Jihočeská univerzita v Českých Budějovicích

Přírodovědecká fakulta

Forenzní analýza mobilních zařízení s operačním systémem Android

Diplomová práce

Bc. Vojtěch Novotný

Vedoucí práce: Ing. Jaroslav Kothánek, Ph.D.

České Budějovice 2016

Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

ZADÁVACÍ PROTOKOL MAGISTERSKÉ PRÁCE

Student: **B13303 / Bc. Vojtěch Novotný**
(jméno, příjmení, tituly)

Obor – zaměření studia: **1802T001 / Aplikovaná informatika**

Katedra: **Ústav aplikované informatiky**

Školitel: **Ing. Jaroslav Kothánek, Ph.D., jkothanek@prf.jcu.cz**
(jméno, příjmení, tituly, u externího š. název a adresa pracoviště, telefon, fax, e-mail)

Garant z PřF:
(jméno, příjmení, tituly, katedra – jen v případě externího školitele)

Školitel – specialista, konzultant: Ing. Jaroslav Kothánek, Ph.D.
(jméno, příjmení, tituly, u externího š. název a adresa pracoviště, telefon, fax, e-mail)

Téma magisterské práce:

Forenzní analýza mobilních zařízení s operačním systémem Android

Cíle práce :

Návrh a metodika forenzního zkoumání mobilních zařízení s operačním systémem Android, popis jednotlivých metod vytěžování datového prostoru, včetně smazaných informací.

Úkoly :

- Seznamte se s problematikou forenzního zkoumání digitálních důkazů

a) zásady při zajišťování digitálních důkazních materiálů

b) zásady při dokumentaci důkazních digitálních materiálů

- Proveďte analýzu běžně používaných komunikačních aplikací v rámci platformy operačního systému Android

a) proveďte analýzu získání informací běžných pro mobilní telefony

b) proveďte analýzu doplňkových komunikačních aplikací

- Popište operační systém Android a jeho běžné komunikační aplikace ve vztahu k forenznímu zkoumání pro orgány činné v trestním řízení
- Definujte rizika při zkoumání uvedené mobilní techniky a navrhněte optimální řešení
- Seznamte se s dostupnými forenzními nástroji a zhodnoťte jejich výsledky při forenzním zkoumání
- Popište umístění a strukturu dat jednotlivých běžných komunikačních aplikací.

- Vyhodnoťte své výsledky analýz a srovnejte je s běžnými forenzními nástroji
- Ve spolupráci s vedoucím práce vytvořte krátký článek s výsledky vašich analýz a tento pokud možno publikujte v odborném časopise

Základní doporučená literatura :

Morrissey, S., iOS Forensic Analysis for iPhone, Ipad and iPod touch, Apress

Sammes, T.,, Jenkinson, B.,, Forensic Computing a Practitioner´s Guide, Springer

Carrier, B., File System Forensic Analysis

Hoog. A, Android Forensic

Odkazy:

www.accessdata.com

www.belkasoft.com

www.mobiledit.com

www.Oxygen-forensic.com

www.cellebrite.com

www.msab.com

Financování práce :.....

Vedoucí práce :.....Ing. Jaroslav Kothánek, Ph.D.....podpis : .....

U externích vedoucích fakultní garant práce.....podpis : .....

Garant oboru mag. studia ..... podpis : .....

Vedoucí oddělení ...Ing. Jaroslav Kothánek, Ph.D..... podpis .....

Případný souhlas vedoucího ústavu AV .....podpis : .....

V Českých Budějovicích dne 28. 2. 2014

Převzal/a dne 25. 2. 2014 podpis : .....

Novotný V., 2016: Forenzní analýza mobilních zařízení s operačním systémem Android. [Forensic analysis of mobile devices running Android. Mgr. Thesis, in Czech.] – 68 p., Faculty of Science, The University of South Bohemia, České Budějovice, Czech Republic.

Název

Forenzní analýza mobilních zařízení s operačním systémem Android

Abstract

Diplomová práce „Forenzní analýza mobilních zařízení s operačním systémem Android“ se zabývá problematikou získávání dat sloužících, jako důkazy pro orgány činné v trestním řízení z mobilních zařízení s tímto operačním systémem. V této práci je navržen postup pro provedení této analýzy a jeho vliv na zkoumané mobilní zařízení. Tento postup byl ověřen na několika modelech mobilních zařízení. Tyto výsledky byly porovnány s výsledky analýz komerčních forenzních nástrojů.

Klíčová slova

Android, Forenzní, Analýza, Postup

Title

Forensic analysis of mobile devices running Android

Summary

The thesis "Forensic analysis of mobile devices running Android" deals with issue of collecting a data used as evidence in criminal justice from mobile devices with this operating system. In this work it is proposed procedure for performing this analysis and its impact on the surveyed mobile devices. This procedure has been validated on several models of mobile devices. These results were compared with the results of analyzes of commercial forensic tools.

Key worlds

Android, Forensic, Analysis, Procedure

Prohlašuji, že svoji diplomovou práci jsem vypracoval/a 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 diplomové 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 22. dubna 2016

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
1.1. Úvod 1
1.2. Cíle práce 2
1.3. Současný stav problematiky 2
2. Digitální důkazy 3
2.1. Zajišťování digitálních důkazů 3
2.2. Dokumentace digitálních důkazů 4
2.3. Druhy digitálních důkazů 4
3. Rozdělení forenzní analýzy 6
3.1. Podle dopadu na zařízení 6
3.2. Podle možnosti vytěžování dat 7
4. Vlastnosti operačního systému ve vztahu k forenznímu zkoumání 8
4.1. Vývoj OS Android 8
4.2. Architektura operačního systému Android 9
4.3. Architektura mobilních zařízení 11
4.4. Bootovací proces 14
4.5. Data v mobilních zařízeních 15
5. Analýza zařízení 18
5.1. Příprava mobilního zařízení 18
5.2. Práce s mobilním zařízením 19
5.3. Zámek obrazovky 22
5.4. Získání dat pomocí ADB 24
5.5. Analýza paměťové karty 25
5.6. Uživatelská práva 27
5.7. Získání dat z mobilního zařízení 29
5.8. Analýza obrazů paměti 37
6. Data v mobilním zařízení 42
6.1. Typy dat 42
6.2. Struktura dat v mobilním zařízení 43
6.3. Informace o mobilním zařízení 44

6.4. Data běžných aplikací 46
6.5. Data doplňkových aplikací 50
7. Komerční forenzní nástroje 55
7.1. Softwarové forenzní nástroje 55
7.2. Hardwarové forenzní nástroje 58
8. Vyhodnocení výsledků 61
8.1. Vyhodnocení navrženého postupu analýzy 61
8.2. Porovnání s komerčními forenzními nástroji 62
9. Závěr 63
10. Použitá literatura 64
11. Přílohy 68

Seznam obrázků

Obrázek č. 1 – Rozložení trhu (OS Android) 8
Obrázek č. 2 – Architektura OS Android 9
Obrázek č. 3 – Schéma YAFFS2 13
Obrázek č. 4 – SDK Manager 20
Obrázek č. 5 – ADB – Prolomení zámku obrazovky 23
Obrázek č. 6 – Obraz karty - dd 25
Obrázek č. 7 – FTK Imager 26
Obrázek č. 8 – Zjištění souborového systému 30
Obrázek č. 9 – Výpis příkazu mount 30
Obrázek č. 10 – Rozložení paměti YAFFS2 31
Obrázek č. 11 – Chybný výpis oddílů 34
Obrázek č. 12 – Rozložení paměti EXT4 34
Obrázek č. 13 – dd a cat přes SSH 36
Obrázek č. 14 – Prostředí programu Yaffey 37
Obrázek č. 15 – Připojení obrazu (YAFFS2) 38
Obrázek č. 16 – FTK Imager – Zkoumání obrazu paměti 40
Obrázek č. 17 – Autopsy – Zkoumání obrazu paměti 41

Obrázek č. 18 – Výpis kořenového adresáře 44
Obrázek č. 19 – LG E440 – last_log 45
Obrázek č. 20 – LG E440 – accounts.db 46
Obrázek č. 21 – LG E440 – wpa_supplicant.conf 46
Obrázek č. 22 – Kontakty z contacts2.db 47
Obrázek č. 23 – Výpis hovorů z contacts2.db 48
Obrázek č. 24 – SMS zprávy 49
Obrázek č. 25 – Data z tabulky events 50
Obrázek č. 26 – Zprávy aplikace Messenger 51
Obrázek č. 27 – Historie konverzací ICQ 52
Obrázek č. 28 – Gmail 54

1. Úvod a cíle práce

1.1. Úvod

Mobilní zařízení jsou v současné době běžnou součástí našeho života. Možnosti těchto zařízení se s vývojem nových technologií stále zvyšují, roste jejich výkon a možnosti využití. Tyto zařízení se architekturou stále více přibližují běžným domácím počítačům. Mobilní zařízení mohou ukrývat důležité důkazy potřebné pro orgány činné v trestním řízení. Proto je potřebné provést forenzní analýzu těchto zařízení.

Přestože jsou mobilní zařízení v současné době velice podobné běžným domácím počítačům, nebo notebookům, nelze při jejich forenzní analýze využít postupů využívaných při forenzní analýze klasických počítačů. To je způsobeno jejich architekturou a operačními systémy, které jsou uzpůsobovány pro tyto zařízení.

V současné době výrobci využívají hlavně operační systémy Android, iOS, Windows Phone a BlackBerry OS. Podíly těchto operačních systémů jsou v posledních dvou letech skoro neměnné. Android si drží podíl okolo 77%, iOS si drží okolo 20%, Windows Phone se přibližuje 3% a BlackBerry OS má pouze 0,5% trhu. Ostatní minoritní operační systémy zabírají pouze 0,5% trhu. [1] Jak je vidět, operační systém Android zaujímá většinovou část trhu a počet mobilních zařízení několikanásobně převyšuje počet mobilních zařízení s ostatními operačními systémy. Proto se tato práce zaměřuje na mobilní zařízení s operačním systémem Android.

Tato práce se zabývá forenzní analýzou mobilních zařízení s operačním systémem Android, popisuje tento operační systém a omezení, které přináší v oblasti forenzní analýzy. Jsou zde analyzovány komunikační aplikace využívané v těchto zařízeních. A obsahuje návrh postupu pro provedení forenzní analýzy.

1.2. Cíle práce

- Návrh a metodika forenzního zkoumání mobilních zařízení mobilních zařízení s operačním systémem android
- Popis operačního systému android a omezení, které tento systém přináší pro provedení forenzní analýzy
- Analýza a popis komunikačních aplikací využívaných v mobilních zařízeních s operačním systémem android pro potřeby forenzní analýzy
- Definice rizik při zkoumání mobilních zařízení s operačním systémem android
- Vyhodnocení dostupných forenzních nástrojů a porovnání jejich možností s navrženým postupem

1.3. Současný stav problematiky

V současné době se pro forenzní analýzu mobilních zařízení s OS Android dají využít komerční nástroje vytvořené speciálně k tomuto účelu. Mezi ně patří například UFED, Oxygen forensic, MPE+, XRY, nebo MobilEdit!. Všechny tyto nástroje pracují na podobném principu a jejich cena se pohybuje řádově až ve statisících korun.

Další možností je využití JTAGu. JTAG funguje na zcela jiném principu než běžné komerční nástroje. Jeho použití má své výhody i nevýhody.

Problematice forenzní analýzy se zabýval ve své knize A. Hoog [5]. Ovšem tato kniha byla vydána v roce 2011, od té doby se OS Android změnil, proto závěry v této knize nelze aplikovat na většinu zařízení vyrobených po roce 2011. Ovšem aktuální vydané materiály k této problematice jsou velice povrchové a v českém jazyce nejsou dostupné.

2. Digitální důkazy

Většina digitálních zařízení v sobě uchovává velké množství dat. Tyto data mohou být využity jako digitální důkazy pro orgány činné v trestním řízení. Avšak tyto důkazy musí být správně zajištěny a zadokumentovány, aby nebylo možné zpochybnit jejich pravost.

2.1. Zajišťování digitálních důkazů

Při zkoumání digitálních dat může snadno dojít k jejich změně, poškození, nebo zničení. Proto je vhodné zajistit kopii dat a na té následně provést potřebné postupy pro analýzu dat. Je více možností, jak získat kopii dat. Každá přináší výhody, ale také nevýhody oproti ostatním. Proto je vždy třeba předem zvážit, jaká metoda bude nejvhodnější pro konkrétní případ.[2]

2.1.1. Kopie dat pomocí jiného systému

Při tomto postupu dochází k nabootování Live verze operačního systému z externího média, například DVD, nebo Flash disku na zkoumaném zařízení a pomocí něj provést kopii dat. Výhoda je, že takový operační systém nepotřebuje pro svou činnost pevný disk, ale pouze operační paměť, díky tomu nedochází ke změnám dat na zkoumaném disku.[2]

Nevýhodou je nutnost vypnutí zařízení před nabootováním operačního systému, to vede ke ztrátě dat z operační paměti a dalším možným komplikacím.

2.1.2. Kopie dat pomocí zkoumaného systému

V některých zařízeních není možné nabootovat jiný operační systém, nebo by mohla při vypnutí zařízení hrozit ztráta důležitých dat, nebo jejich následná nemožnost čtení, například obsah operační paměti, obsah diskového pole RAID, šifrovaný disk.[2]

Ovšem tato metoda přináší rizika, protože prací ve zkoumaném operačním systému muže dojít k modifikaci nebo poškození dat na pevném disku.

2.2. Dokumentace digitálních důkazů

Všechny kroky provedené při zajišťování digitálních důkazů by měly být zaznamenávány, aby později nemohlo dojít k zpochybnění jejich pravosti, také by měl být přesně zadokumentován stav zkoumaného zařízení před započetím zkoumání. Obzvláště pokud jsou data získávána prostřednictvím zkoumaného systému je nutné všechny tyto kroky zaznamenat, protože tyto úkony jsou brány jako zásah do systému a mohlo by dojít k situaci, kdy důkazy budou považovány za zmanipulované a nepoužitelné pro orgány činné v trestním řízení. Proto je nutné zaznamenat každý provedený krok, kdy byl proveden a za jakým účelem byl proveden.[2]

2.3. Druhy digitálních důkazů

V úložištích digitálních zařízení se lze setkat s několika kategoriemi souborů, které mohou být cenné jako digitální důkazy. Avšak ne vždy jsou tyto soubory snadno dohledatelné.

2.3.1. Běžné soubory

Tyto soubory jsou uloženy v paměťovém médiu zařízení (HDD, SSD, Nand Flash) a ani při výpadku napájení, ani při vypnutí zařízení nedojde k jejich ztrátě, ani poškození. V těchto souborech lze nalézt uživatelská data, systémová data, data aplikací. Proto jsou velmi cenným zdrojem dat.

2.3.2. Dočasné soubory

Dočasné soubory vytvářejí programy pro ukládání dat, které si potřebují uchovat v průběhu jejich chodu. Při ukončení programu by měl program sám tyto data vymazat, ovšem když dojde k pádu programu, dočasná data nejsou smazána. Některé programy však nevymažou dočasné soubory ani při správném ukončení. Například dočasné soubory webového prohlížeče obsahují údaje o prohlížených stránkách. Tyto soubory v sobě mohou nést důležité informace o činnosti zařízení.[3]

2.3.3. Smazané soubory

Smazáním souboru nedojde k jeho skutečnému odstranění z paměťového média, pouze se místo kde byl soubor uložen, označí za volné a lze ho využít pro zápis jiných dat. Ovšem dokud nedojde k přepsání jinými daty lze smazaná data získat. Uvádí se, že jeden přepis náhodnými daty neznamená definitivní ztrátu smazaných dat. Podle standardu americké NSA se data přepisují sedmkrát, avšak jako nejbezpečnější metoda je uváděna metoda Peter Gutmann, při které dojde k přepisu dat třicet pět krát. Podobné je to i s formátováním paměťového média, kdy veškerá data která paměťové médium obsahovalo, jsou na něm stále fyzicky zapsána.[4]

Proto i když na paměťovém médiu na první pohled nejdou žádná cenná data, nebo vůbec žádná data, může to být významný zdroj digitálních důkazů.

3. Rozdělení forenzní analýzy

Forenzní analýzu lze dělit podle dvou faktorů. Jedním je její dopad na zařízení, kde se rozděluje podle toho, zdali dochází k poškození zařízení, nebo poškození dat v zřízení. Druhým je její schopnost vytěžování dat ze zařízení. [6]

3.1. Podle dopadu na zařízení

3.1.1 Nedestruktivní analýza

V případě nedestruktivní analýzy nedochází k poškození ani ke změnám zkoumaného zařízení. Zároveň nedochází ke změnám ani poškození dat uložených v zařízení. Avšak nedochází ani k možným poškození smazaných dat. Dalším důležitým faktorem je, že zařízení je po dokončení forenzní analýzy ve stejném stavu jako před jejím zahájením.

3.1.2 Částečně destruktivní analýza

V případě částečně destruktivní analýzy může dojít ke změnám v zařízení, které mohou způsobit změny v zařízení, které mohou být nevratné. Proto není možné zaručit, že zařízení bude po dokončení forenzní analýzy přesně ve stejném stavu jako před jejím zahájením. Dalším specifikem částečně destruktivní analýzy je možnost znehodnocení části dat obsažených v zařízení.

3.1.3 Destruktivní analýza

V případě destruktivní analýzy dochází k získání dat za cenu poškození zařízení. V některých případech může dojít až k úplnému zničení zařízení. Tyto metody bývají velmi účinné, avšak v mnoha případech je nežádoucí možné zničení zařízení.

3.2. Podle možnosti vytěžování dat

3.2.1 Logická analýza

Při logické analýze zařízení se pouze se soubory, které jsou uložené v zařízení. Tyto soubory jsou následně analyzovány. Ovšem poškozené či smazané soubory nejsou analyzovány. Logická analýza bývá jednodušší a rychlejší možností provedení analýzy.

3.2.2 Fyzická analýza

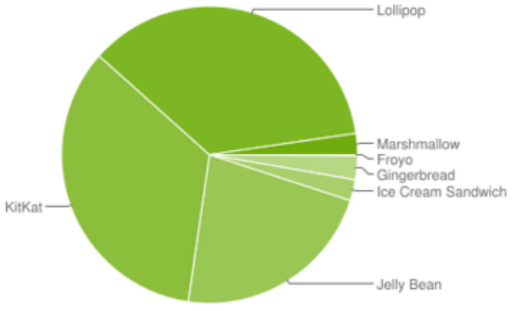
V případě fyzické analýzy je situace komplikovanější. Dochází při ní ke kompletní analýze celé paměti. Proto je tato analýza pomalejší a náročnější. Avšak umožňuje získat smazaná či poškozená data.

4. Vlastnosti operačního systému ve vztahu k forenznímu zkoumání

4.1. Vývoj OS Android

První Alfa verze operačního systému Android byla představena na podzim roku 2007. První oficiální verze označená Android 1.0 byla představena o rok později. Od té doby do dnes byly vydány různé verze tohoto operačního systému. Každá verze přinesla vylepšení operačního systému jak po stránce aplikační vybavenosti, tak po stránce hardwarové optimalizace. První opravdu rozšířenou verzí byl Android 2.3.x (Gingerbread), který měl ve své době majoritní podíl v zařízeních s operačním systémem Android. Poté následovalo vydání verze Android 3.0 (Honeycomb), ten byl určen pouze pro tablety. Ovšem po uvedení verze Android 4.x, který byl určen jak pro tablety tak i pro mobilní telefony, byl Android 3.0 zapomenut. V současné době je nejrozšířenější verzí Android 4.x (Ice Cream Sandwich, Jelly Bean, KitKat), tyto verze jsou ve více než polovině zařízeních s operačním systémem Android. Ovšem pozvolně jsou vytlačovány Androidem 5.x (Lollipop) a nejnovější verzí Android 6.0 (Marshmallow), který je teprve na vzestupu. [8]

Version	Codename	API	Distribution
2.2	Froyo	8	0.1%
2.3.3 - 2.3.7	Gingerbread	10	2.6%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	2.3%
4.1.x	Jelly Bean	16	8.1%
4.2.x		17	11.0%
4.3		18	3.2%
4.4	KitKat	19	34.3%
5.0	Lollipop	21	16.9%
5.1		22	19.2%
6.0	Marshmallow	23	2.3%



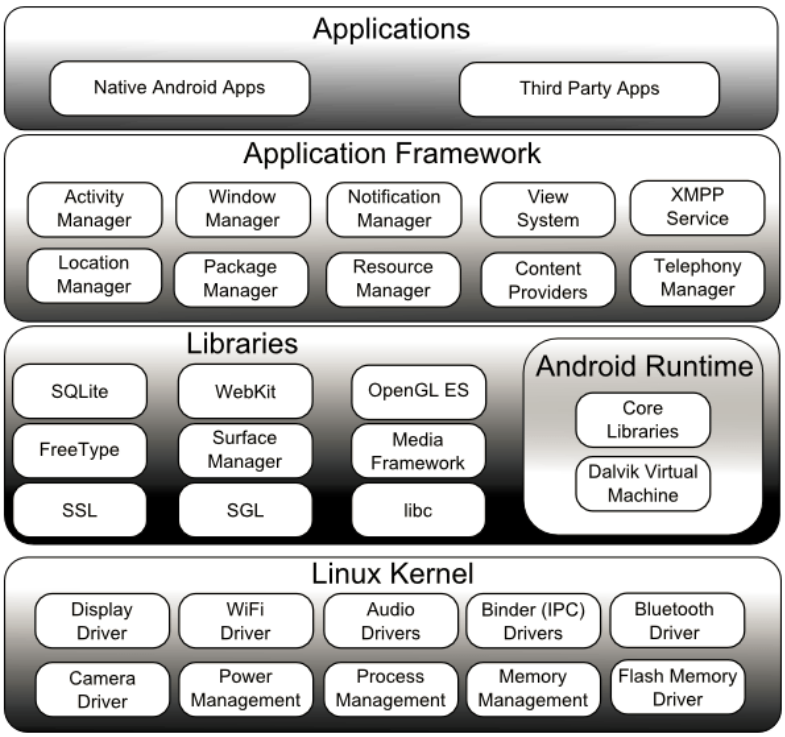
Obrázek č. 1 – Rozložení trhu (OS Android) [7]

Jak je vidět výše, v současné době je využíváno několik verzí operačního systému Android. Naneštěstí, kvůli odlišnostem verzí, není možné aplikovat stejný postup analýzy zařízení, pro každé zařízení. Navíc, protože je operační systém Android „otevřený“ operační systém, mohou si ho výrobci zařízení upravovat podle svých potřeb. V mnohých případech přidává výrobce svou grafickou nadstavbu operačního systému, například Samsung (TouchWiz), LG (Optimus UI), Sony (Sony UI), HTC (Sense), Huawei (Emotion UI), nebo Xiaomi (MIUI). [9]

Využívání těchto nadstaveb způsobuje, že zařízení se stejnou verzí operačního systému jsou odlišné u každého výrobce a není možné na ně aplikovat jeden pevně daný postup forenzního zkoumání. To značně znesnadňuje analýzu těchto zařízení a to i vývojářům komerčních forenzních nástrojů.

4.2. Architektura operačního systému Android

Architektura operačního systému Android se skládá z pěti základních vrstev, viz. Obrázek č. 2. Každá z těchto vrstev je důležitou součástí operačního systému a dohromady tvoří plně funkční celek.



Obrázek č. 2 – Architektura OS Android [10]

- **Linux kernel** – Operační systém Android je postaven na Linuxovém jádře. Linuxové jádro tvoří abstraktní vrstvu mezi hardwarem a softwarem zařízení. Ovšem, operační systém Android není další distribucí Linuxu, Architektura operačního systému Android je jiná než ostatní Linuxové distribuce, s nimi má společné pouze jádro systému, které je mírně upravené. [11] Díky Linuxovému jádru lze v určitých případech využít podobné techniky analýzy zařízení jako v případě operačního systému Linux, to je velice užitečná vlastnost.
- **Libraries** – Knihovny operačního systému Android jsou napsány v jazyce C, nebo C++. Knihovny umožňují zařízení práci s různými typy dat. Mezi důležité knihovny patří například Surface manager, který je využíván pro práci s displejem zařízení. Media Framework se využívá při nahrávání a přehrávání multimediálních záznamů v různých formátech. Dále, SQLite je databázový engine využívaný při práci s daty. WebKit je jádro internetového prohlížeče, které sloužící ke zpracování HTML kódu. Za zmínku stojí ještě OpenGL, která se využívá pro zpracování grafického obsahu. [11]
- **Android Runtime** – Android Runtime se skládá z Dalvik virtual machine (DVM) a Core Java Libraries. Každá aplikace využívá vlastní instanci DVM, které běží nezávisle na sobě. To zvyšuje bezpečnost, vylepšuje zprávu paměti a podporuje práci s vlákny. Od verze Android 5.0 je DVM nahrazen ART. ART také jako virtualizační nástroj, avšak má vylepšené vlastnosti oproti DVM. Core java libraries obsahují knihovny jazyka JAVA, který se využívá pro tvorbu aplikací pro operační systém Android. [11]
- **Application Framework** – Vrstva Aplikačních frameworků umožňuje aplikacím pracovat se základními funkcemi zařízení, dále umožňuje zpravovat životní cyklus aplikací, sdílení dat mezi aplikacemi, spravovat hlasové hovory, nebo například zpravovat polohu zařízení. [11]
- **Applications** – Nejvyšší vrstvou je vrstva Aplikace, do této vrstvy patří uživatelské aplikace vyvinuty pro operační systém Android. [11]

4.3. Architektura mobilních zařízení

Architektura hardware mobilních zařízení je velice podobná běžným počítačům. Ovšem je zde několik odlišností, které mají značný vliv na způsob provedení forenzní analýzy těchto zařízení.

Mobilní zařízení se skládají, podobně jako počítače, z procesorové jednotky, grafického jádra a paměťových modulů. Všechny tyto komponenty jsou pevně připájeny na základní desce zařízení. Mobilní zařízení navíc mají různé moduly, které rozšiřují jejich funkčnost. Mezi ně patří například WiFi modul, GSM modul, Modul pro připojení paměťových karet, GPS modul a spousty dalších. Dále jsou popsány základní součásti mobilních zařízení. [5]

- **Procesor** – Mobilní zařízení s operačním systémem Android využívají procesory s ARM architekturou. Tyto procesory jsou dostatečně výkonné pro tyto zařízení, mají malou spotřebu a nepotřebují aktivní chlazení. Proto jsou vhodné do těchto malých zařízení.
- **Grafický čip**
- **Paměťová úložiště** – V mobilním zařízení se nachází několik druhů pamětí. Tato problematika je velice důležitá pro forenzní analýzu, proto budou paměti zařízení detailněji popsány v následující podkapitole.
- **Slot pro SIM kartu**
- **GPS modul**
- **WiFi modul**
- **Fotoaparát**
- **Baterie**
- **Display**
- **USB interface**
- **Reproduktor/Mikrofon**
- **A další…**

4.3.1. Paměti zařízení

V mobilních zařízeních s operačním systémem Android se využívá několik druhů pamětí. Mobilní zařízení obsahují paměť RAM a vnitřní paměť zařízení. U většiny mobilních zařízení lze paměť rozšířit pomocí SD karet. Ovšem existují zařízení, které slot pro paměťovou kartu nemají.

4.3.1.1. Paměť RAM

Paměť RAM (Random Access Memory) je rychlá paměť sloužící pro dočasné uložení dat, která jsou přístupná rychleji než data z vnitřní paměti zařízení. Proto je tato paměť využívána operačním systémem a aplikacemi pro ukládání dat, které jsou nutné pro jejich běh, ale zároveň není třeba je trvale uchovat. Tato paměť je napěťově závislá, to znamená, že při odpojení napájení dojde nenávratně ke ztrátě dat. Velikost této paměti se pohybuje od 512 MB většinou až do 2 GB. [12]

4.3.1.2. Vnitřní paměť

Vnitřní paměť slouží pro trvalé uložení dat v mobilním zařízení. Aby bylo možné data uchovávat trvale, není tato paměť napěťově závislá. To znamená, že po odpojení napájení jsou data v paměti stále uchována. V této paměti jsou uložena zdrojová data operačního systému, aplikací nainstalovaných v mobilním zařízení a uživatelských dat. [12] V některých zařízeních se část této paměti tváří jako paměťová karta, na kterou si může uživatel ukládat jakákoliv data. Z pohledu forenzní analýzy je tato část zařízení nejzajímavější, protože je z ní možné získat velké množství dat.

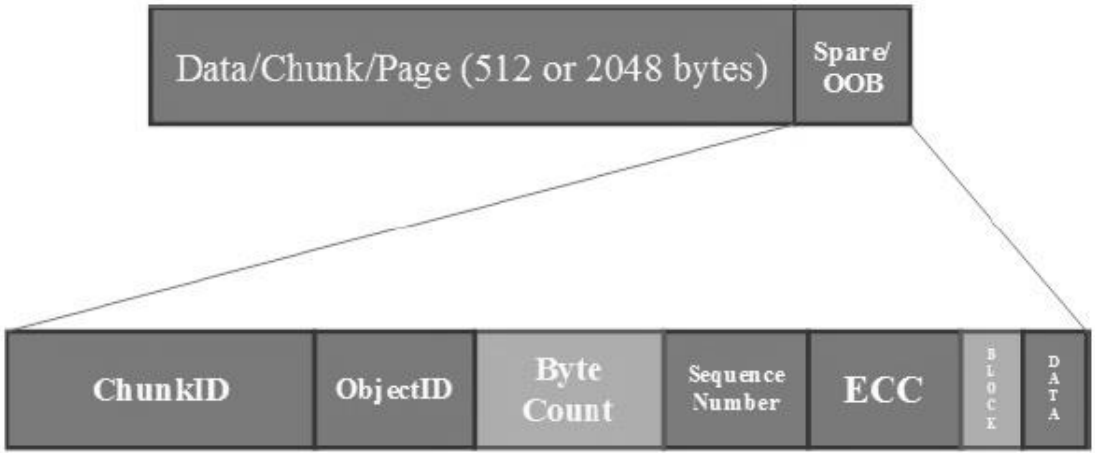
Operační systém Android prošel za dobu své existence množstvím úprav. I v případě vnitřní paměti došlo od jeho vydání k velkým změnám, proto je třeba odlišit dvě možnosti. Dříve byl využíván souborový systém YAFFS2, ovšem s příchodem více jádrových procesorů se začal využívat souborový systém EXT4. Tato změna se začala objevovat u verze Android 2.3 (Gingerbread). [13] V současné době už je mobilní zařízení využívající souborový systém YAFFS2 spíše vzácností, avšak stále je třeba s tímto souborovým systémem počítat.

4.3.1.2.1 YAFFS2

Dnes už skoro nepoužívaný souborový systém YAFFS2 byl vyvinut pro NAND Flash paměti, které jsou využívány v mobilních zařízeních. Původní verze souborového systému YAFFS1 se od YAFFS 2 lišila hlavně velikostí Chunku (512 B místo 2048 B).

Paměť zařízení je rozdělená do bloků, kde každý blok tvoří 64 tzv. Chunků. Do Chunku se ukládají požadovaná data, v případě YAFFS2 má Chunk velikost 2048 B. Ke každému Chunku náleží Out Of Band (OOB) oblast o velikosti 64 B. OOB oblast obsahuje metadata o datech uložených v Chunku. [15]

Při ukládání dat do paměti se data ukládají do jednotlivých Chunků nezávisle na ostatních. Avšak, jsou-li data mazány, vždy dojde ke smazání celého bloku, mazání dat po jednotlivých Chunkách není možné. [15]



Obrázek č. 3 – Schéma YAFFS2 [14]

4.3.1.2.2. EXT4

S příchodem více jádrových procesorů začal být souborový systém YAFFS2 nedostačující. Proto byl nahrazen souborovým systémem EXT4, ten umožňuje práci s pamětí více vlákny najednou, což umožnilo velký nárůst výkonu mobilních zařízení.

EXT4 je souborový systém vyvinutý pro operační systém Linux jako další vývoj Linuxových souborových systémů EXT2 a EXT3. EXT4 má spoustu zajímavých

vlastností, ovšem pro mobilní zařízení zůstává nejhlavnější možnost práce s více vlákny najednou. Díky tomu, že operační systém Android využívá Linuxové jádro, nebylo potřeba výrazně měnit datovou strukturu operačního systému. [13]

Vítanou vlastností ve vztahu k forenzní analýze je podpora souborového sytému EXT4 u většiny běžných forenzních nástrojů.

4.3.1.3. Externí paměť

Většina mobilních zařízení s operačním systémem Android je vybavena slotem pro připojení paměťové microSD karty. MicroSD karta je napěťově nezávislá paměť, takže i po odpojení napájecího napětí nedojde ke ztrátě dat uložených v paměti. Tyto karty obsahují NAND Flash chip pro ukládání dat.[16] MicroSD karty obvykle využívají souborový systém VFAT (FAT32), který je plně kompatibilní s operačním systémem Windows. To umožňuje uživatelům kartu vyjmout ze zařízení a připojit ji ke svému počítači, na kterých má většina uživatelů nainstalovaný operační systém Windows. Ovšem, lze se setkat i s případy, kdy microSD karta využívá souborový systém EXT3, nebo EXT4.

MicroSD karta je v zařízení využívána pro ukládání všech druhů uživatelských dat. Může obsahovat různé dokumenty, fotografie, videa, či zvukové stopy. Dále se na paměťovou kartu mohou ukládat data některých aplikací. Maximální velikost microSD karet je 32 GB, díky tomu může být karta velkým zdrojem dat.

4.4. Bootovací proces

Bootovací proces zařízení s operačním systémem Android je odlišný od bootovácího procesu běžných počítačů. To je dáno odlišnou architekturou ARM procesorů od procesorů x86, které využívají pro bootování operačního systému BIOS, nebo UEFI. Bootovací sekvence zařízení s operačním systémem Android je následující [17]:

1. **Power ON** – Po zapnutí zařízení dojde k načtení boot ROM. Boot ROM je malý kousek kódu, který je obsažen v procesoru zařízení. Tento kód nahraje data Boot loaderu do paměti RAM a poté jej spustí.

2. **Boot loader** – Boot loader je program oddělený od Linuxového jádra, který umožňuje spuštění Linuxového jádra. Boot loader nejdříve detekuje paměť RAM. Poté nastaví vše potřebné. Poté dojde k nabootování Linuxového jádra, kterému je Boot loader schopen předat různé parametry.
3. **Linuxové jádro** – Linuxové jádro nastavuje vše potřebné pro běh systému. Inicializuje kontroler přerušení, nastavuje ochranu paměti, cache a další. Díky tomu je možné začít využívat virtuální paměť. Poté dojde ke spuštění initial user space proces.
4. **Init proces** – Init proces je mateřský proces všech systémových procesů. Každý další proces je spuštěn tímto procesem, procesem jím spuštěným.
5. **Zygote a Dalvik** – Zygote je spuštěn Init procesem a má za úkol spuštění Dalvik Virtual Machine.
6. **System server** – System server je první Java komponenta, která je v systému spuštěna. Jejím úkolem je spustit služby v zařízení jako je například telephony manager, nebo bluetooth.
7. **Dokončení bootování** – Když System server spustí všechny služby a bootování systému je dokončeno, je pomocí broadcastu vyslán signál ACTOIN_BOOT_COMPLETED. To značí, že je bootování zařízení kompletní.

4.5. Data v mobilních zařízeních

V mobilních zařízeních se nachází velké množství dat. Existují data, která jsou typická pro všechny mobilní zařízení a jsou data, která jsou v zařízení díky uživatelem nainstalovanými aplikacemi. Tyto data mohou prozradit velké množství informací o uživateli mobilního zařízení.

4.5.1. Běžná data mobilních zařízení

Mezi běžná data obsažená v mobilních zařízeních patří data, která jsou běžná pro všechny mobilní zařízení. Tyto data jsou tvořeny aplikacemi, které tvoří základní

funkčnost zařízení. Mezi tyto data patří:

- Informace o zařízení – Výrobce, Model, Sériové číslo a další…
- SMS a MMS zprávy
- Seznam kontaktů
- Protokoly – Výpis volání a zpráv
- Záznamy z kalendáře
- Fotky a videa z fotoaparátu
- Další doplňkové informace o používání zařízení

4.5.2. Doplňkové aplikace

Mezi tyto aplikace se řadí ty, které nejsou nezbytné pro funkčnost mobilního zařízení, avšak jeho možnosti značně rozšiřují. Typů takovýchto aplikací je obrovské množství a aplikace jsou snadno dostupné na Google Play (internetový obchod s aplikacemi pro operační systém Android). Ovšem z pohledu forenzní analýzy mohou obsahovat užitečné informace komunikační aplikace, aplikace pracující se zeměpisnou polohou, nebo webové prohlížeče. Mezi takovéto nejpoužívanější aplikace patří následující aplikace. [18]

- **Facebook** – V současnosti nejvyužívanější sociální síť, podle Google Play si tuto aplikaci stáhlo přes miliardu uživatelů. Tato aplikace může ukrývat spoustu informací o činnostech uživatele mobilního zařízení.
- **Messenger** – Doplňková komunikační aplikace k aplikaci Facebook, tato aplikace má rovněž přes miliardu stažení a v současné době je nejvyužívanější komunikační aplikací. Aplikace obsahuje data z chatu a údaje o kontaktech
- **ICQ** – Aplikace ICQ je dnes již zřídka využívanou komunikační aplikací, kterou využívá pouze malé množství uživatelů. Avšak, dříve byla tato aplikace velice rozšířená a je možné se s ní setkat hlavně u starších mobilních zařízení. Proto je nutné brát tuto aplikaci v potaz.

- **Hangouts** – Komunikační aplikace od firmy Google. Tato aplikace není oproti ostatním tolik využívána. Avšak i ona může obsahovat záznamy o komunikaci uživatele mobilního zařízení.
- **Emailový klient** – V mobilních zařízeních jsou často využívány aplikace pro zprávu Emailové komunikace. Existuje více Emailových klientů, mezi nejpoužívanější patří:
    - **Gmail**
    - **E-mail** – Základní Emailový klient operačního systému Android
- **Webový prohlížeč** – Data webových prohlížečů obsahují historii prohlížení webových stránek a také mohou obsahovat záznamy o poloze zařízení. Mezi nejpoužívanější webové prohlížeče patří:
    - **Internet** – Základní webový prohlížeč operačního systému Android
    - **Opera**
    - **Chrome**
- **Mapy** – Aplikace sloužící k navigaci pomocí map od společnosti Google. Tato aplikace zaznamenává polohu zařízení.

5. Analýza zařízení

Forenzní analýza mobilních zařízení není úplně snadná činnost. Při jejím provádění může dojít k poškození dat, či dokonce ke zničení mobilního zařízení. Proto je nutné provádět tuto analýzu s velkou opatrností a pečlivostí. Následující způsob provedení forenzní analýzy ukazuje, jak je možné provést analýzu zařízení s co nejmenšími riziky na ztrátu dat, či zničení zařízení.

Pro potřeby forenzní analýzy je třeba mít připravenou pracovní stanici, pomocí které bude analýza mobilního zařízení provedena. Jako pracovní stanice slouží počítač s operačním systémem Windows. Ovšem obdobně lze použít pracovní stanici s operačním systémem Linux. Pracovní stanice s operačním systémem Windows je vhodnější, protože pro analýzu mobilních zařízení je nutné využít různé nástroje, které ne vždy podporují operační systém Linux.

Tento postup byl testován na několika zařízení s různými verzemi operačního systému Android. Tyto zařízení jsou: Sony Ericsson Xperia Mini Pro (Android 2.3), LG Optimus L4 II E440 (Android 4.1) a Samsung Galaxy A3 (Android 5.0.2).

5.1. Příprava mobilního zařízení

Na začátku analýzy je třeba zařízení „odříznout“ od okolního světa. Je to z důvodu, aby mobilní zařízení nebylo připojené k mobilní síti, aby nedošlo k interakci zařízení s okolím například příchozí SMS zprávou, nebo příchozím hovorem. Navíc existují aplikace, které jsou schopné na dálku mobilní zařízení zablokovat. Zde je možné zvolit dva různé způsoby jak mobilní zařízení izolovat od okolí. [19]

První možností pro odstínění mobilního zařízení je využití tzv. Faraday bag. Mobilní zařízení se vloží do speciálního pytle, které znemožní kontakt zařízení s okolím pomocí bezdrátových technologií, jako jsou 2G, 3G, 4G, WiFi, Bluetooth, GPS, nebo RFID. Odstínění zařízení pomocí Faraday bag funguje na principu Faradayovi klece. [20]

Druhou možností je vytvoření duplicitní SIM karty, která se v zařízení tváří stejně jako originální SIM karta, avšak mobilní zařízení ses s ní nepřipojí k síti. Díky využití duplicitní SIM karty odpadá problém se znalostí PINu SIM karty.

Krajní možností je provedení analýzy na zařízení s jinou SIM kartou, nebo úplně bez SIM karty. Ovšem, tato možnost může ovlivnit výsledky analýzy zařízení.

5.2. Práce s mobilním zařízením

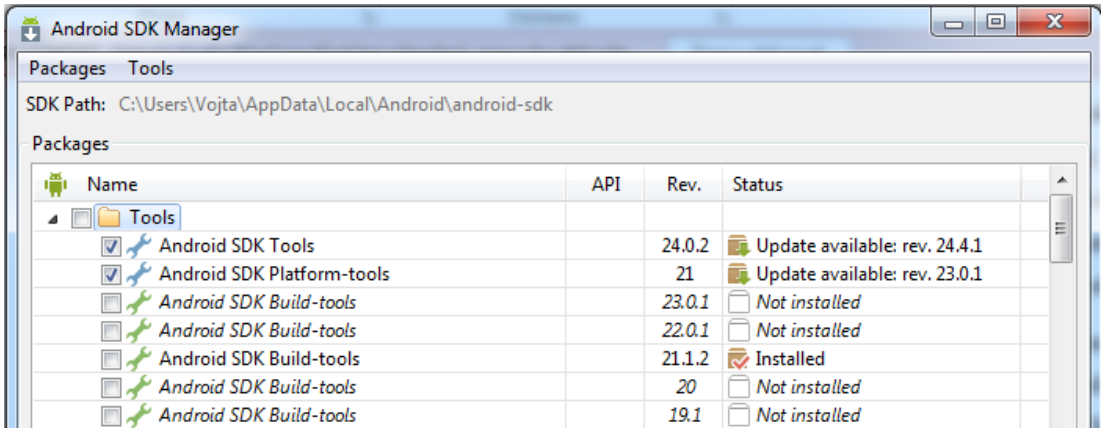
Aby bylo možné pracovat s mobilním zařízením, je nutné ho připojit k pracovní stanici. Toto propojení je zrealizováno za pomocí rozhraní USB, které se využívá pro nabíjení a sdílení dat mezi mobilním zařízením a počítačem. Ovšem po připojení mobilního zařízení k pracovní stanici pomocí přes USB je možné pouze pracovat s daty uloženými na paměťově kartě a v některých případech ve velmi omezené míře s daty uloženými ve vnitřní paměti, která je vyhrazena pro data uživatele. Aby bylo možné s mobilním zařízením plnohodnotně pracovat, je nutné využít Android Debug Bridge (ADB).

ADB je univerzální nástroj, který umožňuje komunikovat s mobilním zařízením přes pracovní stanici s využitím příkazové řádky. ADB funguje na principu Klient/Server a je tvořena třemi komponentami. První komponentou je **Klient**, Klient běží na pracovní stanici a slouží pro interakci s mobilním zařízením pomocí příkazové řádky. Jako klient slouží například Příkazový řádek operačního systému Windows. Druhou komponentou je **Deamon**, Deamon běží v mobilním zařízení jako proces na pozadí. Deamon v mobilním zařízení umožňuje vykonat příkazy zadané v Klientu na pracovní stanici. Poslední komponentou ADB je **Server**, Server pracuje jako proces na pozadí na pracovní stanici. Jeho úkolem je řízení komunikace mezi Klientem v pracovní stanici a Deamonem v mobilním zařízení. [21] Ovšem, aby bylo možné ADB využívat, je nutné správně nastavit pracovní stanici i mobilní zařízení.

5.2.1. Nastavení pracovní stanice

Aby bylo možné využívat ADB, je nutné na pracovní stanici připravit následující:

1. Instalace JDK – JDK (Java Development Kit) je soubor nástrojů pro vývoj aplikací v programovacím jazyce JAVA od firmy Oracle. Instalační soubor JDK lze stáhnout přímo z webových stránek společnosti Oracle, na kterých se nachází vždy aktuální verze těchto nástrojů. [22] Nainstalování JDK je nezbytné pro provedení následujícího kroku.
2. Instalace Android SDK – Dalším nezbytným krokem je instalace Android SDK, jehož součástí je požadovaný ADB. Aktuální instalační balíček Android SDK lze stáhnout na webových stránkách Android Developers. [23]
3. Instalace Android SDK Platform-tools – Po úspěšné instalaci Android SDK je nutné nainstalovat Platform-tools. Pro tuto instalaci je nutné spustit aplikaci SDK Manager, ve které je nutné zaškrtnout položku Android SDK Platform-tools viz Obrázek č. 4 a po té tento balíček nainstalovat.



Obrázek č. 4 – SDK Manager

4. Nastavení proměnné PATH – Aby bylo možné používat v příkazovém řádku operačního systému Windows příkazy pro operační systém Android, je nutné vložit cestu k Android SDK Platform-tools do proměnné PATH. Nastavení této proměnné lze najít následovně. Pravým

tlačítkem myši kliknout na **Počítač** a zvolit možnost **Vlastnosti**. Po zobrazení okna zvolit položku **Upřesnit nastavení systému**, to způsobí zobrazení dalšího okna. V tomto okně je nutné zvolit záložku **Upřesnit,** ve které se nachází položka **Proměnné prostředí**. Poté dojde k otevření dalšího okna, které obsahuje pole proměnných s názvem **Systémové proměnné** a v tomto poli se nachází potřebná proměnná **Path**. Do hodnoty této proměnné je nutné přidat cestu k Android SDK Platform-tools. Tuto cestu lze zjistit v aplikaci SDK Manager pod položkou SDK Path viz Obrázek č. 4. Do hodnoty proměnné Path se poté přidá cesta v následujícím tvaru: **;cesta_z_SDK_Path\Platform-tools**. Středník na začátku cesty je povinný!

5. Nakonec je nutné mít nainstalované ovladače pro mobilní zařízení, ty lze získat z webových stránek výrobce zařízení. Pokud by byly nainstalovány špatné ovladače pro mobilní zařízení, mohlo by to způsobit, že pracovní stanice nebude schopna detekovat připojené mobilní zařízení přes rozhraní USB.

5.2.2 Nastavení mobilního zařízení

Nastavení mobilního zařízení je značně jednodušší. Stačí na něm nastavit pouze jeden parametr a to povolit Ladění USB. Díky tomu lze poté pracovat se zařízením pomocí příkazového řádku v operačním systému Windows přes ADB. U různých mobilních zařízení může být cesta k této položce odlišná, to je způsobeno tím, že si každý výrobce zařízení upravuje operační systém Android podle svého. Ovšem umístění těchto položek je ve všech případech velice podobné.

Dříve byla položka Ladění USB umístěna v **Nastavení** zařízení, zde se zvolila položka **Aplikace** a v ní možnost **Vývoj**. Zde se již nachází možnost povolení Ladění USB. Avšak, od verze Android 4.2 je tato položka v továrním nastavení mobilního zařízení skryta. Pro její zobrazení je opět nutné jít do **Nastavení** zařízení, kde se nachází položka **O zařízení.** V ní sedmkrát poklepat na položku **Číslo sestavení.** Poté se v **Nastavení** zařízení objeví nová položka **Vývojářské možnosti**, ve které už se nachází položka pro povolení Ladění USB. [24]

Ovšem zde je možné narazit na největší komplikaci, která může znemožnit provedení forenzní analýzy mobilního zařízení. Tou komplikací je zámek obrazovky, kvůli kterému nemusí být možné povolit Ladění USB.

5.3. Zámek obrazovky

Zámek obrazovky může být největší výzvou při analýze mobilního zařízení. Je to proto, že jeho překonání může být velice obtížné, v některých případech dokonce nemožné.

Existují tři běžně používané typy zámku obrazovky. Prvním z nich je odemčení obrazovky pomocí tahu prstem kdekoliv po displeji mobilního zařízení, tento zámek obrazovky je defaultně nastaven u všech nových mobilních zařízení s operačním systémem Android. Tento zámek obrazovky je v ohledu k překonávání nejlepší, protože pro jeho překonání není potřeba žádné speciální znalosti ani nástroje. Stačí pouze přejet prstem kdekoliv po obrazovce a mobilní zařízení je odemčeno.

S dalšími dvěma typy zámků už je situace složitější. Jedním z nich je odemknutí obrazovky pomocí speciálního gesta, druhým je odemknutí obrazovky pomocí kódu. Neexistuje univerzální postup pro všechny mobilní zařízení, jak obejít zámek obrazovky, proto je vždy nutné najít správný postup pro konkrétní mobilní zařízení. Proto jsou zde popsány pouze principy prolomení zámku obrazovky

5.3.1 Prolomení zámku obrazovky přes ADB

K tomu, aby bylo možné prolomit zámek obrazovky přes ADB, je nutné, aby bylo v mobilním zařízení povoleno Ladění USB a možnost získání ROOT oprávnění. ROOT oprávnění bude popsáno detailněji později. V této možnosti dojde ke smazání souborů s nastavením zámku obrazovky. [25]

Mobilní zařízení je nutné připojit k pracovní stanici pomocí USB kabelu a na pracovní stanici otevřít příkazový řádek. Nyní stačí zadat následující příkazy:

```
adb shell
su
rm /data/system/locksettings.db
rm /data/system/locksettings.db-wal
rm /data/system/locksettings.db-shm
```

Obrázek č. 5 – ADB – prolomení zámku obrazovky

První příkaz umožňuje zadávání příkazů pro mobilní zařízení, druhý příkaz umožní využít ROOT oprávnění a zbylé tři příkazy odstraní soubory s nastavením zámku obrazovky. Nyní stačí pouze restartovat zařízení a zámek obrazovky se změní na defaultní zámek obrazovky, který je pouze náhodné přejetí prstem po displeji mobilního zařízení.

5.3.2 Prolomení zámku obrazovky pomocí Recovery menu

Další možností jak prolomit zámek obrazovky je využití tzv. Recovery menu. Do Recovery menu je možné se dostat díky podržení kombinace tlačítek při zapínání mobilního zařízení. Tato kombinace není stejná pro všechny zařízení, ovšem většinou jde o současné stlačení tlačítka pro zapnutí zařízení a tlačítka na úpravu hlasitosti. [26] Ovšem, u všech mobilních zařízení není Recovery menu přístupné. Proto tato možnost nefunguje u všech mobilních zařízení.

5.3.2.1. Tovární nastavení

První možností, jak prolomit zámek obrazovky je vrácení mobilního zařízení do továrního nastavení. Pro tuto možnost existuje v Recovery menu položka Tovární nastavení, nebo Smazat uživatelská data. Ovšem, při této metodě dojde ke smazání dat v zařízení, proto tuto metodu nelze doporučit. Ovšem i při smazání uživatelských dat, je možné data následně získat jako smazaná data. [26]

5.3.2.1. Smazání souborů zámku obrazovky

Pomocí Recovery menu je možné provést ROOT zařízení a poté smazat soubory s nastavením zámku obrazovky stejným způsobem jako při prolomení zámku obrazovky pomocí ADB.

Díky těmto metodám lze prolomit zámek obrazovky mobilního zařízení, ovšem nelze je aplikovat na všechna mobilní zařízení. Proto u některých zařízení není možné prolomit zámek obrazovky a není díky tomu možné zapnout režim Ladění USB. Kvůli tomu může být u některých mobilních zařízení nemožné provedení forenzní analýzy podle tohoto postupu.

5.4. Získání dat pomocí ADB

Nyní uvažujme možnost, že máme mobilní zařízení, které má povolené Ladění USB. V tuto chvíli můžeme začít získávat data ze zařízení pomocí ADB. ADB je mocný nástroj, díky kterému lze získat informace o mobilním zařízení. Pro jeho využití je nutné připojit mobilní zařízení k pracovní stanici pomocí USB kabelu a na pracovní stanici spustit příkazový řádek. Nyní lze využít několik příkazů, pomocí kterých lze získat data z mobilního zařízení.

```
adb pull [zdrojový adresář] [cílový adresář]
```

Tento příkaz umožní zkopírování dat z mobilního zařízení do pracovní stanice. Jako zdrojový adresář je vhodné zvolit ‘/‘, to označuje kořenový adresář mobilního zařízení. Jako cílový adresář je zvolen adresář v pracovní stanici, do kterého budou data z mobilního zařízení uložena. Ovšem, ve většině adresářů v mobilním zařízení dojde k odepření přístupu, proto je množství dat získaného z mobilního zařízení velice omezené. Jediná kompletní data, která jsou ze zařízení získána, jsou data uložená na paměťové kartě.

Provedením tohoto příkazu sice není možné získat mnoho dat z mobilního zařízení, ovšem tyto data mohou být užitečná v případě zablokování zařízení při následné analýze, tyto data slouží jako bezpečnostní záloha.

5.5. Analýza paměťové karty

Analýzu paměťové karty je vhodné provézt mimo zkoumané mobilní zařízení. Je to proto, že provedení analýzy mimo mobilní zařízení umožní důkladnější analýzu a tím i možnost získání více dat z paměťové karty.

Nejprve je nutné kartu vyjmout z mobilního zařízení. Zde je možné zvolit dva odlišné způsoby. Jedním z nich je v nastavení zařízení zvolit možnost **Odpojit SD kartu** a poté kartu vyjmout ze zařízení, nebo kartu vyjmout ze zařízení přímo bez předchozího odpojení. Vhodné je zvolit druhou možnost. A to proto, že paměťovou kartu využívají různé aplikace, které si na ni mohou zapisovat různá dočasná data. Při odpojení paměťové karty mohou být tyto data odstraněny mateřskými aplikacemi.

5.5.1 Obraz paměťové karty

Nyní, když je karta vyjmuta je vhodné vytvořit její obraz. Obraz není nic jiného než bitová kopie celé paměťové karty. Obraz se vytváří i z nealokovaných částí paměti. Obraz paměti se využívá k forenzní analýze proto, že při následné analýze nemůže dojít k žádnému poškození paměťového média, ani dat na tomto médiu.

K vytvoření obrazu je poté využita pracovní stanice. Paměťová karta je připojena pomocí čtečky paměťových karet. Zde jsou dvě možnosti jak obraz paměťové karty vytvořit. První možností je pracovní stanice s operačním systémem Windows. V tomto systému je nutné využít aplikaci určenou pro vytvoření obrazu paměti, tou je například FTK Imager, ve kterém lze obraz vytvořit pomocí několika kliknutí za pár minut. Druhou možností je pracovní stanice s operačním systémem Linux v ní lze snadno vytvořit obraz paměti v Terminálu pomocí následujících příkazů: [27]

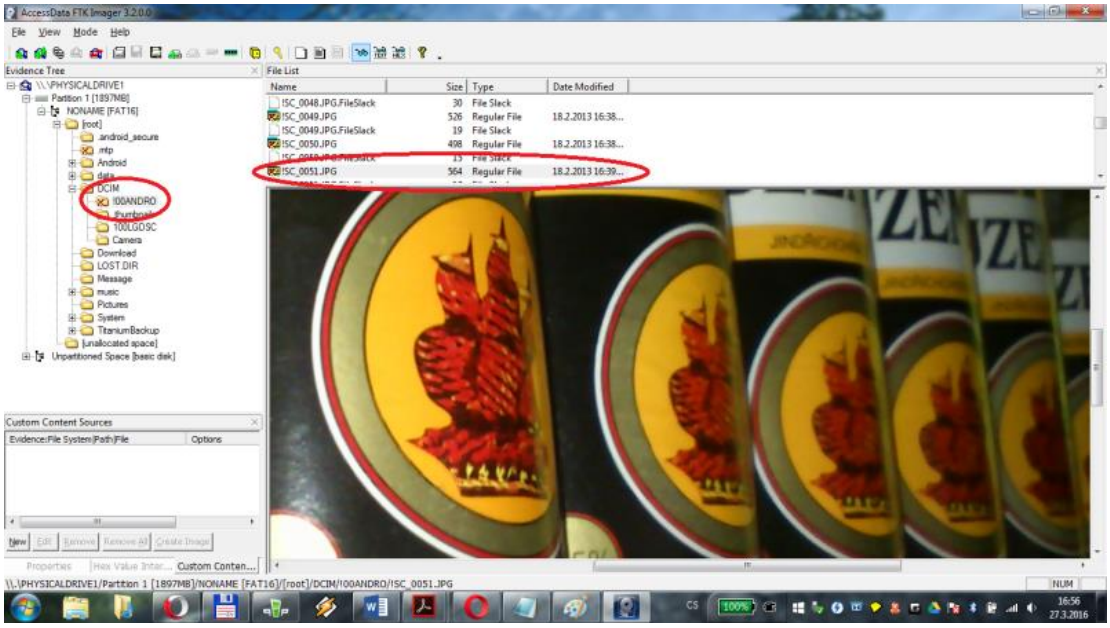
```
fdisk -l
...zde fdisk vypíše připojená paměťová média...
dd if=[zdroj] of=[cíl] conv=noerror
```

Obrázek č. 6 – Obraz karty – dd

Příkaz **fdisk** vypíše všechna paměťová média připojená k pracovní stanici, mezi nimi se nachází i cesta ke zkoumané paměťové kartě. Ta se poté využije jako zdrojový parametr v následném příkazu **dd**, který vytvoří požadovaný obraz. Parametr cíl určuje složku v pracovní stanici, do které bude výsledný obraz uložen. Následný přepínač conv umožňuje přidat další parametry, které ovlivní vytvoření obrazu. V tomto případě byl použit parametr noerror, který způsobuje, že když by byla na zdrojovém médiu chybná oblast, došlo by k jejímu nahrazení logickými nulami.

5.5.2 Analýza obrazu

Paměťové karty obvykle využívají souborový systém VFAT, tento souborový systém je široce podporovaný většinou forenzních nástrojů. Proto je nejlepší možností pro analýzu obrazu využít právě jeden z těchto nástrojů. V tomto případě byl využit nástroj FTK Imager, který je zdarma a umožňuje procházet adresářovou strukturu obrazu totožnou s paměťovou kartou. Navíc v adresářové struktuře zobrazuje smazané složky a soubory.



Obrázek č. 7 – FTK Imager

Na obrázku č. 7 je ukázáno prostředí nástroje FTK Imager. V levém sloupci je zobrazena adresářová struktura paměťové karty, ve které je možné vidět i smazaný adresář !00ANDRO. V pravé horní části je zobrazen obsah smazaného adresáře,

který je plný smazaných obrázků. V pravé dolní části jsou již zobrazené smazané soubory. V tomto případě je to fotka smazaná z paměťové karty. Názvy smazaných souborů a složek vždy začínají vykřičníkem.

Z paměťové karty je možné získat více než jen data uživatelů, jako jsou obrázky, fotky, audio a video záznamy. Díky tomu že paměťovou kartu mohou využívat aplikace pro ukládání svých dat. Může paměťová karta obsahovat data o činnosti těchto aplikací a například záznamy polohy mobilního zařízení. Navíc jsou na kartu často ukládány zálohy dat z mobilního zařízení, jakými jsou například zálohy kontaktů.

5.6. Uživatelská práva

Dalším omezením, které komplikuje analýzu mobilního zařízení, jsou oprávnění v operačním systému Android. To je způsobeno tím, že mobilní zařízení jsou běžně prodávána s omezenými uživatelskými právy. Pro běžné používání mobilního zařízení to nepředstavuje žádný problém a uživatele toto omezení uživatelských práv nikterak neomezuje. Ovšem, ve vztahu k analýze zařízení, tyto omezená práva přináší omezení, která znemožňují vykonat plnohodnotnou analýzu mobilního zařízení, protože neumožňují přístup do všech částí paměti zařízení, ani vytvoření jejího obrazu, ze kterého by bylo možné získat smazaná data. Ovšem i toto omezení lze obejít.

Díky tomu, že operační systém Android běží na jádře operačního systému Linux, jsou zde oprávnění řešena stejným způsobem. Proto i v operačním systému android existují neomezená uživatelská práva, která se označují jako ROOT oprávnění. Ovšem, získání těchto oprávnění není zcela jednoduché a neexistuje univerzální postup, který by byl funkční pro všechny typy mobilních zařízení. Zde jsou popsány možnosti, pomocí kterých je možné ROOT práva získat. [28]

5.6.1. Aplikace pro ROOT mobilních zařízení

Pro získání ROOT oprávnění existuje několik aplikací, které umožní tzv. ROOT zařízení. Získání ROOT oprávnění pomocí těchto aplikací je velice snadné, stačí aplikaci nainstalovat na pracovní stanici a připojit k ní mobilní zařízení pomocí USB

rozhraní. Po té stačí v aplikaci zvolit zařízení, u kterého je požadováno zpřístupnění ROOT práv a zmáčknout tlačítko pro začátek procesu. Ve většině případů je nutná interakce s mobilním zařízením, většinou jde pouze o povolení zahájení procesu na mobilním zařízení. Celý proces získání ROOT oprávnění trvá pouze několik minut, je jednoduchý a nehrozí skoro žádné riziko poškození zařízení a dat v něm.

Ovšem, ani tyto aplikace nejsou zcela univerzální a nejsou schopna zpřístupnit ROOT oprávnění ve všech typech mobilních zařízení. Proto je nutné zvolit aplikaci podporující zkoumané mobilní zařízení. Z dostupných aplikací se osvědčil například Unlock Root, který je vhodný zejména pro mobilní zařízení se starší verzí operačního systému Android. Pro novější mobilní zařízení byly vhodné aplikace iROOT, nebo SRS Root. Podobných aplikací existuje více, a každá z nich podporuje různá mobilní zařízení, proto je nutné zvolit správnou aplikaci podle typu zkoumaného mobilního zařízení.

Všechny tyto aplikace fungují na stejném principu, nejdříve připojí oddíl paměti **System** jako s možností do něj zapisovat, běžně je tento oddíl určen pouze ke čtení, a zapíše do něj tzv. **su binary, Superuser.apk** a **busybox.** Pak připojí oddíl System opět pouze ke čtení. Su binary v systému způsobí nastavení uid (user-id) na 0, nula značí ROOT oprávnění. Superuser.apk je instalační balík aplikace pro zprávu oprávnění mobilního zařízení, která se objeví mezi ostatními aplikacemi v mobilním zařízení. Busybox doplňuje do mobilního zařízení doplňující nástroje, díky kterým je možné využívat více příkazů v terminálu zařízení. Uid bylo pro správu oprávnění využíváno do verze Android 4.3, ve vyšších verzích je využíván deamonsu, který funguje na podobném principu. [29]

5.6.2. Ostatní způsoby pro získání ROOT oprávnění

V případě, že žádná z aplikací nebude schopna provést ROOT zařízení, je nutné zvolit alternativní způsob pro získání potřebných oprávnění. Tento způsob je odlišný u každého mobilního zařízení, proto je nutné zvolit ho přímo podle typu zkoumaného mobilního zařízení. Jedním z nejlepších zdrojů pro nalezení správného postupu je fórum komunity XDA Developers, kde se nachází velké množství rad jak získat ROOT oprávnění. Ovšem, zde je nutné zvolit správný způsob, pro určité zařízení

může existovat více možností jak získat oprávnění ROOT, je dobré zkontrolovat komentáře uživatelů, kteří určitý způsob vyzkoušeli, protože v některých případech může dojít ke ztrátě dat v mobilním zařízení, nebo dokonce k jeho zablokování. [30]

5.6.3. Návrat změn v mobilním zařízení

Po dokončení analýzy mobilního zařízení je vždy vhodné vrátit zařízení do stavu, ve kterém bylo před jejím započetím. Proto je dobré zvolit metodu získání ROOT oprávnění i podle toho, jak je možné tyto změny vrátit.

Při použití některé z aplikací pro získání ROOT oprávnění, je návrat zařízení do původního stavu ve většině případů jednoduchý. Aplikace totiž umožňují odebrání ROOT oprávnění. To znamená, že změny, které aplikace udělá při získávání ROOT oprávnění, dokáže poté aplikace vrátit zpět.

V případě zvolení alternativního způsobu získání ROOT oprávnění může být situace složitější. V některých případech může být obtížné, někdy až nemožné vrátit zařízení do původního stavu.

5.7. Získání dat z mobilního zařízení

Když je mobilní zařízení připravené, je možné z něj začít získávat data. Nejlepší způsob jak získat kompletní data z vnitřní paměti mobilního zařízení je vytvořit její bitovou kopii tzv. obraz paměti. Před začátkem vytváření obrazu paměti je nutné vložit do zařízení paměťovou kartu, na kterou se výsledný obraz paměti uloží. Není vhodné pro to použít původní paměťovou kartu, protože by mohlo dojít ke zničení dat na ní uložených. Z toho důvodu je vhodné k tomuto účelu použít vlastní paměťovou kartu.

Nyní je možné připojit mobilní zařízení přes USB rozhraní k pracovní stanici a s využitím ADB může začít proces získání obrazu paměti. Protože dříve operační systém Android využíval jiný souborový systém, než v současné době. Je nutné odlišit tyto dvě možnosti. Pomocí následujících příkazů lze zjistit, jaký souborový systém je v mobilním zařízení využit.

```
adb shell
su

mount
```

Obrázek č. 8 – Zjištění souborového systému

Pomocí příkazu **adb shell** dojde k připojení se k terminálu mobilního zařízení, díky tomu je možné pracovat s terminálem. Příkazem **su** dojde k přidělení ROOT oprávnění, která jsou nezbytná pro vytvoření obrazu paměti. Přidělení ROOT oprávnění lze rozeznat díky tomu, že dojde ke změně symbolu na začátku příkazové řádky z **$** na **#**. Příkaz **mount** zobrazí, která paměťová média jsou připojeny v operačním systému i s jejich použitým souborovým systémem. Část výsledku příkazu je zobrazen na Obrázku č. 9.

```
...
/dev/block/bootdevice/by-name/modem on /firmware-modem type vfat
(ro,context=u:object_r:firmware_file:s0,relatime,uid=1000,gid=1000,fmask=0337,
1,shortname=lower,errors=remount-ro)
/dev/block/bootdevice/by-name/system on /system type ext4 (ro,seclabel,relatim
/dev/block/bootdevice/by-name/userdata on /data type ext4
(rw,seclabel,nosuid,nodev,noatime,discard,journal_checksum,journal_async_commi
/dev/block/bootdevice/by-name/cache on /cache type ext4
(rw,seclabel,nosuid,nodev,noatime,discard,journal_checksum,journal_async_commi
/dev/block/bootdevice/by-name/persist on /persist type ext4
(rw,seclabel,nosuid,nodev,noatime,discard,journal_checksum,journal_async_commi
/dev/block/bootdevice/by-name/efs on /efs type ext4
(rw,seclabel,nosuid,nodev,noatime,discard,journal_checksum,journal_async_commi
...
```

Obrázek č. 9 – Výpis příkazu mount

Jak je možné vidět v části výpisu příkazu mount na Obrázku č.9 pořízeného ze zařízení Samsung Galaxy A3, opakuje se zde položka **type ext4**. To znamená, že v mobilním zařízení je používán souborový systém EXT4. Druhou možností by bylo, zobrazení **type yaffs2**, to by znamenalo využití souborového systému YAFFS2. Podle typu použitého souborového systému je nutné zvolit jeden z následujících postupů.

5.7.1. Souborový systém YAFFS2

Nejprve je nutné zjistit strukturu paměti v zařízení. V případě použití souborového systému se rozložení paměti zjistí následovně.

```
cat /proc/mtd

dev: size erasesize name
mtd0: 19000000 00020000 "system"
mtd1: 00600000 00020000 "appslog"
mtd2: 06580000 00020000 "cache"
mtd3: 1a400000 00020000 "userdata"
```

Obrázek č. 10 – Rozložení paměti – YAFFS2

Na Obrázku č. 10 je vidět příkaz pro získání rozložení paměti mobilního zařízení a jeho následný výpis ze zařízení Sony Ericsson Xperia Mini Pro. Ve výpisu příkazu je možné vidět čtyři sloupce, kde první sloupec udává název oddílu, pod kterým je připojen v operačním systému. Druhý sloupec udává velikost oddílu v Bytech. Je nutné dát pozor na to, že velikost oddílu je zapsána v šestnáctkové soustavě. Ve čtvrtém sloupci je jméno oddílu, které slouží pro orientaci, který oddíl slouží k jakému účelu. U některých zařízení nemusí být ve výpisu čtvrtý sloupec obsažen.

Nyní je možné přejít k samotné tvorbě obrazu paměti. Ovšem, i zde je nutné odlišit dvě možnosti získání obrazu paměti.

5.7.1.1. Vytvoření obrazu paměti pomocí nástroje dd

Nástroj dd je běžně využíván pro tvorbu obrazů pevných disků v operačním systému Linux. Tento nástroj je možné využít i v operačním systému Android zadáním následujícího příkazu.

```
dd if=[Zdroj] of=[Cíl] conv=noerror
```

Tento příkaz se skládá z klíčového slova dd, zdrojového oddílu a cílového místa, kam je výsledný obraz uložen. Zdroj se vždy nachází v adresáři /dev/mtd ve kterém je nutné zvolit oddíl, kterého obraz je požadován vytvořit. Výsledná zdrojová cesta má pak následující tvar: **/dev/mtd/mtd*,** kde * je nahrazena číslem oddílu, které je zobrazeno ve výpisu dříve. Cílový soubor udává, kam se výsledný obraz paměti uloží. Aby byl obraz paměti uložen na paměťovou kartu, bude mít následující tvar: **/mnt/sdcard/mtd*.dd**, mtd*.dd určuje název výsledného souboru, kde * opět označuje číslo oddílu. Parametr conv=noerror opět způsobuje nahrazování vadných míst v paměti logickými nulami. Tento příkaz vytvoří obraz požadovaného oddílu paměti. Není možné vytvořit obraz všech oddílů najednou a je nutné je vytvořit postupně.

Může nastat případ, kdy bude tento případ vypisovat následující chybové hlášení.

```
dd: /dev/mtd/mtd*: Invalid argument
```

Díky parametru noerror v příkazu dd, dojde k vytvoření obrazu oddílu, ovšem obraz je tvořen samými nulami, takže v něm nejsou obsažena žádná data. To je způsobeno úpravou systému, kterou provedl přímo výrobce mobilního zařízení. V tomto případě není možné vytvořit obraz oddílu pomocí nástroje dd. Tento případ nastal i při analýze Sony Xperia Mini Pro. Přesto existuje způsob jak obraz oddílu vytvořit pomocí následujícího příkazu. [31]

```
cat [Zdroj] > [Cíl]
```

Pomocí nástroje cat je možné vytvořit obraz oddílu, stejný jako by byl vytvořen pomocí nástroje dd. Nevýhodou nástroje cat je nemožnost používat přidané parametry, které ovlivňují tvorbu obrazu oddílu. V případě použití cat je zdrojový, i cílový soubor totožný jako v případě nástroje dd. Jediný rozdíl je v příponě výsledného souboru, kde je přípona .dd nahrazena příponou .img.

5.7.1.2. Vytvoření obrazu paměti pomocí nástroje nanddump

Další možností jak vytvořit obraz paměti pomocí nástroje nanddump. Tento nástroj byl vyvinut pro tvorbu obrazů pamětí čipů NAND Flash. Obraz oddílu lze vytvořit pomocí následujícího příkazu. [5]

```
nanddump [Zdroj] > [Cíl]
```

Tento příkaz obsahuje klíčové slovo nanddump, zdroj a cíl. Jako zdroj opět slouží cesta k oddílu, ze kterého je požadováno vytvoření obrazu. Jeho tvar má stejnou podobu jako v případě nástroje dd: **/dev/mtd/mtd***, kde * označuje číslo požadovaného oddílu. Jako cílové uložení obrazu je opět nutné zvolit paměťovou kartu. Cílová cesta po té vypadá následovně: **/mnt/sdcard/mtd*.nanddump**, kde * opět označuje číslo oddílu. K příkazu nanddump se nepřipisují žádné parametry jako v případě nástroje dd. V tomto případě to však není nutné, protože nanddump nahrazuje poškozená místa v paměti logickými nulami automaticky.

Při tvorbě obrazu oddílu může dojít k následující chybové hlášce a nevytvoření obrazu oddílu.

```
nanddump: not found
```

Toto chybové hlášení znamená, že nástroj nanddump není v mobilním zařízení dostupný. To je způsobeno tím, že tento nástroj není v operačním systému Android běžně obsažen. Řešení tohoto problému je instalace balíčku BusyBox do mobilního zařízení. BusyBox se balík nástrojů, který doinstaluje nástroje pro terminál operačního systému Android, jehož součástí je i nástroj nanddump. Možností jak doinstalovat BusyBox do mobilního zařízení, je stažení instalačního souboru s příponou .apk, který se uloží na paměťovou kartu mobilního zařízení a pomocí nástroje **adb install** se provede jeho instalace. [32]

5.7.1.3. Rozdíl obrazů paměti

U zařízení Sony Ericsson Xperia Mini Pro byly použity oba nástroje pro vytvoření obrazů všech čtyř oddílů. Na výsledných obrazech oddílů bylo možné pozorovat, že obrazy jednoho oddílu vytvořené nástrojem dd a nástrojem nanddump mají odlišnou velikost. Tento rozdíl je možné pozorovat ve všech čtyřech případech. Obraz oddílu vytvořený pomocí nanddump byl vždy o několik MB větší než obraz téhož oddílu vytvořený pomocí nástroje dd. V případě oddílu mtd3 byl rozdíl velikosti obrazů 13 MB. Tento rozdíl je dán tím, že nástroj dd není schopen do výsledného obrazu oddílu zahrnout OOB oblast paměti. Výsledné obrazy jsou proto menší o velikost OOB oblasti daného oddílu. [5]

Díky znalostem o souborovém systému YAFFS2, které byly rozebrány dříve je možné tento fakt ověřit pomocí následujícího výpočtu.

- Paměť je složena z chunků o velikosti 2048 B
- Velikost obrazu oddílu mtd3 bez OOB oblasti je 420 MB / 2 MB (2048 B), to znamená, že obraz je tvořen z 210 chunků.
- Ke každému chunku náleží OOB oblast o velikosti 64 B, to znamená, že velikost OOB oblasti paměti tvořené 210 chunky je 210 * 64 B = 13 MB.

13 MB je rozdíl mezi velikostí obrazů vytvořených nástroji dd a nanddump.

5.7.2. Souborový systém EXT4

V případě souborového systému EXT4 je postup získání obrazu paměti podobný, avšak jsou zde odlišnosti. Opět je nejprve nutné zjistit rozložení paměti. Ovšem, při použití stejného příkazu jako v případě souborového systému YAFFS2 dojde k vypsání prázdného seznamu oddílů pamětí.

```
cat /proc/mtd
dev:    size   erasesize  name
```

Obrázek č. 11 – Chybný výpis oddílů

Informace o rozložení oddílů paměti v mobilním zařízení, které využívá souborový systém EXT4 lze získat pomocí příkazu **cat /proc/partitions**. Jeho výpis má následující podobu.

```
cat /proc/partitions

major minor  #blocks  name
179        0   15388672 mmcblk0
179        1      15360 mmcblk0p1
179        2      58816 mmcblk0p2
179        3        512 mmcblk0p3
179        4         32 mmcblk0p4
179        5       2048 mmcblk0p5
179        6        512 mmcblk0p6
179        7        512 mmcblk0p7
179        8        512 mmcblk0p8
179        9       3072 mmcblk0p9
179       10         16 mmcblk0p10
179       11      10768 mmcblk0p11
179       12      10240 mmcblk0p12
179       13      14336 mmcblk0p13
179       14       3072 mmcblk0p14
179       15       3072 mmcblk0p15
179       16      13312 mmcblk0p16
179       17      15360 mmcblk0p17
179       18       5121 mmcblk0p18
179       19       7159 mmcblk0p19
179       20       3072 mmcblk0p20
179       21          8 mmcblk0p21
179       22       8192 mmcblk0p22
179       23       9216 mmcblk0p23
179       24    2514944 mmcblk0p24
179       25     204800 mmcblk0p25
179       26      51200 mmcblk0p26
179       27   12429292 mmcblk0p27
179       32       4096 mmcblk0rpmb
253        0    1048576 vnswap0
179       64    1943552 mmcblk1
179       65    1920955 mmcblk1p1
```

Obrázek č. 12 – Rozložení paměti EXT4

Na Obrázku č. 12 je možné vidět rozložení pamětí v zařízení Samsung Galaxy A3. Výpis je složen ze čtyř sloupců, stejně jako v případě YAFFS2. V tomto případě jsou ale nejdůležitější poslední dva sloupce. První z nich je sloupec **#blocks**, který udává velikost jednotlivých oddílů v dekadické soustavě a druhý sloupec **name**, který udává jméno oddílu, které bude použito pro vytvoření obrazu paměti. Ve výpisu je možné vidět více oddílů, než v případě Sony Ericsson Xperia Mini Pro. Z výpisu je možné zjistit, že paměť zařízení je tvořena vnitřní pamětí zařízení **mmcblk0** o velikosti 16 GB, která je rozdělena na několik oddílů, z nichž jeden je v zařízení využit jako nevyjímatelná paměťová karta, na kterou si může uživatel ukládat svá data. Dalším paměťovým médiem v mobilním zařízení je **mmcblk1**, to to je paměťová karta o velikosti 2 GB vložená v mobilním zařízení.

Nyní opět přichází na řadu vytvoření obrazu paměti. I v tomto případě je nutné mít ROOT oprávnění, které se zpřístupní pomocí příkazu **su**. Pro tvorbu obrazů paměti se souborovým systémem EXT4 se využívá pouze nástroj **dd**, při pokusu o vytvoření obrazu paměti pomocí nástroje **nanddump**, nebylo možné obraz vytvořit a proces tvorby obrazu paměti ani nezapočal. Ovšem, souborový systém EXT4 nemá OOB oblast jako souborový systém YAFFS2, díky tomu lze pomocí nástroje **dd** vytvořit plnohodnotný obraz paměti a není nutné využít nástroj **nanddump**. Obraz paměti lze vytvořit pomocí následujícího příkazu.

```
dd if=[Zdroj] of=[Cíl] conv=noerror
```

Tento příkaz je stejný jako v předchozím případě. Jiná je pouze zdrojová a cílová cesta. Zdrojovou cestu je nutné zadat ve tvaru **/dev/block/mmcblk*p***, kde první hvězdička označuje číslo paměti. V případě zařízení Samsung Galaxy A3 je použita 0. Druhá hvězdička určuje číslo oddílu. Je možné zadat pouze **mmcblk***, tím dojde k vytvoření obrazu celé paměti. Jako cíl slouží opět SD karta vložená do mobilního zařízení. Cesta k SD kartě má opět tvar **/mnt/sdcard/mmcblk*p*.dd**. Mobilní zařízení Samsung Galaxy A3 má část vnitřní paměti připojenou jako SD kartu, v takovémto případě by podle této cílové cesty byl obraz paměti ukládán opět do vnitřní paměti zařízení. Cílová cesta k externí SD kartě vložené do mobilního zařízení má tvar **/mnt/extSdCard/mmcblk*p***.

5.7.3 Vytvoření obrazu paměti přes SSH

Může nastat případ, že nebude možné do mobilního zařízení vložit SD kartu, na kterou by byl uložen vytvořený obraz paměti. To může být způsobeno tím, že existují mobilní zařízení, které nemají slot pro paměťovou kartu. Nebo zařízení, které má slot pro paměťovou kartu poškozený. V takovémto případě je možné výsledný obraz paměti uložit přímo do pracovní stanice pomocí SSH.

SSH je protokol, který umožňuje zabezpečenou komunikaci po síti mezi zařízeními. Komunikaci přes SSH lze označit za bezpečnou díky tomu, že je komunikace mezi zařízeními šifrována. [33] SSH funguje na principu klient-server. Proto pracovní stanice bude využita jako SSH server a zkoumané mobilní zařízení bude SSH klient. Jejich komunikace pak probíhá pomocí bezdrátové WiFi sítě. Mezi nevýhody SSH patří nutnost většího zásahu do zkoumaného zařízení a omezená rychlost přenosu, díky které je tvorba obrazu paměti pomalejší, než při použití SD karty.

Aby bylo možné připojit mobilní zařízení k SSH serveru, je nutné do něj nainstalovat emulátor Terminálu, který podporuje SSH komunikaci. Na zkoumaných zařízeních se jako dobrá volba ukázala aplikace Better Terminal Emulator Pro, který umožňuje zadat příkazy přímo ve zkoumaném zařízení. Dále je na pracovní stanici nutné nainstalovat SSH server. Poté již stačí připojit pracovní stanici a zkoumané mobilní zařízení do stejné WiFi sítě. WiFi síť by měla být zabezpečena a neměl by do ní být umožněn přístup žádným dalším zařízením. Nyní lze již v emulátoru terminálu na mobilním zařízení získat ROOT oprávnění pomocí příkazu **su** a po té vytvořit obraz paměti pomocí nástroje **dd**, případně nástroje **cat** následujícími příkazy.

```
dd if=[Zdroj] | ssh userName@ipAdresaServeru "dd of=[Cíl]"
cat [Zdroj] | ssh userName@ipAdresaServeru cat ">" [Cíl]
```

Obrázek č. 13 – dd a cat přes SSH

Zdroj a cíl v příkazech jsou stejné jako v předchozích případech. Ovšem, Cíl určuje, kam bude výsledný obraz uložen v pracovní stanici. Místo **userName** se udává jméno uživatelského účtu na pracovní stanici a **ipAdresaServeru** je IP adresa pracovní stanice.

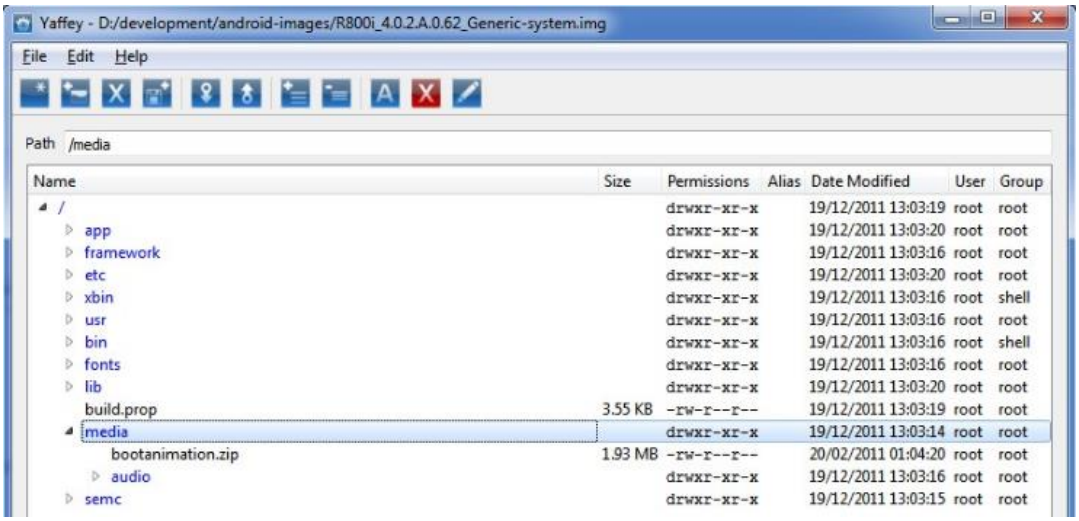
5.8. Analýza obrazů paměti

Po vytvoření obrazu paměti mobilního zařízení je nutné z něj získat obsažená data a to jak data obsažená v paměti zařízení, tak i smazaná data. I v tomto případě je nutné odlišit obrazy paměti podle použitého souborového systému.

5.8.1. Souborový systém YAFFS2

V případě analýzy obrazu paměti souborového systému YAFFS2 je situace opět složitější, než v případě souborového systému EXT4. Největším problémem je, že běžné forenzní nástroje, jako je FTK, FTK Imager, nebo Autopsy, nepodporují souborový systém YAFFS2. Proto je nelze využít pro analýzu obrazu paměti se souborovým systémem YAFFS2. Přesto existují možnosti, jak data z obrazu paměti získat.

Jednou z možností je program Yaffey. Tento program umožňuje vyextrahovat z obrazu paměti adresářovou strukturu se soubory. V tomto programu je možné měnit obsah obrazu paměti, to je ovšem pro potřeby forenzní analýzy nepřípustné. Program má jednoduché grafické prostředí, díky kterému je práce s ním velice jednoduchá. Ovšem, důležité je použít obraz paměti vytvořený pomocí nástroje nanddump, protože obsahuje OOB oblast, která je nezbytná pro práci s programem Yaffey. Pokud by obraz paměti neobsahoval OOB oblast, Yaffey není schopný tento obraz paměti otevřít. [34]



Obrázek č. 14 – Prostředí programu Yaffey [33]

Další možností, jak získat data z obrazu paměti je jeho připojení v operačním systému pracovní stanice pomocí příkazu **mount.** V tomto případě je nutné použít na pracovní stanici operační systém Linux. Přestože operační systém Android využívá Linuxové jádro, není možné připojit obraz paměti jednoduše jako v případě obrazů běžných souborových systémů jako jsou FAT32, NTFS, EXT3, nebo EXT4. Obraz paměti lze připojit následujícím způsobem.

```
sudo modprobe mtd
sudo modprobe mtdblock
sudo insmod yaffs2.ko
sudo modprobe nandsim first_id_byte=0x20 second_id_byte=0xac ...
                ... third_id_byte=0x00 fourth_id_byte=0x15

sudo nandwrite --autoplace --oob /dev/mtd0 mtd*.nanddump

mkdir /mnt/yaffs2
sudo mount -t yaffs2 /dev/mtdblock0 /mnt/yaffs2
```

Obrázek č. 15 – Připojení obrazu (YAFFS2)

V operačním systému Linux v pracovní stanici je nejprve nutné nasimulovat NAND Flash paměť. K tomu slouží první čtyři příkazy z Obrázku č. 15. Příkazy **modprobe** vytvoří simulovanou NAND Flash paměť, jejíž velikost je nutné přizpůsobit velikosti obrazu paměti, který je potřebné připojit. Y**affs2.ko** je kernel modul YAFFS2 pro operační systém Linux, který umožní pracovat s tímto souborovým systémem na pracovní stanici. Příkaz **nandwrite** zkopíruje data a OOB oblast do simulované NAND Flash paměti. Zde je opět nutné použít obraz paměti, který obsahuje OOB oblast. Hvězdičku v příkazu je opět nutné nahradit číslem připojovaného obrazu paměti. Příkaz **mkdir** pouze vytvoří adresář, do kterého bude obraz paměti připojen. Cesta k tomuto adresáři může být libovolná. Nyní už je možné připojit simulovanou NAND Flash paměť k vytvořenému adresáři pomocí příkazu **mount**. Nyní jsou data z obrazu paměti přístupná v připraveném adresáři v pracovní stanici. [5]

Všechny tyto metody umožňují získat data, která byla uložená v paměti mobilního zařízení. Ovšem, smazaná či poškozená data nelze pomocí nich získat. Aby bylo možné získat smazaná data, je nutné využít metodu takzvaného File carvingu. Při této metodě dochází k analýze hrubých dat obrazu paměti. Soubory jsou vyhledávány podle jejich typu, protože každý typ souboru má v paměti specifická metadata, podle kterých lze soubor identifikovat. V některých případech je možné, že smazaný soubor byl v paměti mobilního zařízení částečně přepsaný, to může například u obrázku způsobit, že bude možné získat pouze část původního obrázku. [35]

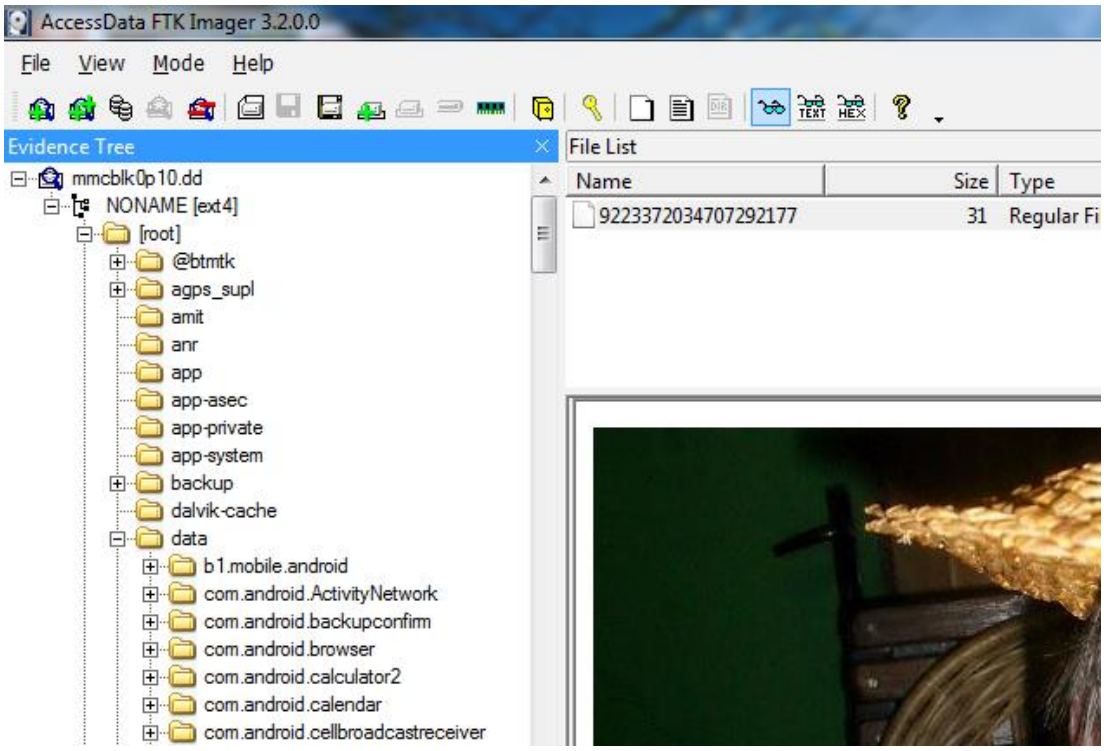
Pro File carving existují různé nástroje, které dokáží soubory z obrazu paměti vyextrahovat. Zajímavou volbou je nástroj **Scalpel 2.0**. Tento nástroj je možné použít na různých platformách, jako jsou operační systémy Windows, Linux, nebo Mac OS X.

File carving byl vyzkoušen na obrazech paměti vytvořených pomocí nástroje **dd**, i pomocí nástroje **nanddump**. Ve všech případech přinesly lepší výsledky analýzy obrazů vytvořené pomocí nástroje **dd**. To bylo způsobeno tím, že tyto obrazy pamětí neobsahují OOB oblast. To ukazuje, že pro File carving je lepší použít obraz paměti bez OOB oblasti.

5.8.2. Souborový systém EXT4

V případě analýzy obrazu paměti souborového systému EXT4 je situace jednodušší. Souborový systém EXT4 je běžně používán operačním systémem Linux, díky tomu je tento souborový systém podporován forenzními nástroji. Mezi vhodné forenzní nástroje patří Autopsy, FTK, případně jeho odnož FTK Imager, který je k dispozici zdarma.

Forenzní nástroj FTK Imager umožní procházení adresářové struktury obrazu paměti a dokáže z obrazu paměti získat i smazaná data. Na obrázku č. 16 je možné vidět část adresářové struktury, kterou lze procházet. Soubory z adresářové struktury jsou poté zobrazeny v pravé části okna. Jeho nevýhodou je, že dokáže data pouze zobrazit, ale nedokáže je analyzovat a roztřídit podle typu dat. To je způsobeno tím, že je tento nástroj odnož placeného FTK. V případě FTK je možné data z obrazu paměti analyzovat.



Obrázek č. 16 – FTK Imager – Zkoumání obrazu paměti

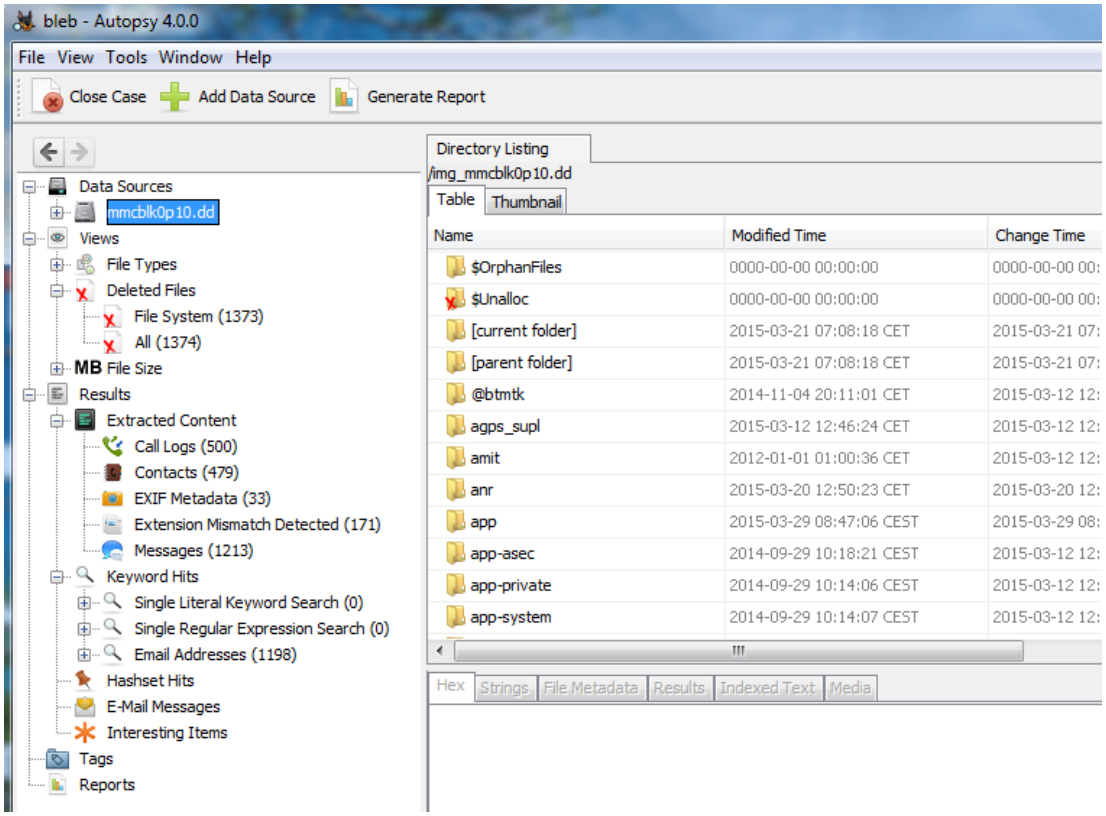
Dalším nástrojem, který lze použít k analýze obrazu paměti je forenzní nástroj Autopsy. Tento nástroj umožňuje analýzu obrazu paměti podobně jako FTK Imager. Autopsy umožňuje procházet adresářovou strukturu obrazu paměti a zobrazuje v ní soubory uložené v paměti mobilního zařízení a také smazané soubory. Autopsy dokáže navíc provést základní analýzu dat obrazu paměti, která dokáže seskupit data, jako jsou Kontakty, Výpis hovorů, SMS zprávy, nebo třeba smazané soubory, do přehledných seznamů. Prostředí programu Autopsy je možné vidět na Obrázku č. 17.

Analýzu obrazu je možné provést pomocí připojení obrazu paměti v operačním systému Linux. Díky tomu, že je souborový systém EXT4 běžně využíván operačním systémem Linux, je připojení obrazu paměti pomocí příkazu **mount** jednodušší, než v případě souborového systému YAFFS2. Lze ho provést pomocí následujícího příkazu.

```
mount -o loop,ro [Zdroj] [Cílový adresář]
```

V tomto příkazu je možné nastavit připojení obrazu paměti pouze pro čtení, tudíž není možné, aby došlo ke změně dat. Tato vlastnost je nastavena parametrem **ro** (read only). Dále je nutné zadat zdrojovou cestu k obrazu paměti, který bude připojen. Tato cesta má tvat **/cesta/obraz.dd**. Dále je nutné zadat cestu k adresáři,

do kterého bude požadovaný obraz paměti připojen. Tato cesta tvar **/cesta/adresar/**. V tuto chvíli jsou data z obrazu paměti přístupná v cílovém adresáři.



Obrázek č. 17 – Autopsy – Zkoumání obrazu paměti

6. Data v mobilním zařízení

6.1. Typy souborů

Mobilní zařízení s operačním systémem Android využívá pro ukládání datových a konfiguračních souborů několik formátů souborů. Pro ukládání dat aplikací jsou využívány SQLite 3 databáze, pro ukládání konfiguračních souborů jsou převážně využívány soubory typu .conf, nebo XML soubory. Aby bylo možné z mobilního zařízení získat co nejvíce informací, je třeba dokázat pracovat s těmito typy souborů.

6.1.1. SQLite 3

SQLite je integrovaný SQL databázový engine. Na rozdíl od ostatních SQL databází, SQLite nemá oddělený proces serveru. SQLite dokáže číst a zapisovat přímo do běžných souborů uložených v paměti mobilního zařízení. Kompletní SQL databáze se všemi tabulkami, indexy, triggery a pohledy, je uložena do jednoho souboru v paměti mobilního zařízení. Formát databázových souborů je multiplatformní, je možné kopírovat soubory mezi 32 bitovými a 64 bitovými systémy, nebo mezi big-endian a little-endian architekturami. Tyto vlastnosti dělají z SQLite oblíbený formát pro soubory aplikací. [36]

Díky tomu, že je SQLite volně k použití, existují aplikace, pomocí kterých lze s SQLite 3 soubory pracovat. Mezi tyto aplikace patří například DB Browser for SQLite, která je zdarma ke stažení a práce s SQLite 3 databázemi je v něm jednoduchá a přehledná.

6.1.2. XML

XML (eXtensible Markup Language) je značkovací jazyk, který ukládá data strukturovaně do XML souborů. Data jsou strukturována do takzvaných tagů, které jsou ohraničeny lomenými závorkami <, >. Tyto tagy jsou párové, takže data se ukládají mezi počáteční a koncový tag. Data mohou vypadat následovně **<Mesto>České Budějovice</Mesto>.** [37]

Je více možností, jak zobrazit XML soubory. Mezi nejsnadnější způsob patří otevření XML souboru v aplikaci Poznámkový blok, která je součástí operačního systému Windows. Další možností jak zobrazit XML soubor je pomocí kteréhokoliv webového prohlížeče.

Mezi zajímavé aplikace pro práci s XML soubory patří PSPad editor od českého vývojáře. Tato aplikace přináší více možností při práci s těmito soubory. Například zvýrazňování tagů je velice užitečná vlastnost, díky které je XML dokument mnohem více přehledný.

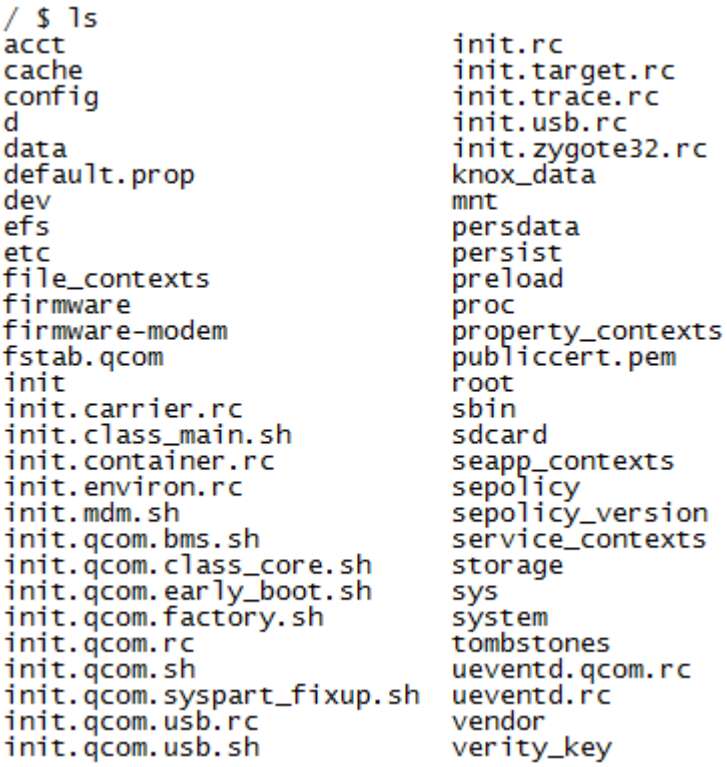
6.1.3. soubory .conf

Soubory s příponou .conf jsou konfigurační soubory operačního systému a aplikací. Tyto soubory jsou běžné textové soubory obsahující konfigurační data operačního systému a aplikací v testové podobě. Tyto soubory je možné otevřít pomocí aplikace Poznámkový blok, nebo jakéhokoliv textového prohlížeče. Opět je možné využít i PSPad editor.

6.2. Struktura dat v mobilním zařízení

Struktura kořenového adresáře a uložení konfiguračních souborů mobilního zařízení s operačním systémem Android je velice podobné operačnímu systému Linux, to je způsobeno využitím Linuxového jádra. Díky tomu se lze v těchto adresářích orientovat podobně jako v operačním systému Linux.

Na Obrázku č. 18 je zobrazen výpis kořenového adresáře mobilního zařízení Samsung Galaxy A3, tento výpis je uspořádán do dvou sloupců kvůli úspoře místa. Výpis obsahuje různé soubory a složky, kde mezi soubory jsou zastoupeny hlavně soubory init.*, které slouží k inicializaci komponent operačního systému. Z hlediska získávání informací z mobilního zařízení jsou zajímavější adresáře, které jsou v kořenovém adresáři obsaženy.



Obrázek č. 18 – Výpis kořenového adresáře

Z těchto adresářů stojí za zmínku adresář **cache**, do kterého jsou ukládány nejčastěji používaná data a komponenty aplikací. Dále adresář **data**, ve kterém jsou uloženy uživatelská data, jako jsou data aplikací, kontakty, zprávy, výpisy hovorů a další podobná data. Dalším adresářem je **dev**, to to je jeden z důležitých adresářů, protože může obsahovat zdrojové soubory pro tvorbu obrazu paměti. Adresář **mnt** je místem, kde jsou připojeny paměťová média, jako jsou oddíly vnitřní paměti a paměťové karty. Složka **proc** obsahuje data o paměti zařízení, která jsou využívána jádrem operačního systému. Složka **misc** obsahuje informace o nastavení hardware mobilního zařízení. Ve složce **system** jsou obsaženy zdrojová data operačního systému, knihovny a další data spojená s operačním systémem.

6.3. Informace o mobilním zařízení

V mobilním zařízení existuje několik souborů, ze kterých lze získat velké množství informací o zařízení. Mezi tyto soubory patří:

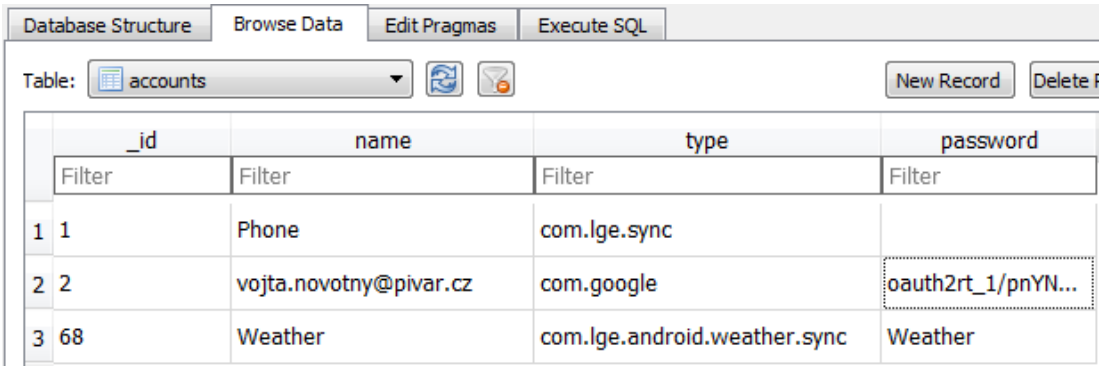
- **/cache/recovery/last_log** – V tomto souboru lze nalézt základní údaje o zařízení, jako je rozložení oddílů paměti i s popisem jaké obsahují data a dále veškeré základní údaje o typu mobilního zařízení, jeho výrobci i použitém operačním systému. Na obrázku č. 19 je možné vidět část tohoto souboru.

```
recovery filesystem table
=========================
  0 /tmp ramdisk (null) (null) 0
  1 /boot emmc boot (null) 0
  2 /cache ext4 /dev/block/mmcblk0p9 (null) 0
  3 /data ext4 /dev/block/mmcblk0p10 (null) 0
  4 /misc emmc misc (null) 0
  5 /recovery emmc recovery (null) 0
  6 /system ext4 /dev/block/mmcblk0p8 (null) 0

I:no boot messages
recovery.cpp : FRSTSTATUS=3
E:Can't open /persist-lg/callduration/CallDuration
Command: "/sbin/recovery"

============================
[ASP] SECURE BOOT INIT 'Wed Aug 8 15:59:54 CST 2012(ASF.JB)'
============================
[SEC] no check. ret 0x9007

ro.boot.serialno=7LHASKNVAYKVYPYT
ro.serialno=7LHASKNVAYKVYPYT
ro.bootmode=unknown
ro.baseband=unknown
ro.bootloader=unknown
ro.hardware=mt6575
```

Obrázek č. 19 – LG E440 – last_log

- **/data/system/packages.xml** – Tento soubor obsahuje seznam aplikací nainstalovaných v mobilním zařízení a k tomu informace o těchto aplikacích.

- **/systém/users/0/accounts.db** – Tento databázový soubor obsahuje seznam uživatelských účtů v mobilním zařízení. Tato SQLite 3 databáze obsahuje tabulku **accounts**, ve které jsou uživatelské účty spojené s mobilním zařízením. Tato tabulka obsahuje uživatelské jméno, typ účtu a heslo k účtu. Ovšem v případě Google účtu **vojta.novotny@pivar.cz** v zařízení LG E440 bylo heslo nahrazeno následujícím řetězcem: `oauth2rt_1/pnYNDtPHQyh_lUdTcpuiRr_cxQF-E8sx_DAtGC1rC-c`



Obrázek č. 20 – LG E440 - accounts.db

- **/data/misc/wifi/wpa_supplicant.conf** – Toto je konfigurační soubor pro WiFi, který obsahuje seznam WiFi sítí, ke kterým se mobilní zařízení automaticky připojí, jsou-li dostupné. Tento konfigurační soubor obsahuje SSID sítě, typ zabezpečení, klíč pro přihlášení k síti a prioritu, podle které mobilní zařízení zvolí, ke které WiFi síti se připojí. Část tohoto konfiguračního souboru je možné vidět na obrázku č. 21.

```
network={
  ssid="JU_wireless_WebAAA"
  key_mgmt=NONE
  priority=2
}

network={
  ssid="Pani_Kluci"
  psk="pekelnaSekana666"
  key_mgmt=WPA-PSK
  priority=3
}
```

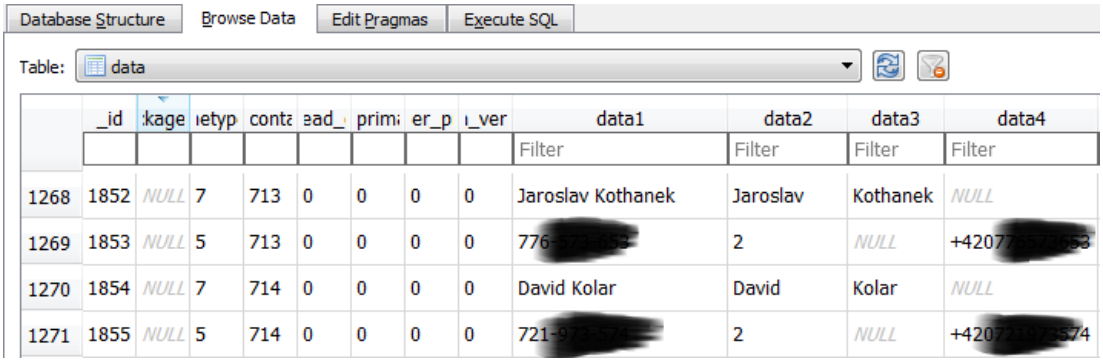
Obrázek č. 21 – LG E440 – wpa_supplicant.conf

6.4. Data běžných aplikací

Mezi tyto data patří data, která jsou typická pro všechny mobilní zařízení, jako jsou **Kontakty**, **Výpisy hovorů**, **SMS zprávy**, **MMS zprávy**, nebo data z **Kalendáře**. Všechny tyto data jsou uložena v adresáři **/data**, který se v případě zařízení LG E440 nachází v oddílu **mmcblk0p10**. V této složce se nachází data aplikací nainstalovaných v mobilním zařízení. Jejich struktura má následující strukturu.

6.4.1. Kontakty v mobilním zařízení

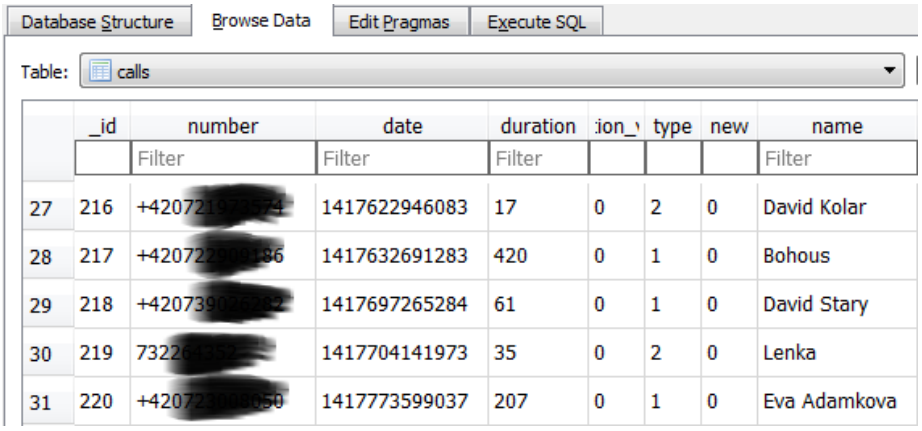
Kontakty uložené v mobilním zařízení jsou uloženy v adresáři **/data/com.android.providers.contacts**. V tomto adresáři se nachází pět podadresářů. **Cache**, **databases**, **files**, **lib** a **shared_prefs**. Z těchto adresářů jsou nejzajímavější dva. Prvním je adresář **files**, který obsahuje několik podadresářů, ve kterých je možné najít například profilový obrázek účtu mobilního zařízení. Druhým je adresář **databases**, ve kterém se nachází soubor **contacts2.db**. Tato databáze obsahuje celkem 38 tabulek, ovšem v tomto případě je důležitá tabulka **data**, která obsahuje seznam kontaktů, který není seřazen podle abecedy, ale podle toho, kdy byl kontakt přidán. Jak je vidět na Obrázku č. 22, jeden kontakt je v tabulce reprezentován dvěma řádky, **raw_contact_id** je stejný vždy pro oba řádky, v případě Obrázku č. 22 je to 713 a 714.



Obrázek č. 22 – Kontakty z contacts2.db

6.4.2. Výpis hovorů

Výpis telefonních hovorů je uložen ve stejné databázi, jako kontakty. Výpisy hovorů jsou obsaženy v tabulce **calls**. Jak je vidět na Obrázku č. 23, tato tabulka obsahuje seznam hovorů, který se skládá z čísla kontaktu, datu uskutečnění hovoru, délku hovoru ve vteřinách, jméno kontaktu a několik dalších informací.



Obrázek č. 23 – Výpis hovorů z contacts2.db

Datum používané v mobilních zařízeních s operačním systémem Android nemá běžný formát obsahující den, měsíc a rok, ale je ve tvaru třináctimístného čísla. Toto číslo se nazývá Unix epoch, toto číslo znázorňuje počet vteřin uplynulých od 1. 1. 1970.[38] To znamená, že v případě data 1417622946083, je datum uskutečnění hovoru 3. 12. 2014 17:09:06.

6.4.3. SMS zprávy

SMS zprávy jsou v mobilním zařízení uloženy v adresáři **/data/com.android.providers.telephony**, kde se nachází čtyři podadresáře. Jsou to **app_parts**, **databases**, **lib** a **shared_prefs**. Ve složce **databases** se nachází databázový soubor **mmssms.db**, který obsahuje celkem 22 tabulek. SMS zprávy jsou uloženy v tabulce **sms**, část této tabulky je zobrazena na Obrázku č. 24. Tato tabulka obsahuje číslo, ze kterého, nebo na které byla zpráva odeslána, datum odeslání a tělo zprávy. Důležitý atribut této tabulky je sloupec **date_sent**, pokud obsahuje hodnotu 0, znamená to, že jde o zprávu odeslanou ze zkoumaného mobilního zařízení. Pokud obsahuje časový údaj, znamená to, že jde o zprávu, která byla přijata z jiného mobilního zařízení.

6.4.4. MMS zprávy

Data MMS zpráv jsou opět uloženy v adresáři **/data/com.android.providers.telephony** a jeho podadresáři **app_parts**. Tento adresář obsahuje obrázky poslané pomocí MMS zpráv. Tyto obrázky jsou pojmenovány předponou PART_, datu doručení ve formátu Unix Epoch time_ a názvu odeslaného souboru, například **PART_1413321126238_NazevObrazku.jpg**.

Database Structure | Browse Data | Edit Pragmas | Execute SQL

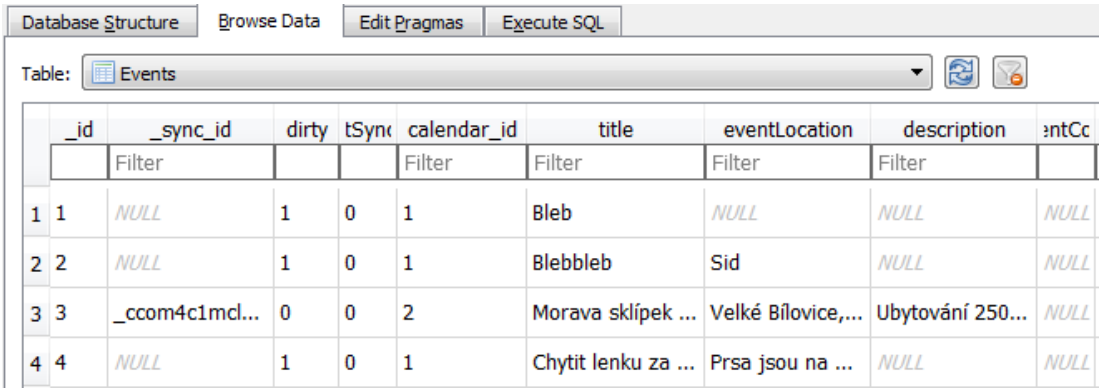
Table: sms

	_id	read_	address	erso	date	date_sent	mest	otoc	read	status	type	ath_	ubje	body
	Filter		Filter		Filter	Filter								Filter
1	1	1	+420722[redacted]	NULL	1411978277770	1411924338000	NULL	0	1	-1	1	0	NULL	Mate 6 zmeskanych...
2	2	2	+420721[redacted]15	708	1412074871761	1412074869000	NULL	0	1	-1	1	0	NULL	Cetls mail? :D
3	3	2	+420721[redacted]15	NULL	1412074994274	0	NULL	0	1	0	2	NULL	NULL	Ted uz jo. To se mi...
4	4	2	+420721[redacted]	708	1412075027426	1412075026000	NULL	0	1	-1	1	0	NULL	I me :D
5	5	2	+420721[redacted]15	NULL	1412075093834	0	NULL	0	1	0	2	NULL	NULL	Nechystas se dnesk...
6	6	2	+420721[redacted]15	708	1412075195361	1412075194000	NULL	0	1	-1	1	0	NULL	Asi tam zajdu no

Obrázek č. 24 – SMS zprávy

6.4.5. Kalendář

Data kalendáře jsou ukládána do adresáře **/data/com.android.providers.calendar**. V tomto adresáři se nachází podadresáře **cache**, **databases**, **lib** a **shared_prefs**. V adresáři **databases** se nachází databázový soubor **calendar.db**. Tato databáze obsahuje šestnáct tabulek, z nichž je zajímavá tabulka **Calendars**, která obsahuje seznam kalendářů použitých v zařízení. V případě zařízení LG E440 byl použit kalendář mobilního zařízení, synchronizovaný kalendář účtu od Googlu, Narozeniny a Státní svátky České republiky. Druhou důležitou tabulkou je tabulka **Events**. V této tabulce jsou atributy s názvem události, místem konání události, popisu události, datum zahájení a datum ukončení události opět ve formátu Unix epoch time.



	_id	_sync_id	dirty	tSync	calendar_id	title	eventLocation	description	entCc
		Filter			Filter	Filter	Filter	Filter	
1	1	NULL	1	0	1	Bleb	NULL	NULL	NULL
2	2	NULL	1	0	1	Blebbleb	Sid	NULL	NULL
3	3	_ccom4c1mcl...	0	0	2	Morava sklípek ...	Velké Bílovice,...	Ubytování 250...	NULL
4	4	NULL	1	0	1	Chytit lenku za ...	Prsa jsou na ...	NULL	NULL

Obrázek č. 25 – Data z tabulky Events

6.5. Data doplňkových aplikací

Mezi doplňkové aplikace patří aplikace, které jsou většinou využívány v mobilních zařízeních, ale nepatří mezi základní aplikace potřebné pro základní používání mobilního zařízení. Mezi tyto aplikace patří například aplikace **Facebook**, **Messenger**, **ICQ**, **Gmail**, **Skype**, **Vibre**, **Mapy** a webový prohlížeč. Data těchto aplikací se stejně jako v předchozím případě v adresáři **/data**, který se v případě mobilního zařízení LG E440 nachází v oddílu **mmcblk0p10**.

6.5.1. Facebook

Tato aplikace je klient pro mobilní zařízení, který slouží k interakci se sociální sítí Facebook. Data této aplikace se nachází v adresáři **/data/com.facebook.katana**. V tomto adresáři se nachází podadresáře s názvy **app_***, **cache**, **databases**, **files**, **lib** a **shared_prefs**. V adresáři databases se nachází několik databázových souborů, které obsahují veškeré informace o používání aplikace Facebok a o aktivitách uživatelů.

6.5.2. Messenger

Aplikace Messenger je doplňková aplikace k aplikaci Facebook, která slouží pro posílání zpráv pomocí aplikace Facebook. Data této aplikace se nachází v adresáři **/data/com.facebook.orca**. Struktura podadresářů je velice podobná struktuře podadresářů aplikace Facebook. Zde je opět nejzajímavější adresář **databases**, ve kterém se nachází několik databázových souborů. Jedním z nich je soubor

contacts_db2, tato databáze obsahuje devět tabulek, z nichž tabulka **contacts** obsahuje kontakty z aplikace Messenger. Druhou důležitou databází obsaženou v tomto adresáři je databáze **threads_db2**, tato databáze obsahuje dvanáct tabulek, z nichž tabulka **messages** obsahuje odeslané a přijaté zprávy. Mezi důležité atributy této tabulky patří atribut **thread_key**, který určuje, zda se jedná o zprávu poslanou mezi dvěma uživateli (ONE_TO_ONE) a skupinovou zprávou (GROUP). Dále atribut **text** obsahuje text poslané zprávy. Atribut **timestamp_ms** určuje čas odeslání, nebo přijetí zprávy. Odesílatele zprávy určuje atribut **sender**, tento atribut je tvořen dlouhým řetězcem, který obsahuje jméno odesílatele zprávy. Příklad tohoto řetězce může vypadat následovně: **{"email":"100002078305639@facebook.com","user_key":"FACEBOOK:100002078305639","name":"Vojta Novotný"}**. Další zajímavou tabulkou je **thread_users**, tato tabulka obsahuje kontakty, se kterými byla uskutečněna konverzace.

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: messages

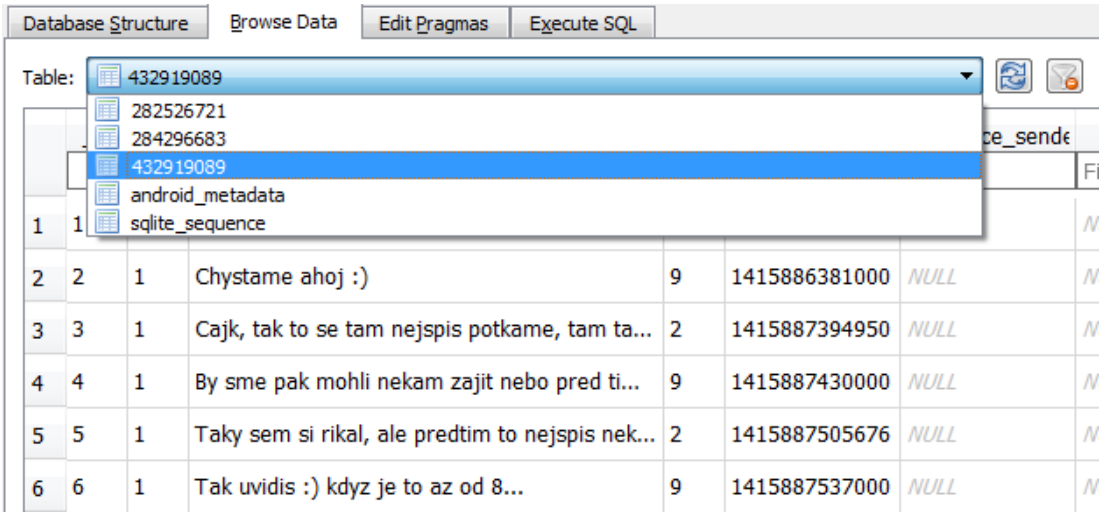
	msg_id	thread_key	_thre	tion_	text	sender	timestamp_ms
	Filter	Filter			Filter	Filter	Filter
361	m_mid.142...	ONE_TO_ONE:...	t_i...	14...	Tak vzejtra tam mam bejt na deva...	{"email":"1000...	1421605348115
362	m_id.84238...	GROUP:842384...	t_i...	14...	http://papagajuvhlasatelrecords.b...	{"email":"1000...	1423426977825
363	GROUP:842...	GROUP:842384...	NULL	0	NULL	NULL	0
364	m_mid.142...	ONE_TO_ONE:...	t_...	14...	Cau, k tomu nic asi nemam, ale je...	{"email":"1000...	1423470433416
365	m_mid.142...	ONE_TO_ONE:...	t_...	14...	Zdarec Vořech, heleď tys říkal, že ...	{"email":"1464...	1423470316830
366	m_mid.142...	ONE_TO_ONE:...	t_...	14...	Cau, tak to uz si vubec nepamatuju	{"email":"1000...	1422183352622

Obrázek č. 26 – Zprávy aplikace Messenger

6.5.3. ICQ

Data aplikace ICQ se v mobilním zařízení opět nachází v adresáři /data, konkrétně v adresáři **/data/com.icq.mobile.client**. Tento adresář obsahuje několik podadresářů, do kterých jsou ukládány například profilové obrázky kontaktů, soubory přijaté přes ICQ a XML soubory, které obsahují data pro nastavení aplikace ICQ. Nejvíce informací lze nalézt opět v adresáři **databases**. První databázi obsaženou v tomto adresáři je databáze **agent-dao**. Tato databáze je tvořena celkem

čtrnácti tabulkami, z nichž nejzajímavější je tabulka **CONTACT_DATA**, která obsahuje seznam všech kontaktů. Druhá databáze v tomto adresáři má název **history-258192943-2**. Tato databáze obsahuje historii konverzací. Šestimístné číslo v názvu databáze označuje číslo ICQ účtu, každý ICQ účet má svou vlastní databázi s historií zpráv. V této databázi tvoří konverzace s jedním kontaktem vlastní tabulku. To znamená, že s čím více kontakty bude uskutečněna konverzace, tím více tabulek zde bude. Tabulky jsou pojmenovány podle ICQ čísla kontaktu, s kterým je konverzace vedena. V této tabulce jsou nejzajímavější atributy **content**, který obsahuje text odeslané zprávy, dále **flag**, který označuje, zda se jedná o odeslanou, nebo přijatou zprávu. Pokud má flag hodnotu 2, jde o zprávu odeslanou, pokud má hodnotu 9, jde o zprávu přijatou. Atribut **timestamp** opět určuje čas odeslání, či přijetí zprávy ve formátu Unix epoch time. Další tabulkou v této databázi je **sqlite_sequence**. Tato tabulka obsahuje pouze ICQ čísla kontaktů a počet zpráv, které byli s konkrétním kontaktem vyměněny.



2	2	1	Chystame ahoj :)	9	1415886381000	NULL	
3	3	1	Cajk, tak to se tam nejspis potkame, tam ta...	2	1415887394950	NULL	
4	4	1	By sme pak mohli nekam zajit nebo pred ti...	9	1415887430000	NULL	
5	5	1	Taky sem si rikal, ale predtim to nejspis nek...	2	1415887505676	NULL	
6	6	1	Tak uvidis :) kdyz je to az od 8...	9	1415887537000	NULL	

Obrázek č. 27 – Historie konverzací ICQ

6.5.4 Skype

Data aplikace Skype se nachází v adresáři **/data/com.skype.raider**. V případě aplikace Skype se data o aktivitách uživatelů neukládají do adresáře databases, jako v předchozích případech. Tyto informace jsou ukládány do adresáře **files**, který obsahuje několik podadresářů. Pro každý Skype účet použitý v mobilním zařízení je vytvořen vlastní adresář s daty. V případě zařízení LG E440 byl použit pouze jeden

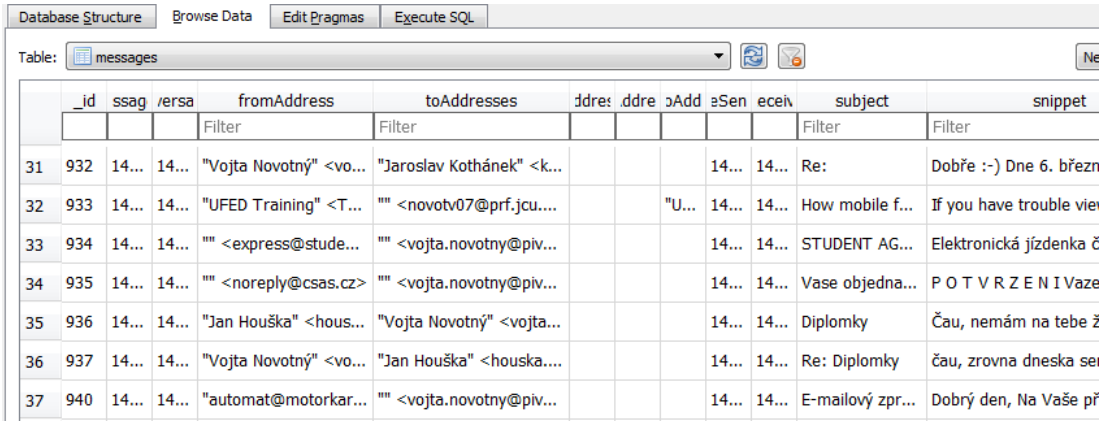
Skype účet a tím byl **vorech.cz**. Stejný název má i adresář s daty tohoto účtu. V tomto adresáři je obsaženo několik adresářů, databází a konfiguračních souborů. Všechny tyto soubory a složky obsahují informace o aktivitách konkrétního Skype účtu. Základní informace, jako jsou kontakty, historie zpráv, historie hovorů a podobné, je možné nalézt v databázi **main.** Tato databáze obsahuje dvacet tabulek, do kterých jsou tyto data rozdělena.

6.5.5. Viber

Data aplikace Viber jsou uloženy v adresáři **/data/com.viber.voip**. V tomto adresáři se opět nachází podadresář **databases**, který obsahuje dva databázové soubory **viber_data** a **viber_messages**. Databáze viber_data obsahuje seznam kontaktů uživatele. Databáze viber_messages obsahuje data s konverzacemi, tato databáze obsahuje tabulku s konverzacemi, zprávami a voláním provedených přes aplikaci Viber.

6.5.6. Gmail

Data aplikace Gmail se nachází v adresáři **/data/com.google.android.gm**. Tento adresář obsahuje několik podadresářů, z nichž adresář **cache** obsahuje data dočasně uložená v zařízení. V případě aplikace Gmail byly v tomto adresáři obsaženy soubory, jako jsou PDF přílohy a obrázky odeslané a přijaté pomocí emailu aplikací Gmail. Dalším zajímavým adresářem je adresář **databases**. Tento adresář obsahuje několik databázových souborů, z nichž databáze **mailstore.vojta.novotny@pivar.cz**. Název databáze je tvořen předponou mailstore a emailovou adresou vojta.novotny@pivar.cz. Tuto databázi tvoří dvacet jedna tabulek. Tyto tabulky obsahují veškeré informace o emailové komunikaci. Základní informace jsou obsaženy v tabulce **messages**, která obsahuje data o emailových zprávách. Jsou zde například atributy **fromAddres** a **toAdresses**, znamenající od koho komu byla zpráva odeslána. Dále atributy **subject** a **snippet** obsahují předmět emailové zprávy a samotné tělo zprávy. Datum odeslání a přijetí emailové zprávy je opět ve formátu Unix epoch time.



	_id	ssag	ersa	fromAddress	toAddresses	ddres	ddre	oAdd	eSen	eceiv	subject	snippet
				Filter	Filter						Filter	Filter
31	932	14...	14...	"Vojta Novotný" <vo...	"Jaroslav Kothánek" <k...				14...	14...	Re:	Dobře :-) Dne 6. březn
32	933	14...	14...	"UFED Training" <T...	"" <novotv07@prf.jcu....			"U...	14...	14...	How mobile f...	If you have trouble viev
33	934	14...	14...	"" <express@stude...	"" <vojta.novotny@piv...				14...	14...	STUDENT AG...	Elektronická jízdenka č
34	935	14...	14...	"" <noreply@csas.cz>	"" <vojta.novotny@piv...				14...	14...	Vase objedna...	P O T V R Z E N I Vaze
35	936	14...	14...	"Jan Houška" <hous...	"Vojta Novotný" <vojta...				14...	14...	Diplomky	Čau, nemám na tebe ž
36	937	14...	14...	"Vojta Novotný" <vo...	"Jan Houška" <houska....				14...	14...	Re: Diplomky	čau, zrovna dneska se
37	940	14...	14...	"automat@motorkar...	"" <vojta.novotny@piv...				14...	14...	E-mailový zpr...	Dobrý den, Na Vaše př

Obrázek č. 28 – Gmail

6.5.7. Mapy společnosti Google

Data této aplikace jsou uloženy v adresář **/data/com.google.android.apps.maps**, v tomto adresáři se nachází záznamy o poloze, které byly zaznamenány při používání této aplikace. Data o polohách jsou ukládána do dvou databází, které se nachází v adresáři **databases**. První z nich je databáze s názvem **gmm_myplaces**, do této databáze jsou ukládány údaje o poloze, které byly uloženy samotným uživatelem. Druhou databází je **gmm_storage**, do této databáze jsou zaznamenávány záznamy polohy, vznikající automaticky při používání této aplikace.

6.5.8. Webový prohlížeč

Pro mobilní zařízení s operačním systémem Android existuje několik webových prohlížečů, mezi nejpoužívanější patří Google chrome, jehož data se nachází v adresáři **/data/com.android.chrome** a Opera, jejíž data se nacházela v adresáři **/data/com.opera.browser.classic**. Opera existuje ve více verzích, proto název tohoto adresáře může být odlišný pro různé verze tohoto prohlížeče. V adresářích webových prohlížečů je možné získat data o historii prohlížení webových stráněk, data o polohách mobilního zařízení, záložky webových stránek, nebo přihlašovací údaje k různým webovým stránkám.

7. Komerční forenzní nástroje

V současné době existuje několik komerčních nástrojů pro forenzní analýzu mobilních zařízení s operačním systémem Android. Tyto nástroje lze rozdělit do dvou základních skupin. První jsou softwarové nástroje, které jsou nainstalovány na pracovní stanici, a mobilní zařízení je poté připojeno k této stanici pomocí USB rozhraní. Druhou skupinou jsou hardwarové nástroje, tato nástroje využívají pro získání dat z mobilního zařízení speciální zařízení, které potřebná data získá, ovšem následná analýza získaných dat je provedena pomocí nástrojů nainstalovaných v pracovní stanici. V těchto případech se však mobilní zařízení nepřipojuje k pracovní stanici, ale ke speciálnímu zařízení. [19]

7.1. Softwarové forenzní nástroje

Mezi výhody softwarových forenzních nástrojů patří fakt, že k jejich použití není nutné žádné zařízení navíc, kromě pracovní stanice. Protože se mobilní zařízení připojí k pracovní stanici pomocí USB kabelu. Ovšem je nutné na mobilním zařízení zapnout režim Ladění USB. Zapnutí tohoto režimu bylo popsáno v předchozích kapitolách. Pokud má však mobilní zařízení zapnutý zámek obrazovky a vypnutý režim Ladění USB, není možné tento režim zapnout bez dalšího zásahu do zařízení a tyto nástroje nejsou schopné s mobilním zařízením pracovat.

7.1.1. Oxygen forensic

Aplikace Oxygen Forensic od ruských vývojářů z Oxygen Forensics v současné době patří mezi nejlepší dostupné forenzní nástroje. Mezi jeho výhody patří velké množství dat, které je tento nástroj schopný získat z mobilního zařízení. Oxygen Forensic zvládl získat z mobilního zařízení, jak základní informace o mobilním zařízení, seznam kontaktů, výpisy hovorů a zpráv a data z kalendáře mobilního zařízení. Navíc tato aplikace umožňuje získání ROOT oprávnění u některých typů mobilních zařízení, díky kterému umožňuje získat navíc data z doplňkových aplikací, jako je Facebook, Messenger, Mapy, data z webových prohlížečů a část adresářové

struktury mobilního zařízení. V případě získání ROOT oprávnění je možné provést fyzickou analýzu mobilního zařízení. Ze získaných dat je možné vytvořit report v různých formátech. Mezi nevýhody tohoto nástroje patří nutnost placení licenčních poplatků každý rok. Pokud nedojde po roce k zaplacení licenčních poplatků na další rok, dojde k zablokování tohoto nástroje.

Použití tohoto nástroje je velice jednoduché, nejprve je nutné připojit mobilní zařízení k pracovní stanici přes USB rozhraní. Je nutné v mobilním zařízení zapnout režim Ladění USB. Poté je nutné vybrat v aplikaci konkrétní typ mobilního zařízení a zapnout analýzu zařízení. V tu chvíli dojde k nainstalování malé aplikace do mobilního zařízení, pomocí které jsou data z mobilního zařízení získávána, tento nástroj se při analýze mobilního zařízení pokouší získat ROOT oprávnění. Po dokončení analýzy mobilního zařízení jsou data zobrazena v přehledných strukturách a aplikace je z mobilního zařízení smazána.

7.1.2. MOBILedit Forensic

MOBILedit Forensic je aplikace od české firmy Compelson Labs. Tato aplikace umožňuje získat z mobilního zařízení základní informace o mobilním zařízení, výpisy hovorů, SMS a MMS zprávy, seznam kontaktů a informace z kalendáře mobilního zařízení. U zařízení s ROOT oprávněním nebyl tento nástroj schopen získat moc informací navíc. Ovšem jeho výhodou je nízká cena oproti ostatním forenzním nástrojům.

Použití nástroje MOBILedit Forensic je opět jednoduché. Opět stačí připojit mobilní zařízení přes USB rozhraní se zapnutým režimem Ladění USB k pracovní stanici. Poté je nutné v aplikaci zvolit typ mobilního zařízení a zapnout analýzu. Opět dojde k instalaci malé aplikace do zkoumaného mobilního zařízení, pomocí které jsou získávána data z mobilního zařízení. Po dokončení analýzy dojde k odinstalování aplikace z mobilního zařízení. Získaná data jsou dostupná v aplikaci v pracovní stanici a je možné generovat reporty se získanými daty v různých formátech.

7.1.3. XRY

XRY je softwarový nástroj od švédské firmy MSAB. Ačkoliv je tento nástroj softwarový, dodává se k němu USB HUB, který slouží jako roztrojka pro USB. Díky tomu je možné analyzovat až tři mobilní zařízení najednou. XRY je dražší než ostatní forenzní nástroje, avšak po propadnutí roční licence, nedojde k znemožnění používání tohoto nástroje. Pouze není možné aktualizovat tento nástroj, to způsobuje, že nová mobilní zařízení nemusí být podporována, pokud byla jejich podpora implementována až po propadnutí licence. Ovšem, starší mobilní zařízení je možné analyzovat bez jakéhokoli omezení. Tento nástroj byl schopný z mobilního zařízení získat základní informace o zařízení, seznam kontaktů, SMS a MMS zprávy, výpisy hovorů a data z kalendáře.

Použití XRY je snadné. Nejprve je nutné připojit USB HUB k pracovní stanici a po té přes něj připojit zkoumané zařízení pomocí USB rozhraní, opět je nutné zapnout na zkoumaném zařízení režim Ladění USB. Poté je nutné vybrat v aplikaci typ zkoumaného zařízení a spustit analýzu zařízení. Při analýze dojde k instalaci malé aplikace do zkoumaného zařízení, díky které jsou získávány data z mobilního zařízení. Po dokončení analýzy je aplikace z mobilního zařízení odinstalována a získaná data je možné analyzovat v aplikaci XRY na pracovní stanici.

7.1.4. MPE+

Aplikace MPE+ (Mobile Phone Examiner Plus) od společnosti Access Data je poměrně nový produkt. I to je důvod, proč je MPE+ schopen z mobilního zařízení získat pouze základní data, jako jsou základní informace o mobilním zařízení, kontakty, výpisy hovorů, SMS a MMS zprávy a data z kalendáře. Také podpora různých mobilních zařízení není tak široká jako u ostatních forenzních nástrojů.

Použití MPE+ je opět velice snadné, aplikaci stačí nainstalovat na pracovní stanici a připojit zkoumané mobilní zařízení k pracovní stanici se zapnutým režimem Ladění USB. Poté je nutné pouze vybrat v aplikaci typ zkoumaného zařízení a spustit analýzu. Po dokončení analýzy je možné výsledky prohlížet v aplikaci MPE+.

7.2. Hardwarové forenzní nástroje

Hardwarové forenzní nástroje využívají pro získání dat z mobilního zařízení speciální nástroj, pomocí kterého lze získat data. Tyto data se poté analyzují na pracovní stanici pomocí aplikací k tomu určených. Tyto aplikace umí pouze analyzovat získaná data, nelze jejich pomocí data z mobilního zařízení získat. Tyto nástroje jsou v některých případech schopné analyzovat mobilní zařízení, které nemá povolený režim Ladění USB.

7.2.1. UFED

UFED od firmy izraelské firmy Cellebrite je v současné době nejlepší nástroj pro analýzu mobilních zařízení s operačním systémem android. Celý nástroj UFED je tvořen speciálním přenosným počítačem a sadou kabelů sloužících k připojení mobilních zařízení k přenosnému počítači. Dále je nutné mít paměťové médium, které lze pomocí USB rozhraní připojit k přenosnému počítači. Na toto médium jsou ukládány data získávána při analýze mobilního zařízení. Toto paměťové médium je nezbytné, protože není možné tyto data ukládat přímo do paměti přenosného počítače. Dále je nutné na pracovní stanici nainstalovat aplikaci, pomocí které je možné získaná data analyzovat.

UFED je schopný provést jak logickou, tak fyzickou analýzu mobilních zařízení, ovšem fyzickou analýzu není možné provést se všemi mobilními zařízeními. Zda je možné u konkrétního mobilního zařízení provést fyzickou analýzu, lze zjistit přímo v zařízení UFED, po zvolení typu zkoumaného zařízení. V případě testovaných mobilních zařízení byl u zařízení LG E440 provést pouze logickou analýzu, zatímco u zařízení Samsung Galaxy A3 bylo možné provést fyzickou analýzu zařízení.

Dochází-li k provedení logické analýzy, je zkoumané mobilní zařízení připojeno přes USB rozhraní a je nutné povolit režim Ladění USB. Poté dojde k instalaci malé aplikace do mobilního zařízení, pomocí které jsou z mobilního zařízení získávána data. Po dokončení analýzy je tato aplikace smazána a data jsou uložena na paměťové médium připojenému k přenosnému počítači UFED.

V případě fyzické analýzy je nutné provést několik kroků, které jsou pro každé mobilní zařízení unikátní. Tyto kroky jsou vždy zobrazeny a popsány na mobilním počítači UFED. Tyto kroky mohou vypadat následovně. Nejprve je nutné vypnout mobilní zařízení a vyndat z něj paměťovou kartu. Poté Je mobilní zařízení připojeno pomocí speciálního kabelu k přenosnému počítači UFED přes USB rozhraní. Tyto speciální kabely jsou obsaženy v sadě UFED, pro různá mobilní zařízení se používají různé kabely, které jsou určitým způsobem upraveny. V tomto případě není nutné mít zapnuty režim Ladění USB. Poté dojde k zapnutí mobilního zařízení, avšak při zapnutí zařízení je nutné podržet určitou kombinaci tlačítek mobilního zařízení, která způsobí, že mobilní zařízení nabootuje do Recovery menu. V některých případech je možné, že bude UFED vyžadovat vložení prázdné paměťové karty do zkoumaného zařízení. Poté se již spustí samotný proces fyzické analýzy zařízení a získaná data jsou opět uloženy na paměťové médium připojenému k mobilnímu počítači UFED.

V případě provedení logické analýzy je UFED schopný získat podobná data, jako ostatní softwarové forenzní nástroje, avšak UFED podporuje větší množství mobilních zařízení. V případě fyzické analýzy mobilního zařízení bylo získáno velké množství dat i z doplňkových aplikací.

7.2.2. JTAG

JTAG je standard, který je využíván při výrobě mobilního zařízení ke komunikaci s procesorem přes speciální interface, to je využíváno pro testovaní mobilního zařízení při jeho výrobě. Interface pro připojení JTAGu se nachází na základní desce mobilního zařízení, pro jeho zpřístupnění je většinou nutné mobilní zařízení rozebrat. V některých případech není možné mobilní zařízení složit zpátky do původního stavu a zařízení je poté nepoužitelné. Proto se tato metoda označuje jako destruktivní. Někteří výrobci při výrobě odpojí interface pro připojení JTAGu po vyzkoušení funkčnosti mobilního zařízení. V takovém případě není možné JTAG použít. [39]

Při použití JTAGu dojde k připojení pinů na základní desce s RIFF boxem pomocí jednotlivých pinů. RIFF box je připojen k pracovní stanici pomocí USB kabelu a slouží k zprostředkování komunikace mezi pracovní stanicí a procesorem

mobilního zařízení. Při práci s JTAGem není využit žádný software z mobilního zařízení, proto zde není žádné omezení způsobené oprávněními v operačním systému Android, nebo nutnost zapnutého režimu Ladění USB. Díky tomu lze pomocí JTAGu snadno vytvořit kompletní obraz paměti mobilního zařízení, ze kterého je možné získat kompletní data mobilního zařízení například postupem stejným, jako je popsán v předchozích kapitolách.

RIFF Box je krabička sloužící ke komunikaci mezi pracovní stanicí a procesorem zkoumaného zařízení pomocí standardu JTAG. Ovládání mobilního zařízení pomocí RIFF Boxu z pracovní stanice je možné, díky aplikaci JTAG Manager, která slouží jako uživatelské rozhraní. Jejím prostřednictvím lze snadno získat obraz paměti mobilního zařízení. [40]

8. Vyhodnocení výsledků

8.1. Vyhodnocení navrženého postupu analýzy

Pomocí navrženého postupu forenzní analýzy mobilních zařízení s operačním systémem Android bylo možné získat velké množství dat ze zkoumaného mobilního zařízení. Ovšem i zde existují situace, které analýzu mobilního zařízení zkomplikují, nebo naprosto znemožní. Jak bylo rozebráno v této práci, největší komplikací může být zámek obrazovky, který může analýzu zařízení tímto postupem zcela znemožnit. Další komplikací mohou být uživatelská oprávnění v operačním systému a systém samotný.

Výše popsaným postupem bylo možné z mobilního zařízení získat základní informace o mobilním zařízení, data běžných aplikací pro mobilní zařízení, jako jsou výpisy hovorů, SMS a MMS zprávy, kontakty uložené v mobilním zařízení a data z kalendáře. Dále bylo možné získat data doplňkových aplikací, mezi které patří například Facebook, Messenger, ICQ, Skype, Viber, Gmail, údaje o poloze z aplikace Mapy a například historii webového prohlížeče. Tyto data bylo možné získat z vytvořených obrazů paměti, v těchto obrazech by se nacházely data všech aplikací nainstalovaných v mobilním zařízení. Díky tomu lze pomocí tohoto postupu získat data z jakékoli aplikace nainstalované v mobilním zařízení, bez ohledu na strukturu jejích dat. Další výhodou, kterou tento postup přináší, je možnost získání smazaných dat. Tyto data lze získat z obrazů paměti mobilního zařízení. Proto se tento postup označuje jako fyzická analýza mobilních zařízení.

Jako nevýhoda navrženého postupu se dá označit jeho samotné provedení. Protože při provedení tohoto postupu dochází k práci s operačním systémem přímo v mobilním zařízení a může dojít k úpravě dat, či přepsání smazaných dat při pokusu o prolomení zámku obrazovky, nebo získávání ROOT oprávnění. Je tato tento postup označován jako částečně destruktivní. Data, která mohu být změněna, nebo přepsána při prolamování zámku obrazovky, nebo zpřístupnění ROOT oprávnění, jsou uložena v systémových oddílech paměti. To znamená, že jsou tyto data oddělena od uživatelských dat, které jsou primárním cílem této analýzy.

8.2. Porovnání s komerčními forenzními nástroji

Aby bylo možné demonstrovat účinnost navrženého postupu, byly testované mobilní zařízení analyzovány i pomocí komerčních nástrojů. V případě softwarových forenzních nástrojů byly ze zkoumaných mobilních zařízení získány pouze základní informace o mobilním zařízení, kontakty, výpisy hovorů, SMS a MMS zprávy a data z kalendáře mobilního zařízení. Pouze Oxygen Forensic byl schopný získat informace o několika doplňkových aplikacích. Ovšem bylo nutné, aby byl v mobilním zařízení zapnutý režim Ladění USB. Bez toho jsou softwarové forenzní nástroje zcela neúčinné.

V případě hardwarových forenzních nástrojů byla úspěšnost získávání dat vyšší, než u softwarových nástrojů. UFED byl schopen provést s některými mobilními zařízeními fyzickou analýzu. Díky tomu bylo z některých mobilních zařízení získat kompletní data. Tyto softwarové a hardwarové forenzní nástroje provádí nedestruktivní analýzu mobilních zařízení.

Navržený postup umožnil získat ze zkoumaných mobilních zařízení více dat než komerční forenzní nástroje. Fyzickou analýzu bylo díky němu možné provést i u mobilních zařízení, u kterých to nebylo možné pomocí nástroje UFED. Proto jeho jasnou výhodou je schopnost získat data z mobilního zařízení. Jeho nevýhodou je však náročnější provedení jak po časové, tak po technické stránce. Pomocí navrženého postupu není v určitých případech možné provedení analýzy zařízení, ovšem v těchto případech není možné použít ani ostatní forenzní nástroje. V takovýchto případech existuje poslední možnost a tou je použití JTAGu. Bohužel použití JTAGu je destruktivní metoda, proto by jeho použití mělo být až poslední možností.

9. Závěr

V této diplomové práci je navržen způsob, pomocí kterého je možné provést plnohodnotnou fyzickou analýzu mobilního zařízení s operačním systémem Android. V této metodě jsou popsány možnosti a omezení analýzy mobilního zařízení i s jejich dopady na zkoumané zařízení. Dále jsou v této práci zmapována místa v paměti, kde jsou uloženy data o mobilním zařízení a jeho aplikacích a také jejich formát. Tento postup byl testován na několika mobilních zařízeních a výsledky analýz byly porovnány s výsledky analýz pomocí komerčních forenzních nástrojů.

Postup pro forenzní analýzu mobilních zařízení popsaný v této práci má oproti komerčním forenzním nástrojům své výhody, ale i nevýhody. Je možné ho klasifikovat, jako alternativu k současným forenzním nástrojům. Díky úspěšnému návrhu tohoto postupu je možné považovat cíle této diplomové práce za splněné.

10. Použitá literatura

[1] IDC: Analyze the future. IDC CORPORATE USA. *Smartphone OS Market Share, Q4 2014* [online]. 2014 [cit. 2015-04-09]. Dostupné z: http://www.idc.com/prodserv/smartphone-os-market-share.jsp

[2] RISK ANALYSIS CONSULTANTS. *Forenzní zkoumání digitálních důkazů: Příručka vyšetřovatele*. Praha, 2005. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/ZU-FA/$FILE/Guide%20051230.pdf

[3] Dočasné soubory systému windows. MICROSOFT. *Microsoft: Pomoc a podpora* [online]. 2014, 2015-05-22 [cit. 2015-04-10]. Dostupné z: https://support.microsoft.com/cs-cz/kb/92635/cs

[4] DVOŘÁK, Jakub. Nenechte se šmírovat. Data z disku nestačí smazat, musíte je skartovat. *Technet.cz* [online]. 2013 [cit. 2015-04-10]. Dostupné z: http://technet.idnes.cz/jak-skartovat-data-0nk-/software.aspx?c=A130118_185552_software_dvr

[5] HOOG, Andrew. Android forensics: investigation, analysis, and mobile security for Google Android. Amsterdam: Elsevier, c2011, xix, 372 s. ISBN 978-1-59749-651-3.

[6] KADLEC, Josef. Forenzní analýza (2). In: *ROOT.cz* [online]. 2005 [cit. 2016-03-14]. Dostupné z: http://www.root.cz/clanky/forenzni-analyza-2/

[7] Developers: Platform versions. *Developers* [online]. 2016 [cit. 2016-03-19]. Dostupné z: http://developer.android.com/about/dashboards/index.html

[8] ORF, Darren. A History of Android, From Cupcake to Marshmallow. In: *GIZMODO* [online]. 2015 [cit. 2016-03-19]. Dostupné z: http://gizmodo.com/a-history-of-android-from-cupcake-to-m_____-1707432419

[9] KILIÁN, Karel. Grafická nadstavba, nebo čistý Android? In: *Svět Androida* [online]. 2015 [cit. 2016-03-19]. Dostupné z: http://www.svetandroida.cz/vikendova-hlasovacka-nadstavba-201510

[10] An Overview of the Android Architecture. In: *Techotopia* [online]. 2016 [cit. 2016-03-19]. Dostupné z: http://www.techotopia.com/index.php/An_Overview_of_the_Android_Architecture

[11] SHIU, John P. Android Architecture. In: *Eazy tutz* [online]. 2015 [cit. 2016-03-19]. Dostupné z: http://www.eazytutz.com/android/android-architecture/

[12] SCHIESSER, Tim. Guide to smartphone hardware (3/7): Memory and Storage. In: *Neowin* [online]. 2012 [cit. 2016-03-20]. Dostupné z: http://www.neowin.net/news/guide-to-smartphone-hardware-37-memory-and-storage

[13] RYAN, Paul. Ext4 filesystem hits Android, no need to fear data loss. In: *Ars technica* [online]. 2010 [cit. 2016-03-20]. Dostupné z: http://arstechnica.com/information-technology/2010/12/ext4-filesystem-hits-android-no-need-to-fear-data-loss/

[14] QUICK, Darren a Mohammed ALZAABI. Forensic analysis of the android file system YAFFS2. *Australian Digital Forensics Conference* [online]. 2011, , 11 [cit. 2016-03-20]. Dostupné z: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1100&context=adf

[15] WEINBRENNER, Jan. Pohled na NAND FLASH paměti. *Součástky*. 2010, **2010**(Listopad/Prosinec), 2.

[16] TRANSCEND. *TS256M~2GUSD: microSD memory card* [online]. , 25 [cit. 2016-03-20]. Dostupné z: http://www.mikroe.com/downloads/get/1624/microsd_card_spec.pdf

[17] MATTIAS. The Android boot process from power on. In: *Android Blog* [online]. 2009 [cit. 2016-03-20]. Dostupné z: http://www.androidenea.com/2009/06/android-boot-process-from-power-on.html

[18] *Google Play* [online]. Google, 2016 [cit. 2016-03-25]. Dostupné z: https://play.google.com/store

[19] KOŽUŠNÍK, Dušan. Forenzní analýza mobilních telefonů: Není telefon jako telefon. In: *Computer World*[online]. 2012 [cit. 2016-03-25]. Dostupné z: http://computerworld.cz/securityworld/forenzni-analyza-mobilnich-telefonu-neni-telefon-jako-telefon-48872

[20] Disklabs Faraday Bags. In: *TEEL Technologies* [online]. 2015 [cit. 2016-03-25]. Dostupné z: http://www.teeltech.com/mobile-device-forensics-equipment/disklabs-faraday-bags/

[21] Android Debug Bridge. *Android Developers* [online]. 2016 [cit. 2016-03-26]. Dostupné z: http://developer.android.com/tools/help/adb.html

[22] *Java SE downloads* [online]. Oracle, 2016 [cit. 2016-03-26]. Dostupné z: http://www.oracle.com/technetwork/java/javase/downloads/index.html

[23] *SDK Tools only* [online]. Android Developers, 2016 [cit. 2016-03-26]. Dostupné z: http://developer.android.com/sdk/index.html

[24] *Enabling adb Debugging* [online]. Android Developers, 2016 [cit. 2016-03-26]. Dostupné z: http://developer.android.com/tools/help/adb.html#Enabling

[25] BENNETT, Dave. Bypass Android Lock screen. In: *Dave Bennett* [online]. 2015 [cit. 2016-03-27]. Dostupné z: http://www.davebennett.tech/bypass-android-lock-screen/

[26] DALLAS, Thomas. 7 Ways to Bypass Android's Secured Lock Screen. In: *Wonder How To* [online]. 2015 [cit. 2016-03-27]. Dostupné z: http://android.wonderhowto.com/how-to/7-ways-bypass-androids-secured-lock-screen-0165540/

[27] SAMMES, T a B JENKINSON. *Forensic Computing*. London: Springer London, 2007. ISBN 978-1-84628-397-0.

[28] WHITSON, Gordon. Everything You Need to Know About Rooting Your Android Phone. In: *Lifehacker*[online]. 2013 [cit. 2016-03-28]. Dostupné z: http://lifehacker.com/5789397/the-always-up-to-date-guide-to-rooting-any-android-phone

[29] MATIX2267. How does su work on android? And what are the pre-requisites for it to work? What is rooting on Android? In: *Stack overflow* [online]. 2012 [cit. 2016-03-28]. Dostupné z: http://stackoverflow.com/questions/10028032/how-does-su-work-on-android-and-what-are-the-pre-requisites-for-it-to-work-wha

[30] *Forum XDA Developers* [online]. 2016 [cit. 2016-03-28]. Dostupné z: http://forum.xda-developers.com/

[31] [DEV][THE S-OFF CAMPAIGN] We need electrical engineers & experts in JTAG, OpenOCD!. In: *Forum XDA Developers* [online]. 2012 [cit. 2016-03-28]. Dostupné z: http://forum.xda-developers.com/showthread.php?p=23222889#post23222889

[32] Download BusyBox 40 APK from APK4Fun Server. *APK4Fun* [online]. 2016 [cit. 2016-03-28]. Dostupné z: http://www.apk4fun.com/int/6139/apk4fun/

[33] SSH – bezpečné používání vzdáleného počítače a kopírování dat. In: *Dsl.cz* [online]. 2015 [cit. 2016-04-02]. Dostupné z: http://www.dsl.cz/jak-na-to/jak-na-ssh

[34] MUSTANGTIM49. Yaffey for All Your YAFFS2 Needs. In: *XDA Developers* [online]. 2012 [cit. 2016-04-03]. Dostupné z: http://www.xda-developers.com/yaffey-for-all-your-yaffs2-needs/

[35] File carving. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2015 [cit. 2016-04-03]. Dostupné z: https://en.wikipedia.org/wiki/File_carving

[36] About SQLite. *SQLite* [online]. [cit. 2016-04-10]. Dostupné z: https://www.sqlite.org/about.html

[37] KOČÍ, Michal. Co je XML? In: *Interval.cz* [online]. 2000 [cit. 2016-04-10]. Dostupné z: https://www.interval.cz/clanky/co-je-xml/

[38] *Epoch converter* [online]. 2016 [cit. 2016-04-12]. Dostupné z: http://www.epochconverter.com/

[39] TAMMA, Rohit a Donnie TINDALL. *Learning Android Forensic*. Birmingham: Packt Publishing Ltd., 2015. ISBN 978-1-78217-457-8.

[40] *RIFF Box* [online]. 2016 [cit. 2016-04-17]. Dostupné z: http://www.riffbox.org/

11. Přílohy

[1] DVD obsahující vybrané obrazy pamětí a jejich popis, získané z testovaných mobilních zařízení a vybrané soubory aplikací získané z těchto obrazů.