Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta
Ústav aplikované informatiky

Forenzní analýza mobilních telefonů s OS Android

Vypracoval: Jiří Chaloupka
Vedoucí práce: Ing. Jaroslav Kothánek, Ph.D

České Budějovice 2018

Chaloupka J., 2018: Forenzní analýza mobilních telefonů s OS Android. [Forensic analysis of mobile devices running Android. Bc. Thesis, in Czech.] – 48 p., Faculty of Science, University of South Bohemia, České Budějovice, Czech Republic.

Název

Forenzní analýza mobilních telefonů s OS Android

Abstract

Bakalářská práce „Forenzní analýza mobilních telefonů s OS Android“ se zabývá problematikou forenzní analýzy vybraných komunikačních aplikací fungujících na mobilních zařízení využívajících OS Android, které je momentálně nejpoužívanějším OS a dokumentuje umístění jednotlivých zájmových informací v rámci struktury OS Android.

Klíčová slova

OS Android, digitální důkaz, forenzní analýza, zajišťování dat, komunikační aplikace

Title

Forensic analysis of mobile devices running Android

Summary

Thesis „Forensic analysis of mobile devices running Android“ is focused on analysis of selected few communication applications running on OS Android, which is currently the most used OS for mobile devices. Main goal of this thesis is to find, analyse and document locations of data that can be potentially used as evidence.

Key worlds

OS Android, digital evidence, forensic analysis, data acquisition, communication applications

Prohlašuji, že svoji bakalářskou práci jsem vypracoval 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 jejich internetových stránkách, a to se zachováním mého autorského práva k odevzdání 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.

České Budějovice …….

…….
podpis

Poděkování

Zde bych chtěl poděkovat Ing. Jaroslavu Kothánkovi, Ph.D za odborné rady a vedení při tvorbě této práce.

Obsah

1. Úvod a cíle práce

1.1. Úvod

Digitální technika dnes zasahuje do všech oblastí lidských aktivit. V posledním desetiletí se díky rychlému vývoji a snadné dostupnosti stala běžnou součástí každodenního života. Málokdo si ale uvědomuje, že každé z těchto zařízení, které pracuje s daty, zanechává o všech činnostech záznamy, které nazýváme digitální stopa.

Vzhledem k rostoucí popularitě sociálních sítí a komunikačních aplikací, a to nejen v běžné populaci, ale i v části populace páchající trestnou činnost, stává se často důkazní stopa digitálním důkazem. Tento trend úzce souvisí s problematikou zajišťování digitálních stop, s právním rámcem a s uznatelností zadržených dat v procesu dokazování.

V úvodní částí této práce se zabývám definování základních pojmů spojených s touto problematikou jako je důkazní stopa, popisem možných postupů PČR při zajišťování dat, jako důkazních stop, forenzním zkoumáním dle jednotlivých úrovní a možnostmi forenzního zajišťovaní dat z OS Android.

Hlavní část se věnuje dokumentaci umístění jednotlivých zájmových složek a souborů a informací, které obsahují, v rámci struktury OS Android a to na příkladech nejpoužívanějších komunikačních aplikací – Facebook, WhatsApp, Twitter a Viber.

V závěru práce je pak vyhodnocení srovnání těchto dokumentací.

1.2 Cíle práce

- Definování základních pojmů jako je digitální stopa a OS Android
- Definování možných postupů PČR při zajišťování datových důkazních stop
- Definování forenzního zkoumání dle jednotlivých úrovní a možnosti forenzního zajišťování dat z OS Android
- Dokumentace umístění jednotlivých zájmových informací v rámci struktury OS Android

2. Zajišťování Digitálních stop pro účely trestního řízení

2.1. Digitální stopa

Digitální stopa je každá, ale zároveň jakákoliv, využitelná informace uložená, zpracovaná nebo přenášená v digitální formě. Tato skupina je velmi široká a zahrnuje oblast počítačů a komunikace mezi nimi, data uložená v internetové síti, mobilní zařízení; dále zde mohou být začleněny také kamerové systémy, moderní automobily a jiná zařízení pracující s uživatelskými daty.

Jelikož je tato skupina velmi rozsáhlá, je nutno stopy dále dělit např. podle jejich zdroje nebo podle druhu techniky a její specifikace. Dle těchto specifikací pak volíme konkrétní metodu zajišťování digitálních stop pro účely trestního řízení. V případech, kdy k zajišťování důkazních stop dochází na jednom zařízení, využíváme buď metodu nejvhodnější, nebo volíme takovou kombinaci metod, která je finančně i časově dostupná. Získáme tak komplexnější obraz o datech v zařízení, který vychází z více výsledků šetření.

Pro potřeby trestního řízení zajišťuje orgán činný v trestním řízení digitální stopy podle zákona 144/1961 Sb. během vykonávání následujících úkonů:

1. domovní prohlídka, prohlídka jiných prostor a pozemků - § 82 trestního řádu;
2. vydání nebo odnětí věci - § 78 a § 79 trestního řádu;
3. ohledání věci nebo místa činu - § 158 a § 113 trestního řádu;
4. zajištění dat z internetu, odposlech a jiné metody podle odpovídajících právních nařízení.

Také v ostatních případech, které přímo nesouvisí s trestním řízením, je nutné dodržet příslušné předpisy, jako např. Závazný pokyn policejního prezidenta č. 100/2001 ke kriminalisticko- technické činnosti PČR nebo Metodický pokyn ředitele KÚP č.7/2001, kterým se upravuje činnost orgánů PČR při zajišťování výpočetní techniky a dat pro účely následného znaleckého zkoumání.

Před samotným zajištěním je nutné vykonat několik kroků, které mají za úkol zrychlit samotné zajištění stop a co nejvíce ochránit integritu důkazů.

Pokud osoba nevydá elektrické zařízení, to jest na výzvu § 78 trestního řádu o vydání věci, tuto věc vydat odmítne, je na místě postup podle § 79 trestního řádu. Odejmutí věci policejní orgán učiní až po rozhodnutí dozorujícího státního zástupce. Nejběžnějšími překážkami jsou: zatajení osobní věci, nenávratné zničení dat v zařízení a neposkytnutí součinnosti v prolomení vstupních hesel do zařízení, zejména u mobilních telefonů.

Obvyklý způsob zkoumání je tedy na specializovaných pracovištích v ČR, kterými jsou OKTE jednotlivých krajských ředitelství, případně kriminalistický ústav KÚP v Praze. V jednodušších případech, kdy je třeba v zařízení zjistit konkrétní informaci (jako např. konkrétní SMS nebo protokol o uskutečněném hovoru), je možné je se souhlasem vlastníka zařízení tyto informace zadokumentovat, např. fotograficky nebo pouhým přepisem výslechu osoby. Fotografie se pak přikládá jako příloha k protokolu o výslechu (výslech podle § 61 zákona o PČR, úřední záznam o podaném vysvětlení § 158/6 trestního řádu atd.). Naopak, ve složitějších případech, je na místě zařízení nechat odzkoumat externím znalcem na konkrétní problematiku (dle požadavku zajištění). Výsledkem může být odborné vyjádření či znalecký posudek.

Výsledkem zkoumání je pro potřeby PČR prakticky vždy výsledek analýzy, který je vyhotovený v písemné formě s přílohami, které obsahují data na samostatném médiu (např. otisk disku, excelové soubory; pro mobilní telefony je specifický výstup pomocí zařízení UFED). Nejčastější obsahem jsou pak data z emailu, SMS zprávy, protokoly hovorů, facebooková komunikace a sociální sítě obecně; vždy se řídíme konkrétními potřebami v dané trestní věci.

2.2. Příprava před samotným zajištěním stop

Před samotným zajišťováním důkazního materiálu lokalizujeme veškerou zájmovou techniku (popř. data) v cílovém prostoru – je nutné primárně odhadnout počet zařízení a alespoň přibližný objem dat, který je nezbytné zajistit. Další možné kroky, které PČR provádí, mohou být např.: předběžné seznámení s datovou

sítí a s druhy používaných software, s bezpečnostními opatřeními, ale např. i s odborností lidí v lokaci. Posledním krokem je obvykle příprava technických prostředků, které budou na místě využity – nářadí, pevné disky na bitové kopie atd. Ve firemním prostředí navíc dále zajišťujeme provozní informace nebo informace o zabezpečení – hesla k systémům, informace o tom, zda se používá šifrování apod. Nedílnou součástí je zhodnocení dopadu této činnosti na činnost zúčastněných subjektů. Zde řešíme zásadní rozhodnutí, zda je nutné zařízení odeslat na zkoumání nebo zda je možné ho odzkoumat na místě za přítomnosti znalce.

3. OS Android

Android je open source mobilní operační systém, jehož základem na Linuxové jádro. V dnešní době je vyvíjen pro širokou škálu zařízení v různých formách, avšak primárně byl a stále je vyvíjen pro chytré mobilní telefony a tablety. Z počátku na systému pracovala firma Android Inc., kterou v roce 2005 koupila firma Google. Ta ho také následně v roce 2007 odhalila veřejnosti. První zařízení, fungující s tímto systémem, šlo do prodeje v srpnu 2008 a šlo o HTC Dream, který fungoval na verzích od *m3-rc22a* po verzi *1.6*. Poslední hlavní verze je *8.1* vydaná v prosinci 2017.

3.1. Procentuální rozdělení uživatelů OS Android

Systém Android má na světe mezi uživateli největší zastoupení mezi všemi operačními systémy. Na tabletech je nejprodávanějším systémem od roku 2013 a na mobilních telefonech je dominantní dle všech možných specifikací – jedná se zhruba o ¾ podíl na trhu. V celkových prodejích je Android na prvním místě od roku 2015, následuje ho iOS a Windows.

Tabulka níže naznačuje rozložení uživatelů OS Android mezi jeho konkrétní verze. Tato data jsou za období 29. ledna až 5. února roku 2018. Jedná se o data zveřejněná firmou Google, která byla získaná skrz distribuční centrum aplikací. Do tohoto průzkumu bylo zahrnuto každé unikátní zařízení, které v tomto termínu navštívilo aplikační distribuční centrum. Z výsledků byly vynechány verze, které nedosáhly 0,1 % z celkového počtu uživatelů.

Tabulka 1: Uživatelé jednotlivých verzí OS Android v daném období

Verze	Kódové označení	Verze API	Počet uživatelů (%)
2.3.3 - 2.3.7	Gingerbread	10	0.3
4.0.3 – 4.0.4	Ice Cream Sandwich	15	0.4
4.1.x	Jelly Bean	16	1.7
4.2.x		17	2.6
4.3		18	0.7
4.4	KitKat	19	12.0
5.0	Lollipop	21	5.4
5.1		22	19.2
6.0	Marshmallow	23	28.1
7.0	Nougat	24	22.3
7.1		25	6.2
8.0	Oreo	26	0.8
8.1		27	0.3

Zdroj: Vlastní zpracování

3.2. Rozdíly mezi verzemi

Podle číslování verzí OS lze rozdělit změny do 3 skupin a to:

- A.x.x → B.x.x – V tomto případě se jedna o změny zásadního rozsahu; většinou jde o přepracované uživatelské rozhraní, aktualizace API, podpůrných knihoven, případně i jádra systému na novější verzi.
- A.A.x → A.B.x – Zde se jedná o změny malého rozsahu; přidávání nových funkcí ke stávající verzi.
- A.A.A → A.A.B – Změna verze v tomto rozsahu většinou indikuje pouze opravu nalezených chyb v systému.

Hlavní rozdíly mezi jednotlivými verzemi jsou uvedeny v tabulce níže. Tabulky neobsahuje všechny verze, ale pouze ty, které přinesly nějaké zásadní změny nebo funkce nebo které přinesly úpravu funkcionality.

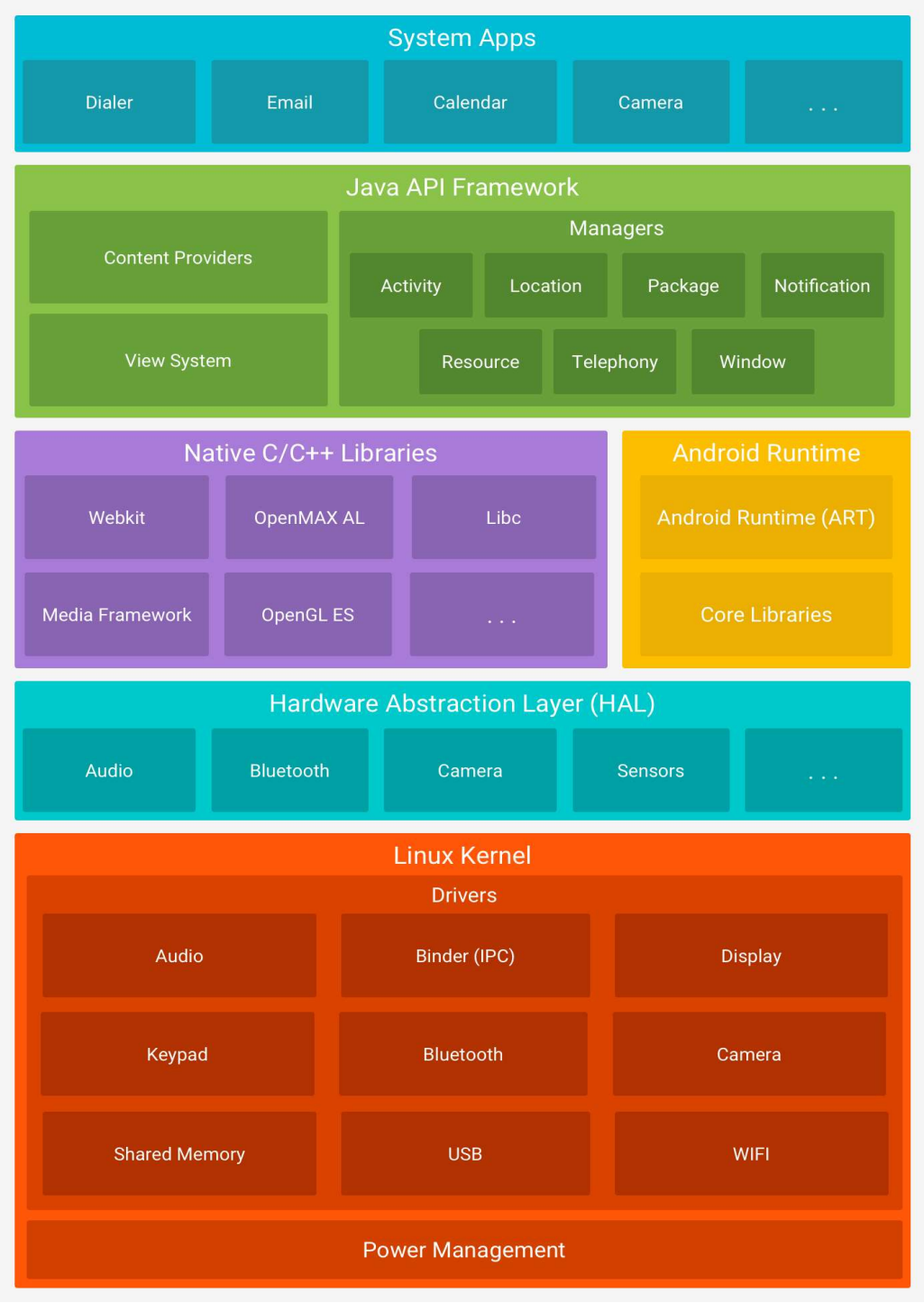
Tabulka 2: Zásadní funkční změny OS Android

Verze	Seznam změn
1.0	aktualizace aplikace a systému skrz centralizovanou distribuční platformu
1.5	podpora Bluetooth režimů A2DP (Advanced Audio Distribution Profile) a AVRCP (Audio/Video Remote Control Profile)
2.2	možnost instalovat aplikace na externí úložiště
2.3	• změna souborového systému z YAFFS na ext4 • vylepšení výkonu v rámci optimalizace běhu garbage collectoru • rychlejší metoda vyřizování systémových událostí
2.3.4	rozhraní pro práci s externím zařízením připojeným přes USB
3.0	podpora více-jádrových procesorů
4.0	• možnost P2P připojení v rámci Wi-Fi sítě • možnost řízení síťového provozu a API pro VPN klienty
4.1	• detekce služeb v síti • navýšení propustnosti a zároveň maximální velikosti souborů přenositelných přes bluetooth
4.2.2	zákaz ladění přes USB na neověřených počítačích
4.4	emulace NFC čipových karet (pro platby zařízením)
5.1	• možnost uzamknout zařízení po síti v případě ztráty • podpora více SIM karet současně
6	podpora biometrického zabezpečení (otisk prstu)
7.1	• Vulkan API • podpora konferenčních hovorů
8.1	• API pro neuronové sítě pro použití s umělou inteligencí • API pro sílení paměti • verze Android GO – varianta systému pro starší zařízení s velmi výrazně sníženými systémovými nároky

Zdroj: Vlastní zpracování

3.3. Architektura Systému

Ilustrace 1: Struktury systému Android



Zdroj: Https://developer.android.com/index.html [online]. [cit. 2018-04-08]. Dostupné z: https://developer.android.com/guide/platform/index.html

Systém se skládá z pěti hlavních komponent a systémových aplikací, přičemž čtyři jsou zásadní pro jeho funkčnost a to:

Linux Kernel

Jako první a nejnižší část je Linuxové jádro, které má na starosti obvyklé operace, jako je zajištění bezpečnosti celého systému nebo přidělování zdrojů a práce s pamětí.

Hardware Abstraction Layer

Druhou částí je *Hardware Abstraction Layer* (HAL), který poskytuje spojení mezi kernelem a vyššími vrstvami, umožňuje také ale implementaci ovladačů pro konkrétní zařízení. Tato vrstva obsahuje také knihovny pro specifické komponenty jako je například Bluetooth modul nebo fotoaparát.

Android Runtime

Třetí části je tzv. *Android Runtime* (ART). Toto prostředí zprostředkovává běh aplikací a některých systémových služeb. Od verze 5.0 (API v21) vytváří každá spuštěná aplikace instanci ART. Samotné prostředí se tak stará o to, že bytecode aplikací je přeložen do nativních instrukcí pro zařízení.

Native C/C++ Libraries

Protože mnoho součásti Androidu je postaveno tak, že vyžadují knihovny v C/C++, tak je nutné zde tyto knihovny zmínit jako důležitou součást systému. Tyto knihovny nám umožňují využívat i jiné funkce aplikací, využívajících tyto knihovny a to i těch, které nevyužívají C/C++.

Java API framework

Rozhraní napsané v jazyce Java, umožňující přístup ke všem prvkům OS Android, poskytují prostředí pro vývoj aplikací, které mohou teoreticky využívat každou součást systému.

V tomto rozhraní je umístěna také součást systému, která se jmenuje *Content providers.* Tento modul může existovat pro každou nainstalovanou aplikaci a součást systému - není ale určen pro aplikaci samotnou, ale slouží k tomu, aby umožnil

přístup ostatních aplikací k žádaným datům. Modul vytváří standardizované komunikační rozhraní mezi aplikacemi s různými datovými výstupy. Při zkoumání je tato funkce užitečná hlavně proto, že nám pomocí doinstalované aplikace pro extrakci dat umožní získat přístup ke všem datům, které aplikace sdílejí. Standardní součástí systému je provider pro SMS, kontakty, kalendář a e-mailový klient. Existují i další, ale tyto jsou v systému přítomny vždy.

4. Prvotní kroky při zajištění zařízení

Jedním ze stále debatovaných téma při zajišťování mobilních zařízení je volba postupu ve chvíli, kdy je zařízení zajištěné. Je nutné ho zběžně ohledat a zjistit, jestli je vypnuté nebo zapnuté, případně chráněné heslem. Jelikož uživatelé začínají stále více dbát o bezpečnost vlastněných zařízení, tak alespoň základní kontrola přístupu ve formě hesla nebo gesta bývá obvykle zapnuta.

Pokud se nám podaří zařízení zajistit ve stavu, kdy je odemknuté, je vhodné udělat dvě základní operace a to:

a) Vypnout automatické zamykání obrazovky nebo alespoň zvýšit časový interval, po který zařízení zůstane odemčené a snažit se ho udržet aktivní.
b) Povolit režim ladění přes USB, zapnout režim pro vývojáře a vypnout ochranu vyjímatelného úložiště. Režim ladění nám později umožní přístup k zařízení a následnou analýzu dat.

Všechny výše uvedené operace je nutné dokumentovat pro účely důkazního řízení, jinak by bylo možné takovýto důkaz snadno zpochybnit.

Dalším důležitým krokem je znemožnit zařízení připojení k jakékoliv síti – tím zabráníme například smazání dat přes síť. Zde je třeba myslet na to, že mazání zařízení lze spustit i pomocí SMS. Je proto nutné ošetřit i tuto cestu. Toho docílíme jednou z pěti nebo libovolnou kombinací níže uvedených možností:

a) Přepnutím zařízení, pokud je odemčené, do režimu letadlo. Výhoda této možnosti zachování dat související s chodem zařízení, nevýhodou další modifikace zařízení.
b) Vyjmutím SIM karty. Tato možnost je rychlá, nemodifikuje potenciálně zájmová data v systému, avšak nepřeruší práci Wi-Fi modulu ani jiných připojení.
c) Blokací ze strany poskytovatele služeb. Výsledek, výhody i nevýhody jsou stejné, jako při vyjmutí SIM karty, navíc je ale v tomto případě nutný soudní příkaz.
d) Umístěním zařízení do odstíněného obalu/prostředí. Tato metoda je efektivní v případech, kdy předchozí metody nelze použít. Při správném použití dojde k odstínění veškerého signálu z vnějšího prostředí. Nevýhodou je,

že se zařízení neustále pokouší připojovat k síti, což má zásadní vliv na životnost baterie.

e) Vypnout zařízení. Při této variantě přijdeme o dočasná data, navíc může být zapnuté heslo po spuštění, které nám zamezí přístup k zařízení.

5. Analýza možností forenzního zajišťování dat ze zařízení s OS Android

5.1. Modifikace dat na zařízení

Základním principem při zajišťování důkazů je, že stopa musí zůstat neporušená, aby mohla být přípustná. Tento princip ale není v případě digitálních stop možné dodržet – pokud je zařízení vypnuté a pro zkoumání ho zapneme nebo ho naopak kvůli přenesení vypneme, vznikají v tomto okamžiku záznamy, které modifikují digitální stopu.

U mobilních zařízení toto platí v naprosté většině případů. Jedním z důvodů je, že ze zařízení nelze úložiště snadno vyjmout (pokud se nejedná o externí paměť, např. paměťovou kartu) a změnám při zapnutí, vypnutí a dalších operací, nelze zabránit např. použitím blokátoru zápisu. Pro mobilní zařízení, a to nejen s OS Android, existují dva základní druhy forenzních postupů a to:

a) **Logická analýza**

   Logická analýza typicky pracuje s alokovaným prostorem a je možné jí provést jednoduchým přistoupením k souborovému systému. Tímto způsobem se dostaneme ke všem aktuálním datům, která jsou v zařízení, ke konfiguračním souborům, ale i k operačnímu systému samotnému, tzn. ke všem datům, která nejsou označena jako smazaná. I zde ovšem existuje výjimka a tou jsou *SQLite databáze*, kde mohou být uchovávány záznamy, které jsou pro systém označeny jako smazané, ale ještě nebyly odstraněny z databáze samotné.

b) **Fyzické metody**

   Fyzické metody na druhou stranu pracují s médiem jako takovým, bez ohledu na typ souborového systému, který je používán. Tyto metody mají jednu zásadní výhodu oproti metodám logickým a to tu, že s jejich pomocí lze ve většině případů získat i některé smazaná data. A to proto, že většina souborových systémů kvůli rychlosti data nemaže v plném rozsahu, ale pouze je označí jako smazaná nebo zastaralá. K přepsání a smazání dat pak dochází až ve chvíli, kdy je potřeba místo na data nová.

U mobilních zařízení bývá většinou fyzická analýza komplikovanější a to jak na finanční i technické prostředky, tak na čas. V případě chyby nebo nedodržení korektního postupu zde navíc hrozí riziko zničení zařízení nebo ztráty dat.

Před přistoupením ke zkoumání zařízení jednou z výše uvedených metod je vhodné vyzkoušet, zda není možné k získání informací využít režimu ladění přes USB. Pokud používáme forenzní distribuci nebo libovolnou linuxovou distribuci s nainstalovaným vývojovým prostředím, připojíme zařízení v režimu pouze pro čtení a zadáme příkaz *„adb devices“*. Pokud je ladění povoleno, příkaz k nám vrátí seznam zařízení, která jsou aktuálně připojena. V této chvíli je možné tímto kanálem získat přístup k zařízení a provést logickou analýzu souborového systému.

5.2. Metody zkoumání a nástroje k tomu určené

ADB pull

V případě, že je povoleno ladění a zařízení je zapnuto, tak pomocí příkazu *„adb pull /data adbpull“* je možné rekurzivně stáhnout všechny viditelné, nesmazané nebo jinak blokované složky (tzn. za použití logické analýzy) pro další zkoumání. Efektivita této metody je zásadním způsobem ovlivněna nastavením zařízení. Ve většině případů, v nijak nemodifikované zařízení, běží ADB s právy běžného uživatele a nemá tak přístup ke všem datům. Mnohem lepších výsledků lze dosáhnout ve chvíli, kdy v zařízení běží alternativní ROM nebo pokud je zařízení přepnuto tak, že pracuje s rootovskými právy. Pokud tomu tak není, tak nám tato metoda poskytne většinu aplikací (většinou ty, které nepracují s šifrováním), dočasné soubory (například historii prohlížečů) a systémové informace, které nevyžadují práva k přístupu (složky */proc*, */sys* atd.).

Pokud nastane při extrakci dat touto metodou problém, tak se v naprosté většině jedná o kolizi práv k souborům. Pokud se nám podaří izolovat soubor, který dělá problém, tak je možné extrahovat ostatní přístupná data, ale problémový soubor je nutné vynechat.

Analýza zálohy

Starší verze OS Android neposkytovali možnost zálohy dat, proto vznikla řada aplikací pro zálohování, které využívají pro uchování zálohy vyjímatelné úložiště přímo v zařízení. Tyto zálohy budou dostupné k prozkoumání z místa, kde jsou uloženy, libovolnou metodou. Podle toho, jakou aplikaci pro zálohování používáme, lze objevit různá data. V nejběžnějších případech se bude jednat o kontakty, historii hovorů, SMS, systémová nastavení a kalendáře. Pokud je záloha na cloudové službě, tak k přístupu k ní budeme pravděpodobně nutné provést analýzu ostatních zadržených zařízení nebo získat soudní příkaz pro přístupu k účtům v cloudových službách.

Komerčně nabízené metody a zařízení

Široká skupina forenzních nástrojů je dostupná pouze v placených verzích a žádná z variant není dostupná zdarma. Tyto produkty bývají uzavřené a metody jejich práce nejsou na první pohled zřejmé. Mezi takováto řešení patří např.: UFED od společnosti Cellebrite, MOBILedit od české společnosti Compelson, EnCase Mobile Investigator, XRY, Paraben Device Seizure nebo viaExtract od viaForensics.

Cellebrite UFED

Zde existuje několik verzí – od softwaru, který je možné nainstalovat do obyčejného počítače, až po kompletní přenosná řešení na zkoumání přímo na místě. Přenosné varianty jsou soběstačné a schopné extrakce dat ze stále se rozšiřujícího seznamu zařízení. Dále jsou také schopná získat data z paměťových karet a SIM karet. Možnost udělat kopii SIM karty nám dává záruku, že nepřijdeme o žádná data a že můžeme zjistit PIN kód bez rizika ztráty dat na originální kartě. Zároveň je možné tuto kopii nahrát na přepisovatelnou kartu, se kterou zařízení funguje standardně, ale nemá možnost se připojit k mobilní síti.

Také je k tomuto řešení nabízen a distribuován nástroj na vytváření záznamů/protokolů o tom, co se na zařízení nacházelo, a jejich export do běžně užívaných formátů.

MOBILedit

Jedná se o nástroj, který poskytuje prostředky pro extrakci běžných dat. Mezi tyto „běžná“ data patří smazané soubory, kontakty, SMS, hesla k bezdrátovým sítím a data z některých často užívaných aplikací, jako je například Skype, Dropbox, Facebook a další.

JTAG a chip-off

Zařízení s OS Android v současné chvíli nevyužívají ve velké míře šifrování paměťových čipů. Tato skutečnost otevírá cestu dalšímu způsobu zkoumání a to i v případě, že je zařízení chráněno heslem nebo ho není možné spustit. Existují dvě metody, které jsou technicky náročné a jsou k nim nutné speciální technické vybavení. K provedení obou metod je nutné zařízení částečně nebo úplně rozebrat a následně, pokud se nám povede z paměti data úspěšně extrahovat, je nutná rekonstrukce souborového systému. Z těchto důvodů jsou většinou tyto metody používány až v úplně posledním možném případě, když jiné metody selžou.

Při použití JTAG připojujeme speciální zařízení přímo k vývodům paměťového čip na desce. Poté, co čip připojíme, lze mu odeslat příkaz, aby nám vrátil všechna data, která se na něm nachází.

Metoda *chip-off*, jak už její název napovídá, spočívá v tom, že odstraníme čip fyzicky z desky, na které je umístěn. Poté, co je z desky sundán, je potřeba ho očistit a připojit k zařízení, které je schopné čip číst. Ve většině případů je potřeba použít patici, do které zkoumaný čip vložíme, protože vývody bývají tak malé, že je rukou téměř nemožné je připojit korektně.

6. Vybraná umístění zájmových informací

Zde se zaměřím na vyhledávání a dokumentaci některých zájmových dat v rámci struktury OS Android, přičemž se nebudeme zaobírat způsobem, jakým jsme data získali, ale pouze tím, co a kde se nachází a co je možná z těchto dat zjistit. Zaměřím se hlavně na nejpopulárnější a nejběžněji používané komunikační aplikace, a na to, kam ukládají svá data a na to, co je z těchto souborů možné zjistit o uživateli a jeho komunikaci s ostatními.

Obecně je možné definovat umístění aplikačních dat v interní paměti na následujících cestách:

- */data/app/*
- */data/data/*
- */data/user/<uživatel>/*

Dále mohou být aplikační data na externí paměti ve složkách:

- */Android/data/*
- */Android/obb/*

Toto platí obecně, ale aplikace na paměťové kartě mohou zapisovat kamkoliv. V případě, že jsou spuštěny s právy roota, tak mohou zapisovat kamkoliv a to i na interní paměť zařízení. Naprostá většina ostatních aplikací, nainstalovaných standardní, cestou je uložena v hlavně ve složkách */data/, /app/* a */user/*.

Ve složce */data/app/<jméno balíčku>/* se nachází dvě složky a soubor *.apk*. Soubor *.apk* je archiv, který obsahuje samotnou aplikace v nenainstalované formě. Dalšími položkami v této složce jsou složka *lib* a *oat*. Ve složce oat se nachází soubor *.odex*, který je vygenerovaný při instalaci a obsahuje optimalizovaný kód aplikace. Tento soubor není nutný k jejímu chodu, ale má za úkol odstranit opětovný překlad kódu při jejím spuštění. Tím zrychluje její zapínání a chod. Dále zmíníme složku *lib*, která obsahuje sdílené knihovny ve formátu *.so* (*Shared Object*).

7. Facebook

7.1. Messenger

Jako první se podíváme do složky */data/data/com.facebook.orca,* kde se nachází mnoho SQLite databází a některé dočasné soubory.

První umístění, které je nějakým způsobem zajímavé pro zkoumání, je složka *app_gatekeepers*. Zde se nachází složka *users*, jejíž součástí je složka pojmenovaná podle ID uživatele. Toto ID lze použít i tak, že ho zkopírujeme a dosadíme do adresy www.facebook.com/<id> a tím se dostaneme k profilu uživatele, který byl přihlášen na daném zařízení.

Další zajímavou složkou je */data/data/com.facebook.orca/*cache/image. Zde se nachází řada složek, které obsahují soubory *.cnt*, které lze otevřít stejnými nástroji jako jakýkoliv soubor typu *.jpeg* a lze v nich nalézt profilové obrázky kontaktů, fotografie a obrázky, které jsou poslané nebo přijaté v rámci konverzací. U složky *cache* ještě zůstaneme - nachází se zde ještě textový soubor *mqtt_log_event0.txt* a *mqtt_log_event1.txt*. Zde je možné najít typ posledního připojení, a pokud jde o WiFi síť, tak je zde možné zjistit i SSID.

Další potenciálně zajímavou pro zkoumání je složkou je *databases*, které jak už její název napovídá, obsahuje celou řadu SQLite databází i přesto, že nejsou označeny příponou *.db*. Mezi nejzajímavější v tomto případě patří *contacts_db2*, *threads_db2*, *prefs_db* a *analytics_db2*.

Databáze *contacts_db2* obsahuje seznam kontaktů, ale ani zde to není tak jednoduché, jak se může na první pohled zdát. V této databázi jsou kontakty, které jsou uložené v telefonu samotném a zároveň jsou uloženy v kontaktech na facebookovém účtu. Samotná databáze obsahuje 10 tabulek, ne ale všechny obsahují data, která jsou pro nás v této situaci využitelná.

První tabulka, ve které je možné najít některé informace, se jmenuje *_shared_version. Z*de však nenajdeme žádné konkrétní informace, ale pouze počet kontaktů a verzi aplikace, která s touto databází pracuje.

Contacts_db2

Jako další je pro naše potřeby zajímavá tabulka s názvem *contact,* která obsahuje 36 záznamů. V těchto záznamech nalezneme tyto informace, přičemž níže uvádím jen ty, co jsou pro nás funkčně důležité nebo zajímavé:

Tabulka 3: Vybraná data z tabulky contacts

internal_id	integer, primární klíč
contact_id	unikátní text
fbid	Text
fist_name	Text
last_name	Text
display_name	Text
small_ big_ huge_ picture_url	text (všechny 3 záznamy jsou stejného typu)
communication_rank	real
bday_day	integer
is_messenger_user	Text
veiwer_connection_status	Text
is_indexed	integer
veiwer_connection_status	Text
is_indexed	integer
data	Text

Zdroj: Vlastní zpracování

Položka data obsahuje blok informací o uživateli, který vypadá takto:

```
contactId: <alfanumerický řetězec identifikující uživatele>
profileFbid: <15-ti místné číslo>
graphApiWriteId: contact_<unikátní číslo>
name:
      firstName: <jméno>
      lastName: <příjmení>
      displayName: <zobrazované jméno>
phoneticName:
smallPictureUrl: https://fbcdn-profile-a.<skryto>
bigPictureUrl: https://fbcdn-profile-a.<skryto>
hugePictureUrl: https://fbcdn-profile-a.<skryto>
smallPictureSize: <velikost malého profilového obrázku>
bigPictureSize: <velikost středního profilového obrázku>
hugePictureSize: <velikost velkého profilového obrázku>
communicationRank: 0.03445798
withTaggingRank: 0.3325288
phones
      id: <číslo>
      label: <popis – o jaký typ telefonu se jedná mobilx X pevná linka>
      displayNumber: <telefonní číslo v regionálním tvaru>
      universalNumber: <telefonní číslo v mezinárodním tvaru>
      isVerified: true/false
nameSearchTokens: ["<text>","<text>"] (text zastupuje řetězce podle kterých
je možno uživatele v aplikaci vyhledat)
canMessage: true/false
isMobilePushable: YES/NO
isMessengerUser: true/false
messengerInstallTime: <systémový čas instalace>
isMemorialized: false/false
isOnViewerContactList: true/false
addedTime: <systémový čas přidání uživatele>
friendshipStatus: ARE_FRIENDS
subscribeStatus: IS_SUBSCRIBED
contactType: USER
timelineCoverPhoto:
      focus:
            x: 0.5
            y: 0.5
photo:
```

```
      image_midres:
            uri: https://fbcdn-sphotos-h-a.<skryto>
            width: 320
            height: 179
      image_lowres:
            uri: https://fbcdn-sphotos-h-a.<skryto>
            width: 500
            height: 281
nameEntries: []
birthdayDay: <den narození>
birthdayMonth: <měsíc narození>
cityName: <město>, <stát>
isPartial: false/true
```

Threads_db2

Obecně zde nalezneme jednotlivá vlákna konverzací s jednotlivými uživateli. V mnoha případech je obsah této databáze důležitější než informace o uživatelích a to proto, že obsahuje naprostou většinu nedávných konverzací uživatele. Zde se opět zaměříme na zájmové položky v této databázi.

Z pohledu obsahu je zde nejdůležitější tabulka *messages*, ve které jsou uloženy jednotlivé položky nedávných konverzací a další upřesňující informace, které zprávy jednoznačně identifikují.

Sloupce obsahují mimo jiné následující informace, které pro nás mohou být směrodatné:

Tabulka 4: Vybraná data z tabulky messages

msg_id	• identifikátor zprávy (text) - ve tvaru mid. $gAAW6O87_dmNk4ckNylesIO_DAYSS
thread_key	• textový řetězec, který spojuje více záznamů do jednoho vlákna
text	• pole typu text, obsahuje samotný obsah zprávy
text	• pole typu text, obsahuje samotný obsah zprávy
Sender	• identifikační řetězec odesilatele – {"email":null,"user_key":"FACEBOOK:<id>","name":"<jmeno uživatele>"}
timestamp_ms	• integer, identifikující čas odeslaní
attachments	• text, popisující případné přílohy • přílohu ve formě odkazu - konkrétní odkaz • video/obrázek/soubor - rozměry, velikost a odkaz, na kterém je příloha dostupná
client_tags	• textový řetězec, který v sobě má informaci o zdroji zprávy (zda šlo o aplikaci v telefonu, webový prohlížeč nebo aplikaci třetích stran)

Zdroj: Vlastní zpracování

Další důležité jsou tři tabulky, které obsahují vlákna, uživatele a vazby mezi nimi. Jde o tabulky *thread_participants*, *thread_users* a *threads.*

Thread_users

V tabulce *thread_users* nalezneme seznam uživatelů, kteří mají něco společného s konverzacemi lokálního uživatele; a to ať jde o odesílatele, příjemce nebo účastníka skupinové konverzace. Data, která nejčastěji využíváme, jsou uvedena v tabulce níže.

Tabulka 5: Vybraná data z tabulky thread_users

user_key	ID profilu
firs_name	text, jméno
last_name	text, příjmení
is_messenger_user	1 nebo 0
profile_pic_square	profilový obrázek uživatele
maximum_messenger_version	verze aplikace messenger, kterou daný uživatel vlastní

Zdroj: Vlastní zpracování

Thread_participants

V tabulce *thread_participants* máme vazbu mezi uživateli a jednotlivými vlákny a jsou pro nás zajímavá tři pole:

Tabulka 6: Vybraná data z tabulky thread_participants

thream_key	• standartní konverzace obsahuje ID obou uživatelů • ID skupinové konverzace
user_id	• společná položka s tabulkou thread_users
last_read_receipt_time	• čas, ve kterém byla zobrazena poslední zpráva

Zdroj: Vlastní zpracování

Tabulka je spojena s ostatními tabulkami klíčem *thread_key*, Dále obsahuje název konverzace (pokud není nastaven tak je *null*) nebo např. náhled na poslední odeslanou zprávu (sloupec *snippet*). Další, potenciálně zajímavý, je sloupec *approx_total_message_count*, který obsahuje počet zpráv. Další data pro nás nemají zásadní hodnotu nebo je možné je nalézt i v jiných tabulkách.

Search_cache_db

Poslední z databází, která by mohla obsahovat potenciálně zajímavé informace, je *search_cache_db*, ve které je obsažena nedávná historie další profilů, které uživatel vyhledával.

Obsahuje šest tabulek, přičemž zajímavá je pro nás je pouze tabulka *search_items.* Její strukturu uvádím v následující tabulce.

Tabulka 7: Vybraná data z tabulky search_items

fbid	id profilu
item_type	identifikátor zda jde o profil, skupinu nebo jiné
display_name	jméno účtu
first_name	
last_name	
picture_url	odkaz na profilový obrázek uživatele
client_fetch_time_ms	čas, ve kterém bylo hledání provedeno

Zdroj: Vlastní zpracování

7.2. Facebook – aplikace pro prohlížení

Aplikace je v balíčku *com.facebook.katana*, která se nachází ve složce data a svojí strukturou je, kromě několika málo databází, totožná s aplikací *messenger*. Obsahuje databázi konverzací, upozornění a kontaktů ve stejném tvaru. Jediné, co je v ní navíc, je databáze, která obsahuje za prvé data s příspěvky uživatelů, za druhé dočasné soubory obsahující videa a ostatní grafické soubory.

Video soubory jsou ve složce */data/data/com.facebook.katana/files/video-cache.* Ta obsahuje všechny video soubory, které se konkrétnímu uživateli zobrazili v posledních, nejaktuálnějších příspěvcích. Nejsou však rozděleny podle toho, který uživatel je přidal nebo sdílel.

Ostatní grafické soubory jsou také ve složce *cache* v podsložce *images*, stejně jako u aplikace *messenger.* I zde, stejně jako u výše jmenovaných, jsou videa rozdělena podle uživatelů a jsou ukládány s příponami *.cnt* a ne *.jpg* Je ale možné je otevřít a prohlížet.

Informace v databázi *newfeed_db* obsahují data o příspěvcích, které se uživateli zobrazují. Zde nalezneme, kdo byl autorem, samotný obsah příspěvku, kdy byl sdílen, kdy byl stažen do zařízení a i informaci, zda byl příspěvek zobrazen. Všechny časy (stažení, zobrazení, odeslání) používají unixový čas.

8. WhatsApp

Jedná se o freeware multiplatformní aplikaci, která nabízí textovou komunikaci, ale také VoIP. Její funkce nejsou závislé na službách mobilního operátora, ale pouze na připojení k internetu. V dnešní době jde o jednu z nejpoužívanějších komunikačních aplikací a to nejen na platformě Android. Velké oblíbenosti se těší z části díky velmi snadnému uživatelskému rozhraní, které funguje bez nutnosti registrace a v neposlední řadě i díky tomu, že využívá end-to-end šifrování veškeré komunikace, která jejím prostřednictvím probíhá.

Jako první se podíváme do složky */data/data/com.whatsapp*, kde se nachází rozbalená a nainstalovaná aplikace. Tato složka obsahuje soubory tyto soubory:

- app_minidumps
- cache
- code_cache
- databases
- files
- no_backup
- shared_prefs.

8.1. Zájmové složky a soubory

Jako poslední zmíním několik dalších souborů, které obsahují informace o uživateli. V první řadě jde o profilový obrázek, který vidí všichni ostatní uživatelé. Ten se nachází v */data/data/com.whatsapp/me.jpg* a je volně přístupný bez jakékoliv ochrany. Jako další jde o číslo, které je spojeno s profilem v aplikaci *WhatsApp*. Toto číslo nemusí být společné s telefonním číslem SIM karty, která je vložena v telefonu. Tento soubor nalezneme zde: */data/data/com.whatsapp/files/me.* Soubor „*me*“ obsahuje právě výše uvedené telefonní číslo ve volně přístupné formě.

O úroveň výše, ve složce *com.whatsapp*, nalezneme složku *cache*, ve které se nachází složka pro SSL certifikáty ke všem používaným relacím. Druhá složka obsahuje stažené profilové obrázky kontaktů, s kterými jsme v kontaktu.

Jako poslední ze souborů, které by mohly být důležité, jsou přílohy (jak přijaté, tak odeslané). Ty se nachází na volně přístupné části paměti zařízení, tzn. že nepotřebujeme práva *roota* abychom je mohli prohlížet, nebo na paměťové kartě, kde jsou umístěny v */sdcard/Whatsapp/Media.*

Dále projdeme uživatelská data, stejně jako u první aplikace. Případné potenciálně zájmové položky jsou pravděpodobně umístěny ve složce *databases*. Tato složka obsahuje *SQLite* databáze podobně jako *Messenger*. Soubory databází jsou tyto:

- axolotl.db
- google_app_measurement.db
- google_app_measurement_local.db
- chatsettings.db
- location.db
- msgstore.db
- wa.db.

Níže je výčet databází, které mohou být pro trestní řízení relevantní a mohou obsahovat potenciálně zajímavé informace.

Axolotl.db

Databáze, která je úzce spojena s šifrovacím mechanizmem aplikace *WhatsApp*. Je součástí kryptografického protokolu pro komunikaci, která využívá end-to-end šifrování. Po prvotní výměně klíčů se stará o obnovu klíčů, které mají krátkou platnost. Spojuje v sobě Diffieho-Hollmanovu výměnu klíčů a funkci pro jejich odvozování.

Obsahuje tabulku *identities*, ve které nalezneme dvojici klíčů pro komunikaci (veřejný a privátní klíč), dále je zde lokální ID uživatele, kterému byly klíče vystaveny a časové razítko z doby jejich přidělení.

V tabulce *prekeys* nalezneme sadu předschválených klíčů, které jsou použity v případech, kdy používaný klíč přestane platit nebo ho nelze použít.

Tabulka *signed_prekeys* obsahuje ID klíče, který je právě používán a časové razítko z doby, kdy byl konkrétní klíč podepsán.

Chatsettings.db

Součástí *chatsettings.db* je tabulka s názvem *settings*. Ta obsahuje jeden řádek pro každého uživatele, který byl v aplikaci vytvořen a je v něm obsaženo kompletní nastavení aplikace ve vztahu ke konkrétnímu uživateli. Obsahuje ID uživatele, příznak zde je uživatel smazaný, nastavení upozornění na zprávy, cestu k vyzvánění, nastavení vibrací a informaci o tom, zda je zařízení ztlumené nebo ne.

Location.db

V této databázi jsou uloženy informace o pohybu a poloze uživatele, pokud má sledování polohy povolené. Obsahuje tři tabulky, které by mohly obsahovat uživatelská data: *location_cache, location_key_distribution, location_sharer.* Obsahy těchto databází uvádím v tabulkách níže.

Tabulka 8: Vybraná data ze souboru location_cache

_id	integer, primární klíč
jid	text, not null
latitude	real, not null
longtitude	real, not null
accuracy	integer, not null
speed	real, not null
bearing	integer
location_ts	integer, not null

Zdroj: Vlastní zpracování

Z těchto záznamů je možný vysledovat pohyb uživatele a historii toho, kde se pohyboval.

V další tabulce *location_sharer* jsou sdílená data o umístění, jejich zdroji a uživateli, s kterým jsou spjata. Obsah jednotlivých tabulek uvádím níže.

Tabulka 9: Vybraná data ze sloky location_sharer

_id	integer, primární klíč
remote_jid	text, not null
from_me	boolean
remote_resource	text, not null
expires	integer, not null
message_id	text, not null

Zdroj: Vlastní zpracování

Msgstore

Tato databáze je svým obsahem částečně podobná obsahu databáze *Threads_db2* v aplikaci *Messenger*. Lze v ní nalézt seznam konverzací, smazané konverzace, seznam nejčastěji kontaktovaných uživatelů, skupinové konverzace (od účastníků přes časy, kdy byla skupina vytvořena až po obsahy jednotlivých zpráv), náhledy na konkrétní zprávy, zprávy v plném znění a informace o finančních transakcích.

Tabulka 10: Vybraná data z tabulky msgstore

_id –	integer, primary key
key_remote_jid	text, not null
key_from_me	integer
key_id	text, not null
status	integer
data	text
timestamp	integer
media_url	text
media_mime_type	text
media_wa_type	text
media_size	integer
media_name	text
media_caption	text
media_hash	text
media_duration	integer
latitude	real
longitude	real
received_timestamp	integer
send_timestamp	integer
multicast_id	text
media_enc_hash	text

Zdroj: Vlastní zpracování

Chat_list

Tabulka *chat_list* v sobě zahrnuje všechna komunikační vlákna, jejich identifikační prvky a konfiguraci. Konkrétně je zde: ID vlákna, předmět vlákna, čas vytvoření, informace, zda je vlákno archivováno, počet zpráv, počet zobrazených a nezobrazených zpráv, počet přijatých a nepřijatých hovorů, identifikátor, zda je vlákno šifrováno nebo není. Některé konkrétní názvy položek v tabulce a jejich datové typy jsou shrnuty níže.

Tabulka 11: Vybraná data z tabulky chat_list

_id	integer, primary key
key_remote_jid	text, not null
key_from_me	Integer
key_id	text, not null
status	integer
data	text
timestamp	integer
media_url	text
media_duration	integer
latitude – real, longitude	real
received_timestamp	integer
send_timestamp	integer
multicast_id	text
media_enc_hash	text
media_mime_type	text
media_wa_type	text
media_url	text
media_caption	text
media_size	integer
media_name	text
media_hash	text

Zdroj: Vlastní zpracování

9. Twitter

Klient sociální sítě *Twitter* v sobě obsahuje dvě základní funkce a to možnost prohlížet příspěvky ostatních uživatelů a možnost komunikovat přímo s ostatními uživateli. Tato možnost ale není mezi uživateli v ČR tolik rozšířená jako jinde ve světě, kde se těší značné popularitě.

9.1. Zájmové složky a soubory

Po nainstalování se aplikace nachází ve složce */data/data/com.twitter.android/.* V této složce najdeme také, jako ve všech případech výše, složku *cache* a složku *databases*. Složka *cache* zde obsahuje složky *photos* a *users*. V těch nalezneme soubory s profilovými obrázky z několika posledních zobrazených uživatelských profilů.

Další složka, která je zde přítomna, je *image_cache/v2.ols100.1/,* kde se nachází řada číselně označených složek, ve kterých jsou soubory ve stejné formě jako u aplikace *Messenger*. Jedná se o soubory *.cnt*, které je možné otevřít jako každý jiný soubor *.jpeg*. V těchto souborech jsou profilové obrázky, fotografie a jiné statické grafické soubory, a to nejen z veřejných příspěvků, ale i ze soukromé komunikace mezi uživateli.

Stejně jako v předchozích případech se přesuneme dále do složky */.com.twitter.android/databases/*, kde je 13 databázových souborů, přičemž pět je generovaných a odstraněných při chodu aplikace. Zbytek jsou statické soubory a obsahují různá uživatelská data, na která se podrobně podíváme.

Hlavní databáze

Název této databáze je pokaždé jiný a to podle uživatele, který je přihlášený a podle zařízení, na kterém je aplikace nainstalována. Jedná se o největší databázi, kde je možné najít uživatele, veřejné položky i soukromé konverzace.

Users

V tabulce *users* najdeme, jak název napovídá, seznam uživatelů, dále jejich uživatelské jméno, popis jejich profilu, zvláštní pole na odkazy na internet, ID jak v rámci lokálních dat tak ID v rámci celé služby, odkaz na umístění profilového obrázku, lokace, která byla nastavená uživatelem, počet uživatelů – sledujících i sledovaných konkrétním uživatelem, počet veřejných příspěvků konkrétního uživatele a poznámku o čase, kdy byl profil vytvořen. Níže uvádím výčet některých polí a jejich datové typy.

Tabulka 12: Vybraná data z tabulky users.

user_id	integer, unique, not null
username	text
name	text
description	blob
web_url	text
image_url	text
locatiom	text
followers	integer
statuses	integer

Zdroj. Vlastní zpracování

Statuses

Tabulka, obsahující veřejné příspěvky uživatelů, ID autora i samotného příspěvku, čas vytvoření tohoto příspěvku, počet a druh reakcí na příspěvek, jazyk v jakém byl příspěvek vytvořen a vazby příspěvku s uživateli v rámci vnitřních i vnějších ID v lokální aplikaci i celé službě. Některé důležité položky a jejich datové typy uvádím níže.

Tabulka 13: Vybraná data z tabulky statutes

status_id	integer, unique, not null
author_id	integer
created	integer (čas vytvoření)
favorited	integer
retweeted	integer
favorite_count	integer
retweet_count	integer
view_count	integer
latitude	integer
longtitude	integer (položky jsou přítomny, pokud uživatel povolí sdílení těchto informací)
lang	text

Zdroj: Vlastní zpracování

Timeline

Poslední položkou z této databáze, kterou zmíním je tabulka *timeline*. Není v ní žádný obsah, který by nás mohl zajímat přímo, ale je možné zní vyčíst existující vazby mezi příspěvky a uživateli, v některých případech i mezi skupinami uživatelů. Jinými slovy obsahuje většinu interních a externích ID a popisuje, který obsah náleží kterému příspěvku a který uživatel je za něj zodpovědný.

Conversation

Databáze Conversation obsahuje tabulky *conversation, conversation_entries, conversation_participants a conversation_participants_users*. Poslední dvě zmíněné

jsou zde opět kvůli vytváření vazeb s ostatními daty a fungují velmi podobně jako tabulka *timeline,* pouze s tím rozdílem, že zde jde o soukromé konverzace, nikoliv o veřejný obsah. Konkrétně zde nalezneme lokální ID každé zprávy, dále ID každé konkrétní zprávy a odesílajícího uživatele, dále samotný obsah zprávy uložené v datovém typu *blob*; poslední položkou jsou konkrétní jména uživatelů patřící k ID uvedeným v ostatních sloupcích.

10. Viber

Stejně jako u aplikace *WhatsApp* se zde jedná o freeware multiplatformní komunikační aplikaci. V první veřejné verzi vyšla v roce 2010 na platformách Windows, macOS, Linux, Android a iOS. Umožňuje uživatelům posílat text a datové přílohy a podporuje VoIP. V roce 2016 měla zhruba 800 milionů registrovaných uživatelů.

10.1. Zájmové složky a soubory

Stručně ke struktuře samotné aplikace. Hlavní data se nacházejí stejně jako u všech ostatních aplikací ve složce */data/data/*. Konkrétní balíček patřící k této aplikaci se jmenuje *com.viber.voip*. Pro nás bude opět nejzajímavější složka *databases*, dalšími zájmovými umístěními jsou *cache* a *files*.

Ve složce *files* jsou potenciálně zajímavé tři osubory ve složce *preferences*: *activated_sim_serial*, *display_name* a *reg_viber_phone_num*. *Acivated_sim_serial* obsahuje identifikační číslo SIM karty, která je v současnosti v zařízení nebo byla v zařízení v době aktivace aplikace. *Display_name* je přítomný pouze v případech, kdy si uživatel změní uživatelské jméno, které se zobrazuje. *Reg_viber_phone_num* obsahuje telefonní číslo, které uživatel přihlásil ke svému účtu a na kterém je možné ho zkontaktovat.

Další zájmové umístění je na volně přístupné části paměti nebo na paměťové kartě, jedná se o soubory umístěné zde: */sdcard/viber/media/*. Složka *media* obsahuje tři složky, které jsou pro nás zajímavé a jsou to: *User Photos, Viber Images, Viber Videos*. Tyto tři složky obsahují profilové obrázky všech kontaktů, které jsou v telefonním seznamu bez ohledu na to jestli, používají Viber nebo ne. Složky *Images* a *Videos* obsahují všechny odeslané a přijaté přílohy konkrétních typů.

Databases

V této složce nás potenciálně zajímají pouze dvě databáze a to: *Viber_data* a *Viber_messeges*. Stejně jako dříve se jedná o databáze i přestože nemají příponu .db.

Viber_data – tabulka Calls

Tato tabulka napříč různými verzemi aplikace nevykazuje konzistentní chování a to proto, že i přes existenci relevantních dat nejsou u všech verzí všechna data zaznamenávána. Jak vyplývá z jejího názvu je v ní možné najít u některých verzí všechny hovory, které byly uskutečněny včetně doby trvání a způsobu ukončení.

Viber_data – tabulka Phonebookcontact

Phonebookcontact je pro nás asi nejzajímavější tabulkou z celé této databáze. *Viber* se při prvním spuštění pokusí přistoupit k telefonnímu seznamu a pokud je mu to umožněno, zkopíruje všechny kontakty ze zařízení do svojí databáze. Záznamy z této databáze se neodstraňují, a to i v případě, údaj z kontaktů v zařízení samotném vymažeme. Z této databáze je možné získat seznam všech kontaktů, které v zařízení kdy byly uloženy od okamžiku nainstalování aplikace.

Viber_data – tabulka Phonebookdata

Tato tabulka má totožné funkce jako tablka *phonebookcontact* pouze s tím rozdílem, že obsahuje navíc informace o e-mailové adrese kontaktu a jeho telefonním čísle.

Viber_data – tabulka Vibernumbers

V této tabulce je uloženo telefonní číslo uživatelů v rámci aplikace *Viber,* a to pro každý z kontaktů, pokud ho mají. Dále obsahuje název profilového obrázku, který je uložen pod stejným názvem v */sdcard/viber/media/User Photos/*.

Viber_messages

Viber_messages je databází i přes to, že nemá příponu *.db.* Obsahuje data o používání aplikace. A to od od konverzací, účastníků, obsahu zpráv až po nákupy v aplikaci. Dále jsou uvedeny tabulky, které mohou obsahovat zajímavá data.

Viber_messages – tabulka Conversations

Zde je umístěno unikátní ID každého konverzačního vlákna, příjemce a čas, ve kterém každá z konverzací proběhla.

Viber_messages – tabulka Messages

Soubor *mesages* obsahuje konkrétní zprávy ze všech vláken. Pole *address* je telefonní číslo druhého uživatele, který se na konverzaci podílel. Pole *type* obsahuje příznak o tom, zda byla komunikace příchozí nebo odchozí. Pole *location_lat* a _lng budou zaplněna pouze v případě, že je povoleno sdílení pozice. Poslední pole, *description,* je zaplněno pouze v případě, že posíláme přílohu a k ní připojíme popis.

Viber_messages – tabulka Messages_calls

Tato tabulka se chová stejně jako tabulka *calls* ve *viber_data* a shoduje se ní i svým obsahem.

Viber_messages – tabulka Participants_info

V této tabulce jsou uvedeny informace o všech uživatelích, kteří jsou nebo byly v kontaktu s lokálním uživatelem.

11. Ostatní možnosti využití těchto služeb

Výše jsem se zaměřil na některé často používané služby, uvědomuji si ale, že tyto komunikační prostředky je možné používat a přistupovat k nim i jinými cestami, například webovým prohlížečem. Zkoumání, a případná dokumentace, dat ve webových prohlížečích není cílem práce. Protože ale početná skupina uživatelů využívá tyto služby právě tímto způsobem, zmíním alespoň okrajově data defaultního webového prohlížeče v OS Android – v Google Chrome.

Google Chrome najdeme v balíčku *com.android.chrome* ve složce *data*. V tomto balíčku jsou pro nás zajímavá data o používání aplikace a to ve složce *app_chrome*. Zde jsou zajímavé dvě podložky a to *Default* a *app_ChromeDocumentActivity*.

Ve složce Default se nacházejí: záložky, cookies, historie prohlížení, informace o přihlášeném uživateli, nastavení prohlížeče, nejčastěji navštěvované stránky, data jednotlivých webových stránek a synchronizovaná data (ve formě SQLite databáze). Poslední zmíněná databáze obsahuje asi největší množství dat, která je možné synchronizovat se servery firmy Google. Konkrétním obsahem mohou být data od historie prohlížení, přes vyplňované formuláře, až po uložená hesla nebo záložky. Ke každému záznamu pak nalezneme řadu časových příznaků, z kterých ovšem není úplně jasné, k čemu který patří, protože od sebe bývají vždy jen několik milisekund.

Z výše uvedených databází blíže zmíním ještě databázi s informacemi o prohlížení - *Web Data*. Zde jsou uloženy předvyplněné formuláře s časem, kdy byly uloženy. Dále je zde název pole a obsah, který se má do konkrétního pole vyplňovat.

Poslední složkou je složka *app_ChromeDocumentActivity*, kde se nachází soubory obsahující nedávno otevřené stránky. Z těchto souborů je možné získat URL těchto stránek a čas, kdy byly navštíveny.

12. Vyhodnocení

Z toho důvodu že OS Android je v dnešní době nejpoužívanějším systémem nejen v mobilních telefonech, ale v mobilních zařízeních obecně, tak je možné vyvodit to, že bude ve značné míře využíván i k trestné činnosti. A v takovéto situaci se z pro nás nezajímavé digitální stopy stávají zajímavým digitálním důkazním materiálem.

Vzhledem k tomu, že tato práce je zaměřena právě na umístění potenciálního důkazního materiálu v rámci struktury OS Android, tak zde byly vynechány postupy samotné extrakce dat ze zařízení. Hlavní část práce byla zaměřena na data samotná a na jejich obsah.

Právě na základě této praktické části jsem zjistil, že aplikace pro Facebook a Twitter, jelikož jde o aplikace pro kompletní sociální sítě, ukládají informace o uživatelích, o tom co zveřejňují a s kým komunikují velmi podobným způsobem a ve velmi podobném tvaru. Aplikace WhatsApp a Viber jsou taky velmi podobné, protože se jedná o aplikace určené čistě ke komunikaci a ne ke sdílení obsahu s širokou skupinou uživatelů.

Odlišnosti zásadního charakteru, které jsem nalezl při praktické části byly z velké části očekávané (WhatsApp klade poměrně velký důraz na bezpečnost uživatelských dat a další). Co bylo asi nejvíce překvapivé je zjištění, že aplikace Viber si vytváří a uchovává seznamy kontaktů nejen v rámci aplikace, ale vytváří si bez vědomí uživatele i kopii telefonního seznamu a informace o kontaktech, které uživatel má uloženy ve spojení s nimi.

Vybrané zájmové oblasti a to, zda je aplikace zaznamenává a ukládá, jsem shrnul v tabulce.

Tabulka 14: Přehled vybraných dat ze jmenovaných komunikaních aplikací

	Facebook	WhatsApp	Twitter	Viber
Jméno/Příjmení uživatele	Ano	Ano	Ne	Ano
Uživatelské jméno uživatele	Ano	Ano	Ano	Ano
Jméno/Příjmení ostatních uživ.	Ano	Ano	Ne	Ano
Uživatelská jména ostatních	Ano	Ano	Ano	Ano
Datum narození	Ano (pokud je uvedeno)	Ne	Ano (pokud je uvedeno)	Ano (pokud je uvedeno)
Fotografie uživatelů	Ano	Ano	Ano	Ano
Zprávy (čas, odesílatel)	Ano	Ano	Ano	Ano
Přílohy u zprávy	Ano	Ano	Ano	Ano
Šifrovací klíče pro komunikaci	Ne	Ano	Ne	Ne
Klíče pro šifrování	Ne	Ano	Ne	Ne
GPS pozice uživatele	Ne	Ano	Ne	Ne
GPS pozice ostatních uživatelů	Ne	Ano	Ne	Ne
Kompletní telefonní seznam	Ne	Ne	Ne	Ano
E-mailové adresy kontaktů z tel. seznamu	Ne	Ne	Ne	Ano
Veřejné příspěvky	Ano	Ne	Ano	Ne
Reakce na veř. příspěvky	Ano	Ne	Ano	Ne
Přílohy u veřejných příspěvků	Ano	Ne	Ano	Ne

Zdroj: vlastní zpracování

13. Závěr

OS Android je na trhu mobilních telefonů i ostatních přenosných zařízení jasně dominantní a pokrývá více než ¾ trhu. Kromě standartní komunikace pomocí hovorů a SMS jsou stále oblíbenější různé sociální sítě a komunikační aplikace, jejichž digitální záznamy se v některých případech využívají pro potřeby trestního řízení.

Pokud je splněn právní rámec, je elektrické zařízení podrobené forenzní analýze, která za použití logické analýzy nebo fyzických metod extrahuje potřebná data.

Na základě mnou provedené dokumentace je možné definovat hlavní zájmové složky a soubory informací, které jsou nejčastěji v trestním řízení využívány. Lze říci, že jde vždy o podobné soubory a těmi jsou: uživatelská jména, uživatelské fotografie, kontaktní údaje, různé formy zpráv nebo příspěvků a detaily o jejich odeslání.

Přesto, že mezi veřejností roste povědomí o nutnosti zabezpečení svých údajů v eklektických zařízeních, při výběru komunikační aplikace nebo sociální sítě se ale o údaje, které jsou o nich shromažďovány, nezajímají a jejich výběr a případné stažení aplikace není tímto aspektem ovlivněno.

14. Zdroje

MAHALIK, Heather, Satish BOMMISETTY a Rohit TAMMA. *Practical Mobile Forensics: A hands-on guide to mastering mobile forensicsfor the iOS, Android, and the Windows Phone platforms*. 3rd ed. Birmingham: Packt Publishing, 2018, 402 s. ISBN 978-1-78883-919-8.

ROGERS, Marcus K. a Kathryn C. SEIGFRIED-SPELLAR SPRINGER. *Digital Forensics nad Cyber Crime: 4th International Conference*. Lafayette (USA): Revised Selected Papers, 2012. ISBN 978-3-642-39890-2.

DATT, Samir. *Learning Android Forensics: Community Eyperience Distilled*. Birmingham: Packt Publishing, 2016. ISBN 978-1-78217-457-8.

HOOG, Andrew. *Android Forensics: Investigation, Analysis, and Mobile Security for Google Android*. Waltham: Syngress, 2011. ISBN 978-1-59749-651-3.

CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic science, computers and the internet*. 3rd ed. Publisher Academic Press, 2011. ISBN 9780080921488.

ELENKOV, Nikolay. *Android Security Internals: An In-Depth Guide to Android´s Security Architecture*. 2014. ISBN 978-1-59327-581-5.

Facebook for Android Artifacts. *Free Android Forensics* [online]. 2015 [cit. 2018-04-09]. Dostupné z: http://freeandroidforensics.blogspot.cz/2015/02/facebook-for-android-artifacts.html

Android Internals [online]. Birmingham: Packt Publishing, 2016 [cit. 2018-04-09]. ISBN 978-1-78528-781-7. Dostupné z: https://archive.org/stream/android-internals/android-internals/mastering-mobile-forensics_djvu.txt

MOBILedit Forensic Express v3.5.2.7047: Test Results for Mobile Device Acquisition Tool [online]. Department of Homeland Security, 2017, , 18 [cit. 2018-04-10]. Dostupné z: https://www.dhs.gov/sites/default/files/publications/508_Test%20Results%20for%20Mobile%20Device%20Acquisition%20Tool%20-%20MOBILedit%20Forensic%20Express%20v3.5.2.7047_March%207%2C%202017.pdf

Android versions comparison. *Android versions comparison* [online]. 2018 [cit. 2018-04-10]. Dostupné z: http://socialcompare.com/en/comparison/android-versions-comparison

TAHIRI, Soufiane. Android Forensic Logical Acquisition. *Infosec Institute* [online]. 2016, 16. 4. 2016 [cit. 2018-04-10]. Dostupné z: http://resources.infosecinstitute.com/android-forensic-logical-acquisition/#gref

Seznam tabulek a obrázků:

Seznam tabulek

Seznam ilustrací