Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

Bakalářská práce

2018 **Karolína Pěstová**

Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

Analýza spolehlivosti forenzních nástrojů pro zkoumání malé digitální techniky

Bakalářská práce

Karolína Pěstová

Vedoucí práce: Mgr. Jakub Kothánek LL.M.

České Budějovice 2018

Bibliografické údaje

Pěstová K., 2018: Analýza spolehlivosti forenzních nástrojů pro zkoumání malé digitální techniky [Analysis of forensic tools reliability for investigating small digital devices Bc. Thesis, in Czech] - 51 p., Faculty of Science, The University of South Bohemia, České Budějovice, Czech Republic

Anotace

Tato bakalářská práce se zabývá forenzními nástroji pro zkoumání malé digitální techniky. V teoretické části jsou popsány zásady digitální forenzní analýzy a postupy pro zkoumání mobilních telefonů. V praktické části je provedena analýza vybraných mobilních telefonů nástroji pro zkoumání malé digitální techniky, jsou zde vyhodnoceny výsledky a navrženo řešení pro zajištění co nejvíce relevantních dat.

Klíčová slova

Digitální forenzní analýza, Forenzní nástroj, Mobilní telefon, Extrakce dat

Annotation

This bachelor thesis deals with forensic tools for investigating small digital devices. In theoretical part are described principles in digital forensic analysis and approaches for examining mobile phones. In practical part are analysed selected mobile phones with tools for investigating small digital devices. In this part are evaluated results and proposed a solution for acquiring the most relevant data.

Key words

Digital forensic analysis, Forensic tool, Mobile phone, Data extraction

Poděkování

Chtěla bych poděkovat Mgr. Jakubu Kothánkovi LL.M., vedoucímu mé bakalářské práce za odborné rady a čas věnovaný při konzultacích. Také bych chtěla poděkovat své rodině a přátelům za podporu.

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracovala samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne ..... Podpis.....

Obsah

1. Úvod a cíle

1.1. Úvod

V dnešní době jsou elektronické prostředky běžnou součástí společnosti a mnohé aktivity probíhají skrze ně. Obecně také roste využívání informačních a komunikačních technologií. Z toho vyplývá, že je produkováno velké množství elektronických dat. Pokud jsou elektronické prostředky, konkrétně počítač či mobilní telefon, použity při trestné činnosti, využívá policie nebo znalci v oboru kybernetika, odvětví výpočetní technika, digitálních forenzních prostředků k analýze použité techniky. Jedná se o prostředky, které jsou schopné extrahovat data z příslušné techniky. Data se následně analyzují a poté mohou být použity jako důkaz v trestním řízení.

Předmětem práce jsou právě tyto forenzní nástroje, konkrétně nástroje pro zkoumání malé digitální techniky. Dále se práce bude zabývat zásadami forenzního zkoumání digitální techniky obecně. Práce bude zaměřena zejména na konkrétní analýzu mobilních telefonů. Budou použity forenzní nástroje komerční i opensource. Důraz bude kladen také na dopady a případné důsledky pro vyšetřování trestné činnosti.

1.2. Cíle práce

Cílem práce je v teoretické části popsat zásady digitální forenzní analýzy, postupy při analýze. V praktické části pak samotnou analýzu provést, porovnat a vyhodnotit výsledky analýzy konkrétních mobilních telefonů a porovnat použité forenzní nástroje z hlediska funkčnosti, spolehlivosti, finanční náročnosti a také využití při vyšetřování trestné činnosti s přihlédnutím k právní stránce věci. Na základě tohoto vyhodnocení a porovnání také navrhnout vhodné řešení ve vztahu k zajištění co nejvíce relevantních dat pro vyšetřování trestné činnosti.

2. OS a data v mobilních zařízeních

V mobilních zařízeních – mobilních telefonech se nachází velké množství dat. Data mohou o majiteli zařízení mnoho prozradit. Mimo dat, která se nacházejí ve všech mobilních telefonech se zde nacházejí i data z aplikací přímo nainstalovaných uživatelem. Mezi běžná data patří ta, která jsou produkována aplikacemi tvořícími základní funkčnost zařízení. Jedná se o informace o zařízení, SMS zprávy, kontakty, výpisy hovorů, kalendář a další.

Data, která obsahují uživatelem nainstalované aplikace, jsou z pohledu digitální forenzní analýzy mnohdy důležitější než běžná data. Jedná se především o data z komunikačních aplikací (Facebook, Google+, Messenger, WhatsApp) data z aplikací pracujících s GPS polohou (Mapy.cz, Waze) a webové prohlížeče (Internet Explorer, Google Chrome, Safari). Na data uložená v mobilních telefonech se lze dívat i z jiného úhlu. První kategorií jsou data, která přímo obsahují konkrétní informace. Ta lze dále rozdělit na elektronické dokumenty, metadata dokumentů a provozní data vytvořená aplikacemi.

Elektronické dokumenty obsahují informace, které v nich aktivně zachytil člověk. Jedná se o textové dokumenty, fotografie, videa, audionahrávky, dokumenty stažené z internetu a další. K těmto dokumentům pak aplikace, prostřednictvím kterých dokumenty vznikají, zpravidla přidává metadata.

Metadata obsahují doplňující informace o dokumentu. Například dobu pořízení, verzi a typ aplikace, která ho vytvořila.

Kromě metadat vytvářejí aplikace také provozní a pomocná data, která jsou produktem jejich funkcionality. Jsou to například logy, automaticky pořizované záznamy, dočasné soubory a další.

Druhou kategorií jsou systémová data, která určují co a jak má systém vykonávat. Tyto zprostředkovávají nebo realizují tvorbu klasických dat a také zpětnou interpretaci dat již vytvořených do smyslově vnímatelné podoby. [1]

3. Forenzní analýza digitálních dat

Forenzní analýza digitálních dat patří mezi forenzní vědy, které se využívají při vyšetřování a dokazování v trestním řízení. Zjednodušeně zahrnuje extrakci dat a jejich analýzu.

Definici forenzní analýzy uvádí Michael A Caloyannides ve své knize [2]. Podle něj je forenzní analýza sbírka technik a nástrojů používaných k nalezení důkazů v počítači a jejich následnému použití k znevýhodnění uživatele.

Společnost Tayllor Cox Cyber Lab s.r.o. na svých stránkách uvádí, že digitální forenzní analýza je užití vědecky odvozených a osvědčených metod k izolování (ochraně), sběru, zhodnocení, identifikaci, analýze, interpretaci, dokumentaci a prezentaci digitálních důkazů ze zdrojů digitálních dat s cílem usnadnění rekonstrukce událostí shledaných zločinnými nebo k odhalení neautorizovaných akcí, které působí rušivě na plánovaný běh operací. [3]

Definic je samozřejmě mnoho a v zásadě se neliší. Pokud jsme v kontextu elektronických prostředků a dat, je možné termíny forenzní analýza a digitální forenzní analýza považovat za synonyma.

Můžeme tedy říci, že se jedná o analýzu dat jejímž cílem je určit podrobnosti k danému případu jako je například čas události, důvod a místo. V digitálních datech jsou tyto informace uloženy nebo dokonce skryty v podobě smazaných souborů, fragmentů nebo například logů. K získání těchto dat použitelných jako důkaz, je zapotřebí speciálních nástrojů, kterými se práce bude zabývat v následujících kapitolách.

3.1. Zásady forenzní analýzy

Aby analýza mohla být považována za forenzní musí splňovat určité zásady.

Uvedené zásady nejsou v České republice právně zakotveny a vycházejí pouze z praxe a zahraničních doporučení. Pouze podjatost je specifikována zákonem o znalcích a tlumočnících jako možnost, pro kterou může být znalec ze zkoumání vyloučen. Proto je vyjádření znalce k podjatosti jednou ze standardních součástí znaleckého posudku.

První zásadou je *legalita*. To znamená, že veškeré informace, stopy, vzorky, předměty, dokumenty atp., které slouží jako zdroj/vstup pro digitální forenzní analýzu, metody a způsoby zpracování, a tedy i výstupy digitální forenzní analýzy musí být získány, pořízeny a zhotoveny legálním způsobem.

Druhou zásadou je *integrita*, tj. vše, co bylo prováděno, veškeré způsoby práce se vstupními informacemi (stopy, vzorky...), musí být prováděno způsobem, ze kterého je jednoznačně jasné, že nemohlo dojít k úmyslné nebo neúmyslné manipulaci nebo změně.

Další zásadou je *opakovatelnost/přezkoumatelnost*, tj. použití takových způsobů práce a jejich dokumentace tak, aby metody mohly být opakovaně provedeny stejným způsobem, čímž by se ověřilo, zda se dospěje ke stejným závěrům, nebo aby pomocí jiných ekvivalentních metod (pokud existují) mohla být správnost závěrů ověřena.

Nepodjatost, tj. nezávislost subjektu provádějícího forenzní činnosti na zkoumaném předmětu nebo objektu.

Neodmyslitelným atributem, který podmiňuje všechny výše uvedené, je detailní *dokumentace*. Bez ní by bylo obtížné prokázat nejen faktické závěry, ale i to, že výše uvedené atributy byly bezezbytku naplněny. [4]

3.2. Druhy digitální forenzní analýzy

Digitální forenzní analýza není omezena pouze na získávání dat z počítače. Jedním z dalších druhů je digitální forenzní analýza počítačové sítě, dalším druhem je digitální forenzní analýza databází. K digitální forenzní analýze patří také analýza mobilních zařízení jako jsou například tablety, smartphony, flash disky, protože zákony jsou porušovány i za pomoci malé digitální techniky. Tímto druhem analýzy se bude práce zabývat i v následujících kapitolách.

4. Digitální forenzní analýza mobilních zařízení

4.1. Části forenzní analýzy digitálních dat

Samotnou forenzní analýzu digitálních dat lze rozdělit na několik částí, které na sebe logicky navazují.

4.1.1. Získání a zajištění mobilního telefonu

Získání mobilního telefonu jako důkazu v trestním řízení proběhne podle § 67 – § 88o zákona č. 141/1961 Sb., o trestním řízení soudním. [5]

Na mobilní telefon může být při spáchání trestného činu nahlíženo z několika stran. Za prvé může být mobilní telefon předmětem útoku, kdy je poškozen, odcizen, zničen nebo do něj mohl někdo neoprávněně vniknout a změnit, přidat nebo smazat data. Dále pak může být mobilní telefon použit jako nástroj ke spáchání trestného činu, například při vydírání, manipulaci či pořizování pornografických snímků. Také může být nástrojem pro organizaci trestného činu. To znamená při jeho přípravě či při samotné realizaci. I pokud mobilní telefon není přímou součástí trestného činu, může být zdrojem kriminalisticky relevantních informací, které potvrdí či vyvrátí ostatní důkazy. [1]

Úvodem samotného zajišťování mobilního telefonu, je třeba dbát na to, aby byl mobilní telefon zajištěn bez možnosti změny, smazání či zničení důkazních dat. Mobilní telefony jsou dynamická zařízení a tím, že jsou připojená k WiFi síti či mobilním datům, mohou být důkazní data znehodnocena. Především u některých mobilních telefonů je možné s daty vzdáleně manipulovat nebo je kompletně smazat, proto by se měly mobilní telefony, při zajištění vypnout. Tento krok je rizikový, pokud se telefon po vypnutí uzamkne. Je tedy nezbytné zajistit přístupové údaje. U SIM karty se jedná o PIN kód. Pokud v tomto případě nebude majitel spolupracovat, je možné dotázat se na kód PUK mobilního operátora. [1]

Dotaz je možné vznést, pokud byl mobilní telefon vydán dle § 78 Trestního Řádu (dále jen TŘ), odňat dle § 79 TŘ či byl zajištěn v průběhu domovní prohlídky, prohlídky

jiných prostor a pozemků, osobní prohlídky, při oprávněném vstupu do obydlí, jiných prostor a pozemků (§ 82 – § 85 TŘ). Dále v případě zajištění telefonu při ohledání místa činu dle § 113 TŘ. Od zkoumání SIM karet se již upouští, jelikož se na kartu standardně neukládají ani zprávy ani kontakty. [5]

Z tohoto důvodu nabývá na důležitosti zkoumání vnitřní paměti mobilního telefonu. Ale i v tento okamžik může nastat situace, že mobilní telefon bude zabezpečen, zde pomocí gesta či hesla. V tomto případě je mobilní telefon nelze zkoumat, protože není možné ho správně nastavit pro požadavky forenzních nástrojů. [6]

Při zajišťování mobilního telefonu, je také třeba brát zřetel na ostatní příslušenství, které k němu náleží, a u kterého je reálná šance, že ho pachatel také používal. Jedná se o další SIM karty a paměťové karty. Také je důležité zajistit nabíječku či datový kabel. Tato nutnost ustupuje s příchodem standardu microUSB, který již využívá většina mobilních telefonů. Ale v případě, že se jedná o mobilní telefon staršího typu, mohla by bez příslušného kabelu nastat situace, kdy by nebylo možné jeho vytěžení pomocí forenzních nástrojů. Daný mobilní telefon by musel být vytěžen manuálně. [6]

4.1.2. Extrakce dat

Po zajištění mobilního telefonu nastává fáze získávání informací či extrakce dat. V této fázi získáváme z telefonu data pomocí forenzních nástrojů.

U zajištěných mobilních telefonů je třeba provést extrakci tak, aby vytěžená data bylo možno použít pro účely trestního řízení. Je nutné dodržet určité postupy, aby nedošlo ke změně či zničení důkazního materiálu podle zákona č. 141/1961 Sb. o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. Další nutností je, aby bylo možné zkoumání kdykoli zopakovat a ověřit správnost výsledků. Zde se jedná o zásadu opakovatelnosti viz kapitola 3. 1. Bohužel tyto postupy nelze při extrakci mobilních telefonů a malé digitální techniky vždy dodržet s ohledem na možné typy forenzního zkoumání. Týká se to těch typů zkoumání, kdy je zařízení zapnuto a je třeba ho nastavit pro potřeby zkoumání. Nevyhnutelně tak dochází ke změnám v zařízení. Někdy ale není možné forenzní zkoumání provést jinak. Pokud je tomu tak, je třeba provést důkladnou dokumentaci všech kroků.

Samotnou extrakci dat ze zajištěných mobilních telefonů lze provést manuálně (viz kapitola 4.2.1.) nebo je možné využít forenzních nástrojů, které mohou provést analýzu logickou (viz kapitola 4.2.3.), fyzickou (viz kapitola 4.2.3.) nebo analýzu systémových souborů (viz kapitola 4.2.3.). Dělení typů softwarových zařízení dle technologie zkoumání se uvádí v časopisu DSM.

Za prvé se jedná o technologii, při které je nutné mít mobilní telefon spuštěný a forenzní nástroj využívá komunikace zařízení a technologického PC. Jde většinou o starší řady jednoduchých mobilních telefonů s tzv. modemem nebo si forenzní nástroj nahraje aplikaci do zařízení a cestou komunikace mezi zařízením a technologickým PC provádí dokumentaci dat. Zde se jedná také o starší mobilní telefony s operačním systémem, např. Symbian. Posledním případem je schopnost forenzního nástroje využít technologie tzv. ladění operačního systému Android – je nutné spustit zařízení a nastavit tzv. ladění, v některých případech též povolit aplikace třetích stran, v tomto případě dochází k funkcionalitě jako v předchozích případech.

Za druhé se jedná o technologii, při níž mobilní zařízení nemusí být spuštěno. Je to tzv. fyzická extrakce dat. Forenzní nástroj si cestou servisního kódu načte svůj zavaděč, svůj operační systém, který je využit k vykopírování bitové kopie paměťového média zařízení.

Za třetí je mobilnímu zařízení následně modifikován operační systém. Je provedena tzv. root úprava v rámci zařízení s operačním systémem Android – v tento okamžik dochází k nenávratné změně operačního systému nebo je provedena tzv. jailbreak úprava v rámci zařízení s operačním systémem Apple iOS – zde opět dochází k nenávratné změně operačního systému.

Z těchto důvodů se musí ke každému mobilnímu telefonu přistupovat individuálně a je nutné přesně dodržet návody a postupy popsané výrobcem daného forenzního nástroje. [6] [5]

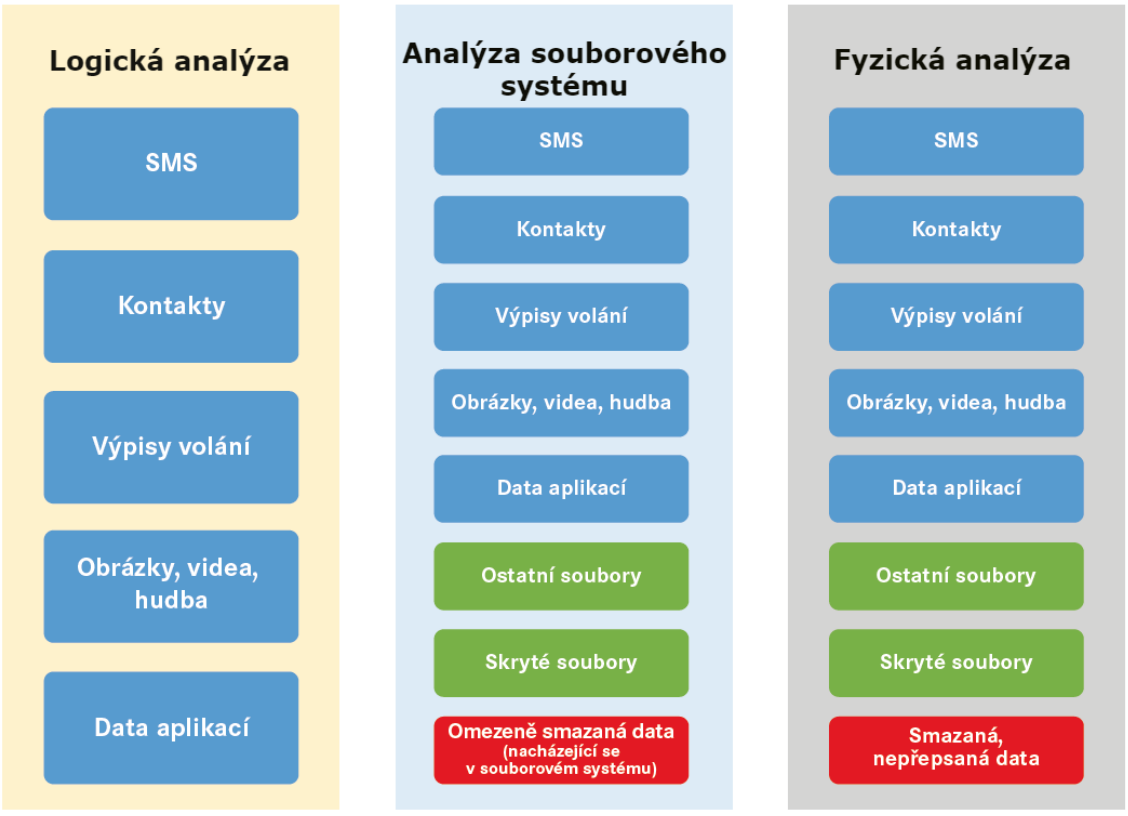
4.1.3. Analýza dat

Jedná se o interpretaci získaných dat. Následuje identifikace a oddělení nepodstatných informací od podstatných – použitelných v rámci trestního řízení.

Podle § 2 odst. 6 TŘ – *Orgány činné v trestním řízení hodnotí důkazy podle svého vnitřního přesvědčení založeného na pečlivém uvážení všech okolností případu jednotlivě i v jejich souhrnu*.

Zákon tedy přesně neurčuje, jaké množství důkazů, s jakou váhou a důkazní silou je potřebné k prokázání skutečnosti. Toto se nepochybně vztahuje i na vytěžená data ze zajištěných telefonů – elektronické důkazy. [1] [5]

4.2. Druhy digitální forenzní analýzy mobilních zařízení



Obrázek 1 Druhy forenzní analýzy [6]

4.2.1. Manuální analýza

Během manuální analýzy se ručně prochází zapnutý telefon a zaznamenávají se veškeré údaje, a to buď písemně nebo fotograficky. Tato metoda je časově velmi náročná a výstupem je jen málo dat, proto ji nelze doporučit. Naopak je výhodou, že tuto metodu lze využít pro všechny typy telefonů, v případě, že jsou funkční. [6]

4.2.2. Logická analýza

Během logické analýzy lze získat větší množství dat než při použití manuální extrakce. Dochází k vytěžení logické struktury a tím související data v telefonu. Touto analýzou není možné zajistit smazané soubory. Analýza interaktivně funguje s telefonem, a proto je třeba mít telefon zapnutý a příslušně nastavený.

Jak je vidět z obrázku, pomocí logické analýzy lze vytěžit například SMS zprávy, kontakty, výpisy volání, obrázky, hudbu, videa, a data aplikací. [7] [6]

4.2.3. Analýza souborového systému

Stejně jako při logické analýze musí být telefon zapnut a příslušně nastaven. Pomocí analýzy souborového systému je možné vyextrahovat souborový systém. Tento druh analýzy umožňuje extrahovat skryté soubory. Je také možné vytěžit i soubory, které jsou v databázi označeny jako smazané, pokud umí forenzní nástroj s takovými databázemi pracovat.

Jak je vidět z obrázku, analýzou souborového systému je tedy možné získat SMS zprávy, kontakty, výpisy volání, obrázky, videa, hudbu, data aplikací stejně jako u logické analýzy, ale nadto také data, která se nacházejí uvnitř souborového systému jako skryté soubory a některé smazané soubory. [7] [6]

4.2.4. Fyzická analýza

Fyzická analýza umožňuje získat bitovou kopii celého telefonu. To znamená, že během fyzické analýzy získáváme vnitřní paměť telefonu bit po bitu, včetně například smazaných dat. Tento druh analýzy bohužel podporuje nejméně telefonů a z toho důvodu je nutné použít jiný druh analýzy.

Fyzická analýza může proběhnout dvěma způsoby. V prvním případě je možné vytěžit mobilní telefon bez znalosti přístupových údajů a není třeba ho zapínat. Do mobilního telefonu je nabootován systém, pomocí kterého je vytvořena bitová kopie telefonu, včetně smazaných souborů.

V druhém případě je třeba mobilní telefon zapnout a nastavit, ale i v tomto případě je získána identická kopie telefonu.

I u fyzické je možné extrahovat SMS, kontakty, výpisy volání, obrázky, hudbu, videa, data aplikací a totožně s analýzou systémových souborů lze i touto analýzou vytěžit ostatní soubory, skryté soubory a smazaná nepřepsaná data. [7] [6]

5. Data jako důkazní materiál

S nárůstem počtu mobilních telefonů se zvyšuje i množství případů, kdy je mobilní telefon a příslušná data v něm, důležitý v trestním řízení. Aby data mohla být použita jako důkaz musí forenzní zkoumání splňovat určité zásady – viz kapitola 3.1, z nichž jsou nejdůležitější přezkoumatelnost důkazu, zachování integrity a objektivita znalce.

To tedy znamená, že veškeré způsoby manipulace se zajištěnými daty se musí provádět tak, aby bylo zřejmé, že nedošlo k úmyslné nebo neúmyslné manipulaci s daty nebo jejich změně.

Ne vždy je ale možné se zásahu do zařízení vyhnout. Do zařízení není zasahováno jen v případě fyzické analýzy, kdy mobilní telefon nemusí být zapnut. V ostatních případech je zásah do zařízení nevyhnutelný a je třeba postup analýzy důkladně zdokumentovat. Jelikož analýzy zpravidla provádějí znalci v oboru kybernetika a výpočetní technika a expertní pracoviště, provedení takto získaných důkazů probíhá obvykle výslechem znalce a čtením znaleckého posudku.

Na dokumentaci jsou připravené i samotné nástroje. V uživatelském rozhraní při analýze je možné vyplnit jméno znalce a jeho další údaje, dále informace o případu například číslo a další podrobnosti. [1]

6. Forenzní nástroje

6.1. Cellebrite UFED

Nástroj umí získat většinu dat z nejvíce mobilních telefonů a aplikací. Překonává snadno bezpečnostní opatření mobilního telefonu. Získá kompletní data z logické extrakce souborového systému. Dokáže i fyzickou extrakci i skrytých a smazaných dat. Zajímavá je funkce spojení času, fotek, hovorů a událostí pro přesnější určení vazeb mezi lidmi a událostmi. Standardem je extrakce kontaktů, zpráv, mailů, dat z aplikací, poznámek, fotek a hesel.

UFED umožňuje uživatelům provádět extrakci, dekódování, analýzu a reportování na jedné platformě. Vykonává fyzické, logické, souborový systém a extrakci hesla ze všech dat (i v případě, že jsou smazány) z nejširšího spektra zařízení, včetně starších a funkčních mobilních telefonů, smartphonů, přenosných zařízení GPS, tabletů a mobilních telefonů vyráběných s čínskými čipy.

Umožňuje:

- Extrakce zařízení přes rozhraní USB a RJ 45
- Klonování a extrakce SIM
- Extrakce pomocí integrovaného modulu Bluetooth

Jedno-v-jednom mobilní forenzní řešení, které zvyšuje flexibilitu a pohodlí při vyšetřování.

- UFED Physical Analyzer - pokročilá aplikace pro dekódování, analýzu a reportování
- UFED Phone Detective - pro okamžitou identifikaci mobilního telefonu
- UFED Reader - Umožňuje oprávněným osobám sdílet informace s ostatními

Tento forenzní nástroj uživatelům poskytuje možnost fyzické, logické extrakce nebo extrakci souborového systému. Umožňuje fyzickou extrakci a dekódování při zablokování gesta, hesla, PINu ze zařízení Android včetně HTC, Motorola, Samsung Galaxy S, SII, rodiny SIII a dalších.

Extrahuje data aplikací, hesla, e-maily, historie hovorů, SMS, kontakty, kalendář, mediální soubory, informace o poloze atd. Obsahuje unikátní, bohatou sadu analytických funkcí, včetně časové osy, analýzy projektů a detekce malwaru. Časté aktualizace zajisťují kompatibilitu s novými telefony při vstupu na trh. [8]

6.2. MSAB XRY

Nástroj opět nabízí jak fyzickou, tak logickou extrakci. Podporováno je více než 23 000 profilů zařízení, nyní včetně dronů. Dokáže vytěžit informace o zařízení, kontakty, výpisy hovorů, schůzky, poznámky, úkoly, SMS, MMS, iMessages, e-maily s přílohami, které je možné okamžitě prohlížet. Dále také mediální soubory jako fotografie, videa, zvukové soubory a hlasové záznamy, které je opět možné okamžitě poslechnout. Nástroj také umí získat geografické údaje, historii připojení WiFi, hesla pro účty vlastníka zařízení.

Obsahuje také technologii rozpoznávání obrazu, která klasifikuje obrázky do kategorií, jako jsou drogy, zbraně a lidé. Umí dekódovat miniatury videa pro prezentaci v XAMN. Podporuje více než 2,109 aplikací, včetně všech hlavních platforem pro zasílání zpráv. Také podporuje nejnovější smartphony, včetně nejnovějších iOS verze 11 a spousty nových zařízení Android. Pokud je to možné extrahuje i smazaná data. [9]

6.3. Oxygen Forensic® Extractor

Oxygen Forensic® je forenzní software pro získávání dat z mobilních zařízení, jejich zálohování a obrázky, paměťové karty, SIM karty, drony a cloud storage.

S Oxygen Forensic® můžete získat a analyzovat informace o zařízení, kontakty, výpisy hovorů, schůzky, poznámky, úkoly, SMS, MMS, iMessages, e-maily s přílohami. Dále také mediální soubory jako fotografie, videa, zvukové soubory a hlasové záznamy. Nástroj také umí získat geografické souřadnice uložené v různých zdrojích, historii připojení Wi-Fi, hesla pro účty vlastníka zařízení. Dokáže také vytěžit smazané údaje (kontakty, zprávy, hovory, fotografie atd.) Nově také dokáže získat umístění GPS a metadata z dronů.

Aktuální verze podporuje 16 900 mobilních zařízení s různými operačními systémy: Android, Bada, Blackberry, iOS, MTK a čipová sada Spreadtrum (čínská zařízení), Symbian,

Windows Mobile 5/6, Windows Phone 8. Detektor Oxygen Forensic® umožňuje importovat různé typy záloh (iTunes, Android, Nokia, BB, BB10 a IPD), stejně jako obrazy iOS a Android vytvořené jinými forenzními nástroji.

Dále je podporován import a analýza různých obrazů zařízení JTAG a Chip-Off. Oxygen Forensic® podporuje kabel USB a Bluetooth spojení. Software pracuje pod 32bitovou nebo 64bitovou verzí Windows 10, Windows 8 a Windows 7. [10]

6.4. MOBILedit Forensic Express

Nástroj umí extrahovat data z mobilních telefonů a cloudů, data analyzuje a okamžitě vygeneruje report, což je v dnešní době mezi nástroji již standard.

MOBILedit Forensic Express je extraktor s velmi širokým spektrem podporovaných mobilních telefonů. Umí prolomit hesla s akcelerací GPU a vícenásobným záběrem pro maximální rychlost.

Nová verze 5 nabízí nové funkce. Například funkce Photo recognizer. Tento modul automaticky vyhledá a rozpoznává podezřelý obsah ve fotografiích, jako jsou zbraně, drogy, nahota, měna a dokumenty. Aplikace Photo Recognizer využívá umělou inteligenci a strojové učení, které umožňuje rychle analyzovat neomezený počet fotografií a je navržena tak, aby eliminovala množství hodin, které by byly vyčerpány ručně při hledání klíčových důkazů v obrovských databázích fotografií.

Další funkce nové verze jsou reporty ve více jazycích, live updates umožňující denně aktualizovat aplikační analyzátory. Všechny aplikace jsou podrobně analyzovány, včetně údajů o smazaných aplikacích, pokud jsou k dispozici. MOBILedit Forensic Express poskytuje detailní report o kontaktech, zprávách a telefonních hovorech, audio a video souborech i smazaných, pokud jsou k dispozici.

Také umí extrahovat a prolomit hesla z účtů a aplikací. Například i z Wi-Fi, kde také umí získat čas posledního připojení, název Wi-Fi sítě a režim zabezpečení. Je také schopen získat GPS lokace z přístroje a aplikací. A v neposlední řadě je schopen vytěžit historii webového prohlížeče. Dále tento nástroj umí extrahovat smazané údaje, které jsou často klíčovými informacemi při šetření. Údaje o odstraněných datech jsou uvedeny ve zvláštní komplexní

datové zprávě a také zobrazeny v rámci každé jednotlivé analýzy. Ať už se jedná o volání, SMS, MMS, události v kalendáři, poznámky, data aplikací nebo jiné důkazy. MOBILedit Forensic Express hlouběji vyhledává v mezipaměti a skrytých souborech.

MobilEdit uvádí, že extrahované údaje budou záviset na konkrétním modelu telefonu, operačním systému a jeho stavu. [11]

6.5. Android Dedug Bridge

Android Debug Bridge je všestranný nástroj příkazového řádku, který umožňuje komunikaci s mobilním telefonem. Jedná se o program fungující na principu klient-server a je tvořen třemi komponentami. První je klient, který běží na pracovní stanici a slouží k interakci s mobilním telefonem zde pomocí příkazové řádky. Druhou komponentou je daemon, který běží jako proces na pozadí v mobilním telefonu a díky němu je umožněno vykonat příkazy z příkazové řádce. Třetí a poslední komponentou je server, který pracuje na pozadí v pracovní stanici. Řídí komunikaci mezi klientem a mobilním zařízením. [12]

7. Forenzní analýza jednotlivých telefonů

Bylo analyzováno tyto mobilní telefony:

- iPhone 5s – iOS 11.1.2
- Microsoft Lumia 550 – Windows 10 Mobile
- Samsung Galaxy A5 – Android 7.0
- Samsung Galaxy J3 – Android 5.1.1
- Samsung Galaxy J5 – Android 6.0.1
- Samsung Galaxy Core Prim – Android 5.1.1
- ZTE Kis 3 – Android 4.4.2

Další mobilní telefony měly být zapůjčeny od firmy Compelson, ale nestalo se tak. Firma v tom čase vyvíjela a testovala MOBILedit Forensic Express verzi 5. Mobilní telefony tedy byly zapůjčeny od rodiny a přátel.

Všechny mobilní telefony byly testovány na všech těchto forenzních nástrojích:

- UFED
- XRY
- MOBILedit Forensic Express
- Oxygen Forensic® Extractor

7.1. Analýza mobilních telefonů nástrojem MOBILedit Forensic Express

7.1.1. Android

Nastavení je pro všechny mobilní telefony s operačním systémem Android stejné.

Mobilní telefony byly načteny do menu po připojení pomocí kabelu. Dalšími možnostmi připojení bylo Bluetooth nebo WiFi. U mobilního telefonu je nutné znát všechny přístupové údaje, jinak analýza není možná. S tím souvisí nutnost mít mobilní telefon po celou dobu zapnutý, mít stažené správné ovladače a mít mobilní telefon správně nastavený.

Pro všechny mobilní telefony s operačním systémem Android je nastavení následující:

- povolit vývojářské možnosti
- ve vývojářských možnostech nastavit režim ladění
- povolit režim ladění vzhledem k počítači – otisk počítače RSA

Po povolení všech nastavení bylo nutné ještě povolit nahrání aplikace Forensic Connector.

Následně bylo možné vybrat typ exportu – celý obsah, specifický výběr, smazaná data nebo rodičovská kontrola. Pro tyto mobilní telefony byla vybrána možnost analýzy celého obsahu. V dalším kroku bylo možné vyplnit detaily o případu, telefonu a vyšetřovateli. Dále pak byla možnost vybrat formáty exportů a reportů, k dispozici byl PDF Report, HTML Report, MS Excel Report a MOBILedit Backup, MOBILedit Export a Cellebrite UFDR jako exporty. Zde byly vybrány všechny možnosti, ale následně byl použit pouze PDF Report.

Forenzní nástroj umožnil využít funkci PhotoRecognizer – lze nastavit specifické kategorie pro rozpoznávání obrázkových souborů – drogy, nahota, mince, dokumenty a dále lze nastavit, zda mají být analyzovány všechny obrázkové soubory nebo pouze fotky či obrázky aplikací. Funkce bylo využito.

V posledním kroku bylo nastaveno místo uložení výsledných souborů a název exportu. Po skončení analýzy vznikla ve vybraném umístění složka, ve které jsou uloženy reporty – html, ufdr, pdf, xlx, a exporty – html, mobiledit, ufdr, pdf a také snímky obrazovky jednotlivých kroků v nástroji. Aplikace, která byla během extrakce nahrána do telefonu zůstala nahrána

v mobilním zařízení i po skončení extrakce, což je jedním z výrazných zásahů do mobilního telefonu, respektive jeho systému a dat jako důkazu.

7.1.2. iOS

Nastavení je pro všechny mobilní telefony s operačním systémem iOS stejné.

Mobilní telefon byl načten po připojení pomocí kabelu. Dalšími možnostmi připojení bylo Bluetooth nebo WiFi. U mobilního telefonu je nutné znát všechny přístupové údaje, jinak analýza není možná. S tím souvisí nutnost mít mobilní telefon po celou dobu zapnutý, mít stažené správné ovladače a mít mobilní telefon správně nastavený.

Pro všechny mobilní telefony s operačním systémem iOS je nastavení následující:

- nastavit možnost automatického zamykání na nikdy
- potvrdit důvěru vzhledem k počítači

Následně bylo možné vybrat typ exportu – celý obsah, specifický výběr, smazaná data nebo rodičovská kontrola. Pro tento mobilní telefon byla vybrána možnost analýzy celého obsahu. V dalším kroku bylo možné vyplnit detaily o případu, telefonu a vyšetřovateli. Dále pak byla možnost vybrat formáty exportů a reportů. K dispozici byl PDF Report, HTML Report, MS Excel Report a MOBILedit Backup, MOBILedit Export a Cellebrite UFDR jako exporty. Zde byly vybrány všechny možnosti, ale následně byl použit pouze PDF Report.

Forenzní nástroj umožnil využít funkci PhotoRecognizer – lze nastavit specifické kategorie pro rozpoznávání obrázkových souborů – drogy, nahota, mince, dokumenty a dále lze nastavit, zda mají být analyzovány všechny obrázkové soubory nebo pouze fotky či obrázky aplikací. Funkce bylo využito.

V posledním kroku bylo nastaveno místo uložení výsledných souborů a název exportu. Po skončení analýzy vznikla ve vybraném umístění složka, ve které jsou uloženy reporty – html, ufdr, pdf, xlx, a exporty – html, mobiledit, ufdr, pdf a také snímky obrazovky jednotlivých kroků v nástroji.

7.1.3. Windows Mobile

Nastavení je pro všechny mobilní telefony s operačním systémem Windows Mobile stejné.

Mobilní telefon byl načten po připojení pomocí kabelu. Dalšími možnostmi připojení bylo Bluetooth nebo Wi-fi.

U mobilního telefonu je nutné znát všechny přístupové údaje, jinak analýza není možná. S tím souvisí nutnost mít mobilní telefon po celou dobu zapnutý a mít stažené správné ovladače. Následně bylo možné vybrat typ exportu – celý obsah, specifický výběr, smazaná data nebo rodičovská kontrola. Pro tento mobilní telefon byla vybrána možnost analýzy celého obsahu. V dalším kroku bylo možné vyplnit detaily o případu, telefonu a vyšetřovateli. Dále pak byla možnost vybrat formáty exportů a reportů. K dispozici byl PDF Report, HTML Report, MS Excel Report a MOBILedit Backup, MOBILedit Export a Cellebrite UFDR jako exporty. Zde byly vybrány všechny možnosti, ale následně byl použit pouze PDF Report.

Forenzní nástroj umožnil využít funkci PhotoRecognizer – lze nastavit specifické kategorie pro rozpoznávání obrázkových souborů – drogy, nahota, mince, dokumenty a dále lze nastavit, zda mají být analyzovány všechny obrázkové soubory nebo pouze fotky či obrázky aplikací. Funkce bylo využito.

V posledním kroku bylo nastaveno místo uložení výsledných souborů a název exportu. Po skončení analýzy vznikla ve vybraném umístění složka, ve které jsou uloženy reporty – html, ufdr, pdf, xlx, a exporty – html, mobiledit, ufdr, pdf a také snímky obrazovky jednotlivých kroků v nástroji.

7.2. Analýza mobilních telefonů nástrojem UFED 4PC

7.2.1. Android

Prvním krokem byl výběr extrakce z mobilního zařízení. Dalšími možnostmi bylo vytěžení SIM nebo jiného zařízení připojeného přes USB. Dalším krokem byla identifikace zařízení buď manuálně přes seznam mobilních telefonů nebo pomocí autodetekce, kdy bylo nutné připojit zařízení přes kabel hned. Následně bylo možné vybrat typ extrakce. Ne u všech

zařízení byla možná extrakce fyzická a u těch, kdy byla nabízena se ne vždy povedla. Poté byla vybrána složka, kam měla být analýza uložena.

Než začala extrakce bylo nutné mobilní telefon nastavit podle pokynů forenzního nástroje. Jednalo se o tyto kroky:

- aktivovat vývojářský režim
- aktivovat ladění USB
- povolit zařízení MTP – mediální zařízení
- nahraje se klient do telefonu pokud je nutný
- nastavit, aby byly potvrzeny všechny výzvy v oknech (jen ro fyzickou)
- povolit neznámé zdroje
- zapojit zařízení do UFED 4PC
- zmáčknout pokračovat

Následně začala extrakce samotná. Po extrakci byl klient – aplikace sama odinstalována. A vznikl soubor .ufdr, který byl následně načten UFED Readerem.

7.2.2. iOS

Prvním krokem byl výběr extrakce z mobilního zařízení. Dalšími možnostmi bylo vytěžení SIM nebo jiného zařízení připojeného přes USB. Dalším krokem byla identifikace zařízení buď manuálně přes seznam mobilních telefonů nebo pomocí autodetekce, kdy bylo nutné připojit zařízení přes kabel hned. Následně bylo možné vybrat typ extrakce. Zde u jediného zařízení s operačním systémem iOS nebyla umožněna fyzická extrakce, na výběr byla pouze logická nebo analýza souborového systému, která byla následně provedena. Poté byla vybrána složka, kam měla být analýza uložena.

Než začala extrakce bylo nutné mobilní telefon nastavit podle pokynů forenzního nástroje.

- zapnout telefon a nechat plně načíst
- v nastavení nastavit auto-lock na nikdy
- zapojit zařízení do UFED 4PC
- zmáčknout pokračovat

A následně začala extrakce samotná. A vznikl soubor .ufdr, který byl následně načten UFED Readerem.

7.2.3. Windows Mobile

Prvním krokem byl výběr extrakce z mobilního zařízení. Dalšími možnostmi bylo vytěžení SIM nebo jiného zařízení připojeného přes USB.

Dalším krokem byla identifikace zařízení buď manuálně přes seznam mobilních telefonů nebo pomocí autodetekce, kdy bylo nutné připojit zařízení přes kabel hned. Následně bylo možné vybrat typ extrakce. Ne u všech zařízení byla možná extrakce fyzická a u těch, kdy byla nabízena se ne vždy povedla. Poté byla vybrána složka, kam měla být analýza uložena.

Dále bylo nutné mobilní telefon nastavit podle pokynů forenzního nástroje.

- zapnout zařízení
- deaktivovat zámek obrazovky, je-li aktivní
- zapojit zařízení do UFED 4PC
- zmáčknout pokračovat

Poté nastala extrakce. A vznikl soubor .ufdr, který byl následně načten UFED Readerem.

7.3. Analýza mobilních telefonů nástrojem Oxygen Forensic® Extractor

7.3.1. Android

Po spuštění zařízení a zobrazení menu byla vybrána možnost automatické detekce telefonu, druhou možností je vybrání zařízení manuálně. Následně se telefon nastavil podle instrukcí:

- odemknout zařízení
- aktivovat ladění USB
- odsouhlasit RSA klíč
- povolit ve vývojářských možnostech funkci zůstat vzhůru
- mít správně nainstalované ovladače zařízení

Po připojení pomocí kabelu se telefon načetl. Byl detekován model, IMEI a další. Následně bylo možné vyplnit informace o případu a o zařízení. V dalším kroku byly vybrány kategorie k extrakci – typ extrakce. U mobilů typu Android byla vytvořena analýza typu Android backup.

Potom nastala samotná extrakce jejímž výsledkem je soubor.ofd, který lze poté načíst pomocí Oxygen Forensic Viewer. Další dva stejné soubory byly zašifrované, jeden pomocí MD5 a druhý pomocí SHA2.

7.3.2. iOS

Po spuštění zařízení a zobrazení menu byla vybrána možnost automatické detekce mobilního telefonu, druhou možností je vybrání zařízení manuálně. Po připojení pomocí kabelu se mobilní telefon načetl. Byl detekován model, IMEI, boot loader a další. Následně bylo možné vyplnit informace o případu a o zařízení. V dalším kroku byly vybrány kategorie k extrakci – typ extrakce. Dle nástroje proběhla klasická logická analýza, ale byla nalezena i smazaná data což odpovídá spíše fyzické analýze nebo analýze systému souborů. Poté začala samotná extrakce. Po jejím skončení byla analýza uložena ve formě tří souborů – jeden pro načtení do prohlížeče forenzního nástroje a další dva stejné soubory byly zašifrované, jeden pomocí MD5 a druhý pomocí SHA2.

7.3.3. Windows Mobile

Po spuštění zařízení a zobrazení menu byla vybrána možnost automatické detekce mobilního telefonu, druhou možností je vybrání zařízení manuálně. Po připojení pomocí kabelu se mobilní telefon načetl. Byl detekován model. Následně bylo možné vyplnit informace o případu a o zařízení. V dalším kroku byly vybrány kategorie k extrakci – typ extrakce – zde MTP – pro mobilní telefony platformy Windows – jedná se o analýzu – zde zkopírování souborového systému, respektive tedy záloha mobilního telefonu.

Poté nastala samotná extrakce jejímž výsledkem je soubor.ofd, který lze násedně načíst pomocí Oxygen Forensic Viewer. Další dva stejné soubory byly zašifrované, jeden pomocí MD5 a druhý pomocí SHA2.

7.4. Analýza mobilních telefonů nástrojem XRY Logical

7.4.1. Android

Mobilní telefon lze připojit a následně je rozpoznán automaticky nebo lze mobilní telefon vyhledat manuálně. Nástroj hned detekuje, jaké informace budou nebo by měly být z mobilního telefonu extrahovány a následně je vybrán druh analýzy. Této nástroj také nainstaloval na mobilní telefon aplikaci, pomocí které extrahoval data. V tomto případě byla aplikace smazána automaticky. Průběh analýzy je k dispozici v podobě logů ve XRY Readeru. Po samotné extrakci vznikl soubor .xrycase, který byl načten do XRY Readeru.

7.4.2. iOS

Připojit lze mobilní telefon, který je rozpoznán nebo mobilní telefon vyhledáme manuálně. Nástroj ihned detekuje, jaké informace je schopen z mobilního telefonu extrahovat, v případě mobilního telefonu iPhone 5s se jedná o kontakty, hovory, kalendář, SMS, MMS, e-maily, soubory – obrázky, hudba, video a soubory z sd karty. Následně je vybrán druh analýzy. Tento nástroj také nainstaloval na mobilní telefon aplikaci, pomocí které extrahoval data. V tomto případě byla aplikace smazána automaticky. Průběh analýzy je k dispozici v podobě logů ve XRY Readeru. Také tentokrát vznikl soubor .xrycase, který byl poté načten do XRY Readeru.

7.4.3. Windows Mobile

Připojit lze mobilní telefon, který je rozpoznám nebo mobilní telefon vyhledáme manuálně. Nástroj ihned detekuje, jaké informace budou nebo by měly být z mobilního telefonu extrahovány. Zde se jedná pouze o soubory typu obrázky, videa, audio. V nastavení je třeba zakázat akce, pokud se zařízení připojí k počítači. Následně je vybrán druh analýzy. Tento nástroj také nainstaloval na mobilní telefon aplikaci, pomocí které extrahoval data. V tomto případě byla aplikace smazána automaticky. Průběh analýzy je k dispozici v podobě logů ve XRY Readeru. Po samotné extrakci vznikl soubor .xrycase, který byl poté do XRY Readeru načten.

7.5. Analýza pomocí Android Debug Bridge

Tímto nástrojem lze testovat pouze mobilní telefony s operačním systémem Android.

Za prvé je nutné nainstalovat JDK – Java Development Kit. JDK je produkt Oracle Corporation, který obsahuje soubor základních nástrojů pro vývoj aplikací na platformě Java. Instalace je nezbytná pro následující krok.

Za druhé je nutné nainstalovat Android Studio, jehož součástí je i Android SDK – Software Development Kit, který obsahuje požadovaný ADB.

Následně je třeba spustit SDK Manager a nainstalovat Google USB drivers. Dále v systémových proměnných je třeba uložit do proměnné PATH cestu k Platform-tools a také je nutné nainstalovat ovladače pro daný mobilní telefon.

Po nastavení mobilního telefonu a pracovní stanice byl mobilní telefon připojen k počítači pomocí USB kabelu. Následně byl otevřen příkazový řádek a pomocí příkazů byla získána data z mobilního telefonu.

```
adb backup -apk -shared -all -f C:\Users\NAME\backup.ab
```

Pomocí tohoto příkazu byla provedena záloha mobilního telefonu. [12]

8. Výsledky forenzní analýzy

8.1. Výsledky forenzní analýzy komerčních nástrojů

Výsledky budou reprezentovány u jednotlivých telefonů a budou porovnány výsledky jednotlivých forenzních nástrojů.

8.1.1. Výsledky analýz jednotlivých nástrojů u mobilního telefonu ZTE Kis 3

Výsledky analýz jednotlivých nástrojů u mobilního telefonu ZTE Kis 3 s operačním systémem Android verze 4.4.2				
	UFED 4PC	**XRY Logical**	**Oxygen Forensic® Extractor**	**MOBILedit Forensic Express**
Typ forenzní analýzy	fyzická	logická	android backup	
Informace o zařízení	ano	ano	ano	ano
Zprávy	ano	ne	ne	ne
Kontakty	ano	ano	ano	ano
Hovory	ano	ne	ne	ano
Uživatelské účty	ano	ano	ne	ano
Hesla	ano	ano	ne	ne
Lokace	ano	ano	ne	ne
Wifi sítě	ano	ne	ne	ano
Historie prohlížeče	ano	ano	ne	ne
Obrázky	ano	ano	ne	ano
Video	ano	ano	ne	ne
Audio	ano	ano	ne	ne
Dokumenty	ano	ano	ne	ne
Kalendář	ano	ano	ne	ano
Poznámky	ne	ne	ne	ne
Úkoly	ne	ne	ne	ne
Logy telefonu	ano	ano	ano	ano
Bluetooth spojení	ne	ne	ne	ano
Aplikace	ano	ano	ne	ano
Smazaná data	ano	ano	ne	ne

Tabulka 1 Výsledky analýz mobilního telefonu ZTE Kis 3

Prvním nástrojem, kterým byl mobilní telefon testován je UFED. Mobilní telefon ZTE Kis 3 se tímto přístrojem podařilo analyzovat fyzickou analýzou.

Data vytěžená z mobilního telefonu jsou obsažena v jednom souboru. ufdr a tento soubor lze spustit v UFED Readeru, kde jsou rozdělena do jednotlivých kategorií. U každé z nich lze vyčíst kolik souborů se v dané kategorii podařilo vytěžit. Jak je vidět z tabulky.

Nástroj dokázal vytěžit i data smazaná. U tohoto mobilního telefonu byla tímto forenzním nástrojem nalezena smazaná data u 20 kategorií.

V prohlížeči tohoto forenzního nástroje lze vyčíst informace o mobilním telefonu jako takovém, například verzi operačního systému, časovou zónu, název zařízení bluetooth, čas poslední aktivace a další.

Dalším nástrojem, který zkoumal tento mobilní telefon je XRY. Nástroj vytěžil telefon logickou analýzou, respektive je tak označena firmou MSAB, ale spíše se jedná o analýzu souborového systému, jelikož byly také nalezeny smazané soubory, jak lze vyčíst i z tabulky. Data vytěžená z mobilního telefonu jsou stejně jako u předchozího nástroje obsažena v jednom souboru .xrycase, který lze následně načíst XRY Readerem. Z mobilního telefonu byly vyextrahovány informace o zařízení samotném. Jedná se o název zařízení, verze operačního systému, časovou zónu, zda je vložená SIM karta a další.

Nástrojem, který tento mobilní telefon testoval je také Oxygen Forensic® Extractor. Tento nástroj udělal pouze velmi omezenou logickou analýzu – respektive zálohování Androidu – Android backup. Z tabulky lze vyčíst, že nástroj vytěžil pouze telefonní kontakty a logy telefonního zařízení. Dále rozpoznal aplikace, ale žádná data z nich nevyextrahoval. Stejně jako předchozí nástroje i tento zjistil operační systém mobilního telefonu a jeho verzi. U tohoto nástroje je k dispozici soubor s informacemi o extrakci – logy extakce, což může být užitečné při následné dokumentaci průběhu analýzy pro trestní řízení.

Posledním nástrojem, který zkoumal mobilní telefon je MOBILedit Forensic Express. Tomuto nástroji se mobilní telefon podařilo vytěžit pouze logickou analýzou. Jedná se tedy o mnohem méně dat než u předchozích nástrojů, ale také získal data o mobilním telefonu samotném. Například operační systém telefonu, jeho verzi, časovou zónu a další.

8.1.2. Výsledky analýz jednotlivých nástrojů u mobilního telefonu iPhone 5s

Výsledky analýz jednotlivých nástrojů u mobilního telefonu iPhone 5s s operačním systémem iOS verze 11.1.2				
	UFED 4PC	**XRY Logical**	**Oxygen Forensic® Extractor**	**MOBILedit Forensic Express**
Typ forenzní analýzy	souborový systém	souborový systém	logická	
Informace o telefonu	ano	ano	ano	ano
Zprávy	ano	ano	ano	ano
Kontakty	ano	ano	ano	ano
Hovory	ano	ano	ano	ano
Uživatelské účty	ano	ano	ano	ano
Hesla	ano	ano	ano	ano
Lokace	ano	ano	ano	ano
Wifi sítě	ano	ano	ano	ano
Historie prohlížeče	ano	ano	ne	ano
Obrázky	ano	ano	ano	ano
Video	ano	ano	ano	ano
Audio	ano	ano	ano	ano
Dokumenty	ano	ano	ano	ano
Kalendář	ano	ano	ne	ano
Poznámky	ano	ano	ne	ano
Úkoly	ne	ano	ne	ano
Logy telefonu	ano	ano	ne	ne
Bluetooth spojení	ano	ne	ne	ne
Aplikace	ano	ano	ano	ano
Smazaná data	ano	ano	ano	ano

Tabulka 2 Výsledky analýz mobilního telefonu iPhone 5s

První nástrojem, který tento mobilní telefon analyzoval je nástroj UFED. Jedná se o analýzu souborového systému. Jak je vidět z tabulky, bylo nalezeno i několik smazaných souborů v kategoriích cookies, konfigurací, výpis hovorů, chaty, webové záložky, webová historie a hledané položky na webu. Nástroj nevytěžil žádné soubory v kategorii úkoly. Tuto kategorii nástroj nevytváří u žádného mobilního telefonu. Data, která ostatní nástroje definují jako úkoly se zde počítají ke kalendáři.

Také o tomto mobilním telefonu lze vyčíst informace v UFED Readeru. Jedná se opět o verzi operačního systému, jméno vlastníka, časovou zónu, název zařízení bluetooth, čas poslední aktivace, název a cestu ke složce se kterou se mobilní telefon synchronizuje.

Dalším nástrojem, který extrahoval data z tohoto mobilního telefonu je XRY. I přesto, že nástroj definuje danou analýzu jako logickou vytěžil i smazané soubory, jak je vidět z tabulky. Jedná se o tyto kategorie – logy, hovory, události, úkoly, webová historie a vyhledávání.

Z mobilního telefonu také získal informace o zařízení samotném. Jedná se o operační systém a verzi, časovou zónu, kapacitu a volnou kapacitu, jméno vlastníka a jeho telefonní číslo.

Dalším nástrojem, který zkoumal tento mobilní telefon je Oxygen Forensic® Extractor. Nástroj opět klasifikuje analýzu jako logickou, ale jak je vidět i z tabulky, dokázal extrahovat i některá smazaná data. A to ze zpráv a z výpisu hovorů. I tento forenzní nástroj dokázal získat informace o mobilním telefonu. Jde o verzi operačního systému a také lze vyčíst ve Oxygen Vieweru data o extrakci – její době, verzi forenzního nástroje a další.

Posledním forenzním nástrojem, který zkoumal tento mobilní telefon je MOBILedit Forensic Express. U tohoto mobilního telefonu nástroj dokázal provést analýzu, kde z mobilního telefonu vytěžil i smazané soubory, jak je vidět z tabulky. Jedná se o tyto kategorie – výpis hovorů, různé zprávy, úkoly a události, lokace a cookies soubory. Také v tomto případě forenzní nástroj získal informace o mobilním telefonu jako takovém. Získal informace například o operačním systému a verzi, vlastníkovi telefonu, časové zóně, telefonním čísle vlastníka, datum posledního backupu a další.

8.1.3. Výsledky analýz jednotlivých nástrojů u mobilního telefonu Microsoft Lumia 550

Výsledky analýz jednotlivých nástrojů u mobilního telefonu Microsoft Lumia 550 s operačním systémem Windows 10 Mobile				
	UFED 4PC	**XRY Logical**	**Oxygen Forensic® Extractor**	**MOBILedit Forensic Express**
Typ forenzní analýzy	logická	logická	MTP	
Informace o telefonu	ne	minimálně	minimálně	minimálně
Zprávy	ne	ne	ne	ne
Kontakty	ne	ne	ne	ne
Hovory	ne	ne	ne	ne
Uživatelské účty	ne	ne	ne	ne
Hesla	ne	ne	ne	ne
Lokace	ne	ano	ne	ano
Wifi sítě	ne	ne	ne	ne
Historie prohlížeče	ne	ne	ne	ne
Obrázky	ano	ano	ano	ano
Video	ne	ano	ano	ano
Audio	ano	ano	ano	ne
Dokumenty	ano	ano	ano	ne
Kalendář	ne	ne	ne	ne
Poznámky	ne	ne	ne	ne
Úkoly	ne	ne	ne	ne
Logy telefonu	ne	ne	ne	ne
Bluetooth spojení	ne	ne	ne	ne
Aplikace	ano	ne	ne	ne
Smazaná data	ne	ne	ne	ne

Tabulka 3 Výsledky analýz u mobilního telefonu Microsoft Lumia 550

Prvním nástrojem, který extrahoval data z tohoto mobilního telefonu je UFED. Provedená analýza je logická. Jak je vidět z tabulky nástroj dokázal vyextrahovat pouze aplikace, některé obrázky, audio a dokumenty. Je otázkou, zda je zabezpečení mobilního telefonu dokonale zabezpečené nebo tomu je jinak.

Druhým nástrojem, který extrahoval data z tohoto mobilního telefonu je XRY. Také provedl logickou analýzu. Jak je vidět v tabulce nástroj získal informace o GPS lokacích, obrázky a videa z SD karty a audio, které je možné přehrát přímo v XRY Readeru.

Nástrojem Oxygen Forensic® Extractor byly extrahovány pouze obrázky, videa, audia a dokumenty, což lze vypozorovat z tabulky. Z informací o zařízení bylo extrahováno pouze jméno výrobce.

Jak je vidět v tabulce, nástroj MOBILedit Forensic Express extrahoval obrázky, GPS polohy a video soubory. Z informací o telefonu získal pouze platformu.

8.1.4. Výsledky analýz jednotlivých nástrojů u mobilního telefonu Samsung Galaxy A5

Výsledky analýz jednotlivých nástrojů u mobilního telefonu Samsung Galaxy A5 s operačním systémem Android verze 7.0				
	UFED 4PC	**XRY Logical**	**Oxygen Forensic® Extractor**	**MOBILedit Forensic Express**
Typ forenzní analýzy	souborový systém	logická	andriod backup	
Informace o telefonu	ano	ano	ano	ano
Zprávy	ano	ne	ne	ano
Kontakty	ano	ne	ano	ano
Hovory	ano	ne	ne	ne
Uživatelské účty	ne	ne	ano	ne
Hesla	ano	ne	ne	ne
Lokace	ano	ano	ne	ano
Wifi sítě	ano	ne	ne	ano
Historie prohlížeče	ne	ne	ne	ne
Obrázky	ano	ano	ano	ano
Video	ne	ne	ne	ne
Audio	ano	ano	ne	ne
Dokumenty	ano	ano	ne	ne
Kalendář	ano	ano	ano	ano
Poznámky	ne	ne	ne	ne
Úkoly	ne	ne	ne	ne
Logy telefonu	ne	ano	ano	ano
Bluetooth spojení	ne	ne	ne	ne
Aplikace	ano	ano	ano	ano
Smazaná data	ano	ano	ne	Ne

Tabulka 4 Výsledky analýz u mobilního telefonu Samsung Galaxy A5

První nástrojem, který tento mobilní telefon analyzoval je nástroj UFED. Jedná se o analýzu souborového systému. Jak je vidět z tabulky byla nalezena i smazaná data v kategorii kalendář. Nástroj nevytěžil žádné soubory v kategorii úkoly ze stejného důvodu jako u prvního mobilního telefonu.

Dalším nástrojem, který extrahoval data z tohoto mobilního telefonu je XRY. I přesto, že nástroj definuje danou analýzu jako logickou, vytěžil, jak je vidět z tabulky, i smazané soubory v kategorii kalendář.

Z mobilního telefonu také získal informace o zařízení samotném. Jedná se například o operační systém a verzi, časovou zónu, mobilního operátora a další.

Dalším nástrojem, který zkoumal tento mobilní telefon je Oxygen Forensic® Extractor. Nástroj opět klasifikuje analýzu jako Andriod backup. Jak je vidět z tabulky nástroj extrahoval z mobilního telefonu kontakty, obrázky, logy zařízení, události z kalendáře, ke kterému se pojí i jediný získaný účet. I tento forenzní nástroj dokázal získat informace o mobilním telefonu. Jedná se o operační systém a jeho verzi.

Posledním forenzním nástrojem, který zkoumal tento mobilní telefon je MOBILedit Forensic Express. Nepodařilo se získat žádná smazaná data, jak lze vidět z tabulky. Také v tomto případě forenzní nástroj získal informace o mobilním telefonu jako takovém. Získal informace například o operačním systému a verzi, vlastníkovi telefonu, časové zóně, mobilním operátorovi a další.

8.1.5. Výsledky analýz jednotlivých nástrojů u mobilního telefonu Samsung Galaxy Core Prime

Výsledky analýz jednotlivých nástrojů u mobilního telefonu Samsung GSM SM-G361F Galaxy Core Prime s operačním systémem Android verze 5.1.1				
	UFED 4PC	**XRY Logical**	**Oxygen Forensic® Extractor**	**MOBILedit Forensic Express**
Typ forenzní analýzy	fyzická	logická	android backup	
Informace o telefonu	ano	ano	ano	ano
Zprávy	ano	ano	ano	ano
Kontakty	ano	ano	ano	ano
Hovory	ano	ano	ano	ano
Uživatelské účty	ano	ano	ano	ano
Hesla	ano	ano	ano	ne
Lokace	ano	ano	ano	ano
Wifi sítě	ano	ano	ano	ano
Historie prohlížeče	ano	ano	ano	ano
Obrázky	ano	ano	ano	ano
Video	ano	ano	ne	ano
Audio	ano	ano	ne	ano
Dokumenty	ano	ano	ne	ano
Kalendář	ano	ano	ano	ano
Poznámky	ano	ne	ne	ne
Úkoly	ne	ne	ne	ne
Logy telefonu	ne	ano	ano	ano
Bluetooth spojení	ne	ne	ne	ano
Aplikace	ano	ano	ano	ano
Smazaná data	ano	ano	ano	ano

Tabulka 5 Výsledky forenzních analýz u mobilního telefonu Samsung Galaxy Core Prime

První nástrojem, který tento mobilní telefon analyzoval je nástroj UFED. Jedná se o analýzu fyzickou. Bylo nalezeno mnoho dat i smazaných. Jak je vidět z tabulky, nástroj nevytěžil žádné soubory pouze v kategorii úkoly a logy. Také o tomto mobilním telefonu lze vyčíst informace v UFED Readeru. Jedná se opět o verzi operačního systému, jméno vlastníka, časovou zónu a mobilního operátora.

Dalším nástrojem, který extrahoval data z tohoto mobilního telefonu je nástroj XRY. Přesto, že nástroj definuje danou analýzu jako logickou opět vytěžil i smazané soubory, jak je vidět z tabulky. Jedná se o tyto kategorie - logy, hovory, události, SMS a MMS zprávy, webová historie a cookies. Z mobilního telefonu také získal informace o zařízení samotném. Jedná se například o operační systém a verzi, časovou zónu a další.

Dalším nástrojem, který zkoumal tento mobilní telefon je Oxygen Forensic® Extractor. Nástroj opět klasifikuje analýzu Android backup. Dokázal extrahovat i některá smazaná data, jak lze vidět z tabulky. A to z výpisu hovorů, lokace, historie prohlížeče a e-mailu.I tento forenzní nástroj dokázal získat informace o mobilním telefonu. Jde o verzi operačního systému, jméno vlastníka a e-mail.

Posledním forenzním nástrojem je MOBILedit Forensic Express. U tohoto mobilního telefonu nástroj vytěžil i smazané soubory, jak je vidět z tabulky, ale pouze kategorie bluetooth párování. Nástroj nevytěžil žádná data pouze v kategorii úkoly a poznámky. Také v tomto případě forenzní nástroj získal informace o mobilním telefonu jako takovém. Získal informace například o operačním systému a verzi, časové zóně, mobilním operátorovi a další.

8.1.6. Výsledky analýz jednotlivých nástrojů u mobilního telefonu Samsung Galaxy J3

Výsledky analýz jednotlivých nástrojů u mobilního telefonu Samsung Galaxy J3 2016 s operačním systémem Android verze 5.1.1				
	UFED 4PC	**XRY Logical**	**Oxygen Forensic® Extractor**	**MOBILedit Forensic Express**
Typ forenzní analýzy	souborový systém	logická	android backup	
Informace o telefonu	minimální	ano	ano	ano
Zprávy	ne	ano	ano	ano
Kontakty	ano	ano	ano	ano
Hovory	ano	ano	ano	ano
Uživatelské účty	ano	ano	ano	ne
Hesla	ano	ne	ne	ne
Lokace	ano	ano	ano	ano
Wifi sítě	ano	ne	ano	ano
Historie prohlížeče	ano	ano	ano	ne
Obrázky	ano	ano	ano	ano
Video	ano	ano	ne	ano
Audio	ano	ano	ano	ano
Dokumenty	ano	ano	ano	ano
Kalendář	ano	ano	ano	ano
Poznámky	ne	ne	ne	ne
Úkoly	ne	ne	ne	ne
Logy telefonu	ne	ano	ano	ano
Bluetooth spojení	ne	ne	ne	ano
Aplikace	ano	ano	ano	ano
Smazaná data	ano	ano	ano	ano

Tabulka 6 Výsledky forenzních analýz u mobilního telefonu Samsung Galaxy J3

První nástrojem, který tento mobilní telefon analyzoval je nástroj UFED. Jedná se o analýzu souborového systému. Jak je vidět z tabulky bylo nalezeno i několik smazaných souborů v kategoriích obrázky, cookies, webová historie a aplikace. Nástroj nevytěžil žádné soubory v kategorii úkoly, logy a bluetooth párování. O tomto mobilním telefonu lze vyčíst v UFED Readeru pouze AndroidID a časovou zónu.

Dalším nástrojem, který extrahoval data z tohoto mobilního telefonu je XRY. I přesto, že nástroj definuje danou analýzu jako logickou vytěžil nástroj i u tohoto mobilního telefonu smazané soubory, jak lze vidět v tabulce. Jedná se o tyto kategorie - logy, kontakty, hovory, zprávy a cookies. Z mobilního telefonu také získal informace o zařízení samotném. Jedná se například o operační systém a verzi, časovou zónu a další.

Oxygen Forensic® Extractor jako další nástroj extrahoval data pomocí Android backup. Byla extrahována i některá smazaná data, jak je vidět z tabulky, a to z webového prohlížeče a hovorů. I tento forenzní nástroj dokázal získat informace o mobilním telefonu. Jde například o verzi operačního systému, jméno vlastníka a e-mail.

Posledním forenzním nástrojem, který zkoumal tento mobilní telefon je MOBILedit Forensic Express. Nástroj dokázal vytěžit i smazané soubory, jak lze vidět v tabulce, ale jen z kategorie bluetooth párování. Také v tomto případě forenzní nástroj získal informace o mobilním telefonu jako takovém. Získal informace například o operačním systému a verzi, časové zóně a další.

8.1.7. Výsledky analýz jednotlivých nástrojů u mobilního telefonu Samsung Galaxy J5

Výsledky analýz jednotlivých nástrojů u mobilního telefonu Samsung GSM SM-J510FN Galaxy J5 s operačním systémem Android verze 6.0.1				
	UFED 4PC	**XRY Logical**	**Oxygen Forensicc® Extractor**	**MOBILedit Forensic Express**
Typ forenzní analýzy	souborový systém	logická	android backup	
Informace o telefonu	minimální	ano	ano	ano
Zprávy	ano	ano	ano	ano
Kontakty	ne	ne	ano	ano
Hovory	ne	ne	ne	ne
Uživatelské účty	ano	ano	ano	ne
Hesla	ano	ne	ano	ne
Lokace		ano	ne	ano
Wifi sítě	ano	ne	ano	ano
Historie prohlížeče	ano	ano	ne	ne
Obrázky	ano	ano	ano	ano
Video	ano	ano	ne	ano
Audio	ne	ano	ne	ano
Dokumenty	ne	ano	ano	ano
Kalendář	ne	ne	ne	ne
Poznámky	ne	ne	ne	ne
Úkoly	ne	ne	ne	ne
Logy telefonu	ne	ano	ano	ne
Bluetooth spojení	ne	ne	ne	ano
Aplikace	ano	ano	ano	ano
Smazaná data	ano	ano	ne	ano

Tabulka 7 Výsledky forenzních analýz u mobilního telefonu Samsung Galaxy J5

První nástrojem, který tento mobilní telefon analyzoval je nástroj UFED. Jedná se o analýzu souborového systému. Jak lze vidět z tabulky, bylo nalezeno i několik smazaných souborů v kategoriích cookies, zprávy, obrázky, videa, aplikace a webová historie. Také o tomto mobilním telefonu lze vyčíst informace v UFED Readeru pouze o AndroidID a časové zóně.

Dalším nástrojem, který extrahoval data z tohoto mobilního telefonu je XRY. I přesto, že nástroj definuje danou analýzu jako logickou, vytěžil i smazané soubory, jak lze vidět i z tabulky. Jedná se o tyto kategorie: logy a zprávy. Z mobilního telefonu také získal informace o zařízení samotném. Jedná se například o operační systém a verzi, časovou zónu a další.

Oxygen Forensic® Extractor je dalším nástrojem, který zkoumal tento mobilní telefon, jednalo se o Android backup. Jak lze vidět z tabulky, nástroj nenašel žádná smazaná data. I tento forenzní nástroj dokázal získat informace o mobilním telefonu. Jde o operační systém, jeho verzi a e-mail uživatele.

Posledním forenzním nástrojem, který analyzoval tento mobilní telefon je MOBILedit Forensic Express. Jak je vidět z tabulky, u tohoto mobilního telefonu nástroj dokázal vytěžit i smazané soubory, ale pouze u bluetooth párování. Také v tomto případě forenzní nástroj získal informace o mobilním telefonu jako takovém. Získal informace například o operačním systému a verzi, časové zóně, mobilním operátorovi a další.

8.2. Výsledky forenzní analýzy pomocí ADB

Výsledný soubor se zálohou lze prohlížet pomocí Andriod Backup Extractor. U souborů s koncovkou .ab není validní zápatí. Tato aplikace pomocí příkazového řádku a příkazu

```
java -jar abe.jar unpack <backup.ab> <backup.tar>
```

přetvoří soubor do souboru s koncovkou .tar, následně po extrahování můžeme procházet složky z vytvořené zálohy. Jedná se ovšem o složky a soubory záloh aplikací a soubory nejsou v čitelné podobě jako je tomu u komerčních prostředků. Byla získána data ze všech mobilních telefonů s operačním systémem Android, až na mobilní telefon ZTE Kis 3.

Z mobilních telefonů byly získány některé obrázkové soubory z aplikací, fotky poslané e-mailem, aplikace, emailové účty, navštívené webové stránky. K většině složek byl odepřen přístup hned při extrakci.

8.3. Porovnání výsledků konkrétních kategorií

Tato část se bude zabývat porovnáním konkrétních kategorií i jednotlivých nástrojů. Jedná se o kategorie zprávy, kontakty, hovory, účty, hesla, WiFi připojení a obrázkové soubory.

8.3.1. Výsledky analýz jednotlivých nástrojů v kategorii zprávy

Výsledky analýz jednotlivých nástrojů v kategorii zprávy				
	UFED 4PC	**XRY Logical**	**Oxygen Forensic® Extractor**	**MOBILedit Forensic Express**
iPhone 5s	836 sms 6098 app	836 sms 6161 app	836 sms 6763 app	836 sms 6519 app
Microsoft Lumia 550				
Samsung Galaxy J3		3604 app	220 sms	221 sms
Samsung Galaxy J5	16 app	6 app	376 sms	313 sms
Samsung GalaxyA5	7915 sms			7655 sms
Samsung Galaxy Core Prim	3492 sms 548 app	3279 sms 548 app	3244 sms	3130 sms
ZTE Kis 3	9189 sms 993 app			

Tabulka 8 Výsledky analýz jednotlivých nástrojů v kategorii zprávy

Nejvíce pozitivních výsledků z oblasti zpráv má na svém kontě nástroj UFED a MOBILedit Forensic Express. Vytěžili 6 telefonů z 8. Nejvíce SMS na počet vytěžil nástroj UFED hlavně z toho důvodu, že jako jediný extrahoval SMS z mobilního telefonu ZTE Kis 3. SMS u nejvíce mobilních telefonů vytěžil nástroj MOBILedit Forensic Express. U všech získaných SMS zpráv byl zjištěn odesílatel a příjemce, čas odeslání. U většiny zpráv i celý text. Nejvíce zpráv z aplikací vytěžil nástroj XRY. Jednalo se o vytěžení konverzací z daných aplikací jako je Facebook Messenger, Whatsapp, Tinder a další. U všech zpráv z aplikací byla zjištěna zdrojová aplikace, čas odeslání zprávy a účastníci konverzace. Všem nástrojům se nejlépe extrahovaly data z mobilního telefonu iPhone 5s. Všechny nástroje získaly stejný počet SMS a relativně se shodly i na počtu zpráv z aplikací. U této kategorie jsou spolehlivé všechny nástroje.

8.3.2. Výsledky analýz jednotlivých nástrojů v kategorii kontakty

Výsledky analýz jednotlivých nástrojů v kategorii kontakty				
	UFED 4PC	**XRY Logical**	**Oxygen Forensic® Extractor**	**MOBILedit Forensic Express**
iPhone 5s	23 tel 388 app	23 tel 348 app	23tel 339app	23tel 42app
Microsoft Lumia 550				
Samsung Galaxy J3	2 app	129 app	74 tel 24 app	46 tel
Samsung Galaxy J5			467 tel	45 tel 239 sim
Samsung Galaxy A5	1736 tel		1831 tel	294tel
Samsung Galaxy Core Prim	106 tel 488 app	5091 app 106 tel	79 tel	66 tel
ZTE Kis 3	583 197	243 tel	500 tel	327 tel

Tabulka 9 Výsledky analýz jednotlivých nástrojů v kategorii kontakty

Nástroj MOBILedit Forensic Express vyextrahoval kontakty ze všech mobilních telefonů. Jedná se hlavně o kontakty uložené přímo v mobilním telefonu nebo na SIM kartě, v případě kontaktů z aplikací už tak úspěšný nebyl, dokázal získat pouze 42 kontaktů z mobilního telefonu iPhone 5s. U tohoto mobilního telefonu se dařilo i ostatním nástrojům, které dokázaly extrahovat více než 300 kontaktů. Nejvíce kontaktů se podařilo získat z aplikace Facebook Messenger.

8.3.3. Výsledky analýz jednotlivých nástrojů v kategorii uživatelské účty

Výsledky analýz jednotlivých nástrojů v kategorii uživatelské účty				
	UFED 4PC	**XRY Logical**	**Oxygen Forensic® Extractor**	**MOBILedit Forensic Express**
iPhone 5s	78	47	47	47
Lumia 550				
Samsung Galaxy J3	3	11	3	
Samsung Galaxy J5	6	2	2	2
Samsung Galaxy A5				
Samsung Galaxy Core Prim	28	24	1	1
ZTE Kis 3	20	11		1

Tabulka 10 Výsledky analýz jednotlivých nástrojů v kategorii uživatelské účty

Nástroj UFED spolu s XRY nezískaly záznamy o účtech pouze u mobilního telefonu Lumia 550 a u mobilního telefonu Samsung A5, u kterého je možné se domnívat, že žádné účty synchronizované se zařízením nemá, jelikož se účty nepodařilo vytěžit žádnému nástroji. Z hlediska kvantitativního by byl nejúspěšnějším nástrojem opět UFED, z čehož se dá usoudit, že i v této kategorii je nejspolehlivějším nástrojem, ale ani nástroj XRY nemůžeme v této kategorii považovat za nespolehlivý.

8.3.4. Výsledky analýz jednotlivých nástrojů v kategorii hesla

Výsledky analýz jednotlivých nástrojů v kategorii hesla				
	UFED 4PC	**XRY Logical**	**Oxygen Forensic® Extractor**	**MOBILedit Forensic Express**
iPhone 5s	284 účty	36 účty 15 wifi	312 wifi a účty	36 účty 17 wifi
Lumia 550				
Samsung Galaxy J3	6 wifi	6 wifi	5 wifi	
Samsung Galaxy J5	2 wifi	2wifi	2wifi	
Samsung Galaxy A5	6			
Samsung Galaxy Core Prim	23 wifi 16 účty	14 wifi	14 wifi 13 účty	
ZTE Kis 3	21 wifi	7 účty		

Tabulka 11 Výsledky analýz jednotlivých nástrojů v kategorii hesla

Všechny nástroje získaly hesla především k účtům, ke kterým se uživatele připojovali ve webovém prohlížeči nebo přes aplikace, a také hesla z připojování k WiFi sítím.Nástroj MOBILedit Forensic Express dokázal získat hesla jen z mobilního telefonu iPhone 5s. Nejspolehlivějším je i v této kategorii nástroj UFED. Nástroj vytěžil hesla především z připojování k WiFi sítím. Většina hesel, která byla nástroji získána je v nešifrované podobě. Například u účtů na github.com, jcu.cz, cinestar.cz, duolingo.com a většiny WiFi sítí v restauracích, barech a dalších.

8.3.5. Výsledky analýz jednotlivých nástrojů v kategorii připojení k WiFi sítím

Výsledky analýz jednotlivých nástrojů v kategorii připojení k WiFi sítím				
	UFED 4PC	**XRY Logical**	**Oxygen Forensic® Extractor**	**MOBILedit Forensic Express**
iPhone 5s	17	37	36	36
Lumia 550				
Samsung Galaxy J3	8	8	8	25
Samsung Galaxy J5	2	2	2	2
Samsung Galaxy A5	9			11
Samsung Galaxy Core Prim	39	37	36	45
ZTE Kis 3	89			89

Tabulka 12 Výsledky analýz jednotlivých nástrojů v kategorii připojení k WiFi sítím

Nejvíce WiFi sítí, ke kterým se mobilní telefony připojily vyextrahovaly nástroje UFED a MOBILedit Forensic Express. Z kvantitativního hlediska nejvíce sítí detekoval nástroj MOBILedit Forensic Express. Nástroje UFED, XRY a MOBILedit Forensic Express také kromě samotných názvů sítí extrahoval i počty spojení a jejich data. Díky tomu lze vyhodnotit, kde se telefon potažmo uživatel nacházel.

8.3.6. Výsledky analýz jednotlivých nástrojů v kategorii obrázkové soubory

Výsledky analýz jednotlivých nástrojů v kategorii obrázkové soubory				
	UFED 4PC	**XRY Logical**	**Oxygen Forensic® Extractor**	**MOBILedit Forensic Express**
iPhone 5s	25873	41879	17060	18246
Lumia 550		561		395
Samsung Galaxy J3	4938	1524	313	317
Samsung Galaxy J5	2998	3657		1422
Samsung Galaxy A5	6986	7801		2689
Samsung Galaxy Core Prim	8790	5290		1322
ZTE Kis 3	6901	703		668

Tabulka 13 Výsledky analýz jednotlivých nástrojů v kategorii obrázkové soubory

Nejméně úspěšným nástrojem je v této kategorii Oxygen Forensic® Extractor, který dokázal vytěžit obrázkové soubory pouze u dvou mobilních telefonů. Ostatní nástroje dokázali vytěžit obrázkové soubory ze všech mobilních telefonů. Kvantitativně nejvíce dat extrahoval nástroj XRY. Je tedy hodnocen jako nejspolehlivější v této kategorii.

8.4. Porovnání z finančního hlediska

Nejlevnějším produktem, který zde byl použit je MOBILedit Forensic Express. Firma jako jediná cenu uvádí na svých webových stránkách. Cena je tedy 40 000 korun českých. Jedná se o českou firmu. V oblasti analýz obsahu mobilních telefonů je od roku 1996. Nástroj využívají ve více než 70 zemích. [13]

Dalším nástrojem je Oxygen Forensic® Extraktor, jehož cena odpovídá přibližně 250 000 korun českých. Firma byla založena v roce 2000 a produkty společnosti Oxygen Forensic® se úspěšně používají ve více než 100 zemích světa včetně USA, Velké Británie, Německa, Rakouska, Francie. Konkrétními organizacemi, které tento nástroj používají jsou americká armáda, FBI, Interpol, Metropolitní policie v Londýně, francouzská národní policie a četnictvo, německá federální kriminální policie a mnoho dalších. [14] [15]

Forenzní nástroj XRY má dvě verze Physical a Logical, které dohromady odpovídají necelým 200 000 korun českých. Společnost MSAB se zabývá mobilními komunikacemi od roku 1984 a nyní má zvláštní pozornost na forenzní obnovu dat z mobilních zařízení. Software XRY je určen k rychlému a efektivnímu získávání informací, jako jsou obrázky, SMS, historie hovorů, seznamy kontaktů a aplikační údaje od roku 2003. XRY používají policejní, vojenské, vládní a zpravodajské agentury a forenzní laboratoře ve více než 100 zemích světa k vyšetřování zločinu, shromažďování informací, vyšetřování podvodů a boj proti korupci. [16] [15]

Posledním nástrojem je UFED verze 4PC. Jeho cena je 300 000 korun českých. Na trhu se nástroje od firmy Cellebrite objevili v roce 2007. UFED má asi 60 000 aktivních licencí UFED ve 150 zemích světa, čímž se Cellebrite stala vedoucí společností na trhu pro mobilní forenzní analýzu po celém světě. [17] [6]

Cena všech komerčních forenzních nástrojů se pohybuje v řádu několika desítek až stovek tisíc korun. Mezi forenzními nástroji se v podstatě podle ceny dá určit kvalita. Za všechny funkce a analyzovaná data se platí, čím více má nástroj funkcí tím více roste cena nástroje. Od levnějších produktů nelze očekávat výsledky jako od dražších.

9. Vyhodnocení a doporučení řešení

Forenzní nástroj UFED splňuje veškeré požadavky na zkoumání. Jako jediný dokázal provést fyzickou analýzu, konkrétně u mobilních telefonů Samsung Core Prime a ZTE Kis 3. U většiny mobilních telefonů získal data z nejvíce kategorií a v porovnáních jednotlivých kategorií byl ve většině případů vyhodnocen jako nejspolehlivější nástroj. Nejvíce dat dokázal nástroj extrahovat z mobilního telefonu iPhone 5s, dalším jsou pak mobilní telefon ZTE Kis 3 a Samsung Galaxy Core Prim se staršími verzemi Androidu. Naopak nejméně dat extrahoval forenzní nástroj z mobilního telefonu Lumie 550.

Také poskytuje nejširší podporu mobilních telefonů a má uživatelsky příjemné prostředí – jednoduché a intuitivní. I když se jedná o produkt izraelské firmy, je k dispozici čeština, i když ne vždy se správným překladem. Ovšem je bohužel nejdražším přístrojem. Jeho cena se pohybuje přes 300 000 korun. I přes to ho lze označit za nejspolehlivější v extrakci dat z mobilních telefonů.

Dalším nástrojem je XRY. Tento forenzní nástroj prováděl všechny analýzy nástrojem XRY Logical u nějž je očekávaná logická extrakce, ale nástroj dokázal získat i smazaná data. Nejvíce dat také získal z mobilního telefonu iPhone 5s a Samsung Galaxy Core Prim. Nejvíce dat a tím pádem nejspolehlivější je v získávání účtů a hesel.

Uživatelsky je také intuitivní, ale oproti nástroji UFED není možné data filtrovat dle potřeby. Například pokud chceme zobrazit všechny zprávy včetně skupinových konverzací, kterých se účastní jedna konkrétní osoba, není to možné zjistit. Podporuje také celou řadu mobilních telefonů a cenově se pohybuje okolo 200 000 korun. I tento nástroj lze označit za spolehlivý, ne však na stejné úrovni jako nástroj UFED.

Nástroj Oxygen Forensic® Extractor neextrahoval informace pomocí fyzické analýzy, takže také u tohoto nástroje byly mobilní telefony při extrakci zapnuty. I když se nikdy nejednalo o fyzickou analýzu, přesto dokázal nástroj najít i některá smazaná data, konkrétně u třech mobilních telefonů. Nejvíce dat extrahoval v kategorii kontaktů, kde ho lze považovat za spolehlivý. V ostatních kategoriích většinou nejméně úspěšný. ´

Nejvíce dat extrahoval z mobilního telefonu Samsung Galaxy J3. Naopak nejméně dat extrahoval z mobilního telefonu ZTE Kis 3. Uživatelsky je tento nástroj také intuitivní a lze se v něm bez problému orientovat. Cenově se pohybuje okolo 250 000 korun, což je vzhledem k malé spolehlivosti, cena poměrně vysoká.

Posledním forenzním nástrojem je produkt české firmy Compelson MOBILedit Forensic Express. I tento forenzní nástroj dokázal extrahovat mnoho dat, mezi jinými i smazaná, ale není jasné, jakou analýzou data extrahoval, což může být problém například pro znalce, kteří musí tuto informaci uvádět do dokumentace. Mobilní telefony musely být zapnuté i při analýzách tohoto nástroje, což není vhodné z hlediska manipulace a zásahu do mobilního telefonu potažmo dat. Nejvíce dat nástroj extrahoval z mobilního telefonu iPhone 5s a nejméně dat extrahoval z telefonu Lumia 550. Nejúspěšnější a tedy nejspolehlivější byl nástroj v oblasti extrakce WiFi připojení a obrázků. Nástroj úspěšně aplikoval novou funkci PhotoRecognizer na vytěžené obrázky. Nejlépe dokázal rozpoznat dokumenty a drogy, konkrétně alkohol, ale již ne tak úspěšně rozpoznal obrázkové soubory zbraní a nahoty. Nástroj nemá zdaleka tak intuitivní prostředí jako nástroje předešlé. O nastavení telefonu si musíme přečíst zvláštní informace, které nejsou součástí samotné analýzy jako u ostatních prostředků. Cenově se pohybuje okolo 40 000 korun.

Pomocí nástroje příkazového řádku ADB jsme získali jen omezené informace z aplikací jako obrázky, webová historie a další. Tento opensource se zdaleka nevyrovná nástrojům komerčním.

Pokud chtějí znalci či expertní pracoviště získat co největší množství relevantních dat, měli by použít více než jeden forenzní nástroj. Jsou-li získána data z více nástrojů, jedna analýza může potvrdit druhou nebo zjistit další relevantní informace. S ohledem na právní stránku věci je třeba využívat prostředky, které co nejméně zasahují do zařízení. Pokud je to možné, analyzovat mobilní telefon fyzickou analýzou. Pokud to možné není, je třeba vše důkladně zdokumentovat a uvést důvody, proč tomu tak muselo být.

10. Závěr

Tato práce se zabývá analýzou spolehlivosti forenzních nástrojů pro zkoumání malé digitální techniky. V teoretické části byly popsány zásady digitální forenzní analýzy, konkrétní postupy při zajišťování, extrakci a analýze mobilních telefonů. Dále byly popsány druhy digitální forenzní analýzy a použité forenzní nástroje UFED 4PC, XRY Logical, Oxygen Forensic® Extractor a MOBILedit Forensic Express a ADB jako nekomerční nástroj.

Praktická část práce zahrnuje analýzy mobilních telefonů provedených všemi nástroji. Dále jsou porovnány výsledky jednotlivých nástrojů u každého mobilního telefonu. Také jsou porovnány výsledky ve vybraných kategoriích a výsledky, které byly získány pomocí ADB. Komerční nástroje jsou hodnoceny i z finančního hlediska.

V deváté kapitole jsou výsledky vyhodnoceny a je doporučeno řešení s ohledem na zajištění co nejvíce dat relevantních pro účely vyšetřování trestné činnosti. Doporučuje se tedy, používat více forenzních nástrojů. Jedna analýza může potvrdit druhou nebo zjistit další relevantní informace právě porovnáním dat získaných z odlišných nástrojů. S ohledem na právní stránku je doporučeno používat nástroje podporující fyzickou analýzu, protože nejméně zasahuje do zařízení.

11. Seznam použité literatury

[1] POLČÁK, Radim, František PÚRY a Jakub HALAŠTA. *ELEKTRONICKÉ DŮKAZY V TRESTNÍM ŘÍZENÍ* [online]. 1. Brno : Masarykova univerzita, Právnická fakulta: Spisy Právnické fakulty Masarykovy univerzity, řada teoretická, Edice Scientia č. 542, 2015 [cit. 2018-04-17]. ISBN 978-80-210-8073-7. Dostupné z: https://science.law.muni.cz/knihy/monografie/Polcak_Elektronicke_dukazy.pdf

[2] CALOYANNIDES, Michael A. Privacy Protection and Computer Forensics. 2. London: Artech House, 2004. ISBN 1-58053-830-4.

[3] Http://cyberlab.cz/index.html. In: Http://cyberlab.cz/forenzni-laborator.html [online]. b.r. [cit. 2018-04-17]. Dostupné z: http://cyberlab.cz/forenzni-laborator.html

[4] SVETLÍK, Marián. Digitální forenzní analýza a bezpečnost informací. Data Security Management [online]. 2010, 2010(1), 20-23 [cit. 2018-04-17]. Dostupné z: https://www.rac.cz/RAC/homepage.nsf/CZ/Clanky/$FILE/DSM-Digit%C3%A1ln%C3%AD%20forenzn%C3%AD%20anal%C3%BDza-01-2010.pdf

[5] ČESKÁ REPUBLIKA. Zákon č. 141/1961 Sb.: o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. In: . Praha Ministerstvo spravedlnosti: Sbírka zákonů Československé socialistické republiky, 1961, ročník 1961, číslo 141. Dostupné také z: https://www.zakonyprolidi.cz/cs/1961-141

[6] KOTHÁNEK, Jakub a Jaroslav KOTHÁNEK. Forenzní analýza mobilních telefonu: Legislativní východiska. Data Security Management. 2016, 2016(1), 28-32.

[7] KOUTSKÝ, Vojtěch. Analýza bezpečnosti jednotlivých druhů mobilních telefonů. České Budějovie, 2017. Bakalářská. Jihočeská univerzita v Českých Budějovicích.

[8] UFED 4PC Ultimate. Cellebrite - UFED 4PC Ultimate [online]. Petah Tikva: Cellebrite, 2014 [cit. 2018-04-17]. Dostupné z: http://ec2-107-23-31-70.compute-1.amazonaws.com/mobile-forensics/products/pc-based/ufed-4pc-ultimate

[9] XRY - Extract. XRY - Extract [online]. Stockholm: MSAB, 2018 [cit. 2018-04-17]. Dostupné z: https://www.msab.com/products/xry/

[10] Oxygen Forensic: Documentation & Guides. *Oxygen Forensic* [online]. Alexandria: Oxygen Forensics, Inc, 2018 [cit. 2018-04-17]. Dostupné z: https://www.oxygen-forensic.com/en/download/documentation

[11] MOBILedit Forensic Express. *MOBILedit* [online]. Praha: Compelson Labs, 2018 [cit. 2018-04-17]. Dostupné z: http://www.mobiledit.com/forensic-express

[12] Android Debug Bridge. Android Debug Bridge - Android Studio [online]. Mountain View: Android Developers, 2018 [cit. 2018-04-17]. Dostupné z: https://developer.android.com/studio/command-line/adb.html

[13] About — MOBILedit [online]. Praha: MOBILedit, 2018 [cit. 2018-04-17]. Dostupné z: http://www.mobiledit.com/company/

[14] Oxygen Forensics - Company [online]. Alexandria: Oxygen Forensics, 2018 [cit. 2018-04-17]. Dostupné z: https://www.oxygen-forensic.com/en/company

[15] Forenzniprodukty.cz [online]. Praha: Risk Analysis Consultants, s.r.o., 2018 [cit. 2018-04-17]. Dostupné z: https://forenzniprodukty.cz/

[16] About MSAB [online]. Stockholm: MSAB, 2018 [cit. 2018-04-17]. Dostupné z: https://www.msab.com/company/

[17] Company profile [online]. Petah Tikva: Cellebrite, 2018 [cit. 2018-04-17]. Dostupné z: https://www.cellebrite.com/en/about/company/

12. Seznam obrázků

13. Seznam tabulek