie, podobně jako u jiných hodinek vymění. Hodinky mají klasické ručičky, ciferník je ale doplněn o dva digitální displeje zobrazující splnění denního cíle nastaveného počtem kroků a dobu, po kterou je majitel hodinek neaktivní."[14]

[14] GARMIN. Garmin Vívomove HR: Dostupné na: https://buy.garmin.com/cs-CZ/CZ/p/583562. [cit. 11. 5. 2021]

6.4.1.2 Garmin Vívomove Optic

Druhá generace v produktové řadě Vívomove. Výrobce o přístroji říká: „Vívomove Optic jsou chytré hodinky s krásným elegantním designem, které v sobě skrývají víc, než je na první pohled patrné. Pod mechanickými ručičkami hodinek se skrývá diskrétní displej ovládaný dotykem a čitelný i ve tmě. Slouží k zobrazení smart notifikací a naměřených fitness hodnot.“[15]

6.4.1.3 Garmin Vívoactive 4S

Hodinky amerického výrobce sportovní elektroniky Garmin představující čtvrtou generaci hodinek pro příležitostné sportovce Vívoactive. Písmeno „S“ v pojmenování modelu znamená „Small“, protože jde o zmenšenou variantu hodinek Garmin Vívoactive 4. Hodinky nabízejí v základní výbavě krokoměr, měřič tepu, senzory pro měření stresu, spánku, aktivity a další. Dále je do nich možné nahrát aplikace třetích stran s využitím specializovaného obchodu Garmin IQ.

6.4.1.4 Mi Band 2

Mi Band 2 je krokoměr pro umístění na zápěstí. Výrobcem je čínská společnost Xiaomi, která má v Česku poměrně silné zastoupení na trhu s osobní elektronikou. Vyrábí telefony, nositelnou elektroniku, zařízení pro elektromobilitu a chytrou domácnost. Mi Band 2 byl na trh uveden v roce 2016 a prodává se globálně. Zajímavou funkcí, kterou nabízí, je možnost odemknutí telefonu jeho přiblížením k hodinkám. Znamená to, že i v terénních podmínkách nemusí technik prolamovat heslo k telefonu, stačí mu obě zařízení k sobě přiblížit.

6.4.1.5 Xiaomi Mi Smart Band 4

Pokračuje v řadě Mi Band, ovšem jde o první náramek čínského výrobce pojmenovaný Mi Smart Band. Podobně jako dřívější modely Mi Band nabízí možnost

[15] GARMIN. Garmin Vívomóve Optic Dostupné na: https://www.garmin.cz/garmin-vivomove-optic-sport-black-velikost-l/78953. [cit. 11. 5. 2021]

odemčení obrazovky spárovaného telefonu pouze přiblížením obou zařízení. Na trh byl globálně uveden v roce 2019 a během prvních osmi dnů se prodal milion kusů

6.4.1.6 Samsung Galaxy Watch Active

Jde o jednodušší chytré hodinky vybavené variantou proprietárního operačního systému Tizen. Díky tomu mohou obsahovat i různé aplikace třetích stran schválené společností Samsung. Hodinky ovšem k plnohodnotnému provozu vyžadují propojení s mobilním telefonem a některé funkce nejsou dostupné, pokud se od něj příliš vzdálí.

6.4.1.7 Samsung Gear S3 Frontier

Chytré hodinky vybavené operačním systémem Tizen. Tento operační systém je vlastní platformou společnosti Samsung pro hodinky, televize i další zařízení. V hodinkách je ve verzi 3.0 a jde o plnohodnotnou verzi systému. Tyto hodinky budeme v práci používat i v praktické ukázce laboratorní akvizice dat, a to na základě postupu, který popisují Bećirovićová a Mrdović ve svém článku Manual IoT Forensics of a Samsung Gear S3 Frontier Smartwatch [23]. Tyto hodinky se prodávají i ve variantě s nanoSIM kartou a v takovém případě mohou zcela nahradit plnohodnotný mobilní telefon.

6.4.1.8 LillyGo T-Watch 2020

Chytré hodinky fungující jako nositelný víceúčelový počítač. Pracují s vlastním operačním systémem běžícím na procesorové platformě ESP32. Podobně jako v případě Samsung Gear S3 Frontier jde o samostatné zařízení, které se obejde bez mobilního telefonu. Jsou plně programovatelné a lze k nim přistupovat prostřednictvím USB portu a propojení na počítač. V laboratorních podmínkách jde tedy z hlediska forenzního IT o nejsnáze analyzovatelné zařízení v této kategorii.

6.4.2 Srovnání důležitých vlastností jednotlivých hodinek

Tabulka 1 na následující straně shrnuje vlastnosti jednotlivých chytrých hodinek, které mohou být podstatné pro objasnění nebo stanovení otázek na místě činu. Tyto vlastnosti tedy představují potenciální digitální důkazy, které může technik z hodinek

vyčíst ještě před jejich zabavením, dokud je oběť má na těle. V případě vhodné analýzy v terénu se pak může zcela vyhnout nutnosti hodinky zabavit a může využít údaje z propojené aplikace, nebo získané přímo na hodinkách a ověřené formou dokumentace. Ukázková fotodokumentace pro vybrané hodinky tvoří Přílohu 1 této práce.

Tabulka 1 – Srovnání informací získatelných z jednotlivých chytrých hodinek bez napojení k telefonu

Název hodinek	**Odemčení telefonu přiblížením**	**Přehrání zvuku na spárovaném telefonu**	**Historie srdečního tepu**	**Aktivity (samostatné sledování pohybu)**	**SOS hovor / zpráva**	**Zobrazení kontaktů z telefonu**	**Zobrazení zpráv z telefonu**	**Zobrazení notifikací z telefonu**	**GPS tracker se sledováním trasy**
Garmin Vivomove	-	-	-	-	-	-	-	-	-
Garmin Vívomove Optic	-	X	X	X	-	-	X	-	-
Garmin Vívoactive 4S	-	X	X	X	X	-	X	X	X
Xiaomi Mi Band 2	X	X	-	X	-	-	-	-	-

Název hodinek	**Odemčení telefonu přiblížením**	**Přehrání zvuku na spárovaném telefonu**	**Historie srdečního tepu**	**Aktivity (samostatné sledování pohybu)**	**SOS hovor / zpráva**	**Zobrazení kontaktů z telefonu**	**Zobrazení zpráv z telefonu**	**Zobrazení notifikací z telefonu**	**GPS tracker se sledováním trasy**
Xiaomi Mi Smart Band 4	X	X	-	X	-	-	X	X	-
Samsung Galaxy Watch Active	-	X	X	X	X	X	X	X	X
Samsung Gear Watch S3 Frontier	-	X	-	X	X	X	X	X	X
LillyGo T-Watch 2020	-	-	-	-	-	-	-	-	-

K posledním třem řádkům tabulky je nutno uvést, že se jedná o stav s výchozími aplikacemi. Tato tři zařízení (Samsung Galaxy Watch Active, Samsung Gear Watch S3 Frontier a T-Watch 2020), stejně jako hodinky Garmin Vivoactive 4S, umožňují uživateli dohrát si externí aplikace třetích stran, které rozšíří možnosti hodinek, zejména pokud jde o komunikační možnosti. Hodinky tak mohou například obsahovat data z populárních messengerů jako WhatsApp, FaceBook Messenger, případně obsahovat historii SMS nebo hovorů uskutečněných ze spárovaného telefonu i v případě, kdy telefon není dostupný. Pro jednoduchost jsou ale v tabulce zahrnuty pouze výchozí stavy hodinek.

Zaměřili jsme se přitom na vlastnosti, které mohou mít využití ve forenzním šetření, jako je nalezení mobilního telefonu s dalšími daty, grafy vývoje určitých hodnot, případně samostatné sledování pohybu aktivované tepovou hodnotou, které může signalizovat prudký pohyb nebo vysokou hladinu stresu. V této souvislosti je dobré podotknout, že vybrané hodinky poskytují také právě funkci měření stresu na základě tepové frekvence, galvanické odpovědi kůže a dalších faktorů. Možné senzory, které do měření stresu u komerčních hodinek vstupují, popisuje Siirtola [27]. Jde o komplexní senzorový systém měřící najednou několik veličin, které jsou poté převáděny do uživatelsky srozumitelné škály. V případě Garminu je to například hodnota od nuly do sta, u hodinek Samsung pouze grafická reprezentace od zelené po červenou. Všechny sledované hodinky, které poskytují hladinu stresu, poskytují také graf jejího vývoje v čase. To umožňuje v terénu odhadnout, jak velkému stresu byla oběť vystavena a po jakou dobu.

Další věcí ovšem je přesnost měření jednotlivých hodnot. V rámci kontrolovaného experimentu popsaného na začátku podkapitoly 4.1.1 této práce jsme zjistili hodnoty krokoměrů zanesené v tabulce 2.

Tabulka 2 - Naměřené hodnoty s jednotlivými hodinkami

Hodinky	**Výchozí počet kroků**	**Počet kroků v mezibodě**	**Koncový počet kroků**	**Naměřené kroky v mezibodě**	**Naměřené kroky celkem**
Garmin Vivomove[16]	0–1 %	10 %	20 %	Cca 800	Cca 1600
Garmin Vívomove Optic	1001	1891	2708	890	1707
Garmin Vívoactive 4S	1302	2120	3051	818	1749
Xiaomi Mi Band 2	1541	2277	3079	736	1538
Xiaomi Mi Smart Band 4	168	979	1947	811	1779
Samsung Galaxy Watch Active	2441	3449	4457	1008	2016
Samsung Gear Watch S3 Frontier	666	1666	2759	1000	2093
LillyGo T-Watch 2020	100	282	2164	182	2064

[16] Tyto hodinky nezobrazují počet kroků jako číslo, ale jen jako přibližné procento denního cíle. V experimentu byly nastaveny na 8000 kroků.

Jak je vidět z této tabulky, v mezibodě se počet naměřených kroků pohyboval mezi 736 (hodinky LillyGo T-Watch 2020 v mezibodě vynecháme, hodnota zjevně vznikla chybou v zobrazení) a 1008 kroky. Průměrná hodnota v prvním segmentu bez hodinek LillyGo T-Watch je 866 zaznamenaných kroků, pro celou trasu 1783 kroků. Směrodatná odchylka po zaokrouhlení je v prvním případě 97 kroků, ve druhém 190 kroků. To znamená, že většina hodinek je na kratší trase přesnější a také že absolutní odchylka vzrůstá lineárně s délkou trasy. Relativní směrodatná odchylka je 11 % v prvním segmentu a 10,5 % v druhém, změnila se tedy o půl procenta, což je zanedbatelný posun. Můžeme tedy říct, že jednotlivé hodinky se od sebe nebudou pravděpodobně lišit o více než 12 %, pokud měření neovlivní další faktory. Toto zjištění je konzistentní například s předchozím výzkumem na toto téma, který provedl kolektiv autorů Witte, Blankenhagel et al. [28] v roce 2019.

Za zmínku stojí ještě jeden fakt – měření kroků na většině hodinek probíhá gyroskopem nebo akcelerometrem, a je tedy závislé na pohybu ruky. Zkreslení počtu ujitých kroků směrem dolů tedy může způsobit například nevhodná manipulace. To může být i důvod zkreslení prvního úseku cesty v našem experimentu u hodinek T-Watch. Pokud má například osoba s hodinkami ruku v kapse nebo položenou na tašce přes rameno, případně pokud v ní drží něco těžkého, nevykonávají hodinky dostatečný pohyb na to, aby došlo k zaznamenávání kroků, a tímto vzniká výrazné zkreslení.

To může na jednu stranu vést ke špatnému vyhodnocení ujité vzdálenosti, ale na druhou stranu může být příčina vzniku zkreslení i důležitým faktem, který může přispět k objasnění situace. A to zejména tehdy, pokud by po započtení naměřeného počtu kroků nebyl reálný cíl, z kterého mohla osoba vyjít – například v odlehlé chatové oblasti, nebo ve městě v průmyslové zóně. I když by osoba jinak nespolupracovala, ze záznamu hodinek by stále šlo usoudit, že buď šla s rukou v kapse, ve které něco držela, nebo že nesla těžší tašku nebo břemeno, které bránilo jejím rukám v pohybu. Rovněž všechny zkoumané aplikace pro telefony, do kterých se dají stahovat údaje, umožňovaly zobrazení dat po hodinách, takže po propojení

s účtem by mělo být možné zachytit podrobný pohybový profil osoby. Toto bohužel není ve většině případů možné přímo z hodinek.

V případě, že osoba měla spuštěnou aktivitu a víme přesně počet ujitých kroků, lze odhadnout vzdálenost, kterou během této aktivity urazila i bez jakýchkoliv dalších údajů. Tento údaj nicméně nebude příliš přesný – závisí na celé řadě faktorů, například zdravotním stavu a fyzické stavbě nositele hodinek. O něco přesnější budou údaje z GPS trackeru, pokud jsou jím hodinky vybaveny.

6.4.3 Experimentální zajištění údajů v terénu

Vraťme se nyní k původnímu scénáři. Zadání zní:

Hlídka při pochůzce přijala ohlášení z operačního střediska tísňové linky, aby zkontrolovala hlášení o ženě sedící bez hnutí na lavičce v potrhaných šatech. Při příchodu si hlídka všimla krve na těle ženy a vyhodnotila, že bude nezbytné přivolat také sanitku a kriminalistického technika, který by posoudil věcné důkazy, které se mohou na místě nacházet. Všimli si také, že žena má na zápěstí chytré hodinky, a technika o této skutečnosti informovali.

Vzhledem k povaze práce se nyní nebudeme zabývat zajištěním dalších stop a zaměříme se čistě na údaje získatelné ze zmíněných chytrých hodinek. Pro experiment budeme předpokládat, že jde o hodinky Samsung Gear S3 Frontier, zejména proto, abychom následně mohli v experimentu pokračovat laboratorním vytěžením podle Bećirovićové a Mrdoviće [23].

V první řadě hodinky nesundáváme ze zápěstí oběti. Pro odečtení kroků stačí oběť požádat, aby s rukou pohnula, čímž se objeví výchozí displej. Velká část displejů dostupných na trhu má krokoměr rovnou na hlavní obrazovce. Z té také odečteme čas hodinek, který je důležitý pro další analýzu.

Pootočením lunety hodinek se dostaneme k dalším údajům. Tyto hodinky mají tepový graf, můžeme nicméně měření provést ručně a hodnotu vyfotit. Zobrazí se také srovnání s obvyklou hodnotou zaznamenanou pro daného uživatele. To může být užitečné pro zjištění míry stresu, které je oběť aktuálně vystavena. Hodinky nenabízí komplexní měření stresu, můžeme tedy vycházet pouze z tepové frekvence. Ve výchozím stavu probíhá měření pouze ručně, ale je možné zapnout i kontinuální měření v určitých intervalech (1 minuta, 10 minut, hodina).

Obdobně zkusíme zjistit, jestli oběť nemá běžící aktivitu. Ty se na hodinkách dají nastavit na automatické zapnutí při překročení určité tepové frekvence, takže přítomnost aktivity může indikovat, že je oběť určitou dobu ve stresu, jelikož zvýšení srdečního tepu je přirozenou stresovou reakcí.

Další měření je již možné provést i v laboratoři, hodinky tedy můžeme sejmout. Předtím nesmíme zapomenout nafotit veškeré výše zmíněné údaje – kroky, tep, přítomnost aktivity.

Pokud oběť nemá u sebe mobilní telefon nebo si není jistá, kde se telefon nachází, můžeme využít hodinky k jeho aktivaci a prozvonění pomocí funkce Najít můj telefon. Tyto hodinky nicméně nenabízí funkci odemknutí telefonu při přiblížení hodinek (tato funkce je k dispozici pouze u modelů čínské značky XiaoMi), takže nepomůže při zajišťování důkazů z telefonu přímo na místě.

Zjištění shrneme do protokolu o provedení obhlídky osoby, který tvoří přílohu č. 4 této práce. V něm stanovíme odborné otázky pro zodpovězení znaleckým pracovištěm, kterému hodinky předáme k další analýze.

V případě OS Tizen (chytré hodinky výrobce Samsung) můžeme navíc zajistit data z hodinek již v terénu. Musíme hodinky přepnout do ladicího módu – obvykle k nalezení v nabídce Nastavení, následně je restartovat a počkat, až získají IP adresu. Poté se připojíme ke stejné síti, ve které jsou hodinky (může jít i o ad hoc Wi-Fi síť poskytnutou naším počítačem) a pomocí vhodného akvizičního skriptu provedeme zajištění dat a jejich verifikaci prostřednictvím vhodného hashového algoritmu. Pokud bude tento postup úspěšný, není nutné hodinky fyzicky brát do laboratoře.

6.4.4 Dokončení analýzy hodinek v laboratoři

Po zajištění hodinek můžeme pokračovat v datové analýze. V závislosti na typu hodinek je provedení buď snadné (hodinky s operačním systémem Tizen), vyžaduje specifické nástroje (Garmin a jeho proprietární systém), případně může být nemožné (XiaoMi a jejich hodinky vyžadují speciální SW, který lze získat pouze v Číně).

Pro účely této práce jsme využili hodinky s OS Tizen. Praktická část zajištění proběhne již v terénu, výsledkem je kopie souborového systému včetně zachování stromové struktury. Hodinky byly zajištěny postupem, který byl navržen pro tento druh akvizice v roce 2015 [23]. Pro ověření univerzálnosti postupu jsme provedli experiment se dvojími hodinkami – v prvním případě se jednalo o stejný model, který

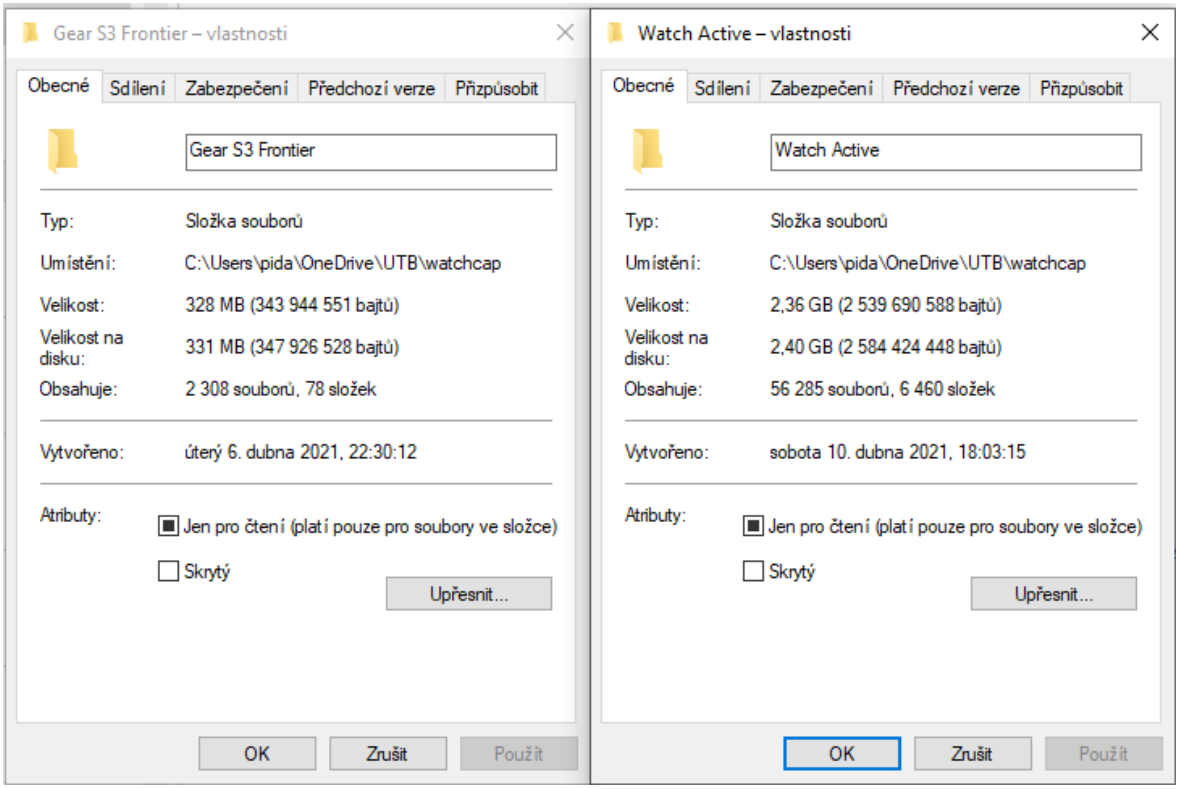
použil předchozí tým, tedy *Samsung Gear S3 Frontier*, a druhé hodinky byly novější: model *Samsung Watch Active*.

Pro účely akvizice jsme se do hodinek nejprve připojili přes SSH konzoli a do souboru nechali spočítat otisk všech souborů ve všech adresářích. Zároveň jsme nechali vytvořit strom adresářové struktury a uložili jej do souboru. Při tomto procesu nebyla porušena integrita žádných dalších souborů na hodinkách – první krok pouze soubor přebírá jako vstup a nemanipuluje s ním, druhý krok pracuje pouze s adresáři a soubory neřeší. Rovněž kopírování pomocí příkazu *sdb pull* nemění informace o souboru v původním zařízení.

Následně byl použit skript v jazyce PowerShell, který jednotlivé soubory včetně seznamu otisků a popisu adresářové struktury přenesl z hodinek bezdrátovým přenosem do forenzního počítače, a to rekurzivně pro celý disk. Vytvoření obrazu například pomocí nástroje DD nebo FTK bránil fakt, že disk hodinek byl příliš plný a bez root přístupu nebylo ani možné nástroje dohrát – program DD se v OS Tizen ve výchozím nastavení nenachází.

Nález z hodinek *Samsung Gear S3 Frontier* víceméně odpovídal zjištěním v původní analýze. Některé zmiňované soubory se přenést nepodařilo, hodinky totiž trpěly opakovanými výpadky komunikace. Důvodem mohl být rozdíl v použité verzi nástroje SDB a OS Tizen v hodinkách. V zařízení *Samsung Watch Active* už se nachází verze OS Tizen, která byla konzolí podporována. To může být důvodem, proč se podařilo zajistit téměř kompletní obraz disku, včetně výpisu stránkovacích souborů běžících procesů, s výjimkou systémových adresářů vlastněných uživatelem *root*. Srovnání výsledků aplikace postupu na obě zařízení najdeme na obrázku 6. Při přenosů dat ze zařízení *Frontier* došlo podle nástroje WireShark k většímu množství chyb, také aplikace Tizen Studio na sledování stavu logu hodinek hlásila přenosové chyby. Kromě nevhodné verze používaných nástrojů je to možné přičíst také věku hodinek – model *S3 Frontier* se například v obchodě CZC.cz nabízel od 26. 10. 2016, zatímco novější *Watch Active* jsou nabízeny až od 12. 2. 2019, tedy jsou o dva a půl roku mladší. Tomu odpovídá i verze OS Tizen – *Frontier* mají verzi 4.0.0, zatímco

Watch Active používají verzi 5.5.0.1 – to může rovněž hrát roli v množství zajistitelných dat, jelikož jsme použili nejnovější verzi SDK.



Obrázek 5 – Srovnání objemu zajištěných dat z hodinek Samsung Gear S3 Frontier (vlevo) a Samsung Watch Active (vpravo)

Z novějších hodinek se dalo zajistit velké množství databází, které obsahovaly různé konfigurační údaje i údaje o uživateli, který hodinky používá. Seznam SQLite souborů, které obsahovaly pro účely analýzy relevantní informace, se víceméně shodoval s výstupem z analýzy předcházejících autorů.

6.5 Souhrnný přehled vypracovaných protokolů

Ke každému praktickému experimentu byly vypracovány v souladu s metodikou odpovídající protokoly – *Protokol o ohledání místa činu* a/nebo *Znalecká zpráva*. Veškeré dokumenty byly vypracovány podle postupů a informací pro tento druh činnosti popsaných v učebnici pro bezpečnostní pracovníky a zájemce o práci v bezpečnostních sborech, kterou využívá Střední odborná škola ochrany osob a majetku s. r. o. [29]. Znalecké posudky navíc budou vypracovány s ohledem na příslušné předpisy, zejména zákon 254/2019 Sb., o znalcích, znaleckých kancelářích

a znaleckých ústavech a jeho prováděcí vyhlášku 503/2020 Sb., o výkonu znalecké činnosti. Z etických a legislativních důvodů ovšem bude v dokumentech vynechána znalecká pečeť a další prvky, jejichž použití podmiňuje zákon složením příslušné znalecké zkoušky nebo zápisem do seznamu znalců.

Přehled jednotlivých čísel protokolů s jejich identifikací je uveden v tabulce 3 a dále v seznamu příloh této práce.

Tabulka 3 – Seznam protokolů v přílohách

Případ	Ohledací protokol	Znalecký protokol
C-ITS systém	-	Příloha 2
Webkamera a router	Příloha 3	Příloha 4
Hodinky	Příloha 5	Příloha 6

Jak je z této tabulky patrné, pro každý prakticky analyzovaný případ kromě C-ITS systému vytvoříme oba protokoly – záznam o ohledání fiktivního místa činu a znaleckou zprávu, která bude obsahovat záznam o laboratorním ohledání zajištěných důkazů. Abychom dodrželi posloupnost vycházející z kriminalistické praxe, jak je popsána v učebnici [29], budou součástí ohledacího protokolu doplňkové otázky pro zodpovězení znaleckým šetřením. Další metody kriminalistického vyšetřování diskutované výše v této práci v protokolech pouze zmíníme jako možný zdroj dalších dat pro možné vyšetřování a nebudeme se jimi zabývat do větší hloubky.

7 SOUHRNNÁ METODIKA SBĚRU DIGITÁLNÍCH STOP

Během celého postupu zajišťování digitálních stop je zapotřebí mít na paměti základní zásady kriminalistické práce v terénu. V praxi to znamená postupovat tak, abychom před každým krokem, který může ovlivnit nějaké místo nebo informace, které z něj lze vytěžit, měli příslušnou dokumentaci a měli jistotu, že jsme dalším postupem získali více informací, než potenciálně riskujeme.

Musíme mít na paměti, že pořizujeme kriminalistickou dokumentaci, zejména v případě ohledání na místě činu, to znamená takovou dokumentaci, která splňuje všechny náležitosti příslušných předpisů. Z hlediska IT se musíme zaměřit na nedestruktivní metody a získávání údajů takovým způsobem, kterým neohrozíme autenticitu zajišťovaných dat, kde je to jen trochu možné.

Z logických důvodů se práce v metodice zaměřuje pouze na akvizici digitálních stop, nikoliv na celý proces ohledání zájmové oblasti. Pro vytvoření izolované metodiky operačního postupu vynecháváme zajištění jiných důkazů, jako jsou daktyloskopické, biologické nebo mechanické stopy. Jejich zajištění považujeme za vhodné mezi prohlídkou kybernetického prostoru, případně během ní a rozhodně je nutné jej udělat před zajišťováním jednotlivých obrazovek zařízení s dotykovým displejem nebo jiným ovládacím prvkem, jelikož tato manipulace může nedigitální stopy ohrozit.

7.1 Zajištění objektů a areálů

7.1.1 Průzkum kybernetického prostoru

Ohledání kybernetického prostoru tedy může začít až ve chvíli, kdy máme zajištěny všechny fyzické stopy, jelikož se dá předpokládat manipulace s různými objekty. Pokud je předmětem technického zkoumání oblast nebo budova, zahajujeme prohlídku skenem dostupných rádiových pásem, zejména se zřetelem na pásma 2,4 GHz (Bluetooth a Wi-Fi), 5 GHz (Wi-Fi) a pro jistotu, pokud je to vzhledem k časovým možnostem proveditelné, také pásmo 3,8 GHz – komunikační pásmo používané pro americké SCADA a back-end přenosové systémy.

Na těchto pásmech musíme projít všechny dostupné frekvence a kanály, nejlépe pomocí vhodného skenovacího nástroje, který zachytí informace o všech sítích nacházejících se ve zkoumaném rádiovém prostoru i tehdy, pokud nevysílají SSID. Měli bychom mít k dispozici tabulku, do které zjištění zapíšeme pro použití v dalších krocích postupu. Tato tabulka tvoří první část výstupního ohledacího protokolu.

Jakmile zjistíme informace o aktivně využívaných kanálech a sítích, zkusíme se zaměřit na zařízení, která by mohla tyto sítě využívat. Pokud je to možné, najdeme přístupový bod a přihlásíme se na něj, nebo k němu získáme přístup pomocí servisního hesla. Z něj vypíšeme MAC adresy aktivních zařízení, a je-li to možné, stáhneme i historii DHCP protokolu, případně adresační tabulku. Tím získáme aktuální IP adresy, spárované s příslušnými MAC adresami. Tyto uchováme v souborech na technickém počítači, které opatříme hashem. Název souboru i kontrolní otisk opíšeme do protokolu jako druhou část výstupu z ohledání.

7.1.2 Identifikace konkrétních zařízení

Následně musíme najít konkrétní zařízení. U počítačů, laptopů, mobilních telefonů a infrastrukturních prvků je situace jasná. Horší je identifikace IoT zařízení. Projdeme s tabulkou všechna známá zařízení, a pokud nám zbývají nějaká neznámá, musíme uvažovat přítomnost IoT prvků. Začneme opět od těch největších – automobily, poté chytré spotřebiče včetně cvičební výbavy, televizí a kuchyňských zařízení, chytrá světla. Pokud stále zbývají nepřiřazené MAC adresy, hledáme hodinky nebo chytré náramky.

Každé nalezené zařízení nafotíme ihned, jakmile jej označíme za potenciální IoT zařízení, obhlédneme fyzické stopy, případně na ovládacím displeji zkusíme daktyloskopickou analýzu. Následně zařízení aktivujeme, a pokud není zamčené, zkusíme z jeho nastavení ověřit MAC adresu podle seznamu. Fotíme přitom údaje, které zařízení poskytuje – čas, údaje senzorů, každou obrazovku, kterou procházíme při hledání IP adresy a konečně vyfotíme i nalezenou IP a MAC adresu.

Jakmile projdeme všechna očekávatelná zařízení, mohou nastat tři případy:

1) Tabulka z AP sedí s nalezenými zařízeními – tato část obhlídky je hotová, do tabulky doplníme typ zařízení a další údaje (např. výrobce) a zaneseme jako část protokolu.
2) V tabulce přebývají řádky – chybí zařízení, která musíme dohledat, případně se znovu připojit na router a zjistit, jestli zařízení nemá být na místě přítomné a neschází, například zda se nedávno neodpojilo ze sítě a není jen stále v DHCP lease tabulce nebo v tabulce stálých adres. Zejména pokud je zařízení v tabulce stálých adres, může se jednat o indikátor odcizení zařízení.
3) Nalezli jsme více zařízení, než odpovídá tabulce – buď některé zařízení nevyužívá v danou chvíli Wi-Fi, nebo je v okolí více než jedna přístupná síť. V obou případech se nemusíme vracet k zařízení, stačí projít pořízenou fotodokumentaci a měli bychom být schopní z některé obrazovky zjistit, k jaké síti bylo zařízení právě připojeno. Pokud síť nenajdeme, je možné, že má skryté SSID. V takovém případě jdeme na místo, kde jsme zařízení fyzicky nalezli, a provedeme sken dostupných Wi-Fi sítí vhodným nástrojem.

Tím je tabulka zařízení pro ohledací protokol kompletní. V této tabulce budou nicméně jen zařízení využívající nebo poskytující Wi-Fi sítě.

Další kroky jsou stejné pro obě části metodiky a pro přehlednost jsou uvedeny v oddíle 7.2 zvlášť.

7.1.3 Dodatková relevantní pásma v kyberprostoru EU

V tomto kroku můžeme volitelně opakovat průzkum objektu, tentokrát ovšem se zaměříme na frekvenční rozsahy mobilních sítí. V evropském prostředí by šlo zejména o rozsahy:

- 824–896 MHz (telefonní sítě první až třetí generace)
- 890–960 MHz (evropské GSM sítě třetí generace)
- 1710–1785 MHz a 1805–1880 MHz (průmyslové sítě DCS)
- 1850–1990 MHz (LTE sítě)
- 2,5–2,7 GHz (WiMax a Clear 4G sítě)

Pokud jsou na místě přítomná vozidla, tak ještě pásmo 5,9 GHz, kde se nachází sítě pro technologii C-ITS.

Takto rozsáhlým skenem bychom odhalili všechna zbývající zařízení, avšak v praxi nebude obvykle nezbytné jej provádět. Využijeme jej zejména v průmyslovém prostředí, kde jím můžeme odhalit potenciální kamerové systémy nebo jiné zdroje dat. Další kroky jsou stejné pro obě části metodiky a pro přehlednost jsou uvedeny v oddíle 7.3 zvlášť.

7.2 Zajištění osob, kontejnerů a vozidel

V tomto případě nemáme k dispozici žádnou infrastrukturu, kterou bychom museli řešit. Jediným nositelem důkazů jsou samostatně působící systémy s maximálně GSM konektivitou.

Metodicky začneme ohledání místa zdokumentováním aktuálního stavu v momentě nálezu. V případě osob sledujeme primárně chytré hodinky nebo jiný tracker s vestavěným displejem. U hodinek se díváme, jestli se dají odemknout, nebo ne. Pokud je toho ohledávaná osoba schopna a hodinky jsou zamčené, požádáme ji o jejich odemknutí. V opačném případě se můžeme pokusit hodinky odemknout, avšak jde o velice pracnou záležitost, takže hodinky spíše nafotíme včetně zamykací obrazovky a poté předáme do laboratoře k prolomení.

Pokud se ovšem do hodinek dostaneme, postupujeme obdobně jako u jiných chytrých zařízení. Snažíme se je projít obrazovku po obrazovce a zjistit co největší množství dat. Zaměřujeme se přitom na zaznamenaný počet kroků, aktuální tepovou frekvenci oběti (může být užitečné také tehdy, pokud na místo voláme záchranku, nebo pro koronera, pokud jde o oběť vraždy – oběť může stále mít v hodinkách tepový graf nebo podrobný záznam, který nás může přivést k upřesnění doby smrti. Například chytré hodinky s OS Tizen zaznamenávají tep každých deset vteřin, hodinky Garmin ještě častěji, proto je zajištění chytrých hodinek v takovémto případě velmi důležité. Chytré náramky Xiaomi MiBand sice měří tep každých deset minut i v klidovém stavu, ale tato měření nezobrazují a vytěžení hodinek technickým způsobem je mimo

území Čínské lidové republiky nemožné. Z tohoto důvodu alespoň opíšeme aktuální tep a hodinky můžeme oběti ponechat.

Další významné obrazovky mohou být záznam o probíhající aktivitě, historie hovorů nebo zpráv, případně informace o poloze a její historii.

Pokud má u sebe oběť hodinky s OS Tizen nebo Garmin WatchOS, zkusíme na místě zajistit kompletní obraz datových důkazů. V případě Tizenu stačí oběť požádat, aby hodinky technikovi na pár minut odemkla a půjčila. Technik si udělá na svém zařízení Wi-Fi hotspot, ke kterému hodinky připojí, přepne je do servisního módu a v tu chvíli je oběti může vrátit – během stahování dat se hodinky sice více zahřívají, ale jinak je možné je klidně používat.

Můžeme také provést fotografickou dokumentaci přítomných zdravotních zařízení. Ačkoliv je interpretace dat v těchto zařízeních otázkou odborníků z příslušné oblasti, v principu není nemožná a může vést k užitečným závěrům například o předcházející aktivitě oběti. Některá takováto zařízení ovšem buď vůbec nemají paměť, nebo je těžké se do ní dostat. V žádném případě nemůžeme se zařízením manipulovat sami. Pokud oběť spolupracuje, můžeme ji požádat, aby nám historii záznamů například z glukometru inzulinové pumpy vyvolala sama a s jejím souhlasem si tyto údaje nafotit.

Nákladní vozidla mohou mít také svoje *fleet management* systémy, které nemusí nezbytně pracovat na bázi C-ITS. V takovém případě mívá vozidlo viditelně v kameře zařízení s dotykovou obrazovkou. To zajišťujeme obdobně jako C-ITS jednotku – zkusíme jej nastartovat a zjistit, jaké údaje jsme schopni zajistit jen procházením obrazovek. Tato zařízení ovšem mívají oproti C-ITS systémům tu výhodu, že mají vnitřní paměť. Odmontování, a tím fyzické zajištění takovéto jednotky jiným způsobem než nafocením ovšem v terénu nemusí být z bezpečnostních důvodů možné – jednotky bývají napojené přímo na elektroinstalaci vozu a neodborná manipulace může vést k jejich poškození nebo ke zničení dat, která se v nich nacházejí. Proto pokud není zařízení jednoznačně odpojitelné (například není připojené do 12V „cigaretového zapalovače“), zůstaneme při manipulaci s ním pro jistotu jen u zajištění fotodokumentace v zapnutém stavu.

V případě zajištění kontejnerů je situace trochu jiná. Jde o specifický případ SCADA systémů, které mívají poziční a senzorická zařízení. Pokud budeme kontejner důkladně obhlížet, dá se čekat, že bude mít ovládací jednotku. Alternativou je obhlídka obvyklých frekvenčních pásem pro SCADA a navigační systémy. V tomto případě tedy budeme postupovat přesně naopak než při obhlídce domu nebo oblasti. Primárně se zaměříme na frekvenční rozsahy mobilních sítí. V Evropském prostředí by šlo zejména o rozsahy:

- 824–896 MHz (telefonní sítě první až třetí generace)
- 890–960 MHz (evropské GSM sítě třetí generace)
- 1710–1785 MHz a 1805– 880 MHz (průmyslové sítě DCS)
- 1850–1990 MHz (LTE sítě)
- 2,5–2,7 GHz (WiMax a Clear 4G sítě)

Pokud jsou na místě přítomná vozidla, tak ještě pásmo 5,9GHz, kde se nachází sítě pro technologii C-ITS.

Tímto získáme rovněž informaci o velké části zařízení s GSM protokolem, která mohou být na místě přítomna. Za zmínku stojí v tomto ohledu ještě jedna varianta, a to aktivace palubní Wi-Fi zajišťovaného vozu (vybrané C-ITS jednotky poskytují Wi-Fi i v konzumním pásmu 5 GHz jako součást palubního zábavního systému, například pro streamování obsahu uloženého v úložišti vozu), pokud je dostupný, prostřednictvím jeho C-ITS jednotky místo technického hotspotu zásahového vozidla nebo notebooku. Nevýhodou je sice menší možnost sledování přenášených informací, výhodou je, že některá zařízení v okolí se na tuto síť mohou v takovém případě pokusit připojit automaticky, čímž technik získá výhodu v podobě zařízení důvěryhodného pro zajišťovaná zařízení. Takovéto párování může u některých bezpečnostních zařízení (chytré zámky, chytré závory, kamery) mít oproti zajištění cizí sítí výhodu, zejména pokud zařízení mají integrovaný IPS nebo IDS okruh, který slouží k aktivnímu odmítnutí připojení nedůvěryhodné sítě. V případě vestavěných prvků inteligentních budov, které jsou napojeny k centrálnímu panelu například technologií ZigBee, se nesoustředíme na tyto jednotlivé prvky, ale projdeme

důkladně údaje, které nám poskytuje panel. Obdobně v případě SCADA infrastruktury není obvykle nutné zajišťovat celý okruh, pokud se nám podaří dostat k řídicí jednotce. Pozor, že většina SCADA aplikací pro servery již data preparsuje a zpracovává, takže v porovnání se zajištěním v samotném kontroléru mohou být tyto důkazy zkreslené. Co ovšem můžeme udělat, je získat patřičným způsobem digitální důkazy na obou místech. Znalec je totiž v laboratoři poté schopen porovnat je se známým způsobem zpracování datových zpráv podle popisu komunikace od výrobce SCADA zařízení a zjistit případné nesrovnalosti, které mohou ukazovat na provedenou sabotáž například přehráním firmware.

Následně provedeme soupisku zajištěných zařízení. Bez infrastrukturního bodu nebo routeru, který bychom mohli zkontrolovat, nám zbývá jen provedení standardní fotodokumentace a zajištění jednotlivých zařízení ve fyzické podobě, je-li to možné. Další kroky jsou stejné pro obě části metodiky a pro přehlednost jsou uvedeny v oddíle 7.3 zvlášť.

7.3 Zajištění jednotlivých zařízení – společná část metodiky

Zařízení, která nemůžeme odstranit (podskupiny H2, S2, S3), zkusíme analyzovat alespoň z hlediska možností nejbližšího infrastrukturního prvku nebo serveru, na který jsou napojeny, a získat z nich a o nich informace tam. Prvky skupiny E má přitom smysl zajišťovat jen tehdy, pokud prokazatelně víme, že k nim jsou připojena zařízení bez vlastní vnitřní paměti, která jsou spojená přímo s Wi-Fi, a tedy je musíme v dalším kroku přenést do laboratoře k analýze provozu, jako například SOHO Wi-Fi kamery.

V případě chytrých hodinek musíme hodinky aktivovat a vyfotit všechna data, která jsou zjistitelná pouze s pomocí jejich displeje. U hodinek s OS Tizen (zjistíme ve volbě „nastavení“, podvolbě „o hodinkách“ položka „software“ nebo „systém“) zapneme ladicí mód, hodinky přepneme do „Always On“ Wi-Fi módu a restartujeme je. Tím odemkneme ladicí konzoli. Po naběhnutí z restartu zjistíme a vyfotíme IP adresu, kterou hodinky obdržely.

U všech zařízení, která umožňují získání logů připojením přes SSH, PowerShell nebo jinou vzdálenou konzoli (například výše zmíněné chytré hodinky s OS Tizen, vybrané routery atd.), provedeme zkopírování obsahu zařízení do technického počítače vhodným způsobem a se zařízením v této fázi dále nemanipulujeme. Pokud zařízení umožňují fyzické připojení, rovněž se pokusíme připojit a data stáhnout, a to s ponecháním zařízení co nejblíže jejich původní pozici. Toto platí zejména pro chytré hodinky (např. výrobce Garmin), sporttestery a další obdobná zařízení.

Zbývající zařízení, která jsme schopni zajistit a mohou být relevantní pro další laboratorní testy, vhodným způsobem připravíme k přepravě. Chytré hodinky a podobná zařízení, z kterých jsme extrahovali data již na místě, nemusíme zajistit nezbytně – laboratorně lze analyzovat i pouze zachycená data – nicméně pokud je to možné, zajistíme je také.

O každém zajištěném zařízení poznamenáme do protokolu, jaké části fotodokumentace se vztahují k jeho zajištění, jaké datové stopy z něj byly získány (jednotlivé soubory / souborový systém / image disku) a zapíšeme do protokolu včetně uložení souboru s kontrolními otisky nebo kontrolního otisku zajištěného image. Vzhledem ke specifické povaze některých souborů nelze doporučit kompresi a následné vytvoření otisku, nicméně pro počítání otisků rozsáhlejších složek lze využít například vytvoření souboru s jednotlivými otisky, jehož otisk následně opíšeme do protokolu. V jazyce Powershell by šlo o následující sekvenci příkazů:

```
Get-ChildItem -Recurse "<ADRESÁŘ SE ZÍSKANÝMI SOUBORY>" | Get-FileHash | Out-File "<SOUBOR S OTISKY ZÍSKANÝCH SOUBORŮ>"
```

```
Get-FileHash "<SOUBOR S OTISKY ZÍSKANÝCH SOUBORŮ>" | Out-File "<SOUBOR S HLAVNÍM OTISKEM>"
```

Díky tomuto postupu je možné ověřit nejen jednotlivé zajištěné soubory, ale také integritu všech získaných hashů způsobem, který umožňuje do protokolu nezapisovat všechny otisky získaných souborů – může totiž jít až o desítky tisíc artefaktů. Další výhoda je, že opakováním celé sekvence velmi snadno získáme ověřovací hash, kterým zjistíme, zda nebylo se soubory dále manipulováno.

Souhrnné informace o počtu a povaze zajištěných zařízení, výsledky prvotní analýzy datových artefaktů a soupisku fotek zaneseme do protokolu. Tím je obhlídka digitálního prostoru na místě hotova.

ZÁVĚR

V práci jsme nejprve stanovili teoretický rámec, který je nezbytné dodržet pro účely akvizice a zpracování digitálních důkazů obecně. Následně jsme jej obohatili o specifika pro systémy IoT a chytrá zařízení. Tím jsme získali teoretický rámec pro následující analýzu.

Pomocí metodiky rozdělení IoT zařízení, kterou využívá Blinowski, jsme dále získali několik různých teoretických scénářů pro zajištění digitálních stop v různých druzích systémů. U každého systému jsme diskutovali možnosti a způsob zajištění dat, která se v něm mohou nacházet. Na konci teoretického diskurzu jsme stanovili v teoretické rovině aplikovatelné metodiky pro zajištění digitálních důkazů v jednotlivých typech těchto zařízení, opět podle Blinowského metodiky.

V praktické části jsme tři vybrané scénáře ověřili a dále popsali včetně kroků, které nebyly jasné z teoretického podchycení metodiky postupů, ale vyplynuly dále z praktických poznatků získaných při experimentech. Čtvrtý scénář byl navržen, ale jeho ověření nebylo možné vzhledem k pandemické situaci, která v Evropě v době psaní diplomové práce panovala.

V rámci praktických pokusů jsme identifikovali společné kroky a společné části postupu, které se pro jednotlivá zařízení neliší, nebo se liší jen velmi málo. Analýzou těchto společných míst jsme potom navrhli metodiku pro řešení problematických oblastí i celkových postupů akvizice IoT zařízení na základě běžných policejních scénářů – zajištění objektu a zajištění osoby či vozidla. Metodický výstup přitom vychází z existujících metodik Evropské agentury pro kybernetickou bezpečnosti (ENISA), která vydává metodiky pro zacházení s digitálními důkazy.

Práce prokázala, že i méně obvyklá IoT zařízení mohou obsahovat relevantní materiály v podobě unikátních digitálních důkazů a že jejich správné zajištění na místě i následná analýza v laboratoři mohou přinést významné výsledky a přispět k objasnění některých aspektů trestné činnosti, a to nejen u násilné kriminality.

Některá témata bohužel nebylo možné v práci dostatečně prozkoumat. Práce tak nabízí prostor pro další bohatý výzkum například v oblasti řídicích systémů chytrých

budov, které jsou jen zmíněny jako potenciální zdroj důkazů. Není to ovšem jediné téma, na které se lze zaměřit. Například klasifikace profesora Blinowskeho je založená na strojovém učení, části zajišťovacího postupu zahrnují využití jednoduchých přístrojů. Je tedy otázka, jestli by alespoň určité části, jako ohledání kybernetického prostoru, nebylo možné automatizovat a za tímto účelem například vyvinout aplikaci nebo zařízení, které by samostatně analyzovalo kybernetický prostor objektu a vrátilo nejpravděpodobnější seznam zařízení, která se v něm aktuálně mohou nacházet podle zjištěných informací.

SEZNAM POUŽITÉ LITERATURY

[1] **POLČÁK, Radim, PÚRY, František a HARAŠTA, Jakub.** *Elektronická důkazy v trestním řízení.* Brno : Masarykova univerzita, 2015. 978-80-210-8073-7.

[2] **KOLOUCH, Jan.** *Cybercrime.* Praha : CZ.NIC, 2016. 978-80-88168-18-8.

[3] **JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef.** *Výkladový slovník kybernetické bezpenčosti.* Praha : Policejní akademie ČR v Praze a česká pobočka AFCEA , 2013.

[4] **VYSKOČIL, Ladislav.** *Zajišťování a analýza digitálních důkazů.* Fakulta aplikované informatiky. Zlín : Univerzita Tomáše Bati ve Zlíně, 2013.

[5] **BENJAMIN, Bob.** *Communication Methods for Data Integrity Using DeltaSigma Data Converters.* Dallas : Texas Instruments, 2020.

[6] **DUBROVA, Elena, a další.** *Cryptographically Secure CRC for Lightweight.* Stockholm : Royal Institute of Technology, 2015.

[7] **International Telecomunications Union.** *SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS.* Ženeva : Mezinárodní telekomunikační unie, 2012.

[8] **WEISSMANOVÁ, Valentýna.** *Internet věcí – kultura sdílení v době nových médií.* Brno : Masarykova univerzita v Brně, 2019.

[9] *Requirements for IoT forensics.* **KRUGER, Jaco-Louis a VENTER, Hein.** Mauritius : IEEE, 2019. Sv. 2. 978-1-7281-1460-6.

[10] **BLINOWSKI, Grzegorz a PIOTROWSKI, Pavel.** *CVE based classification of vulnerable IoT systems* . [online] Warszawa : Warszav University of Technology, 2020.

[11] **Český statistický úřad.** *Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci - 2019.* [editor] Ing. Lenka Weichetová. Praha : Český statistický úřad, 2019. Kód publikace: 062004-19.

[12] **ARRIBA-PÉREZ, de, Francisco, CAEIRO-RODRÍGUEZ, Manuel a SANTOS-GAGO, Juan Manuel.** Collection and Processing of Data from Wrist Wearable Devices in Heterogeneous and Multiple-User Scenarios. *Sensors.* 21. Sep. 2016, Sv. 16, 1538.

[13] **Ministerstvo dopravy České republiky.** C-ROADS CZ: Specifikace systému. *C-ROADS Czech Republic.* [Online] 12 2018. [Citace: 13. únor 2021.] https://c-roads.cz/croads/wp-content/uploads/2019/11/C-Roads_CZ_System_specs_v1.5.pdf.

[14] **ALSHALAWI, Reem M. a ALGHAMDI, Turki Ali.** Forensic Tool for Wireless Surveillance Camera. *ICACT.* 2017, Feb. 19-22, 2017.

[15] **RIJSBERGEN, Kenneth, von.** *The effectiveness of a homemade IMSI catcher build with YateBTS and a BladeRF.* místo neznámé : Semantic Scholar, 2016. Corpus ID: 36320400.

[16] **CHUNG, Hyunji, PARK, Jungheum a LEE, Sangjin.** Digital forensic approaches for Amazon Alexa ecosystem. *Digital Investigation.* ScienceDirect, August 2017, Sv. 22, August 2017.

[17] **VLIET, Pieter, Van, KECHADI, M-T. a LE-KHAC, Nhien-An.** Forensics in Industrial Control System: A Case Study. *Arxiv.org.* [Online] 2016. Listopad 2016. [Citace: 20. Únor 2021.] https://arxiv.org/abs/1611.01754. arXiv:1611.01754.

[18] **DAMIRIS, Giorgos Paraskevas.** Router Forensics. Piraeus, Řecko : Univerzity of Piraeus, 2020. Vedoucí práce: Professor Costas Lambrinoudakis.

[19] **FAHD, Shah, a další.** Integrated Model : Statistical Features, Memory Analysis for scanner and Printer Forensics. *4th International Symposium on Digital Forensics and Security.* ISFSDS, 2016, 16.

[20] **ŠALATA, Martin.** Cloud and on-premise deployment. Brno : Masarykova Univerzita - Fakulta informatiky, 2018. Vedoucí práce: Mgr. Juraj Michálek.

[21] **SADIQ, Muhammad, a další.** MOBILE DEVICES FORENSICS INVESTIGATION: PROCESS MODELS. *International Scientific Journal.* Philadelphia : Thomson Reuters, 2016. Sv. 33, 1. p-ISSN: 2308-4944 (print) / e-ISSN: 2409-0085 (online).

[22] **KANG, Serim, KIM, Soram a KIM, Jongsung.** Forensic analysis for IoT fitness trackers and its application. *Peer-to-Peer Networking and Applications.* 2020, Sv. 13, 2, stránky 564-573.

[23] **BECIROVIC, Seila a MRDOVIC, Sasa.** Manual IoT Forensics of a Samsung Gear S3 Frontier Smartwatch. *Telecommunications and Computer Networks (SoftCOM).* Telecommunications and Computer Networks (SoftCOM), 2019, Sv. 2019.

[24] *EMC for the IoT.* **MYNSTER, Anders P. a JENSEN, Per Thåstrup.** Wroclaw : DELTA - Danish Electronics, Light and Acoustic, 2016. Proc. of the 2016 International Symposium on Electromagnetic Compatibility -. ISBN 978-1-5090-1416-3.

[25] **Pracovní skupina WG 2.1 projektu C-ROADS CZ.** *Specifikace systému: Release 1.0 - Obecná architektura.* [online] Praha : C-Roads Czech republic, 2017.

[26] **JIRÁK, Jakub.** *NÁVRH SYSTÉMU KONTROLY KVALITY KOOPERATIVNÍCH SYSTÉMŮ.* Praha : České vysoké učení technické, 2018. Vedoucí práce doc. Ing. Zdeněk Lokaj, Ph.D..

[27] **SIIRTOLA, Pekka.** UbiComp/ISWC '19 Adjunct: Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers. *Adjunct Proceedings of the 2019.* Září 2019, stránky 1198–1201.

[28] *How accurate is accurate enough? - An Evaluation of Commercial Fitness Trackers for Individual Health Management.* **WITTE, Anne-Katrin, a další.** Cancún : Americas Conference on Information Systems, 2019.

[29] **VICHLENDA, Milan.** *Kriminalistika.* Karviná : Střední odborná škola ochrany osob a majetku s.r.o., 2011.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

C-ITS: City – Intelligent Transport System

DCS: Distributed Control System

EMC: Electromagnetic Compatibility

GPS: Global Positioning System

GSM: Groupe Spécial Mobile

ICS: Industrial Control System

IDS: Intrusion Detection System

IEEE: Institute of Electrical and Electronics Engineers

IoT: Internet of Things

IP: Internet Protocol

IPS: Intrusion Prevention System

LDAP: Lightweight Directory Access Protocol

LTE: Long-Term Evolution

MAC: Mandatory Access Control

OS: Operating System

PoE: Power over Ethernet

RFC: Request for Comments

RSU: Road-Side Unit

SCADA: Supervisory Control and Data Acquisition

SOHO: Small Office / Home Office

SSH: Secure Shell

Wi-Fi: Wireless Fidelity

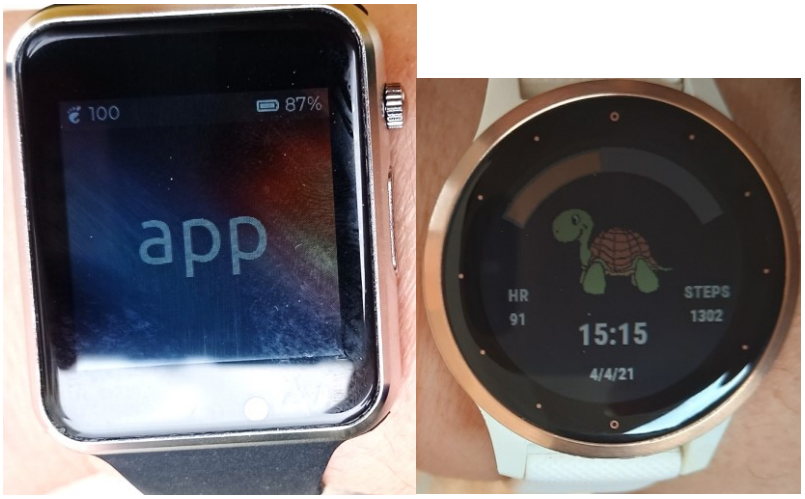
SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

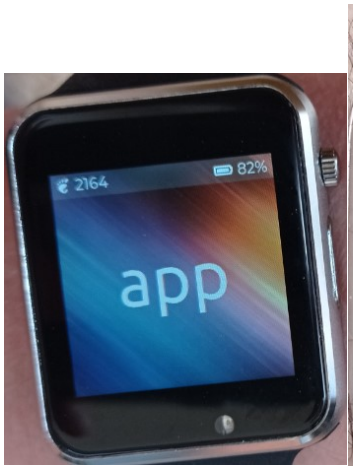
PŘÍLOHA P I: FOTOGRAFIE ZE SMARTWATCH ZAŘÍZENÍ

Fotografie z výchozího bodu cesty se stavem kroků při vyjití. Shoa z leva: Garmin Vívomove, Samsung Gear S3 Frontier, MiBand 4, LillyGo T Watch 2020, Garmin Vívoactive 4S, Samsung Active Watch 2, MiBand2, Garmin Vívomove HR



Fotografie z poloviny ujité vzdálenosti, kontrolní bod 1. Zleva shora: Garmin Vívoactive 4S, MiBand 2, Garmin Vívoactive HR, Samsung Gear S3 Frontier, LillyGo T Watch 2020, Samsung Active Watch 2, MiBand 4, Garmin Vívoactive HR

Fotografie z konce cesty, kontrolní bod 2. Zleva shora: Garmin Vívoactive 4S, MiBand 2, Samsung Active Watch 2, Garmin Vívoactive HR, LillyGo T Watch 2020, MiBand 4, Samsung Galaxy S3 Frontier



PŘÍLOHA P II: ZNALECKÝ POSUDEK C-ITS

ZNALECKÝ POSUDEK

Č. ev. 1113/2021

Vypracovává: Bc. František Sedláček

Zadavatel: Policie České republiky

Posudek byl zadán za účelem objasnění okolností události ze dne 8. 4. 2021 v místě Brno v souvislosti s vyšetřováním nálezu zmatené ženy.

Předmětem tohoto posudku je analýza záznamů z C-ITS jednotek infrastruktury a vozidel v rámci šetření nálezu odstaveného vozidla.

Vypracován byl v oboru *kybernetika a informační technologie* dne 28. 4. 2021.

Vypracoval: Bc. František Sedláček Za zadavatele: Ing. Kpt. Ladislav Vyskočil

Zadání znaleckého posudku

Otázky položené pro objasnění znaleckým posudkem (zadání znaleckého posudku):

Kudy se vozidlo před ostavením pohybovalo?

Odpovídala jeho rychlost a povaha pohybu typu vozidla a předpisům?

Nehlásilo vozidlo během provozu poruchu?

Tyto otázky mají být posudkem zodpovězeny pro účely stanovení kriminalistické teorie pro další šetření, které bude provádět Policie ČR v rámci řešení případu ev. č. KRPB-123457-15/PŘ-2021-123457-IO.

Zadavatel si není vědom žádné skutečnosti, která by mohla mít vliv na zpracování nebo přesnost závěrů tohoto znaleckého posudku.

Výčet předložených podkladů

Pro tento znalecký posudek byly předloženy následující podklady:

Záznam historie z palubní jednotky C-ITS systému vozidla ve formátu pcap získaný majitelem vozidla, společností *Technické sítě Brno, a.s.*

Záznam historie z infrastrukturních jednotek C-ITS systému v předpokládané trase vozidla ve formátu XML

Ověření a fixace autenticity digitálních podkladů

Následující digitální podklady byly pro účely analýzy ověřeny pomocí SHA-256:

Číslo a název	Soubor	Hash	Ověřeno
Záznam z palubní jednotky vozidla získaný ze servisního okruhu	Test4.pcapng	B4AD4FD3E7EF7EAFDE8598 9C1D64200602C51CC4F5B4D4 23A65EE6906177F599	Ano
XML záznam z první stanice infrastruktury v okolí místa nálezu	Nemoboh.xml	3D24EB474F80B9193839B7CE F0FAB1904F498F9E6C185295 0F9A66DC8FFC921C	Ano
XML záznam z tunelu C-Roads stanice Bohunice – Pisárky	TunelBohPis.xml	311E4B3C385A219161FC8AB8 06F93109FDCBBC6DF56833D 721F593601BB91DFD	Ano
XML záznam z C-Roads stanice křižovatka Kamenice – Jihlavská – Dlouhá	KrizJihlKamDlouha.xml	97DD9B9CD807A464DEB1EB 8982CA5F3674EAE5B5A0F73 BFB16A1410C4014A7BA	Ano

Analýza předložených podkladů

Z předloženého záznamu o vozidle vyplývá, že se v předmětné době pohybovalo po území města Brna. Vozidlo udává poslední pozice jako 491738881 šířky a 165741432 délky s nejasnou přesností (4095 v obou osách elipsy). Servisní záznam uložený C-ITS jednotkou poskytuje informace o posledních čtyřech minutách kdy bylo vozidlo v pohybu nebo zastavené, ale se zapnutým motorem. Tento záznam podrobíme nyní analýze.

Rychlost v době posledního vyslání CAM zprávy byla 0,03m/s a směr vůči azimutu 279,7 stupňů. Celkově tedy vozidlo ještě nebylo zastaveno, ale nepochybně provádělo zastavovací manévr.

Zprávě předcházelo přijetí DENM zprávy o průjezdu vozidla IZS, a to pouhou jednu vteřinu před zastavením. Jelikož zpráva je označena jako relevantní pouze v blízkosti do padesáti metrů od místa vzniku, dá se říct, že šlo o poměrně blízký kontakt obou vozidel (předjíždění / minutí). Z podobného směru vůči azimutu (285,4 stupně) lze usuzovat, že vozidlo IZS minulo sledovaný automobil předjížděním. Jeho poziční údaje bylo možné dekódovat na 49° 10’ 32,07‘‘ SŠ a 16° 34‘ 27,29‘‘ ZD. Tato pozice odpovídá pozici areálu Fakultní nemocnice Brno – Bohunice, za kterým (v kopci poblíž sídliště Netroufalky) bylo odstavené vozidlo nalezeno.

Poslední SID zajištěného vozidla nalezené v nejnovější CAM zprávě bylo 1599092108. Porovnáním tohoto SID se SID dostupnými na jednotlivých křižovatkách a zpětně porovnáním s DENM zprávami v logu vozidla bylo možné zjistit, že dne 8. 4. 2021 v čase 06:20:34 vozidlo bylo v pohybu a projelo křižovatkou Kamenice – Jihlavská – Dlouhá. Dále pokračovalo zřejmě už do místa, kde jej kriminalisté nalezli.

V čase 06:24:28 vozidlo zřejmě obdrželo DENM packet z dočasné C-Roads infrastrukturní jednotky umístěné za účelem rekonstrukce vozovky na souřadnicích 49° 11’ 45,74‘‘ SŠ a 16° 37‘ 03,75 ZD – záznam o průjezdu vozidla by mělo na této jednotce možné potvrdit.

První známá poloha vozidla podle sledovaného záznamu v jím vyslané CAM zprávě je 49° 10’ 34,93‘‘ SŠ a 16° 35‘ 28,68 ZD, nicméně tato souřadnice se nachází od ostatních potvrzených bodů ve vzdálenosti, kterou není během čtyř minut možné s tímto typem vozidla urazit.

Průchodem SPATEM zpráv a zaměřením se na ty, které nebyly vozidlem zamítnuty jako příliš vzdálené (neobsahují sekci *Intens CITS Rejected Capture Protocol*) bylo zjištěno, že vozidlo v čase 06:21:55 reagovalo na údaje o křižovatce Heršpická – Strážní a první sledovanou křižovatku projelo v čase 06:20:50 v místě Heršpická – Polní. Předtím vozidlo žádnou sledovanou křižovatkou neprojelo. Průzkum dat ze začátku záznamu nebyl průkazný, pozice se nepodařilo rozkódovat na žádnou pozici která by odpovídala předchozím údajům o známé a potvrzené poloze vozidla – data „skáčou“ od území MČ Brno – Židenice až po Vyškov u Brna.

Žádná ze zachycených CAM zpráv neobsahuje indikační příznaky poruchy ani žádné jiné informace, které by napovídaly tomu, že vozidlo v době zaznamenaného provozu mělo nějakou technickou závadu. Infrastrukturní údaje dodané z jednotlivých křižovatek (stanic systému C-Roads) v podobě agregovaných XML záznamů potvrzují, že vozidlo s odpovídajícím SID se pohybovalo po trase Heršpická-Jihlavská-Nemocnice Bohunice – Netroufalky a to v čase 6:20 až 6:25. Bez dalších záznamů z C-ITS jednotky ovšem není hlubší analýza možná.

Použitá SW platforma pro analýzu

WireShark platforma:

3.4.4 (v3.4.4-0-gc33f6306cbb2)

Compiled (64-bit) with Qt 5.15.1, with libpcap, with GLib 2.52.3, with zlib 1.2.11, with SMI 0.4.8, with c-ares 1.15.0, with Lua 5.2.4, with GnuTLS 3.6.3 and PKCS #11 support, with Gcrypt 1.8.3, with MIT Kerberos, with MaxMind DB resolver, with nghttp2 1.39.2, with brotli, with LZ4, with Zstandard, with Snappy, with libxml2 2.9.9, with QtMultimedia, with automatic updates using WinSparkle 0.5.7, with AirPcap, with SpeexDSP (using bundled resampler), with Minizip.

Running on 64-bit Windows 10 (2009), build 19043, with Intel(R) Core(TM) i5-6440HQ CPU @ 2.60GHz (with SSE4.2), with 16279 MB of physical memory, with
locale Czech_Czechia.utf8, with light display mode, without HiDPI, with Npcap version 1.10, based on libpcap version 1.9.1, with GnuTLS 3.6.3, with Gcrypt 1.8.3, with brotli 1.0.2, without AirPcap, binary plugins supported (21 loaded).

Built using Microsoft Visual Studio 2019 (VC++ 14.28, build 29910).

Platforma byla použita z oficiálních instalátorů bez dalších modifikací. Veškeré použité postupy byly aplikovány podle oficiální dokumentace výrobce.

Zodpovězení otázek ze zadání

K jednotlivým otázkám na základě provedené expertizy uvádím:

Kudy se vozidlo před ostavením pohybovalo?

Z analýzy palubní C-ITS jednotky a dodatkové analýzy C-Roads jednotek lze usoudit, že vozidlo se na odstavnou plochu, kde bylo nalezeno, dostalo z východu, a to po trase Heršpická-Jihlavská-Netroufalky, přičemž tuto trasu absolvovalo během 5ti minut v časovém úseku 6:20 – 6:24.

Odpovídala jeho rychlost a povaha pohybu typu vozidla a předpisům?

Ze zajištěného C-ITS protokolu vyplývá, že vozidlo jelo v souladu s dopravními předpisy a nepohybovalo se nepředvídaně ani nijak nevybočovalo ze stálého kurzu. Odchylky v C-ITS protokolech ve smyslu příliš rychlých změn pozice jsou mimo fyzikální možnosti sledovaného vozidla a odpovídají spíše nepřesnosti nebo špatné kalibraci GPS modulu C-ITS jednotky ve vozidle.

Nehlásilo vozidlo během provozu poruchu?

Žádná z C-ITS zpráv zachycených během posledních čtyř minut pohybu vozidla neobsahuje žádné sdělení o poruše nebo jiné sdělení, které by naznačovalo že by vozidlo mělo jakékoliv technické potíže.

K vypracování posudku nebyl pozván žádný další konzultant, posudek zpracoval znalec osobně a sám.

Odměna za vypracování znaleckého posudku byla stanovena v zákonné výši.

Znalecký posudek jsem podal jako znalec jmenovaný Okresním soudem Brno-Město ze dne 1.4.2021, pod č.j. *(nerel.)* v oboru *Kybernetika a informační technologie*.

Znalecký posudek byl zapsán pod poř. č. XXXX-YY/2021 znaleckého deníku.

Znalec dle § 127a občanského soudního řádu bere na vědomí povinnost oznámit skutečnosti, pro které by byl jako znalec vyloučen, nebo které by mu bránily být činný jako znalec.

Znalec rovněž prohlašuje, že si je vědom následků vědomě nepravdivého znaleckého posudku, zejména skutkové podstaty trestného činu Křivé výpovědi a nepravdivého znaleckého posudku dle § 346 trestního zákoníku.

PŘÍLOHA P III: OHLEDACÍ ZPRÁVA KAMERA

PROTOKOL O PROHLÍDCE

Ohledání provedl: Bc. František Sedláček, vyšetřovatel

Místo úkonu: Popice u Hustopečí

Čas úkonu: 2. 4. 2021 8:46

Předmět úkonu: Ohledání webkamery pro účely zajištění digitálních stop

Zajištěný předmět č. 1: Webkamera nezjištěného výrobce ani modelu, barva bílá s černou krytkou čočky. Bílá otáčivá základna, v zadní části kamery připojení pro mikroUSB napájecí konektor a anténa o délce cca. 7 cm. Mírně opotřebená, základna je zaprášená, kryt čočky lehce poškrábaný. Žádné viditelné sériové číslo ani jiný způsob jednoznačné identifikace.

Zajištěný předmět č. 2: Modem ZyXel, číslo modelu VMG1312-B30B, Sériové číslo: S150Y15056889, MAC adresa z výroby: A0E4CB6CDB10, WPA-PSK Key: 556F22EEB638LBD9C74E (údaje na zadní straně přístroje na nálepce), bílá barva, značně opotřebený, místy hnědé skvrny v plastu, přední část stojky poškrábaná, hnědé skvrny kávové barvy nepatrné velikosti na horní straně routeru, cca. 1,5cm skvrna stejné hnědé barvy na levé hraně routeru

Další přítomné osoby: Josef Novák, nar. 4. 6. 1968 majitel objektu

V rámci prováděné prohlídky na základě ohlášení možné krádeže byla provedena specifická prohlídka webkamery (zajištěný předmět č. 1). Webkamera byla postavena ve stropním podhledu vstupní části zkoumaného objektu. V obvyklém stavu zabírala zádveří vstupní části objektu. V době skutku byla podle přítomného p. Nováka pootočena tak, že její čočka mířila na strop objektu a kamera zabírala pouze malou část sledovaného prostoru, a to ještě nad výší dveří. Její umístění dokladují fotografie DCIM000100 – DCIM000112.

Kamera je při zajištění připojena do napájecí sítě prostřednictvím microUSB konektoru, který vede do napájecího adaptéru ve zdi. Má stabilně aktivní WiFi připojení, je připojena k síti s SSID nowakowci.

Podhled, ve kterém se kamera nachází, je nesnadno přístupný. Nedá se tedy čekat, že by pachatel riskoval posunutí kamery ručně. Z tohoto důvodu bylo přistoupeno k ohledání provozu na nejbližším zařízení se záznamem, kterým je router fungující jako přístupový bod bezdrátové sítě.

Po připojení k jeho monitorovací konzoli bylo zjištěno, že webkamera má přidělenou vnitřní IP adresu 192.168.1.45 a to staticky. Prohlídkou datových toků byla potvrzena komunikace kamery směrem do venkovní sítě. Kamera i router byla zajištěny pro další šetření s podezřením, že k otočení kamery v době objasňovaného incidentu mohlo dojít prostřednictvím vzdáleného přístupu k ovládací aplikaci. Tato ovšem nekomunikuje s kamerou napřímo, ale přenáší příkazy prostřednictvím cloudové infrastruktury výrobce. Tvrzení bylo ověřeno záznamem komunikace a na místě pořízeným výpisem z databáze WHOIS. Z toho důvodu by bylo vhodné replikovat prostředí sítě v laboratoři, aby bylo možné zachytit a analyzovat komunikaci s tímto cloudem.

Manipulace kamerou prostřednictvím aplikace byla provedena za přítomnosti p. Nováka a zdokumentována sérií fotografií (DCIM000113 – DCIM000120). Na záběru DCIM000119 lze nalézt IP adresu přiřazenou kameře. Následně byly kamera i router odpojeny od napájení a demontovány i se zdrojem pro účely transportu k laboratornímu vytěžení.

Otázky pro laboratorní analýzu:

Jakým způsobem probíhá komunikace mezi aplikací a kamerou?

Lze do této komunikace zasáhnout přístupem třetí strany?

Bylo na router v rozhodné době připojeno nějaké neobvyklé zařízení?

Kde se nachází řídící infrastruktura a jak k ní lze přistupovat kromě aplikace a kamery?

Došlo v dobře incidentu ke komunikaci, která by odpovídala otočení kamery tak, aby se vstup do objektu ocitl mimo záběr?

PŘÍLOHA P IV: ZNALECKÝ POSUDEK KAMERA ZNALECKÝ POSUDEK

Č. ev. 1111/2021

Vypracovává: Bc. František Sedláček

Zadavatel: Policie České republiky

Posudek byl zadán za účelem objasnění okolností události ze dne 2. 4. 2021 v místě Popice (u Hustopečí) v souvislosti s vyšetřováním pro podezření na trestný čin loupeže.

Předmětem tohoto posudku je zajištění informací z webové kamery, model YCC365 Plus, nalezené ve zkoumaném objektu a objasnění okolností za kterých došlo k jejímu odklonění během předmětné doby, tj. 2. 4. 2021 v 4:32.

Vypracován byl v oboru *kybernetika a informační technologie* dne 24. 4. 2021.

Vypracoval: Bc. František Sedláček Zadavatel: Ing. Kpt. Ladislav Vyskočil

Zadání znaleckého posudku

Otázky položené pro objasnění znaleckým posudkem (zadání znaleckého posudku):

Jakým způsobem probíhá komunikace mezi aplikací a kamerou?

Lze do této komunikace zasáhnout přístupem třetí strany?

Bylo na router v rozhodné době připojeno nějaké neobvyklé zařízení?

Kde se nachází řídící infrastruktura a jak k ní lze přistupovat kromě aplikace a kamery?

Došlo v dobře incidentu ke komunikaci, která by odpovídala otočení kamery tak, aby se vstup do objektu ocitl mimo záběr?

Tyto otázky mají být posudkem zodpovězeny pro účely stanovení kriminalistické teorie pro další šetření, které bude provádět Policie ČR v rámci řešení případu ev. č. KRPB-123456-15/PŘ-2021-123456-IO.

Zadavatel si není vědom žádné skutečnosti, která by mohla mít vliv na zpracování nebo přesnost závěrů tohoto znaleckého posudku.

Výčet předložených podkladů

Pro tento znalecký posudek byly předloženy následující podklady:

Záznam NAT tabulky z routeru ze zajišťovaného objektu

Přihlašovací údaje k účtu majitele objektu v aplikaci na ovládá kamery

Otisk obrazovky s NAT tabulkou a DHCP tabulkou routeru ke kterému byla kamera v době jejího zajištění připojena

Zajištěný předmět č. 1: Webkamera nezjištěného výrobce ani modelu, barva bílá s černou krytkou čočky. Bílá otáčivá základna, v zadní části kamery připojení pro mikroUSB napájecí konektor a anténa o délce cca. 7 cm. Mírně opotřebená, základna je zaprášená, kryt čočky lehce poškrábaný. Žádné viditelné sériové číslo ani jiný způsob jednoznačné identifikace.

Zajištěný předmět č. 2: Modem ZyXel, číslo modelu VMG1312-B30B, Sériové číslo: S150Y15056889, MAC adresa z výroby: A0E4CB6CDB10, WPA-PSK Key: 556F22EEB638LBD9C74E (údaje na zadní straně přístroje na nálepce), bílá barva, značně opotřebený, místy hnědé skvrny v plastu, přední část stojky poškrábaná, hnědé skvrny kávové barvy nepatrné velikosti na horní straně routeru, cca. 1,5cm skvrna stejné hnědé barvy na levé hraně routeru

Výpis z protokolu WHOIS pro adresu, s kterou byla zjištěná komunikace kamery

Záznam komunikace z kamery zajištěný při připojení na zařízení ZyXel

Popis zajištění jednotlivých předložených podkladů viz protokol ohledání na místě činu předložený technikem PČR.

Ověření a fixace autenticity digitálních podkladů

Následující digitální podklady byly pro účely analýzy ověřeny pomocí SHA-256:

Číslo a název	Soubor	Hash	Ověřeno
Záznam NAT tabulky z routeru ze zajišťovaného objektu	NAT-data.txt	D9CD8B5041EE295A9541E0645090C296F5DC8B85183CFF70BD46956DA4F08F8B	Ano
Otisk obrazovky s NAT tabulkou a DHCP tabulkou routeru ke kterému byla kamera v době jejího zajištění připojena	DCIM0001518.jpg	05F7DD186F68D235EA078B89191927EF481EEEC74A1930DEB6395E23E64FD1B4	Ne (dodáno bez hashe)
Výpis z protokolu WHOIS pro adresu, s kterou byla zjištěná komunikace kamery	WHOIS.pdf	68D4748BC03FE3C9B8BEF0F023322B9750647ED3861C9FA8A088314ECE876502	Ano
Záznam komunikace z kamery zajištěný při připojení na zařízení ZyXel	camcam4.vlan.id==809.pcap	4077F3B80EC7F2A24D85BC006740510D617AB1D4318624CF0164A471B0522D3B	Ano

Analýza předložených podkladů

Ačkoliv součástí předložených podkladů byla již provedená analýza síťového provozu a otázky se zabývají z velké míry předmětnou kamerou (výjimkou je otázka

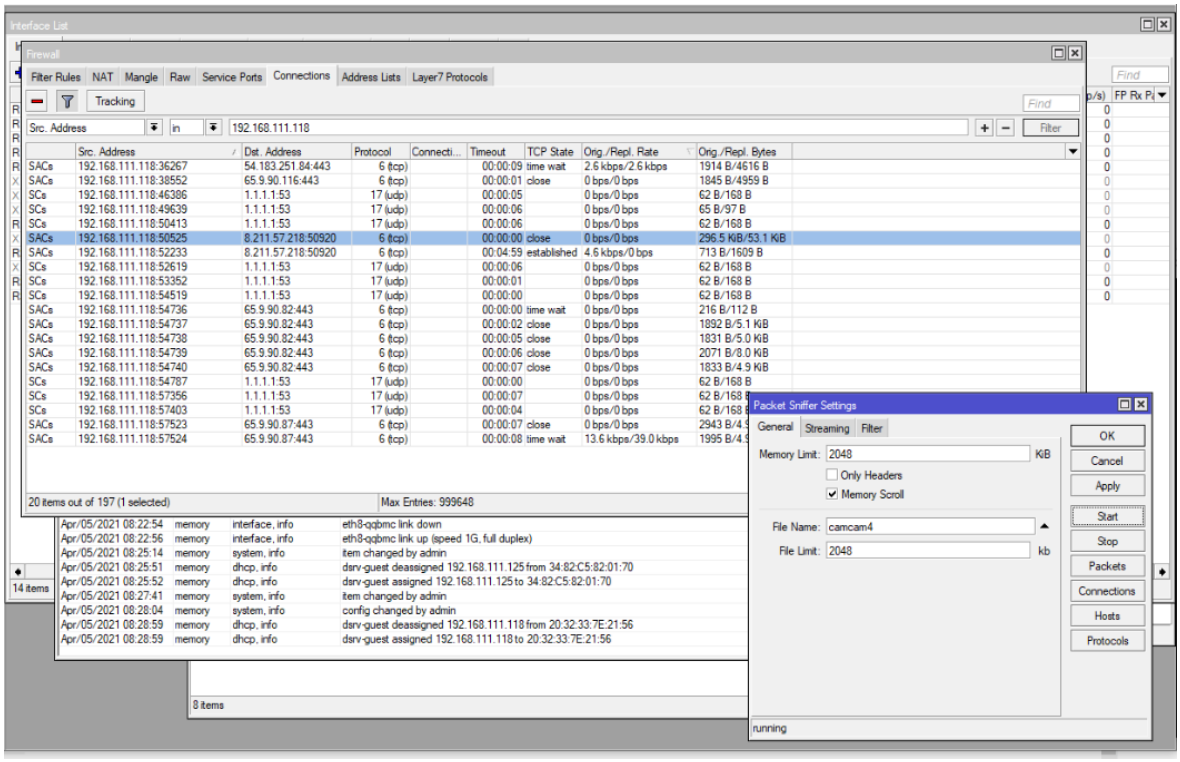
na zařízení připojená na samotný router, která bude zodpovězena analýzou předložených NAT a DHCP záznamů), kamera byla pro účely laboratorního šetření připojena k routeru Microtik který byl zajištěn současně s ní a to za účelem zvýšení autenticity šetření a přiblížení situace zkoumanému místu. Provoz v síti a provoz ven z ní byl dále zaznamenáván dozorovou sondou, která v pravidelných intervalech ukládala své logy na laboratorní disk.

Vytěžovaný router sice neuchovává údaje o provozu, pokud tato funkce není explicitně zapnuta[17], umožňuje ale získat například logy z protokolu DHCP. V případě, že by měl nastavenou statickou adresaci svého prostoru, je situace ještě snazší, protože na základě MAC adresy přidělí webkameře stejnou IP adresu, jako měla „v provozu“.

To znamená, že můžeme rozborem komunikace na cloud ve zkoumané době zjistit, jestli k otočení kamery došlo náhodou, nebo zda útočník nezneužil účet či připojení ke kameře jako prostředek, jak ji otočit na dálku odpovídajícím povelem z cloudové infrastruktury.

Problém může nastat v případě, že by komunikace mezi veřejnou IP adresou a cloudem společnosti Alibaba byly z cílového místa častější, tedy že by se v objektu nacházelo více stejných zařízení, které se spojují s daným cloudem. V takovém případě totiž může ještě být nezbytné zjistit, jak vypadala v danou chvíli tabulka NAT protokolu routeru, a tedy zda došlo k přenesení informace přímo k cílové kameře, nebo k jinému zařízení. Ukázkový výstup z packet snifferu, dokladující že kamera skutečně přes tento router aktuálně komunikuje s cloudovou infrastrukturou a poskytující indicie k vyžádání statistických dat pro analýzu síťového provozu je na obrázku 1.

[17] V kontextu možného kancelářského použití kamery jako součásti bezpečnostního systému se ovšem dá očekávat, že tato funkce použita bude



Obrázek 1 – Ukázka zachycení provozu mezi webkamerou a cloudem Alibaby

Jak tedy vyplývá z výše stanoveného, kamera periodicky komunikuje s řídícím cloudem, od kterého získává příslušné informace. Odposlechem komunikace bylo zjištěno, že je šifrována pomocí TLS1.2 a to jak na straně kamera-cloud, tak na straně cloud-aplikace a je tedy nepravděpodobné, že by do této komunikace zasahoval třetí subjekt.

Z předloženého výpisu historie DHCP vyplývá, že v době, kdy k posunu kamery došlo, byly na tomto přístupovém bodě připojeny celkem čtyři zařízení. Kromě kamery samotné jde nejpravděpodobněji o mobilní telefon, počítač a neznámé zařízení s platformou Android. Nakolik jde o obvyklá zařízení pro tento konkrétní objekt musí zodpovědět až další šetření, v obecné rovině jde ovšem o očekávatelnou skladbu i počet zařízení.

Předložený router byl zapojen a sledován na případné známky kompromitace Ani analýza jeho firmware, ani historie kterou se z něj podařilo získat, nicméně nenasvědčovaly, že by byl kompromitován nebo využíván neobvyklým způsobem.

Zodpovězení otázek ze zadání

K jednotlivým otázkám na základě provedené expertizy uvádím:

Jakým způsobem probíhá komunikace mezi aplikací a kamerou?

Probíhá prostřednictvím zprostředkovatele, kterým je cloudová služba provozovaná čínskou společností Alibaba Cloud Computing (Beijing) Co., Ltd., a využívající služby infrastruktury Amazon Web Services.

Lze do této komunikace zasáhnout přístupem třetí strany?

Komunikace je silně zabezpečena v souladu s aktuálními kryptografickými standardy a průnik do ní v podmínkách běžného provozu je velmi nepravděpodobný či téměř nemožný. Jelikož pro přístup do cloudu a registraci kamery ovšem stačí znát odpovídající uživatelské údaje, je možné, že došlo k odcizení těchto údajů a jejich zneužití třetí stranou.

Bylo na router v rozhodné době připojeno nějaké neobvyklé zařízení?

Nikoliv, podle doložené DHCP tabulky nebylo v době označené jako doba činu na router připojeno žádné neobvyklé zařízení. Mezi připojenými zařízeními je ovšem i mobilní telefon, jehož MAC adresu by bylo nutné srovnat s MAC adresou zařízení majitele objektu, aby bylo možné říct, že jde skutečně o jeho telefon.

Kde se nachází řídící infrastruktura a jak k ní lze přistupovat kromě aplikace a kamery?

Infrastruktura pro řízení aplikace se nachází na serverech, provozovaných společnosti Amazon. Z dostupných adres jmenných serverů se zdá, že v tomto případě je poskytovatelem cloudových služeb tzv. „zóna EU-West“ tedy servery v západní části Evropy. K této infrastruktuře lze kromě aplikace a kamery přistupovat přes účet třetí strany, kterou je právě Amazon.

Došlo v dobře incidentu ke komunikaci, která by odpovídala otočení kamery tak, aby se vstup do objektu ocitl mimo záběr?

Nelze určit bez výpisu z protokolu komunikace. Nicméně vzhledem k zabezpečení aplikace pouze uživatelským jménem a heslem se jeví jako velmi pravděpodobné, že kamera byla otočena pokynem z řídícího účtu.

K vypracování posudku nebyl pozván žádný další konzultant, posudek zpracoval znalec osobně a sám.

Odměna za vypracování znaleckého posudku byla stanovena v zákonné výši.

Znalecký posudek jsem podal jako znalec jmenovaný Okresním soudem Brno-Město ze dne 1.4.2021, pod č.j. *(nerel.)* v oboru *Kybernetika a informační technologie*.

Znalecký posudek byl zapsán pod poř. č. XXXX-YY/2021 znaleckého deníku.

Znalec dle § 127a občanského soudního řádu bere na vědomí povinnost oznámit skutečnosti, pro které by byl jako znalec vyloučen, nebo které by mu bránily být činný jako znalec.

Znalec rovněž prohlašuje, že si je vědom následků vědomě nepravdivého znaleckého posudku, zejména skutkové podstaty trestného činu Křivé výpovědi a nepravdivého znaleckého posudku dle § 346 trestního zákoníku.

PŘÍLOHA P V: OHLEDACÍ ZPRÁVA CHYTRÉ HODINKY
PROTOKOL O PROHLÍDCE

Ohledání provedl: Bc. František Sedláček, vyšetřovatel a Ing. Kpt. Jan Novák, vyšetřovatel

Místo úkonu: Popice u Hustopečí

Čas úkonu: 4. 4. 2021 18:46

Předmět úkonu: Ohledání chytrých hodinek oběti

Zajištěný předmět č. 1: Chytré hodinky Samsung Watch Active 2, bílé s černým displejem, bílý gumový pásek, běžné známky opotřebení. Číslo modelu SR-M500, identifikační číslo RFANA0N2P1M, MAC adresa v době zajištění 34:82:C5:82:01:70.

Další přítomné osoby: Ing. Miriam Sedláčková, oběť

Ohledání osoby bylo provedeno za účelem objasnění okolností, za kterých se tato ocitla na lavičce uprostřed vesnice. Její oblečení neslo stopy krve a oběť sama byla dezorientovaná a podle sdělení, které poskytla hlídce, si nic nepamatuje. Působí orientovaně, dechová zkouška vyloučila přítomnost alkoholu. S krevním testem na přítomnost dalších omamných látek souhlasí. Udává bolest hlavy.

U oběti byly zajištěny chytré hodinky model *Samsung Galaxy Watch Active*, sériové číslo a další identifikátory viz záhlaví dokumentu. Oběť nemá u sebe mobilní telefon, ke kterému jsou hodinky obvykle spárovány, údajně „ho sebou nenosí pořád." Udává, že si nevybavuje, jak se na místo dostala. Zajištění biologických materiálů uvedeno v separátním protokolu, který vypracovává Ing. Kpt. Novák, služební číslo 60186.

Zajišťované chytré hodinky jsou vizuálně nepoškozené, stav krokoměru 5314, tep udávají 96. Podle oběti pro ni obvyklý údaj při námaze. Nevybavuje si, jak k této námaze mohlo dojít. Je si vědoma toho, že před incidentem s někým telefonovala.

Pokus vyhledat telefon pomocí funkce ***Najít můj telefon*** proveden s negativním výsledkem. Hledaný telefon se tedy nachází ve větší vzdálenosti než dvacet metrů od oběti.

Hodinky zajištěny po povolení Ing. Kpt. Novákem a dokončení jejich materiální prohlídky. Odeslány znalci pro získání dat a bližší prozkoumání.

Otázky pro laboratorní analýzu:

Kde se oběť před incidentem pohybovala?

Byla oběť před incidentem v klidu nebo ve stresu?

Kdy přesně mohlo k incidentu dojít?

Přijala oběť bezprostředně před incidentem zprávu nebo telefonní hovor?

PŘÍLOHA P VI: ZNALECKÝ POSUDEK CHYTRÉ HODINKY

ZNALECKÝ POSUDEK

Č. ev. 1112/2021

Vypracovává: Bc. František Sedláček

Zadavatel: Policie České republiky

Posudek byl zadán za účelem objasnění okolností události ze dne 4. 4. 2021 v místě Popice (u Hustopečí) v souvislosti s vyšetřováním nálezu zmatené ženy.

Předmětem tohoto posudku je zajištění informací z chytrých hodinek *Samsung Watch Active* s operačním systémem *OS Tizen* za účelem objasnění okolností, které předcházely nálezu oběti.

Vypracován byl v oboru *kybernetika a informační technologie* dne 24. 4. 2021.

Vypracoval: Bc. František Sedláček Za zadavatele: Ing. Kpt. Ladislav Vyskočil

Zadání znaleckého posudku

Otázky položené pro objasnění znaleckým posudkem (zadání znaleckého posudku):

Kde se oběť před incidentem pohybovala?

Byla oběť před incidentem v klidu nebo ve stresu?

Kdy přesně mohlo k incidentu dojít?

Přijala oběť bezprostředně před incidentem zprávu nebo telefonní hovor?

Tyto otázky mají být posudkem zodpovězeny pro účely stanovení kriminalistické teorie pro další šetření, které bude provádět Policie ČR v rámci řešení případu ev. č. KRPB-123456-15/PŘ-2021-123456-IO.

Zadavatel si není vědom žádné skutečnosti, která by mohla mít vliv na zpracování nebo přesnost závěrů tohoto znaleckého posudku.

Výčet předložených podkladů

Pro tento znalecký posudek byly předloženy následující podklady:

Chytré hodinky Samsung Watch Active 2, bílé s černým displejem, bílý gumový pásek, běžné známky opotřebení. Číslo modelu SR-M500, identifikační číslo RFANA0N2P1M, MAC adresa v době psaní posudku 34:82:C5:82:01:70

Fotodokumentace stavu hodinek při nálezu

Popis zajištění jednotlivých předložených podkladů viz protokol ohledání na místě činu předložený technikem PČR.

Analýza předložených podkladů

Pro získání patřičných údajů jsme na hodinkách povolili *debug mode* volbou z menu. Hodinky jsme následně restartovali a připojili k laboratorní wifi síti. Tím byly připraveny k vykonání akvizice dat. Ta probíhala pomocí toolkitu *Tizen Developer Kit* ve verzi aktuální k datu vypracování posudku (24.4.2021) s nástavbou *Tizen Developer studio* rovněž v aktuální verzi. Žádné nestandardní pluginy ani jiný software nebyly pro připojení použity. Instalátory použitého SDK a návod k instalaci jsou poskytnuty níže.

Pro účely akvizice jsme se do hodinek nejprve připojili přes SSH konzoli a do souboru nechali spočítat otisk všech souborů ve všech adresářích. Zároveň jsme nechali vytvořit strom adresářové struktury a uložili jej do souboru. Při tomto procesu nebyla porušena integrita žádných dalších souborů na hodinkách – první krok pouze soubor přebírá jako vstup a nemanipuluje s ním, druhý krok pracuje pouze s adresáři a soubory neřeší. Rovněž kopírování pomocí příkazu *sdb pull* nemění informace o souboru v původním zařízení.

Následně byl použit skript v jazyce PowerShell, který jednotlivé soubory včetně seznamu otisků a popisu adresářové struktury přenesl z hodinek bezdrátovým přenosem do forenzního počítače, a to rekurzivně pro celý disk. Vytvoření obrazu například pomocí nástroje DD nebo FTK bránil fakt, že disk hodinek byl příliš plný a bez root přístupu nebylo ani možné nástroje dohrát – program dd se v OS Tizen ve výchozím nastavení nenachází.

Zajištění autenticity kopírovaných souborů proběhlo pomocí výpočtu SHA-256 hashe. Následně byly jednotlivé soubory identifikovány a provedena analýza údajů ze souborů s příponami .db pomocí nástroje *DB Browser (SQLite)*.

Použitá SW platforma pro analýzu

Name	Version	Id	Provider
JSDT jQuery Integration	1.7.0	org.eclipselabs.jsdt.jquery_feature.feature.group	Philippe Marschall
ST Things SDK Bridge Tools	2.0.0.201906141449	org.tizen.ocf.bridge.feature.feature.group	The Linux Foundation
ST Things SDK Certificate Tools	2.0.0.202004300845	org.tizen.ocf.cert.feature.feature.group	The Linux Foundation
ST Things SDK Core Tools	2.0.0.202004300800	org.tizen.ocf.core.feature.feature.group	The Linux Foundation
ST Things SDK Extension Tools	2.0.0.202004300815	org.tizen.ocf.ext.feature.feature.group	The Linux Foundation
Tizen Common	2.0.0.202012030914	org.tizen.common.feature.feature.group	The Linux Foundation
Tizen EFL UI Builder	1.0.0.201811300142	org.tizen.efluibuilder.feature.feature.group	The Linux Foundation
Tizen IDE	1.0.0.2020-10-12_13-53	org.tizen.sdk.ide	
Eclipse 4 Rich Client Platform	1.6.1.v20170928-1359	org.eclipse.e4.rcp.feature.group	Eclipse.org
Eclipse Help System	2.2.101.v20171009-0410	org.eclipse.help.feature.group	Eclipse.org
Eclipse Platform	4.7.1.v20171009-0410	org.eclipse.platform.feature.group	Eclipse.org
Eclipse RCP	4.7.1.v20171009-0410	org.eclipse.rcp.feature.group	Eclipse.org
EMF - Eclipse Modeling Framework Core Runtime	2.13.0.v20170609-0707	org.eclipse.emf.ecore.feature.group	Eclipse Modeling Project
EMF Common	2.13.0.v20170609-0707	org.eclipse.emf.common.feature.group	Eclipse Modeling Project
Equinox p2, backward compatibility support	1.3.1.v20170928-1405	org.eclipse.equinox.p2.extras.feature.feature.group	Eclipse.org - Equinox
Equinox p2, headless functionalities	1.4.1.v20170928-1405	org.eclipse.equinox.p2.core.feature.feature.group	Eclipse.org - Equinox
Equinox p2, minimal support for RCP applications	1.3.1.v20170928-1405	org.eclipse.equinox.p2.rcp.feature.feature.group	Eclipse.org - Equinox
Equinox p2, Provisioning for IDEs.	2.3.1.v20170928-1405	org.eclipse.equinox.p2.user.ui.feature.group	Eclipse.org - Equinox
Tizen Base Feature	2.0.0.202010121353	org.tizen.base.feature.feature.group	Tizen
Tizen Native App Common	2.0.0.201811300134	org.tizen.nativeappcommon.feature.feature.group	The Linux Foundation
Tizen Native Common	2.0.0.202010121130	org.tizen.nativecommon.feature.feature.group	The Linux Foundation
Tizen Native Core	2.0.0.202009291005	org.tizen.nativecore.feature.feature.group	The Linux Foundation
Tizen Native Core	1.0.0.202009220732	org.tizen.nativecore.ext.feature.feature.group	The Linux Foundation
Tizen Native Dynamic Analyzer	2.1.0.201910211211	org.tizen.dynamicanalysis.ide.eplugin.feature.feature.group	The Linux Foundation
Tizen Native Enventor	1.0.0.201811301040	org.tizen.nativecore.enventor.feature.feature.group	The Linux Foundation
Tizen Native Unit Test Tools	2.0.0.202009090428	org.tizen.unittest.feature.feature.group	The Linux Foundation
Tizen Profiler	1.0.0.202009290953	org.tizen.profiler.feature.feature.group	The Linux Foundation
Tizen Web JavaScript Code Analyzer	1.0.0.202010130503	org.tizen.web.jsa.feature.feature.group	The Linux Foundation
Tizen Web Dynamic Analyzer	2.1.0.201910160605	org.tizen.dynamicanalysis.ide.web.eplugin.feature.feature.group	The Linux Foundation
Tizen Web Simulator	1.0.0.201705180151	org.tizen.web.simulator.feature.feature.group	Samsung

Platforma byla použita z oficiálního instalátoru bez dalších modifikací. Veškeré použité postupy byly aplikovány podle oficiální dokumentace výrobce.

Zodpovězení otázek ze zadání

K jednotlivým otázkám na základě provedené expertizy uvádím:

Kde se oběť před incidentem pohybovala?

Zajištěné hodinky neměly aktivní GPS modul a k počítání polohy využívaly pouze lokátor telefonu na který byly připojeny. Tyto údaje tedy bez zajištění mobilního telefonu nebo bez kontaktování poskytovatele cloudových služeb, společnosti Samsung, nebude možné zjistit.

Byla oběť před incidentem v klidu nebo ve stresu?

Jak vyplývá z měření srdeční aktivity a dalších údajů, které se podařilo v hodinkách nalézt, oběť se asi dvacet minut před zajištěním hodinek dostala do značného stresu a její reakce pokračovala až do zajištění hodinek.

Kdy přesně mohlo k incidentu dojít?

Ze stresové špičky, která nastala 18:29 a následného trvání zvýšené stresové hladiny až do 18:40 se dá usoudit, že k incidentu došlo někdy kolem časové značky 18:29 a tento s kolísavou intenzitou trval cca. deset minut – od této časové značky stresová úroveň udávaná hodinkami opět klesá až do jejich zajištění.

Přijala oběť bezprostředně před incidentem zprávu nebo telefonní hovor?

Podle zajištěných dat se zdá, že oběť bezprostředně před incidentem obdržela zprávu přes aplikaci SMS, obsah zprávy nicméně z hodinek zajištěn nebyl. Podle dostupných údajů nedošlo v rozhodné době k žádnému telefonnímu hovoru.

K vypracování posudku nebyl pozván žádný další konzultant, posudek zpracoval znalec osobně a sám.

Odměna za vypracování znaleckého posudku byla stanovena v zákonné výši.

Znalecký posudek jsem podal jako znalec jmenovaný Okresním soudem Brno-Město ze dne 1.4.2021, pod č.j. *(nerel.)* v oboru *Kybernetika a informační technologie*.

Znalecký posudek byl zapsán pod poř. č. XXXX-YY/2021 znaleckého deníku.

Znalec dle § 127a občanského soudního řádu bere na vědomí povinnost oznámit skutečnosti, pro které by byl jako znalec vyloučen, nebo které by mu bránily být činný jako znalec.

Znalec rovněž prohlašuje, že si je vědom následků vědomě nepravdivého znaleckého posudku, zejména skutkové podstaty trestného činu Křivé výpovědi a nepravdivého znaleckého posudku dle § 346 trestního zákoníku.