Jihočeská univerzita

Přírodovědecká fakulta

Ústav aplikované informatiky

Forenzní analýza mobilních zařízení s OS Android

Autor: Vojtěch Novotný

Vedoucí práce: Ing. Jaroslav Kothánek, Ph.D

České Budějovice 2013

Novotný, V., 2013: Forenzní analýza mobilních zařízení s OS Android. [Forensic analysis of mobile devices running Android. Bc. Thesis, in Czech.] – 39 p., Faculty of Science, University of South Bohemia, České Budějovice, Czech Republic.

Název

Forenzní analýza mobilních zařízení s OS Android

Abstract

Bakalářská práce „Forenzní analýza mobilních zařízení s OS Android“ se zabývá problematikou forenzní analýzy mobilních zařízení s OS Android. V této práci bude popsán OS Android a specifika zařízení s tímto operačním systémem. Dále budou popsány možnosti a omezení, které mají tyto zařízení ve vztahu k forenzní analýze. Tyto zjištění budou následně demonstrovány na fyzickém zařízení a na jejich základě budou navrženy optimální postupy pro forenzní analýzu těchto zařízení a zjištěné informace budou vyhodnoceny.

Klíčová slova

Forenzní analýza, Android, YAFFS2

Title

Forensic analysis of mobile devices running Android

Summary

Thesis "Forensic analysis of mobile devices running Android" deals with the forensic analysis of mobile devices running Android. In this work will be described Android OS and the specifics of devices with this operating system. Next will be described possibilities and the limitations that have these facilities in relation to forensic analysis. These findings will then be demonstrated on the physical device and based on this practices will be designed optimal procedures for forensic analysis of these devices and the findings will be evaluated.

Key worlds

Forensic analysis, Android, YAFFS2

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

České Budějovice 20. Dubna 2013

……

podpis

Poděkování

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

Obsah

Seznam obrázků

1. Úvod a cíle práce

1.1 Úvod

V dnešní době vývoj mobilních zařízení postupuje neustále kupředu, díky tomu tyto zařízení přináší čím dál větší možnosti pro uživatele a přibližují se klasickým počítačům. Proto mohou tyto zařízení obsahovat důležité informace, využitelné jako důkazy pro usvědčení z páchání trestné činnosti, a proto je potřeba čím dál tím častěji provést forenzní analýzu těchto zařízení.

Podle statistiky[1] se za rok 2012 prodalo 700,1 milionů smartphonů, z toho 64,8 % bylo s operačním systémem Android, 19,4% s operačním systémem iOS a 12,2 % zabrali ostatní operační systémy. Z toho vyplívá, že OS Android je v současné době nejrozšířenější operační systém používaný v mobilních zařízeních.

Tato práce se zabývá forenzní analýzou zařízení s OS Android, obsahuje popis možností, které lze při této činnosti využít, jejich dopad na zařízení a také je zde navržen optimální postup při provádění této činnosti, který je otestován na skutečném zařízení.

1.2 Cíle práce

- Popis OS Android
- Popis možností a omezení forenzní analýzy mobilních zařízení s OS Android
- Návrh možností forenzní analýzy mobilních zařízení s OS Android
- Vyhodnocení SW použitého při forenzní analýze mobilních zařízení s OS Android
- Navržení optimálního řešení forenzní analýzy mobilních zařízení s OS Android

2. Forenzní analýza

Forenzní analýza, respektive její podmnožina forenzní analýza digitálních dat je vědní obor zabývající se technikami získávání dat z digitálních zařízení. Tyto techniky podléhají přísným kritériím, díky kterým lze získané informace využít jako důkazní materiál například při vyšetřování trestných činů. Forenzní analýza má několik částí. První je izolování a ochrana důkazů, při tom je důležité, aby nedošlo ke změně, nebo poškození dat. Následuje Sběr důkazů, ten obnáší získání z média, například z obrazu disku, vytvořeného v předchozím kroku. Následuje identifikace důkazů, při této činnosti se vyhodnocují získané informace. Nakonec se provede interpretace informací, při které je nutné správně a srozumitelně vyložit získané informace. Neméně důležitou součástí forenzní analýzy je dokumentace. Vždy je třeba pečlivě zadokumentovat vše, co bylo v rámci forenzní analýzy provedeno.[2]

Jak bylo zmíněno, při forenzní analýze je důležité zachovat zkoumané médium v nepozměněném stavu a vyhnout se jeho jakékoliv úpravě, nebo poškození. Při forenzní analýze mobilních zařízení s OS Android nastává případ, kdy lze bez zásahů do zařízení provést pouze omezenou analýzu. Proto je důležité minimalizovat jakýkoliv dopad na zařízení, který by tato analýza mohla mít a po jejím skončení ho vrátit v původním stavu.

3. OS Android

Android je operační systém určený převážně pro mobilní zařízení, jako jsou smartphony a tablety. V současné době se Android rozšiřuje i do jiných zařízení, ale jeho hlavní zaměření jsou stále na mobilní zařízení, u kterých je to v současné době nejrozšířenější operační systém.

Společnost Google koupila v roce 2005 malou společnost Android Inc., která položila základ tohoto operačního systému. V listopadu roku 2007 Google potvrdil vstup na pole mobilních zařízení a byla založena Open Handset Alliance, pro podporu nové platformy, která měla 34 členů. Také byla vydána první verze Android Software Development Kit (SDK) pro vývojáře. V srpnu roku 2008 byl představen Android Market (nyní Google Play) a také byl Android uvolněn jako open-source a jeho kompletní kód byl dostupný všem, v září téhož roku byl uveden na trh první mobilní telefon s OS Android T-Mobile G1.[3]

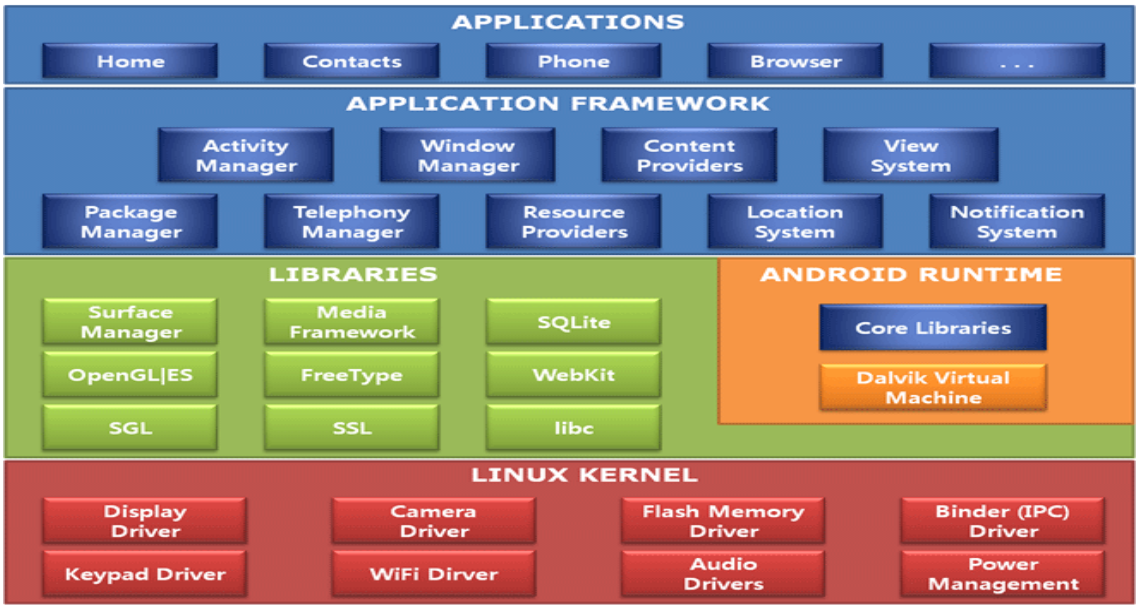
3.1 Struktura OS Android

„Android v podstatě běží na DVM (Dalvik Virtual Machine), který je pomocí Android runtime spojen s Linuxovým jádrem.“[4]

Android se skládá z pěti hlavních částí, jejichž rozložení je zobrazeno níže na obr1. Každá z těchto částí je nezbytná pro chod systému a jejich význam je popsán níže.

3.1.1 Applications

Tato úroveň operačního systému je určena pro aplikace, které jsou určeny uživatelům, jako jsou například kontakty, webový prohlížeč, kalendář, a další takové aplikace. Všechny tyto aplikace jsou napsány pomocí programovacího jazyku Java.[5]



Obr1. Struktura OS Android[4]

3.1.2 Application framework

„Tyto frameworky jsou používány k vytvoření aplikací v Androidu“[5]

Aplikační framework poskytuje všechny druhy API pro vývoj plnohodnotné aplikace pro platformu Android. Pomocí rozhraní API v této oblasti umožňuje vyjádřit tlačítka a text na obrazovce nebo využití dat z jiných aplikací, jako jsou obrázky a znakové řetězce. Také je možné spravovat životní cykly aplikací.[4]

3.1.3 Libraries

Tato část nabízí různé C/C++ knihovny, které mohou být použity pro Android. Všechny knihovny v této oblasti mohou být použity vývojáři prostřednictvím Application framework. Standardní C systémové knihovny založené na BSD (Berkeley Software Distribution) jsou přepracovány tak, aby byly vhodné pro zařízení založeném na Linuxu. Media library založená na OpenCore z PacketVideo podporuje MPEG4, H.264, MP3, AAC, AMR, JPG a PNG. Surface manager podporuje 2D a 3D grafiku, zatímco WebKit podporuje funkce prohlížeče. SQLite je k dispozici i jako databázový stroj, který může být používán aplikacemi.[4]

3.1.4 Android runtime

Android obsahuje sadu základních knihoven, které poskytují většinu funkcí, které jsou dostupné v základních knihovnách programovacího jazyku Java.[4]

Každá aplikace v Androidu běží ve vlastním procesu, s vlastní instancí Dalvik virval machine (DVM). Dalvik byl navržen tak, že na jednom přístroji může efektivne běžet více virtuálních počítačů. DVM spustí soubory v Dalvik Executable (.Dex) formátu, který je optimalizován pro minimální nároky na paměť. VM je register-based, a používá třídy kompilované Java langure compiler, které byly transformované do formátu .Dex pomocí zabudovaného "dx" nástroje.[5]

Dalvik VM se opírá o základní funkce Linuxového jádra, jako je správa vláken a nízko úrovňová správa paměti.

3.1.5 Linux kernel

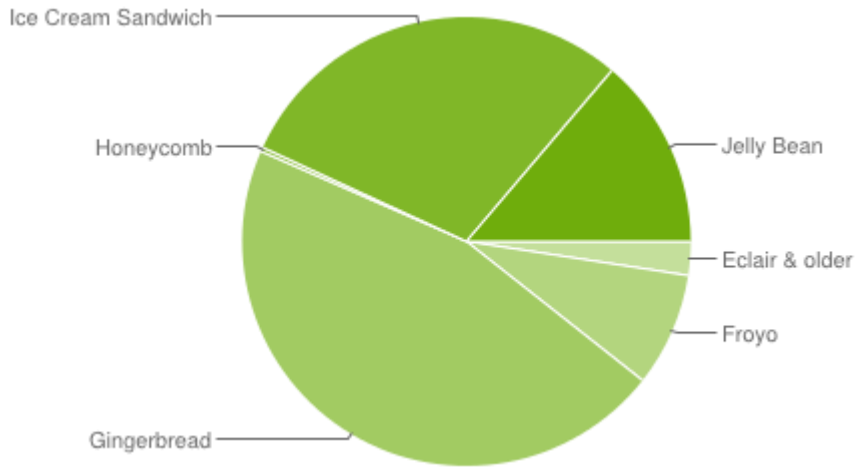
„Android je vyvinut na základě Linuxového jádra 2.6, které poskytuje vysokou bezpečnost, řízení paměti a procesů, síťovou vrstvu a různé ovladače.“[4]

Linuxové jádro je abstraktní vrstva mezi hardwarem a softwarem, která zajišťuje funkční spojení těchto dvou částí. Díky použití Linuxového jádra má Android s Linuxem mnoho společného, díky tomu lze používat v Androidu Linuxové příkazy, jak bude přiblíženo později.

3.2 Verze systému Android

První verze Androidu byla vydána v roce 2008, od té doby jeho vývoj neustále pokračuje kupředu. V průběhu let vyšly verze, které se rozšířily ve velkém počtu, ale také verze které nikdy výrobci zařízení nepoužily, avšak i tyto verze se mohou objevit v zařízeních zkušenějších uživatelů, kteří si je sami nainstalovali. Avšak takový zásah do zařízení je proti záručním podmínkám výrobců a tak takovýchto zařízení není mnoho. Zajímavostí je, že vývojáři pojmenovávají jednotlivé verze podle jmen zákusků. Zde je stručný přehled verzí, sestavený z uvedených zdrojů.[6][7]

- Android 1.0 (Apple pie) září 2008
- Android 1.5 (Cupcake) duben 2009
- Android 1.6 (Donut) září 2009
- Android 2.0 – 2.1 (Eclair) říjen 2009
- Android 2.2.* (Froyo) květen 2010
- Android 2.3.* (Gingerbread) prosinec 2010
- Android 3.* (Honeycomb) únor 2011
- Android 4.0.* (Ice cream sandwich) říjen 2011
- Android 4.1.* (Jelly bean) červenec 2012
- Android 4.2.* (Jelly bean) listopad 2012



Obr2. Podíl verzí OS Android[8]

Podle statistiky[8] jsou nejvíce rozšířené dvě verze Gingerbread 45,4 % a Ice cream sandwich 29 %, jak je vidět na Obr2 níže, tyto dvě verze zaujímají v současné době většinový podíl mezi verzemi. Jelly bean je teprve na vzestupu a podíl ostatních verzí se stále zmenšuje. Verzi Honeycomb výrobci nikdy nepoužili ve svých zařízeních a proto se rozšířila pouze mezi pár uživatelů, kteří si jí sami nainstalovali.

3.3 Druhy pamětí

Mobilní zařízení mají obvykle dva druhy paměťových úložišť. Vnitřní, které je tvořeno NAND Flash čipem a vnější, které představuje SD karta. Existují výjimky, které mají pouze vnitřní paměť a nemají slot pro SD kartu. Příkladem takového zařízení je HTC One, který má pouze vnitřní paměť o velikosti 32/64 GiB.

3.3.1 Vnitřní paměť

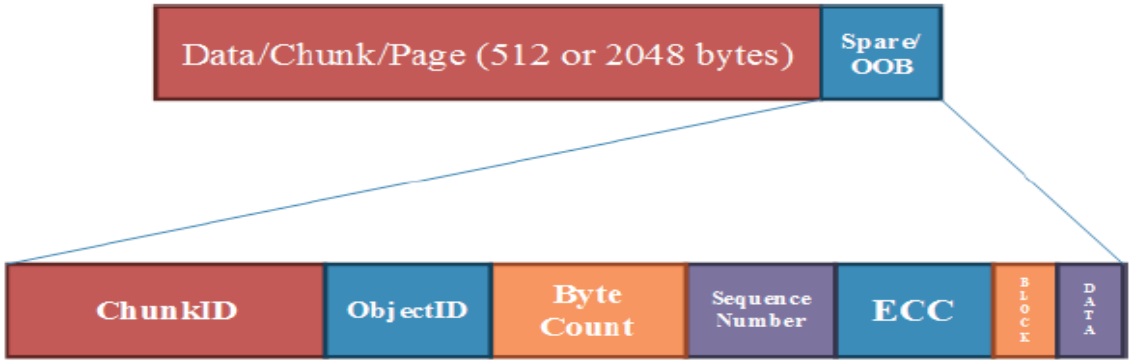
Jako vnitřní paměť se používají čipy typu NAND Flash, tyto čipy jsou typu nonvolatile, to znamená, že po odpojení napájení, data zůstanou uložena na čipu. Paměť obsahuje velké množství buněk, do kterých je pomocí elektrického napětí možno zapisovat, nebo je mazat. Tyto čipy se využívají v mnoha dalších zařízeních, jako jsou SSD disky, flash disky, mp3 přehrávače a podobná zařízení.[9]

3.3.1.1 YAFFS2

YAFFS (Yet Another Flash File Systém) byl vyvinut pro NAND Flash paměti a je používán ve vnitřní paměti mobilních zařízení s OS Android. YAFFS1 a YAFFS2 se od sebe liší velikostí chunku, kdy YAFFS2 ho má větší. V dnešní době se používá výhradně YAFFS2.

NAND Flash paměť je rozdělena na bloky a každý blok obsahuje tzv. chunky. Každý chunk je veliký 2048 B + 64 B OOB oblasti. Každý blok obsahuje 64 chunků. Zapisovat lze do jednotlivých chunků nezávisle na ostatních v bloku, ale při mazání se maže vždy celý blok. Chunky mohou obsahovat buď data souboru, nebo hlavičku objektu.[10]

OOB (Out Of Band) je část chunku, ve které jsou uchovávány informace o chunku viz Obr3, jako jsou ID chunku, ID objektu, počet bytů, pořadové číslo, ECC.[10] Tato oblast v sobě ukrývá zajímavé informace a může mít pro výsledek forenzní analýzy značný přínos.



Obr3. Chunk a obsah OOB[9]

3.3.1.2 Ext4

V současné době většina výrobců začala využívat souborový systém Ext4 namísto YAFFS2. Použití Ext4 přináší výhody, pro práci s pamětí. Ovšem tato práce není zaměřena na jejich porovnání, proto zde tato problematika nebude více rozebrána.

Souborový systém Ext4 je evolucí souborového systému Ext, který je využíván jako hlavní souborový systém operačního systému Linux. Ext4 přišel opět s novými vylepšeními oproti předchozí verzi Ext3. Jednou z nejdůležitějších novinek jsou extenty, to je vlastnost, která dokáže namapovat velké množství bloku disku na jeden ukazatel. To má velký vliv na zvýšení výkonu.[11]

Ext4 má samozřejmě mnohem více zajímavých vlastností a vylepšení o kterých bylo napsáno velké množství informací, avšak z pohledu této práce není třeba je detailněji rozebírat.

3.3.2 Vnější paměť

„Secure Digital (SD) karta je miniaturní paměťová karta použita pro úložiště přenositelné mezi různými zařízeními, jako jsou automobilové navigační systémy,

mobilní telefony, čtečky elektronických knih, PDA, smartphony, digitální fotoaparáty, hudební přehrávače, videokamery a osobní počítače. Karta SD umožňuje vysokou rychlost přenosu dat a nízkou náročnost na baterii, oboje důležité pro přenosná zařízení. Využívá flash paměť k poskytnutí elektricky nezávislého úložiště, což znamená, že napájecí zdroj není zapotřebí pro uchovávání uložených dat.“[12]

SD karta se u mobilních zařízení nejčastěji používá pro ukládání obrázků, audio a video souborů, elektronických dokumentů a dalších věcí co jen uživatele napadnou. Android umožňuje u některých aplikací přesunout jejich data na SD kartu, kvůli úspoře místa ve vnitřní paměti. Proto může být SD karta zdrojem velice zajímavých informací.

SD karty obvykle využívají souborový systém VFAT (FAT32), avšak je možné je přeformátovat na jiný souborový systém. Díky tomu, že je Android postaven na Linuxovém jádře, podporuje stejně jako Linux mnoho typů souborových systémů, mezi nejpoužívanější patří:

- VFAT
- Ext2
- Ext3
- Ext4

3.4 ADB

Android Debug Bridge (ADB) je nástroj který umožňuje práci s terminálem Android zařízení připojeného k počítači, přes příkazovou řádku počítače. ADB pracuje na principu klient-server na portu 5037 a zahrnuje tři komponenty.[13] Díky tomu je ADB velice užitečný při forenzní analýze.

- Klient – Běží na počítači a jeho prostřednictvím se zadávají příkazy, které se mají v prostředí Androidu provést.
- Server – Běží na počítači jako proces v pozadí a zprostředkovává komunikaci mezi klientem a ADB deamonem.
- Deamon – Běží jako proces v pozadí na Androidím zařízení.

Na webu androidaplikace.cz je zveřejněn návod jak zprovoznit ADB v operačním systému Windows.[14]

Nejdříve je třeba nainstalovat JDK (Java Development Kit), který obsahuje soubor nástrojů pro vývoj aplikací v jazyce Java.

Poté je třeba nainstalovat Android SDK, který obsahuje soubor nástrojů pro vývoj aplikací pro Android.

Následně pravým kliknutím na Tento počítač → Vlastnosti → Upřesnit → Proměnné prostředí, tam je nutné v položce PATH změnit cestu ke složce platform-tools, která je umístěna tam kde se zvolila cesta při instalaci Android SDK, před touto cestou musí být středník (např. ;C:\Program Files (x86)\Android\android-sdk\platform-tools). Poté už je možné pracovat s ADB pomocí příkazové řádky počítače.

Při připojování zařízení je důležité, aby bylo zařízení připojeno v režimu ladění přes USB. Nastaví se následovně v prostředí Androidu Nastavení → Aplikace → Vývoj → Ladění USB (povolit). Tyto názvy se mohou mírně lišit u různých zařízení od různých výrobců.

Pokud nastanou problémy s připojením přes ADB, je to nejčastěji chyba špatně nainstalovaných ovladačů k mobilnímu zařízení a je třeba je přeinstalovat.

4. Možnosti a omezení forenzní analýzy

Díky tomu, že je OS Android postaven na Linuxovém jádře, má s tímto operačním systémem hodně podobných vlastností. Mezi tyto vlastnosti patří politika práv uživatelů. Mobilní zařízení s OS Android mohou mít dva druhy práv, první jsou takzvaně „práva běžného uživatele“, tyto práva znamenají pro uživatele omezený přístup k některým částem operačního systému a znemožnění využití některých funkcí operačního systému, nebo aplikací, které právě tyto části využívají. Druhou možností jsou takzvaně „ROOT práva“, která umožňují uživateli, nebo aplikacím neomezený přístup ke všem částem operačního systému.

Výrobci u nových zařízení nastavují omezená práva, která většinu uživatelů nijak neomezují při používání těchto zařízení. Ovšem někteří uživatelé si na svém zařízení provedou ROOT úpravu, díky které získají ROOT oprávnění, aby mohli využívat pokročilejší aplikace, které toto oprávnění potřebují ke správné funkčnosti. Proto je třeba při forenzní analýze brát v potaz obě tyto možnosti.

4.1 Práva běžného uživatele

Kvůli tomu, že je vnitřní paměť připájena uvnitř zařízení, není možné ji vyjmout, aniž by došlo k poškození zařízení. Proto je nutné s touto pamětí pracovat prostřednictvím operačního systému tohoto zařízení. Bohužel toto oprávnění neumožňuje vytvořit obraz této paměti, který by se využil k analýze.

Proto u zařízení s těmito právy lze využít buď specializovaný software, který z něj vytěží omezené množství informací anebo pomocí ADB procházet adresáře přímo v zařízení a případně pořídit jejich kopii. Toto procházení je ovšem omezeno uživatelskými právy. U těchto metod není možné analyzovat smazané soubory.

Analýzu paměťové SD karty lze uskutečnit při analýze specializovaným softwarem anebo opět pomocí ADB. Avšak tyto metody neumožňují analýzu smazaných souborů. Další způsob jak analyzovat SD kartu, je vyjmout ji ze zařízení a vytvořit její obraz, který lze poté analyzovat a lze z něj získat smazané soubory, které mohou obsahovat zajímavé informace.

4.2 Práva ROOT

ROOT oprávnění přináší daleko větší možnosti pro forenzní analýzu. Umožňuje přístup do všech částí kořenového adresáře, díky tomu lze pomocí ADB jeho neomezené procházení a vytvoření jeho kopie, kterou lze poté analyzovat.

Specializovaný software dokáže díky tomuto oprávnění vytěžit ze zařízení veškeré informace, kterých je schopen.

Ovšem největší výhodou je možnost vytvoření obrazu vnitřní paměti, který se dá využít k analýze smazaných souborů.

Při analýze paměťové SD karty nepřináší toto oprávnění žádné další možnosti a výhody oproti zařízení s běžnými právy.

5. Forenzní analýza s právy běžného uživatele

Jak již bylo zmíněno dříve, forenzní analýza s tímto druhem uživatelských práv má omezené možnosti. Přesto lze i v tomto případě získat ze zařízení spoustu informací, které mohou být užitečné.

5.1 ADB

Pomocí ADB lze v omezené míře procházet adresářovou strukturu zařízení a požadované soubory lze ze zařízení zkopírovat pomocí `adb pull` do počítače. Takto se dá získat například soubor s kontakty, který je poté možno prozkoumat například pomocí SQLite Database Browseru. Bohužel tento způsob je časově náročný a neefektivní.

5.2 Oxygen forensic Suite 2013

„Oxygen Forensic Suite 2013 je forenzní software, který je účinnější, než standardní logické analýzy mobilních telefonů, smartphonů a tabletů. Použitím pokročilých proprietárních protokolů umožňuje Oxygen Forensic Suite 2013 extrahovat mnohem více dat, než obvykle umožňují ostatní logické forenzní nástroje, zejména pro smartphony.“[15]

Oxygen Forensic Suite 2013 je v současné době jeden z nejlepších forenzních nástrojů pro mobilní zařízení. Práce s ním je velmi jednoduchá, po instalaci programu stačí připojit mobilní zařízení k počítači, musí být povolen režim Ladění USB, v programu se zvolí možnost připojení zařízení přes USB a program automaticky identifikuje zařízení. Poté lze zahájit analýzu. OF Suit 2013 nainstaluje do zařízení program OxyAgent, prostřednictvím kterého provádí analýzu zařízení. Po dokončení analýzy je program OxyAgent automaticky odstraněn ze zařízení a OF Suite 2013 zobrazí informace zjištěné analýzou zařízení. Následně je schopný vyexportovat zjištěné informace do souboru s možností volby jeho formátu, například pdf, nebo html.

U testovaného zařízení Sony Ericsson sk17i s plně zaplněnou 2 GiB SD kartou tento proces trval zhruba deset hodin. OF Suite 2013 z tohoto zařízení dokázal vyextrahovat následující informace:

- Základní informace o zařízení
- Kontakty
- SMS zprávy
- MMS zprávy
- Výpis hovorů
- Data z kalendáře
- Data o některých aplikacích
- Videa, obrázky, zvukové stopy uložené na SD kartě
- Kompletní adresářovou strukturu SD karty

5.3 MOBILedit! Forensic

„MOBILedit! Forensic je světově nejdůvěryhodnější vyšetřování nástroj telefonů. Vysoce hodnocený Národním institutem standardů a technologií, MOBILedit! Forensic je primární vyšetřování nástroj mobilních zařízení používaný ve více než 70 zemích. Stačí připojit telefon a MOBILedit! Forensic extrahuje veškerý obsah a generuje forenzní zprávu připravenou pro prezentaci v soudní síni. Tyto nepopiratelně bezchybné zprávy slouží ve stovkách soudních síních každý den.“[16]

MOBILEdit! Forensic je forenzní software, určený pro analýzu mobilních zařízení. Jeho použití je jednoduché, stačí nainstalovat MOBILEdit! Forensic do počítače a do zkoumaného zařízení nainstalovat ME! Forensic Connector. Po připojení zařízení k počítači přes USB kabel, MOBILEdit! Forensic sám načte zařízení a umožní jeho okamžité prohlížení. MOBILEdit! Forensic dokáže ze zařízení získat:

- Základní informace o zařízení
- Kontakty
- Výpis hovorů
- SMS zprávy
- MMS zprávy
- Data z kalendáře
- Adresářovou strukturu SD karty

- Adresářovou strukturu vnitřní paměti s omezeným přístupem, daným uživatelskými právy

5.4 Analýza SD karty

Paměťovou SD kartu lze ze zařízení vyjmout bez jakýchkoliv potíží, díky tomu je její analýza velice jednoduchá.

Po vyjmutí SD karty je třeba vytvořit její obraz, který bude následně využit pro analýzu. K tomu se nejlépe hodí využít Linuxového příkazu `dd`. Vhodné je použít Linuxový operační systém DEFT, který je uzpůsoben pro potřeby forenzní analýzy. Příkazem:

```
dd if=/dev/mmcblk0p1 of=obrazKarty.dd
conv=noerror,notrunc,sync
```

Tento příkaz vytvoří obraz SD karty. If v příkaze určuje cestu ke kartě, ze které se má obraz vytvořit. Of určuje, kde bude obraz uložen. Parametry příkazu `dd` upřesňují vlastnosti příkazu, tyto parametry jsou volitelné a mohou být vynechány. Vytvoření Obrazu SD karty o velikosti 2 GiB trvalo pouze několik minut.

Pro následnou analýzu obrazu SD karty lze poté využít specializovaný software, který z obrazu dokáže sestavit adresářovou strukturu a získat smazané soubory viz Obr4. Mezi takovéto softwary patří například Autopsy, nebo FTK Imager.

Obr4. Smazaný obrázek, získaný programem FTK Imager

5.5 Dopad na zařízení

Při využití ADB lze provést analýzu bez nutnosti cokoliv nahrávat, nebo instalovat do zařízení. Díky tomu při použití této metody nehrozí možnost přepsání, nebo pozměnění stávajících a smazaných dat.

Zatímco při použití výše zmíněných forenzních nástrojů je vždy nutné do zařízení nainstalovat aplikaci, přes kterou se analýza provádí. Tyto aplikace jsou malé a v paměti zaberou místo řádově v jednotkách MiB. Avšak díky tomu může dojít k přepsání smazaných dat, které mohou být tímto poškozeny, nebo úplně přepsány.

6. Forenzní analýza s právy ROOT

Tento druh uživatelských práv přináší na poli forenzní analýzy nové možnosti, které umožňují využít při forenzní analýze účinnější postupy, které mohou odhalit více informací ukrývajících se v zařízení.

6.1 ADB

Pomocí ADB lze procházet kompletní adresářovou strukturu bez omezení. Lze opět kopírovat soubory do počítače pomocí následujícího příkazu:

```
adb pull zdroj cíl
```

Jako zdroj tohoto příkazu lze zvolit kořenový adresář a tím dojde k jeho zkopírování, avšak i přes ROOT oprávnění dojde u některých adresářů k přeskočení, kvůli tomu kopie není kompletní. Ovšem i tak je toto zdroj cenných informací.

6.2 Oxygen Forensic Suite 2013

Postup při forenzní analýze tímto nástrojem je stejný jako v případě analýzy s právy běžného uživatele popsané v předchozí kapitole. Ovšem s ROOT oprávněním dokáže Oxygen Forensic Suite 2013 vydolovat ze zařízení více dat.

Na testovaném zařízení Sony Ericsson sk17i s ROOT právy trval tento proces zhruba dvanáct hodin a díky těmto právům z něj byli získány navíc tyto informace:

- Více dat o aplikacích
- Data z Google Talk
- Data z webového prohlížeče
- Data z Facebook
- Data z Google Maps
- Část adresářové struktury vnitřní paměti

6.3 MOBILEdit! Forensic

Postup při forenzní analýze tímto nástrojem je stejný jako při analýze zařízení s právy běžného uživatele popsaném v předchozí kapitole.

Analýza zařízení s ROOT právy nepřinesla žádné informace navíc a i při procházení adresářů pořád platilo omezení, jako kdyby zařízení tyto uživatelská práva nemělo. Podle záznamů ze zařízení se ME! Forensic Connector, ani MOBILEdit! Forensic nepokusili získat ROOT práva.

6.4 Obraz paměti

Obraz paměti je při forenzní analýze velmi užitečný, díky tomu může být zařízení bez omezení používáno ihned po zhotovení obrazu a zařízení již dále není k analýze potřeba. Práce s ním umožňuje bezpečnou analýzu, u které nehrozí poškození originálního paměťového média. Největším přínosem je však možnost získání smazaných souborů, které jsou stále obsaženy v paměti zkoumaného zařízení.

Aby mohl být obraz paměti pořízen, je nejprve třeba zjistit kde a pod jakým názvem se v zařízení paměť nachází. Pro tyto účely se používá Linuxový příkaz:

```
fdisk –l
```

Avšak tento příkaz nezobrazí žádný výsledek. Je to z důvodu, že mobilní zařízení s OS Android neobsahují klasický pevný disk, ale mají NAND Flash čip. Pro zobrazení rozložení a názvu paměti existuje příkaz[17]:

```
cat /proc/mtd
```

U zařízení Sony Ericsson sk17i byly zobrazeny tyto výsledky:

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

Na nich je vidět, že paměť zařízení je rozdělena na části system, appslog, cache a userdata, které mají označení mtd*. Každý výrobce používá jiné názvy a jiný počet oddílů. Někteří paměť rozdělí až na osm, ale vždy jsou označeny mtd*.

Nyní, je díky získaným informacím možné vytvořit obraz, není možné vytvořit jeden obraz obsahující všechny oddíly, proto je nutné vytvořit obraz pro každý oddíl zvlášť.

6.4.1 dd

Jednou z možností, jak vytvořit obraz je použití příkazu `dd`. Tento příkaz se velmi často využívá při vytváření obrazů pevných disků a dají se u něj nastavit vlastnosti, které mohou ovlivnit tvorbu obrazu.

Pro vytvoření obrazu ze zařízení s OS Android vypadá příkaz následovně:

```
dd if=/dev/mtd/mtd* of=/mnt/sdcard/mtd*.dd
conv=noerror,notrunc,sync
```

Tímto příkazem je vytvořen obraz, kde hvězdička v příkazu je nahrazena číslem požadovaného oddílu, který je uložen na paměťovou kartu v zařízení. U testovaného zařízení se po zadání tohoto příkazu začala zobrazovat chybové hlášení:

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

Obraz se i přesto vytvořil, díky parametru v příkazu `noerror`, ale tento parametr způsobil, že celý obraz byl tvořen samými nulami, takže byl „prázdný“. Tento problém je způsobený firmwarem zařízení, řešením by se vyřešil nahráním jiné ROM do zařízení[18]. Lepším řešením je vytvořit obraz pomocí příkazu `cat`, který vypadá následovně:

```
cat /dev/mtd/mtd* > /mnt/sdcard/mtd*.img
```

Tímto je vytvořen obraz bez nutnosti nahrání jiné ROM do zařízení. Nevýhodou tohoto příkazu je, že u něj není možnost použití parametrů jako u příkazu `dd`. Výsledný obraz je stejný u obou příkazů.

6.4.2 nanddump

Nanddump je příkaz vyvinutý pro tvorbu obrazu NAND Flash paměti. Tento příkaz automaticky nahrazuje poškozené bloky nulami, proto není třeba k němu připisovat další parametry jako je u příkazu `dd` parametr `noerror`. Obraz paměti lze vytvořit následujícím příkazem[17]:

```
nanddump /dev/mtd/mtd* > /mnt/sdcard/mtd*.nanddump
```

Tímto příkazem se vytvoří obraz, kde hvězdička je nahrazena číslem požadovaného oddílu, který je uložen na paměťovou kartu v zařízení. U testovaného zařízení se tento obraz vytvořil bez problémů, které nastaly u příkazu `dd`. Nastane li případ, že se po tomto příkazu vypíše chyba:

```
nanddump: not found
```

Je to zapříčiněno tím, že OS Android obsahuje omezené množství příkazů a tento příkaz mezi nimi není. Proto je potřeba nainstalovat do zařízení balík nástrojů mtd-util, do kterého tento nástroj patří. Nejjednodušší řešení tohoto problému je nainstalovat do zařízení BusyBox.

BusyBox je aplikace pro operační systémy s neúplným výčtem příkazů, která doinstaluje chybějící příkazy, které poté lze využívat[19].

6.4.3 Využití SSH

Mohou nastat případy, kdy nelze vytvořený obraz uložit na paměťovou SD kartu, potom je třeba zvolit alternativní způsob a tím je použití SSH[20]. Nevýhoda tohoto způsobu je omezená rychlost přenosu a zkoumané zařízení se serverem musejí být připojeni ve stejné síti, nebo mít veřejné IP adresy.

K tomu je třeba na zařízení nainstalovat emulátor terminálu s podporou SSH, Dobrou volbou je Better Terminal Emulator Pro, který se osvědčil na testovaném zařízení. Dále je nutné mít na počítači SSH server, MobaSSH Server Home 1.22 je k těmto účelům plně dostačující, stačí ho nainstalovat a není třeba ho nijak nastavovat.

Poté stačí v Better Terminal Emulatoru Pro zadat požadované příkazy a dojde k vytvoření obrazů:

```
dd if=/dev/mtd/mtd* | ssh userName@ipAdresaServeru "dd
of=cesta/mtd*.dd"
```

případně:

```
cat /dev/mtd/mtd* | ssh userName@ipAdresaServeru cat
">" cesta/mtd*.img
```

6.4.4 Rozdíl obrazů

Přestože jsou příkazy nanddump i dd určeny k tvorbě obrazu paměti, výsledné obrazy získaná z testovaného zařízení mají různou velikost. Například obraz oddílu mtd3 vytvořený pomocí dd respektive cat má velikost 420 MiB, zatímco obraz stejného oddílu vytvořený pomocí nanddump má velikost 433 MiB. To znamená, že je mezi nimi rozdíl 13 MiB. Rozdíl je u obrazů všech oddílů a vždy jsou větší obrazy vytvořené pomocí nanddump.

Je to dáno tím, že nanddump při tvorbě obrazu bere v potaz i OOB oblast, zatímco dd a cat ji vynechávají[17].

Toto lze ověřit, za pomocí informací o YAFFS2 souborovém systému. Díky tomu, že je paměť složená z chunků o velikosti 2048 B a každý chunk má OOB oblast o velikosti 64 B, lze pomocí jednoduchého výpočtu potvrdit toto tvrzení.

Obraz bez OOB oblasti má velikost 420 MiB / 2 MiB (2048 B) = 210 chunků. Pokud ke každému chunku náleží OOB oblast o velikosti 64 B, bude velikost OOB oblasti 210 * 64 B = 13 MiB, což je rozdíl mezi velikostmi obrazů mtd3.

6.4.5 Analýza obrazu YAFFS2

Pro analýzu obrazu se souborovým systémem YAFFS2 nelze použít běžně používané forenzní nástroje, jako je FTK Imager, nebo Autopsy, které byli použity při

analýze obrazu paměťové karty. Je to dáno tím, že tyto nástroje nepodporují souborový systém YAFFS2 a jediné co s obrazem zvládnou, je zobrazit ho v hexadecimální podobě. To lze využít pouze pro vyhledávání řetězců obsažených v obrazu. Proto je třeba při této analýze využít jiných metod.

6.4.5.1 Mount obrazu

Přestože vytvořené obrazy jsou obrazy oddílů a OS Android používá Linuxové jádro, nelze připojit obraz pouze pomocí příkazu `mount` v operačním systému Linux, jako je to běžné u obrazu oddílů využívající jiné souborové systémy, jako jsou například NTFS, nebo Ext3/4. Je to způsobeno odlišností YAFFS2 od ostatních souborových systémů.

Pro připojení YAFFS2 obrazu je třeba nasimulovat v prostředí operačního systému, NAND Flash paměť potřebné velikosti. Tento postup popsal A. Hoog ve své knize[17]. Připojení obrazu se provede následovně:

```
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
```

Tyto čtyři příkazy vytvoří za pomoci YAFFS2 kernel modulu a nástroje pro simulaci NAND Flash paměti nandsim simulovanou NAND Flash paměť o velikosti kterého měl největší obraz velikost 433 MiB. Velikost simulované NAND Flash se nastavuje pomocí hodnot parametru v příkazu `modprobe nandsim`.

Nyní je třeba zkopírovat data a OOB z obrazu do simulované NAND Flash příkazem `nandwrite`, který vypadá následovně:

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

Nyní je možné připojit obraz pomocí příkazu `mount`, do adresáře k tomu určenému:

```
mkdir /mnt/yaffs2

sudo mount –t yaffs2 /dev/mtdblock0 /mnt/yaffs2
```

Obraz je nyní připojen v adresáři /mnt/yaffs2, ve kterém je možné pracovat s jeho obsahem.

6.4.5.2 Yaffey

Yaffey je jednoduchý program s grafickým prostředím, který umožňuje prohlížet, upravovat a vytvářet YAFFS2 obrazy v prostředí OS Windows[21]. Po spuštění programu stačí kliknout na Open image a zvolit požadovaný obraz, je třeba vybrat obraz obsahující OOB oblast, jinak dojde k chybě. Poté program zobrazí adresářovou strukturu, kterou je možné procházet a případně ji i upravovat.

6.4.5.3 Unyaffs

Unyaffs je nástroj kterým lze vyextrahovat soubory z YAFFS2 obrazu[22]. Extrakce tímto programem je jednoduchá, stačí stáhnout Unyaffs, který obsahuje dva soubory, unyaffs.exe a cygwin.dll. Tyto soubory je poté třeba umístit do složky společně s obrazem obsahujícím OOB oblast a pomocí příkazového řádku se dostat do této složky a spustit program následujícím příkazem:

```
C:\cesta\unyaffs>unyaffs.exe mtd*.nanddump
```

Poté začne extrakce, při které se ve složce ve které se nachází unyaffs a obraz vytvoří adresáře s obsahem obrazu, s kterými je poté možno dále pracovat. Po dokončení extrakce se v příkazovém řádku objeví následující hlášení, značící dokončení celého procesu extrakce:

```
end of image
```

6.4.5.4 File carving

File carving je metoda umožňující získat z obrazu paměti smazané, nebo poškozené soubory. Tato metoda prochází obsah obrazu a extrahuje z něj soubory, nebo jejich části, které v něm jsou uloženy. Jedním z nástrojů, který se dá pro file carving využít, je Scalpel. Hlavní platformou pro Scalpel je OS Linux, ale lze ho využít i v jiných operačních systémech, jako je Windows či Mac OS X.[23]

File carving lze provést jak s obrazem obsahujícím OOB oblast, tak i s obrazem, který jí neobsahuje. Avšak s odlišnou úspěšností. U obrazu mtd3, který neobsahoval OOB oblast, bylo vyextrahováno více než dvojnásobek souborů, než u obrazu obsahující OOB oblast. Z toho vyplívá, že je OOB oblast při file carvingu spíše na obtíž a je lepší použít obraz bez této oblasti.

6.4.6 Analýza obrazu Ext4

Při vytvoření obrazu pomocí nástroje `dd` vznikne plnohodnotný obraz a nenastává zde problém jako s OOB oblastí u YAFFS2.

Díky tomu, že je souborový systém Ext4 využíván v Linuxových operačních systémech, je tento souborový systém poměrně rozšířen. Proto hodně forenzních nástrojů Ext4 podporuje.

Pro následnou analýzu obrazu lze využít forenzní software, jako je například FTK Imager nebo Autopsy. Ty umožňují procházet adresářovou strukturu obrazu a zobrazují smazané soubory.

Mount obrazu souborového systému Ext4 je v operačním systému Linux možný pomocí příkazu:

```
mount -o loop,ro /cesta/obraz.dd /cesta/adresar/
```

Parametr `ro` v příkazu má za následek připojení obrazu v režimu read only, který umožňuje pouze čtení a brání provedení jakýchkoliv změn obrazu.

6.5 Analýza SD karty

Na analýzu SD karty nemá ROOT oprávnění žádný vliv, proto se způsob její analýzy neliší od způsobu analýzy s právy běžného uživatele popsané v předchozí kapitole. Z toho důvodu zde nebude žádný další popis této problematiky.

6.6 Dopad na zařízení

Při použití stejných technik jako v případě forenzní analýzy s omezenými právy, jsou dopady na zařízení totožné.

Pokud se pro vytvoření obrazu využije nástroj `dd`, který je součástí každého zařízení, nedojde k žádným změnám v zařízení. Ovšem při využití `nanddump` je nutné do zařízení nainstalovat balík mtd-util, to opět může způsobit přepsání, nebo poškození smazaných dat.

7. ROOT zařízení

Jak vyplívá z předešlých zjištění, zařízení s ROOT oprávněním přináší výhody pro forenzní analýzu. Proto, pokud je třeba provést analýzu zařízení, které má standardní práva, je výhodné na něm provést takzvanou ROOT úpravu. To sebou ovšem přináší možná rizika jako je ztráta dat, nebo brick zařízení.

„Brick je stav, kdy telefon nepřijímá žádné příkazy a bez speciálního vybavení s ním už nic neuděláte.“[24]

7.1 Unlock Root

Nejjednodušší způsob jak provést ROOT úpravu zařízení, je použít program Unlock Root, který provede změnu práv pro uživatele pohodlným způsobem. Tento program podporuje většinu verzí operačního systému Android a vývojáři se chlubí tím, že použití tohoto programu je bezpečné a nemůže dojít ke ztrátě dat, nebo bricku zařízení.[25]

ROOT úprava tímto programem je jednoduchá a rychlá, nejprve je nutné stáhnout aplikaci Unlock Root z oficiálního webu a poté ji nainstalovat. Poté je třeba připojit zařízení k počítači pomocí usb kabelu, zařízení musí mít povoleno Ladění USB, popsáno výše. Aplikace Unlock Root načte zařízení a poté stačí kliknout na tlačítko Root a aplikace už provede celí proces. Mobilní zařízení se poté restartuje a mezi aplikacemi se objeví aplikace Superuser, to je aplikace, která zobrazuje, co a kdy využilo ROOT oprávnění.

Pokud by měl program problém s načtením zařízení, pravděpodobně se bude jednat o problém s ovladači telefonu, který vyřeší jejich reinstalace.

Na testovaném Sony Ericssonu sk17i tento proces trval zhruba dvě minuty, nedošlo při něm k žádným problémům a všechna data zůstala v zařízení bez újmy.

7.2 „Ruční“ ROOT zařízení

Pokud by nastal případ, že by ROOT pomocí programu Unlock Root nebyl možný, je třeba ROOT tohoto zařízení provést ručně. Bohužel neexistuje univerzální postup, kterým by se tento postup dal popsat, protože každý výrobce konstruuje svá zařízení odlišně, je vždy třeba najít konkrétní návod pro určité zařízení. Tyto návody se dají najít na různých fórech, které se touto problematikou zabývají, ovšem, je třeba dát si pozor na neověřené postupy, které by mohli vést ke ztrátě dat, nebo bricku zařízení. Některé postupy i při úspěchu vedou ke ztrátě dat, proto je dobré projít komentáře uživatelů, které mnohdy prozradí více o dané metodě.

Pro představu co tento způsob získání ROOT oprávnění obnáší, je zde uveden princip ROOTu podle návodu na jeho provedení u Sony Ericssonu sk17i[26], při kterém nedojde ke ztrátě dat:

1. Záloha původního Firmware – U SE lze provést prostřednictvím aplikace PC Companion, aplikací určenou pro aktualizaci systému zařízení od Sony
2. Stažení souborů potřebných pro ROOT zařízení
3. Nahrání a spuštění stažených souborů do zařízení, které vykonají potřebné změny.

Další možností jak získat ROOT oprávnění spočívá v nahrání jiné ROM (upravená verze operačního systému). Kdy se stávající ROM nahradí jinou, která umožňuje využití ROOT práv. Ovšem to obnáší větší zásah do softwaru zařízení a větší možnost výskytu problémů při této činnosti. Nebo lze ROOT provést nahráním upraveného jádra operačního systému.[27]

7.3 Dopady na zařízení

ROOT zařízení může mít fatální vliv na data uložená v zařízení. Při využití aplikace Unlock Root však nedošlo ke strátě žádných dat a proto jediné riziko hrozí přepsání smazaných dat při instalaci aplikace, kterou tento program do zařízení instaluje. Naproti tomu při pokusu o ROOT zařízení za použití alternativních způsobů při kterých dochází k přehrávání částí, nebo celého operačního systému dojde

k přepsání velké části smazaných dat, která jsou poté ztracena. Navíc může dojít k poškození, nebo ztrátě dat uložených v paměti. Proto je využití těchto metod pro data uložená v zařízení velmi nebezpečné.

8. Odebrání ROOT práv

Pokud je při forenzní analýze proveden ROOT zařízení, je vhodné vrátit toto zařízení do stavu, v jakém bylo před zahájením zkoumání. Možnost návratu zařízení do továrního nastavení závisí na tom, jaký způsobem byl v zařízení ROOT proveden.

Když je ROOT zařízení proveden pomocí aplikace Unlock Root, je návrat do původního stavu opět jednoduchý. Zařízení se připojí k počítači pomocí usb kabelu, zařízení musí mít povoleno Ladění USB, popsáno výše. Aplikace Unlock Root načte zařízení a poté stačí kliknout na tlačítko UnRoot a aplikace už provede celí proces. Poté se zařízení restartuje a ROOT práva jsou odebrána.

Při použití jiné metody pro ROOT zařízení nelze u všech zaručit možnost návratu do původního stavu. U návodů pro ROOT bývá uvedeno, zdali je to možné, či ne, proto i toto je důležité kritérium při volbě metody pro ROOT zařízení.

Možností, kterou se provádí návrat zařízení do továrního nastavení, je obnova původního firmware, který byl zálohován před provedením ROOTu zařízení.

9. Vyhodnocení použitého softwaru

9.1 Forenzní nástroje pro mobilní zařízení

9.1.1 Oxygen Forensic

Oxygen Forensic je v současné době nejlepší nástroj pro forenzní analýzu mobilních zařízení nejen s OS Android. Dokáže ze zařízení dostat velké množství informací, které přehledně roztřídí do kategorií, které je pak možné velice přehledně procházet. Umožňuje též vygenerovat dokumentaci zařízení v různých formátech, která obsahuje veškeré informace o zařízení. Kompletní dokumentace Testovaného zařízení s právy ROOT má ve formátu pdf 2170 stran. V nejvyšší verzi umožňuje provést ROOT zařízení. Jeho nevýhodou je cena, která se pohybuje v řádu deseti tisíců korun v závislosti na verzi.

9.1.2 MOBILEdit! Forensic

MOBILEdit! Forensic dokáže získat ze zařízení základní informace, které jsou přehledně zobrazeny. Jeho použití je velice jednoduché a analýza zařízení je hotova během několika minut. Tento nástroj je k dostání zdarma, avšak s malými omezeními. To je například možnost vygenerování dokumentace pouze v placené verzi. Největší nevýhodou je, že analýza zařízení s omezenými právy přináší stejné výsledky, jako analýza zařízení s ROOT právy.

9.2 Běžné forenzní nástroje

9.2.1 FTK Imager

FTK Imager je forenzní nástroj, který umožňuje prohlížení obrazů paměti. Zobrazuje adresářovou strukturu obrazu i se smazanými soubory, které jsou označeny červeným křížkem. Jeho nevýhodou je chybějící podpora souborového systému YAFFS2. Avšak lze ho využít k analýze obrazu SD karty, nebo obrazu ze souborového systému Ext4, pro ty je to velice užitečný nástroj.

9.2.2 Autopsy

Autopsy je zdarma přístupný forenzní nástroj, který je určen pro analýzu obrazu paměti. Po provedení analýzy rozdělí soubory do skupin podle jejich typu a umožní jejich prohlížení. Navíc umožňuje vyhledávat řetězce obsažené v obrazu. Nevýhodou je opět chybějící podpora souborového systému YAFFS2. Ovšem na analýzu obrazu SD karty a obrazů souborového systému Ext4 lze spolehlivě použít.

9.2.3 DEFT

DEFT je Linuxový operační systém, který byl vytvořen pro účely forenzní analýzy. Proto obsahuje různé forenzní nástroje, které lze k analýze využít. Jednou z jeho výhod oproti jiným operačním systémům je ta, že při připojení disku k počítači, se disk automaticky nepřipojí. To je velmi užitečné při vytváření obrazu SD karty, který lze pomocí tohoto operačního systému snadno vytvořit.

9.3 Ostatní nástroje

9.3.1 Unyaffs

Unyaffs je jednoduchý program, který se ovládá přes příkazový řádek. Unyaffs vyextrahuje z obrazu souborového systému YAFFS2 adresářovou strukturu. Jeho použití je jednoduché a rychlé.

9.3.2 Yaffey

Yaffey je program napsaný v jazyce JAVA, který umožňuje zobrazit a upravovat obsah obrazu souborového systému YAFFS2. V současné verzi 0.2 má tento program velice omezené funkce, které se v případě dalšího vývoje budou rozšiřovat a tento nástroj by mohl být velice zajímavý pro forenzní analýzu.

9.3.3 Unlock Root

Unlock Root je velice užitečná aplikace, která umožňuje ROOT mobilních zařízení s OS Android a následně i UnROOT těchto zařízení, bez toho aby došlo ke ztrátě dat. Vývojáři této aplikace se chlubí tím, že její použití je naprosto bezpečné a

nemůže dojít k poškození zařízení. Bezplatná verze tohoto programu umožňuje provést ROOT zařízení s většinou verzí OS Android. Použití této aplikace je velice jednoduché a celý proces trvá jen několik minut. Vývoj této aplikace drží krok s vydávanými verzemi OS Android, proto je a bude velmi užitečná pro forenzní analýzu mobilních zařízení s OS Android.

9.3.4 ADB

ADB je nejdůležitější nástroj při provádění forenzní analýzy mobilních zařízení s OS Android. Umožňuje práci se zařízením přes PC, díky tomu je nutná jen minimální manipulace se zkoumaným zařízením a práce s jeho terminálem je komfortnější. ADB navíc přináší zajímavé funkce pro práci s mobilním zařízením.

10. Optimální řešení forenzní analýzy

Díky poznatkům o možnostech forenzní analýzy mobilních zařízení s OS Android testovaných na skutečném zařízení je nyní možné navrhnout optimální postup této analýzy.

Při forenzní analýze je třeba rozlišit, jakým druhem práv mobilní zařízení, u kterého je požadována analýza disponuje. To lze jednoduše zjistit za pomoci ADB dvěma jednoduchými příkazy.

```
adb shell
```

```
su
```

První příkaz provede připojení ke konzoly mobilního zařízení a druhý příkaz se pokusí získat ROOT oprávnění. Pokud se tento příkaz vykoná úspěšně, změní se znak na začátku řádky na #, to symbolizuje získání ROOT práv. V opačném případě zařízení nemá možnost získat oprávnění ROOT.

10.1 Zařízení s právy běžného uživatele

1. Provedení analýzy pomocí forenzního nástroje Oxygen Forensic, nebo MOBILEdit! Forensic. Tímto se ze zařízení získají základní informace a také je to vhodné, pro případ, že při dalším postupu dojde k poškození dat, nebo zařízení.
2. Vytvoření obrazu SD karty.
3. ROOT zařízení. Nejvhodnější je použít program Unlock Root, tento způsob je nejbezpečnější v ohledu k zachování zájmových dat. V případě jeho selhání, je potřeba zvolit alternativní způsob.
4. Připojení se za pomoci ADB do terminálu zařízení, následujícím příkazem:

```
adb shell
```

5. Zjištění, na jaké části je paměť rozdělena pomocí příkazu:

```
cat /proc/mtd
```

6. Zjištění použitého souborového systému. Pro to je vhodné využít následující příkaz, jehož výstup tyto informace obsahuje:

```
mount
```

7. Vytvoření obrazů paměti. Zde záleží na použitém souborovém systému. V případě YAFFS2 je lepší využít pro vytvoření obrazu paměti `nanddump`, avšak i obraz vytvořený pomocí `dd` může mít přínos pro následnou analýzu. Proto je dobré vytvořit obě varianty. V případě Ext4 nezáleží na zvoleném nástroji, proto je lepší pro vytvoření obrazu použít `dd`, který je již součástí operačního systému. Při ukládání obrazu na SD kartu, musí být vždy použita jiná SD karta, aby nedošlo k přepsání smazaných dat na zkoumané kartě.
8. Kvůli zachování důvěryhodnosti obrazu je nutné pro každý obraz vypočítat kontrolní součet. Kontrolní součet zaručuje, že obsah obrazu nebyl nijak pozměněn. Kontrolní součet lze v operačním systému Linux následujícím příkazem:

```
md5sum /cesta/mtd*.dd > /cesta/mtd*md5sum.txt
```

9. Odebrání ROOT práv.
10. Analýza získaných dat.

Mezi bodem 3 a 4 je možné provést opětovnou analýzu zařízení pomocí nástroje Oxygen Forensic, který ze zařízení získá více dat než při analýze v bodě 1.

10.2 Zařízení s právy ROOT

1. Vytvoření obrazu SD karty.
2. Vytvoření obrazů paměti. Tento postup je analogický s postupem popsaným v předchozí části kapitoly v bodech 4 až 8.
3. Provedení analýzy pomocí forenzního nástroje Oxygen Forensic, nebo MOBILEdit! Forensic. Tento bod není nezbytný, avšak lze díky němu získat přehledně zařazené informace, které usnadní následnou analýzu získaných dat.
4. Analýza získaných dat.

10.3 Vyhodnocení postupu

Výše uvedené metody jsou navrženy tak, aby byl dopad na zařízení co nejmenší. Avšak určitým zásahům do zařízení se nelze vyhnout. Proto se tyto metody dají označit jako částečně destruktivní, protože dochází k instalaci byť malých aplikací. To může způsobit částečné, nebo úplné přepsání některých smazaných dat obsažených v paměti. Pro úspěšné provedení forenzní analýzy je toto riziko nutné podstoupit.

Další věcí k zamyšlení je, zda li je nutné provádět ROOT zařízení ve všech případech. Z hlediska forenzní analýzy přináší zařízení s právy ROOT mnohem lepší možnosti pro získání dat ze zařízení. Avšak při pokusu o ROOT může dojít až ke ztrátě zájmových dat. To ovšem závisí na použité metodě. Při použití správné metody hrozí pouze částečné, nebo úplné přepsání některých smazaných dat. Výhody analýzy zařízení s právy ROOT jsou značné, proto tyto výhody převažují nevýhody, které vznikají při pokusu o získání těchto práv. Avšak je dobré zvážit, na základě dat získaných před pokusem o ROOT zařízení, zdali je potřeba získat další data ze zařízení, nebo zdali jsou do té doby získaná data dostačující. V takovém případě by byl takovýto zásah do zařízení zbytečným rizikem.

11. Závěr

Tato bakalářská práce obsahuje popis operačního systému Android zaměřený na vlastnosti důležité pro forenzní analýzu mobilních zařízení s tímto operačním systémem. Dále jsou zde popsány možnosti a omezení, které přináší analýza těchto zařízení a jejich vliv na zkoumané zařízení. Tyto postupy byly testovány na fyzickém zařízení. Na základě získaných poznatků byl navržen optimální postup pro forenzní analýzu mobilních zařízení s operačním systémem Android.

Forenzní analýza mobilních zařízení s operačním systémem Android sebou přináší omezení způsobená vlastnostmi těchto zařízení. I přes tyto omezení byl navržen optimální postup pro forenzní analýzu těchto zařízení, bylo tedy dosaženo cílů této práce.

12. Použitá literatura

[1] DOSEDĚL, Tomáš. Androidu se daří, drtivě válcuje konkurenci. [online]. 2013 [cit. 2013-03-04]. Dostupné z: http://www.mobinfo.cz/androidu-se-dari-drtive-valcuje-konkurenci/

[2] KADLEC, Bc. Josef. Forenzní analýza unixových systémů. Hradec Králové, 2006. Diplomová práce. Univerzita Hradec Králové.

[3] KLEPETEK, Martin. Android slaví 3. narozeniny. [online]. 2010 [cit. 2013-03-05]. Dostupné z: http://www.svetandroida.cz/android-slavi-3-narozeniny-201011

[4] HO HAN, Dong. Android, at a glance. [online]. 2011 [cit. 2013-03-07]. Dostupné z: http://www.cubrid.org/blog/dev-platform/android-at-a-g

[5] . Android Architecture. [online]. 2010 [cit. 2013-03-07]. Dostupné z: http://technodiscuss.wordpress.com/2010/10/18/android-architecture/

[6] YADAV, Manish. History of Android. [online]. 2011 [cit. 2013-03-07]. Dostupné z: http://www.tech2crack.com/history-android/

[7] ALEXIS. Android versions comparison. [online]. 2013 [cit. 2013-03-07]. Dostupné z: http://socialcompare.com/en/comparison/android-versions-comparison

[8] Developers [online]. 2013 [cit. 2013-03-12]. Dostupné z: http://developer.android.com/about/dashboards/index.html

[9] WEINBRENNER, Ing. Jan. Pohled na NAND FLASH paměti. 2010, roč. 2010, Listopad/Prosinec. Dostupné z: http://www.mikrozone.sk/soubory/downloads/print/dps-az/2/soucastky-pohled_na_nand.pdf

[10] QUICK, Darren a Mohammed ALZAABI. Forensic analysis of the android file system YAFFS2. 2011. Dostupné z: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1100&context=adf

[11] ŠTRAUCH, Adam. Ext4: evoluční souborový systém. [online]. 2008 [cit. 2013-03-28]. Dostupné z: http://www.root.cz/clanky/ext4-evolucni-souborovy-system/

[12] ROUSE, Margaret. Secure Digital card (SD card). [online]. 2006 [cit. 2013-03-08]. Dostupné z: http://searchstorage.techtarget.com/definition/Secure-Digital-card

[13] DEVELOPER, Android. Android Debug Bridge. [online]. 2012 [cit. 2013-03-08]. Dostupné z: http://developer.android.com/tools/help/adb.html

[14] REDAKCE. ADB Shell - Jak se připojit. [online]. 2011 [cit. 2013-03-08]. Dostupné z: http://androidaplikace.cz/index.php/2011/03/adb-shell-jak-se-pripojit/

[15] OXYGEN SOFTWARE. Oxygen Forensic Suite 2013 [online]. 2013 [cit. 2013-03-13]. Dostupné z: http://www.oxygen-forensic.com/en/

[16] COMPELSON LABS. MOBILEdit! Forensic [online]. 2013 [cit. 2013-03-14]. Dostupné z: http://www.mobiledit.com/mef-overview.htm

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

[18] [DEV][THE S-OFF CAMPAIGN] We need electrical engineers & experts in JTAG, OpenOCD!. In: XDA Developers [online]. 2012 [cit. 2013-04-03]. Dostupné z: http://forum.xda-developers.com/showthread.php?p=23222889

[19] BusyBox. BusyBox: The Swiss Army Knife of Embedded Linux [online]. 2008 [cit. 2013-04-03]. Dostupné z: http://www.busybox.net/about.html

[20] CONE, Matthew. Copying a Disk Image Over SSH. Copying a Disk Image Over SSH [online]. 2012 [cit. 2013-04-03]. Dostupné z: http://library.linode.com/migration/ssh-copy

[21] Yaffey. Yaffey [online]. 2012 [cit. 2013-04-03]. Dostupné z: http://code.google.com/p/yaffey/

[22] Unyaffs. Unyaffs [online]. 2012 [cit. 2013-04-03]. Dostupné z: http://www.bernhard-ehlers.de/projects/unyaffs.html

[23] Scalpel: A Frugal, High Performance File Carver [online]. 2011 [cit. 2013-03-27]. Dostupné z: http://www.digitalforensicssolutions.com/Scalpel/

[24] FOLTÝNEK, Libor. Root očima laika: ano či ne?. [online]. 2012 [cit. 2013-03-12]. Dostupné z: http://www.svetandroida.cz/root-ocima-laika-ano-ci-ne-201204

[25] UNLOCK ROOT. Unlock Root [online]. 2013 [cit. 2013-03-12]. Dostupné z: http://www.unlockroot.com/unlockroot.html

[26] IJK. Jak na root a CWM bez odemykání bootloaderu. [online]. 2012 [cit. 2013-03-12]. Dostupné z: http://forum.xperia.cz/viewtopic.php?f=21&t=1095#p17250

[27] TYKAL, Jaromír. Seznámení s rootem HTC telefonů. [online]. 2012 [cit. 2013-03-12]. Dostupné z: http://www.svetandroida.cz/seznameni-s-rootem-htc-telefonu-201211

13. Přílohy

[1] DVD obsahující obrazy a jejich popis, získané z mobilního zařízení Sony Ericsson sk17i a dokumentaci vygenerovanou programem Oxygen Forensic Suite 2012 ve formátu .pdf.