Pedagogická fakulta
Faculty of Education

Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Jihočeská univerzita v Českých Budějovicích
Pedagogická fakulta
Katedra informatiky

Bakalářská práce

iOS Forenzní analýza iPad, iPhone, iPod

Vypracoval: Artem Plachotňuk
Vedoucí práce: Ing. Jaroslav Kothánek, Ph.D.
České Budějovice 2014

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH
Fakulta pedagogická
Akademický rok: **2011/2012**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Artem PLAKHOTNYUK**
Osobní číslo:	**P10357**
Studijní program:	**B7507 Specializace v pedagogice**
Studijní obor:	**Informační technologie ve vzdělávání**
Název tématu:	**iOS Forenzní analýza iPad, iPhone, iPod**
Zadávající katedra:	**Katedra informatiky**

Zásady pro vypracování:

Cíle práce:
Nález odpovídajících metod forenzního zkoumání produktů firmy Apple, tvorba odpovídajících metod forenzní analýzy za účelem důkazního řízení před soudy a jejich řešení v souvislosti se specifikami mobilních zařízení tohoto typu.

Úkoly:

- seznámení se souborovým systémem operačního systému (iOS 4, iOS 5)
- zhodnocení úprav iOS a následné možnosti, vlastnosti využitelné ve forenzní praxi (Jealbreak apod.)
- bezpečnostní prvky zařízení a následné omezení forenzního zkoumání
- seznámení se s postupy forenzní praxe při řešení informační kriminality
- nastínění možností získávání klíčových informací pro řešení informační kriminality (nainstalovaný software, analýza softwarových komunikačních prostředků, atd.)
- vyhodnocení forenzních softwarových prostředků pro řešení informační kriminality
- vytvoření jednoduchého výstupu forenzního zkoumání uvedené techniky

Rozsah grafických prací: **CD ROM**

Rozsah pracovní zprávy: **40**

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

1. **Kothánek, J. Zajišťování výpočetní techniky a dat pro potřeby důkazního řízení. Praha: Policie ČR, 2008.**
2. **Luis Gómez-Miralles, Joan Arnedo-Moreno, Versatile iPad forensic acquisition using the Apple Camera Connection Kit. Barcelona: Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya, 2011.**
3. **www.accessdata.com**

Vedoucí bakalářské práce: **Ing. Jaroslav Kothánek, Ph.D.**
Katedra informatiky

Datum zadání bakalářské práce: **12. dubna 2012**

Termín odevzdání bakalářské práce: **26. dubna 2013**

Mgr. Michal Vančura, Ph.D.
děkan

L.S.

doc. PaedDr. Jiří Vaníček, Ph.D.
vedoucí katedry

V Českých Budějovicích dne 12. dubna 2012

Prohlášení

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

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

V Českých Budějovicích dne 17. dubna 2014 Artem Plachotňuk

Poděkování

Touto cestou bych rád poděkoval vedoucímu této kvalifikační práce, Ing. Jaroslavu Kothánkovi, Ph.D., za jeho odborné a cenné připomínky, které mi udávaly směr, kterým se mám vydat s tvorbou této práce. Stejně tak bych rád poděkoval rodině, za podporu jak finanční, tak i psychickou, kterou mi věnovala v těžkých chvílích.

Anotace

Bakalářská práce „iOS Forenzní analýza iPad, iPhone, iPod“ se zabývá problematikou forenzní analýzy mobilních zařízení s operačním systémem iOS. V této práci bude popsán operační systém iOS 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

OS, iOS, forenzní analýza, Apple, souborový systém, zabezpečení systému, uživatelský kód, jailbreak, záloha, izolace zařízení,

Abstract

Thesis "iOS Forensic Analysis iPad, iPhone, iPod" deals with the forensic analysis of mobile devices running iOS. This paper will describe a specific OS iOS devices with this operating system. Next will be described the capabilities and limitations which have these devices in relation to forensic analysis. These findings are then illustrated on a physical device and on the basis of best practices will be designed for forensic analysis of these devices and the findings will be evaluated.

Keywords

OS, iOS, forensic analysis, Apple, filesystem, systém security, passcode, jailbreak, backup, device izolation

Obsah

1 ÚVOD 1
2 HISTORIE IOS 2
3 DIGITÁLNÍ FORENZNÍ ANALÝZA 5
4 OPERAČNÍ SYSTÉM IOS 7
4.1 Souborový systém 7
4.1.1 HFS+ Volume header 8
4.1.2 HFS+ Allocation file 8
4.1.3 HFS+ Extents overflow file 8
4.1.4 HFS+ Catalog file 8
4.1.5 Oddíly souborového systému 9
4.2 Architektura systému iOS 9
4.2.1 Vrstva Cocoa Touch 10
4.2.2 Vrstva Media 10
4.2.3 Vrstva Core Service 11
4.2.4 Vrstva Core OS 11
5 ZABEZPEČENÍ SYSTÉMU IOS 12
5.1 Systémová architektura 12
5.2 Secure Boot Chain 12
5.3 Šifrování a ochrana dat 13
5.4 File Data Protection 14
5.5 Uživatelský kód 15
5.5.1 Bypass uživatelského kódu 16
5.6 Classes 18
5.6.1 Complete Protection 19
5.6.2 Protected Unless Open 19
5.6.3 Protected Until First User Authentication 19
5.6.4 No Protection 19
5.6.5 Keychain Data Protection 19
5.7 Keybags 20
6 JAILBREAK 21
6.1 Provedení jailbreak 21
6.2 Výhody jailbreak na zařízení 23
6.3 Dopady jailbreak na zařízení 23
7 METODY ZÍSKÁVÁNÍ DAT 25
7.1 Backup metoda 25
7.2 Logická metoda 26
7.3 Fyzická metoda 26
7.4 Jailbreak metoda 27
8 NÁSTROJE 29
8.1 Find My iPhone / iPad 29
8.2 Backup iTunes 32
8.3 iPhone Backup Extractor 35
8.4 MOBILedit! Forensics 39
8.5 iPhone Analyzer 41

8.6 Oxygen forensic Suite 2013 44
8.7 iFunBox 45
8.8 UFED Physical Analyzer 3 46
8.9 Internet Evidence Finder 48
9 VYHODNOCENÍ SOFTWARU 50
9.1 Forenzní nástroje 50
9.1.1 MOBILedit! Forensics 50
9.1.2 iPhone Backup Extractor 51
9.1.3 iPhone Analyzer 51
9.1.4 Oxygen forensic Suite 2013 51
9.1.5 UFED Physical Analyzer 3 52
9.1.6 Internet Evidence Finder 52
9.2 Ostatní nástroje 52
9.2.1 Find My iPhone / iPad 53
9.2.2 Backup iTunes 53
9.2.3 iFunBox 53
10 DŮLEŽITÉ ADRESÁŘE 54
10.1 Fotografie 54
10.2 Klávesnice 54
10.3 Hesla 55
10.4 Poznámky 55
10.5 Zprávy 55
10.6 Historie prohlížeče 55
10.7 Adresář kontaktů 56
10.8 Historie volaní 56
11 DOPORUČENÝ POSTUP FORENZNÍ ANALÝZY 57
11.1 Postup před forenzní analýzou 57
11.2 Postup při forenzní analýze 57
12 ZÁVĚR 61
13 TERMINOLOGICKÝ SLOVNÍK 62
14 POUŽITÁ LITERATURA 64

1 Úvod

Již delší dobu můžeme být svědky bouřlivého rozvoje výpočetní techniky. U některých činností si již ani nedokážeme představit, že bychom se bez této techniky dokázali obejít. Využití je velmi široké, vždyť více než 43% všech domácností v ČR má 2 a více počítačů připojených do sítě internet.[1]

Ovšem ne všichni využívají svoji techniku pro osobní a pracovní účely. Ze statistik[2] vyplývá, že čím dál více roste počet trestných činů spáchaných pomocí výpočetní techniky. Nejčastěji jde o podvody spáchané právě pomocí internetové sítě na aukčních portálech, internetových bazarech, apod. Pachatelé zde mívají větší pocit bezpečnosti a spoléhají na anonymitu, kterou jim internet zdánlivě poskytuje.

K páchání informační kriminality se ovšem kromě počítačů také často využívá služeb mobilních telefonů, které se mnohdy blíží jejich možnostem. Čísla ukazují[3], že nejlépe se prodávají zařízení s operačním systémem Android, následované systémem iOS od Apple. Z toho se dá vyvodit, že zařízení s operačním systémem iOS může být často využíván k páchání trestné činnosti.

Cílem této práce je nalezení vhodných metod forenzního zkoumání produktů firmy Apple, za účelem důkazního řízení před soudy, vyhodnocení těchto metod a zjištění jejich případných dopadů na zařízení.

2 Historie iOS

Operační systém iOS od Applu, dříve známý také jako iPhone OS, ušel velmi dlouhou cestu od svého vzniku. Během necelých sedmi let bylo vydáno hned sedm generací operačního systému. V roce 2007, kdy byla představena první generace iPhoneOS, byly možnosti zařízení iPhone velmi omezené. Neexistoval například App Store, kde by si uživatelé mohli stahovat aplikace třetích stran, ani multitasking, pro přepínání mezi nainstalovanými aplikacemi. Zatímco ale konkurence tehdy používala ve svých telefonech rezistivní (odporové) dotykové displaye, Apple vsadil na kapacitní display, který poskytoval uživatelům větší komfort při využívání funkcí telefonu. Práce s vestavěnými aplikacemi, jako byli např. Google maps a Safari web browser, které vyžadovali zoomování a scrolování, se stala příjemnější zkušeností.

Rok 2008, který přinesl druhou generaci iOS, označovanou jako iPhoneOS 2, odstranil jeden neduh první generace, kterým byla absence App Store. Uživatelé s touto verzí operačního systému si již mohli stahovat aplikace třetích stran do svých zařízení. Zároveň byl propojen App Store s iTunes účty, takže uživatelé mohli zaplatit za aplikace stejnou kreditní kartou, kterou používali pro stahování hudby na počítačích. Další přidanou funkcí byl Microsoft Exchange, který umožňoval přístup ke kalendáři a adresáři z jiného zdroje.

Třetí generace iOS, iPhoneOS 3, vyšla v roce 2009, spolu s telefonem iPhone 3GS. Tato verze přinesla funkce vyjmout, kopírovat a vložit, tak jak je známe dnes. Dále také tzv. Push notifikace, které umožňují aplikacím třetích stran informovat uživatele na nějakou událost prostřednictvím krátkých zpráv. Objevila se tu i možnost sdílení internetu přes USB a Bluetooth. Poprvé se zde vyskytuje i funkce Find My iPhone, které se věnuje kapitola 8.1.

V roce 2010 vyšla již čtvrtá generace operačního systému od Applu, tentokrát již pod názvem iOS4. Do této doby byly všechny předešlé generace

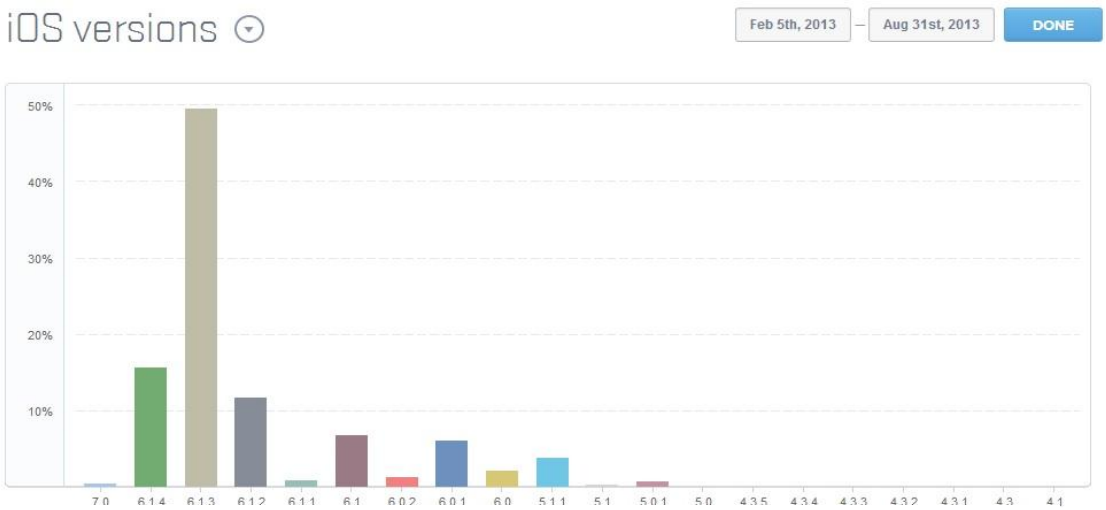
bez možnosti využívání multitaskingu. iOS4 je spojovaný právě se vznikem podpory více běžících aplikací na této platformě. Uživatelé s touto verzí OS tedy mohli aplikace nechat běžet na pozadí a přepínat mezi nimi rychleji. Mohli si také vytvořit složky pro nainstalované aplikace a zpřehlednit si tak plochu. Ke sdílení internetu přes USB a Bluetooth se v této verzi přidává ještě WiFi.

iOS ve verzi 5, který vyšel na trh v roce 2011, je spolu s předchozí verzí považován za nejpřínosnější update. Poprvé se zde objevuje „Siri“, který slouží jako inteligentní osobní asistent a navigátor. iCloud byl v této verzi také poprvé vypuštěn, umožňujíc vytváření záloh a zjednodušení nastavení nového zařízení.

Rok 2012 přinesl šestou generaci iOS, ve které se Apple rozhodl vydat své vlastní mapy spolu s hlasovou navigací a vystoupit tak ze stínu Google a jejich Google maps. Pro řadu lidí byl ale výsledek zklamáním a tak byli Google maps umístěny do App Store pro uživatele. Byla zde představena i aplikace Passbook, která umožňuje uchovávání uživatelovo letenek, vstupenek a dalších různých mobilních plateb.

V době psaní této bakalářské práce je nejnovější verze iOS 7, která vyšla v roce 2013. Přidává například funkci AirDrop, která umožňuje sdílení souborů mezi zařízeními, která jsou připojena ve stejné WiFi síti.

Během těchto let a vývoje jednotlivých verzí OS, vznikali mobilní telefony, tablety a hudební přehrávače, které tyto systémy integrovali. Je třeba si uvědomit, že ne všechny zařízení lze aktualizovat na nejnovější OS, a to ať už z marketingového důvodu, kdy je výhodnější pro Apple prodat nové zařízení, než poskytnout aktualizaci zdarma, nebo z technického důvodu, kdy zařízení má nedostatečný nebo nevhodný hardware pro novější OS. Faktem tedy zůstává, že uživatelé nemají vždy nejnovější OS. Na následujícím grafu je vidět, jakých verzí využívají zákazníci Applu nejvíce. Měření bylo prováděno v období 05.02. – 31.08.2013.



Obrázek 1 Verze iOS podle použití [9]

3 Digitální forenzní analýza

Digitální forenzní analýza patří mezi jednu z nejmladších forenzních věd. Její záběr je velmi široký, zkoumá totiž veškerá digitální data. Všude, kde dojde ke spáchání trestného nebo jiného protiprávního činu, se lze setkat i s digitálními daty, na kterých může být v rámci vyšetřování potřeba provést forenzní analýzu k získání potřebných důkazů.

Aby ale bylo možné mluvit o forenzní analýze a možnosti využití získaných dat pro soudní řízení, je třeba, aby splňovala určité zásady a vlastnosti.

První zásadou je nutnost legality. Jinými slovy je třeba, aby veškeré pořízené stopy, informace, dokumenty, atd., které se používají pro forenzní analýzu, byly získány legální cestou. Určitým problémem zde může být podoblast DFA, která se nazývá Live Forensics. Jde o zkoumání dat z běžících systémů, většinou z operační paměti. To lze považovat za aktivní monitoring, který může kolidovat s komunikačním zákonem nebo zákonem na ochranu osobních údajů.

Druhou zásadou je integrita, to znamená, že u veškerých činností, které byly prováděny s digitálními daty, musí být nezpochybnitelně dokazatelné, že nemohlo dojít k úmyslnému ani neúmyslnému pozměnění.

Třetí zásadou je potřeba možnosti přezkoumatelnosti. Tím je míněno to, že pro forenzní analýzu je třeba zvolit takový způsob práce, který umožňuje ověření výsledků opakováním metody nebo, pokud je to možné, zvolení ekvivalentní metody, pro ověření správnosti výsledků.

Čtvrtou zásadou je nepodjatost. Znalec, provádějící forenzní analýzu, nesmí být žádným způsobem ovlivněn zkoumaným předmětem nebo objektem.

Společným prvkem, který se dotýká všech výše zmíněných zásad, je potřeba kvalitní, detailní dokumentace. Bez ní by nebylo možné podat závěry analýzy a ani dokázat, že zmíněné zásady byly splněny. Zásadním požadavkem pro

forenzní analýzu je také odbornost znalce. V oblastech, kde je vysoká dynamika vývoje, kam informační technologie jednoznačně patří, musí znalec svoji odbornost neustále doplňovat.

Samotný proces forenzní analýzy začíná izolováním důkazů, aby nemohlo dojít ke změně nebo poškození dat. Následuje sběr dat, při kterém je třeba důkazy dostat ze zařízení v podobě kopie, se kterou se bude pracovat. Dalším krokem je identifikace důkazů, při kterém se určují důkazy na médiu, které může kromě samotných důkazů obsahovat i nerelevantní informace. Poté se provede interpretace důkazů, která spočívá ve správném a srozumitelném vyložení získaných informací. Základem je zmíněná dokumentace, ve které je vše, co bylo provedeno od začátku až do konce forenzní analýzy.

Forenzní analýza na mobilních zařízeních bývá často znesnadněna operačními systémy, které neumožňují forenzním nástrojům přístup do všech jeho částí. Poněvadž se zajištěné důkazní materiály musí vrátit majiteli v původním stavu, znalec je povinen opatrně volit metody zkoumání.

4 Operační systém iOS

První iOS systém známý jako iPhone OS byl představen 9. ledna 2007 na konferenci MacWorld. Označení iPhone OS společnost používala až do června 2010. iOS je operační systém navržený společností Apple Inc. Svojí architekturou je podobný Mac OS, který se používá pro počítače. Jedná se o systém UNIXového typu, a je tedy multitaskingový. iOS je odlehčenou verzí Mac OS, který je podporován dotekovým ovládáním pro displeje. Operační systém iOS je využíván v zařízeních iPhone, iPad, iPod touch a Apple TV. Apple nezapomněl ani na vývojáře aplikací a vydal Software Development Kit (SDK). Díky tomuto nástroji lze vytvářet aplikace třetích stran. Některé aplikace jsou již předinstalované, jako například mobilní Safari, Mapy, Mail. S každou novou verzí iOS se jejích počet zvyšuje.

4.1 Souborový systém

Zatímco Microsoft pro práci s daty nejčastěji využívá souborový systém NTFS (New Technology File System), Apple začátkem 90. let přišel se svým vlastním systémem, nazývaným HFS (Hierarchical File System), který více vyhovoval jejich požadavkům. Byl to nový dynamický souborový systém, který byl postavený na 512 bajtových blocích. V tomto systému existují 2 typy těchto bloků – logické bloky a alokační bloky. Logické bloky jsou na svazku očíslované od prvního bloku do posledního, přičemž zůstávají statické. Na druhou stranu alokační bloky mohou být spojeny do skupin za účelem vyšší efektivity práce. Struktura tohoto souborového systému obsahuje Volume Header (hlavička svazku), Startup file (spouštěcí soubor), Allocation file (alokační soubor), Attributes file (soubor atributů), Extents overflow file a Catalog file (katalogový soubor).

4.1.1 HFS+ Volume header

Hlavička svazku je určena k tomu, aby obsahovala základní informace o struktuře HFS svazku. Sektory 0 a 1 na svazku slouží jako bootovací bloky. Hned za nimi se nachází volume header, který má 1024 bajtů. Kvůli bezpečnosti existuje i záloha této hlavičky, která se nachází na posledních 1024 bajtech svazku. V případě poškození primární hlavičky je využita záloha a poškozená hlavička je nahrazena. Hlavička uchovává řadu důležitých údajů, například velikost alokačních bloků, informaci o tom, kdy byl svazek vytvořen nebo umístění dalších výše zmíněných struktur, jako je třeba katalogový soubor.[4]

4.1.2 HFS+ Allocation file

Alokační soubor určuje, které z alokačních bloků jsou využity systémem a které nejsou. Zda je alokační blok volný se určuje pomocí tzv. „clear bitu“. Pokud je v něm uložena 0, je blok volný.[4]

4.1.3 HFS+ Extents overflow file

Tento soubor má za úkol sledovat všechny alokační bloky, které náleží jednotlivým souborům. Každý záznam v katalogovém souboru je schopen uchovávat až osm umístění částí souboru. Jakmile je tento počet vyčerpán, jsou přebývající informace o umístění uchovávány v Extents overflow file. [4]

4.1.4 HFS+ Catalog file

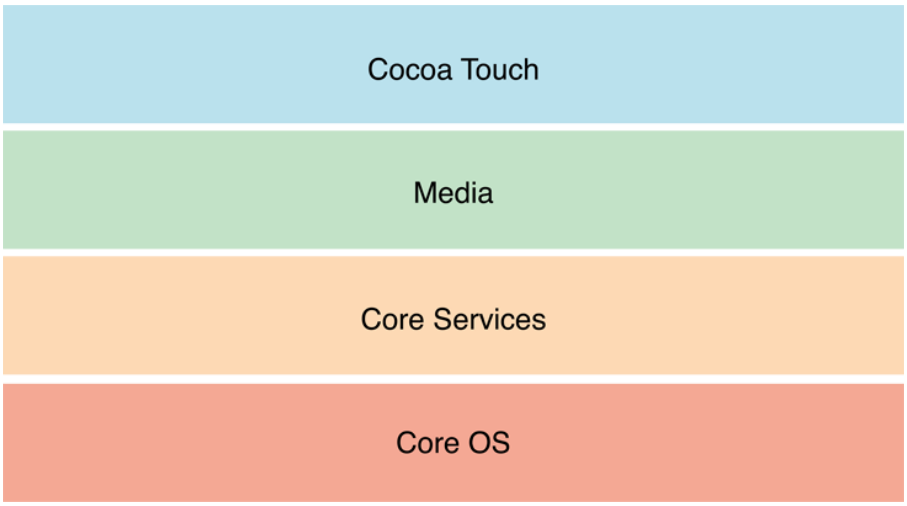
Katalogový soubor popisuje hierarchii souborů a adresářů uložených na svazku. Obsahuje také metadata o každém souboru a adresáři na svazku, včetně časových informací o modifikaci, přístupu a vytvoření. Každému vytvořenému souboru je přiřazeno catalog ID, které je automaticky navyšováno.[4]

4.1.5 Oddíly souborového systému

Zařízení s operačním systémem iOS má standardně 2 oddíly. Prvním oddílem je oddíl určený pro firmware. Na tento oddíl nelze zapisovat s výjimkou aktualizací firmwaru. Když je prováděna aktualizace přes iTunes, je oddíl přepsán novým oddílem. Tento oddíl nás také zajímá, pokud chceme provést jailbreak zařízení. Obvykle je v rozmezí 0.9 až 2.7 GB, v závislosti na velikosti NAND paměti a neobsahuje uživatelská data. Druhý oddíl obsahuje uživatelská data. Na tomto oddílu jsou uloženy všechny aplikace z iTunes spolu s informacemi o uživateli.

4.2 Architektura systému iOS

Operační systém iOS se skládá ze čtyř hlavních vrstev, které zajišťují základní funkčnost a poskytují vývojářům API a frameworky potřebné pro vývoj aplikací. Rozložení vrstev je zobrazeno na obrázku 2.



Obrázek 2 Rozložení vrstev [5]

4.2.1 Vrstva Cocoa Touch

Tato vrstva je nejdůležitější pro vývojáře aplikací. Obsahuje frameworky, které ulehčují práci při vytváření aplikací. Vrstva obsahuje také High-Level funkci Multitasking, která po stisknutí tlačítka Home přesune aplikaci do pozadí. Posléze aplikace je uložená v paměti a lze jí opět obnovit. Od verze iOS 4.0 se tato funkce využívá pro maximální výdrž baterie. Vrstva Cocoa Touch zprostředkovává také rozpoznání jednoduchých a vícenásobných gest prstů. Mimo těchto funkcí, vrstva obsahuje i další frameworky.[5]

Příklady frameworků:

- Address Book UI Framework (rozhraní pro zobrazování a úpravu kontaktních informací)
- Game Kit Framework (podpora peer to peer komunikace pomocí Bonjour)
- Event Kit UI Framework (umožňuje práci s událostmi, např. položky v kalendáři)
- Message UI Framework (zajišťuje vytváření a odesílaní SMS a emailů)

4.2.2 Vrstva Media

Tato vrstva obsahuje grafické, audio a video technologie pro vývoj aplikací. Grafické technologie poskytují funkce pro práci s grafikou a animací. Audio technologie umožňují nahrávaní a přehrávání zvuku v nejvyšší kvalitě. Technologie AirPlay se stará o streamování. Vrstva zahrnuje také používání vibračních funkcí pro některá zařízení.[5]

Příklady frameworků:

- OpenGL ES Framework (hardwarově akcelerované vykreslení 2D/3D objektů)

- Image I/O (čtení a zápis rozšířených grafických formátů)
- Media Player Framework (přístup k iTunes knihovně a přehrávání skladeb)
- Assets Library Framework (přístup k obrázkové knihovně uživatele)

4.2.3 Vrstva Core Service

Vrstva Core Service zajišťuje základní systémové služby pro všechny ostatní aplikace, mezi které patří úložiště iCloud, sdílení uživatelských souborů přes iTunes, podpora sociálních sítí a přístup ke kontaktům. Vrstva zajišťuje také podporu SQL a XML. Odlehčená verze databáze SQL, označovaná jako SQLite, umožňuje ukládání uživatelských dat. XML podporuje zpracovávání dokumentů.[5]

Příklady frameworků:

- Store Kit Framework (přístup k iTunes a možnost nákupů)
- CFNetwork Framework (komunikace pomocí síťového rozhraní)
- Core Data Framework (ukládání strukturovaných dat)
- System Configuration Framework (nastavení připojení k internetu a zajištění dostupnosti)

4.2.4 Vrstva Core OS

Tato vrstva nám poskytuje nízkoúrovňové funkce, na kterých jsou postaveny téměř všechny ostatní technologie. V aplikacích nejsou využívány přímo, ale využívají je vysokoúrovňové komponenty systému. Vrstva obsahuje Accelerate Framework, který nabízí rozhraní pro práci s matematickými funkcemi, nebo Security Framework, zaručující bezpečnost citlivých dat.[5]

5 Zabezpečení systému iOS

Zařízení s iOS systémem (iPhone, iPad, iPod touch) jsou navrženy s několika typy vrstev zabezpečení. Vrstva Low-level obsahuje funkce pro ochranu proti malwaru a dalším virům. Zatímco High-level vrstva obsahuje funkce umožňující bezpečný přístup k osobním informacím, které zabraňují k neoprávněnému přístupu a pomáhají likvidovat útoky, které se chtějí k osobním a citlivým informacím dostat.

iOS zařízení poskytují přísné bezpečnostní technologie a funkce pro ochranu dat, zároveň dbají o minimální omezení běžného uživatele při práci. Zařízení jsou navrženy tak, že některé bezpečnostní funkce jsou již přednastavené. Proto funkce šifrování dat není možné konfigurovat a uživatel je nemůže omylem zakázat.

5.1 Systémová architektura

Díky těsné integraci hardwaru a softwaru systém iOS umožňuje využívání ověřovacích činností ve všech vrstvách. A to od doby zapnutí zařízení, instalace softwaru iOS až po aplikace třetích stran. Jakmile je systém spuštěn, dochází k boot-up procesu a ověřování základní položky UID přístroje. Každé další kroky procesu jsou analyzovány, jestli jsou důvěryhodné. O důvěryhodnost a bezpečnost se stará XNU a jádro systému iOS. XNU vyhodnocuje bezpečnostní prvky za běhu systému a je nezbytné, aby byl schopen důvěřovat všem vyšším úrovním, funkcím a aplikacím. [6]

5.2 Secure Boot Chain

Boot-up proces obsahuje komponenty, které jsou kryptograficky podepsané Applem a podléhají ověření řetězcem důvěry. Tento řetězec obsahuje základní zavaděče, jádro s jeho rozšířením, a další firmware. Pokud je zařízení zapnuté, Boot ROM kód je kontrolován jako první. Kód Boot ROM je zapsaný v read-

only paměti, je vytvořen během výroby čipu a nastavený jako implicitně důvěryhodný, proto se nedá změnit. Obsahuje Apple Root CA veřejný klíč, který se používá k ověření LLB, jedná se o první krok v ověřovacím řetězci. Takto probíhá krok za krokem a je ověřován, zdali je podepsán Applem. Když LLB dokončí své úkoly, spustí se další fáze iBoot, která ověří a spustí jádro systému iOS. Tato fáze zajišťuje, že při bootovacím procesu není manipulováno s nejnižšími úrovněmi softwaru, a umožňuje systém iOS spustit pouze na ověřených zařízeních. Jakmile jeden z kroků nelze načíst nebo ověřit, boot-up je zastaven a přístroj zobrazí varovaní pro připojení k iTunes. Pokud Boot ROM není schopen načíst nebo ověřit LLB, přístroj vstoupí do DFU režimu. Pomocí iTunes pak dojde k obnovení továrního nastavení.[6]

5.3 Šifrování a ochrana dat

Zařízení má další bezpečnostní prvky k ochraně uživatelských dat. A to v případech, kdyby byly napadeny jiné prvky bezpečnostní ochrany. Jde především o šifrování a ochranu dat pomocí šifrovacích klíčů. Tyto šifrovací prvky umožňují používat integrované vrstvy softwarových a hardwarových technologií. Každé zařízení má jedinečný identifikátor (UID), s AES 256-bitovým klíčem, který je vygenerován při výrobě. Identifikátor UID je unikátní pro každé zařízení, díky kterému jsou data kryptograficky vázaná na konkrétní zařízení. GID je identifikátor celé skupiny zařízení, všechny zařízení používající čip Apple A5 a vyšší, používají tento identifikátor jako další stupeň ochrany. Vypálení identifikátoru do křemíku zabraňuje obejití nebo manipulaci a zaručuje přístupnost pouze z AES klíčů. Identifikátory není možné zjistit, můžeme vidět pouze výsledky šifrování nebo dešifrování. V případě přesunutí procesoru fyzickou cestou z jednoho zařízení na druhé, data zůstanou nepřístupna. UID by se neshodoval se zařízením, na kterém data byla zašifrovaná.[6]

Kromě UID a GID, jsou další šifrovací klíče, které jsou vytvářeny pomocí generátoru náhodných čísel (RNG). Pro vytvořené klíče, které už nejsou používané, je důležité i jejich správné odstranění a to kvůli tomu, aby nedošlo k jejich zneužití. Proto systém iOS obsahuje speciální funkci pro bezpečné mazání dat tohoto typu. [6]

5.4 File Data Protection

Kromě hardwarového šifrování do mobilních zařízení s iOS systémem bylo zapotřebí navrhnout i technologii, která by umožňovala kdykoliv se připojit k internetu, provádět telefonní hovory, pracovat s textovými zprávami a e-maily. Proto byla vytvořena tato technologie, která dokáže reagovat na všechny tyto události, bez dešifrování citlivých dat, stahovaní nových informaci, a to i přesto, že je přístroj uzamčen. Data jsou rozdělena do jednotlivých tříd, kde každá třída má svoje zabezpečení. Data Protection chrání data v každé třídě a přístup je určen pomocí generovaných klíčů.[6]

Pro každý nový oddíl dat Data Protection vytvoří nový 256-bitový klíč, který předává do AES a následně pomocí tohoto klíče soubor zašifruje. Tento klíč je zabalen jedním nebo několika dalšími klíči, v závislosti na okolnostech, při kterých soubor může být otevřen a je uložen do souborových metadat. Při otevření takového souboru dojde k rozbalení jeho metadat, která jsou následně dešifrována klíčem systému souborů. Metadata všech souborů v systému iOS jsou šifrována náhodným klíčem, který je vytvořen při první instalaci systému. Tento klíč je uložen přímo na zařízení a nepodléhá zabezpečení důvěryhodných dat a to kvůli tomu, aby nemohlo dojít k jeho zneužití. Jeho prioritou však je, aby ho uživatel mohl rychle a snadno vymazat. To může uživatel provést přímo na zařízení pomocí funkce smazat data a nastavení anebo na dálku, pomocí iCloud. Pokud klíč bude jedním z těchto způsobu vymazán, všechny soubory se stanou kryptograficky nepřístupné. Obsah souboru je šifrován klíčem, který je vnořen do třídy klíčů. Posléze je klíč uložen v metadatech souboru, kde je

šifrován dalším klíčem systému souborů. Třídy klíčů jsou chráněny pomocí UID a pro některé třídy i uživatelským heslem. [6]

5.5 Uživatelský kód

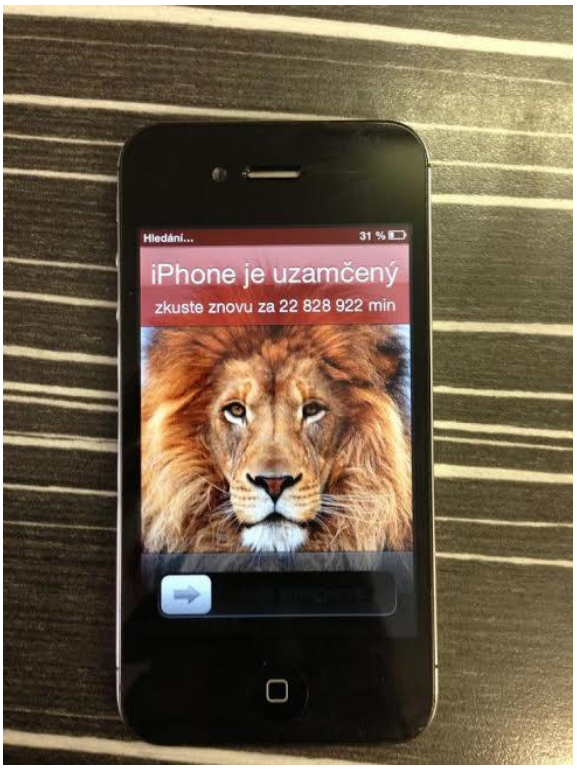
Další bezpečnostní funkcí je uživatelský kód. Zařízení je chráněno minimálně čtyř-číselným kódem. Systém iOS podporuje nastavení libovolné délky hesla s využitím alfanumerických znaků. Kromě odblokování zařízení, poskytuje přístupový kód i entropii pro šifrovací klíče, které nejsou uloženy na zařízení. Systém také dbá na pokusy o prolomení hesla pomocí tzv. hrubé síly a to tak, že každý neúspěšný pokus prodlouží další pokus. Počet opakovaní je nastaven tak, že jeden pokus trvá přibližně 80 milisekund a následně se stupňuje. Uživatel si také může nastavit počet neúspěšných pokusu, po kterém se zařízení automaticky vymaže. V následující tabulce je vidět, jak dlouho by přibližně trvalo prolomení hesla.

	Délka	**Průměrný čas**
Čísla	4	20 minut
	6	35 hodin
	7	2 týdny
	8	4.5 měsíce
	10	40 let
Malá písmena a mezera	5	3 týdny
	6	1.5 roku
	8	1000 let
Velká a malá písmena a mezera	4	11 dní
	5	1.6 roku
	6	88 let

Tabulka 1 Potřebná doba pro prolomení uživatelského hesla

Uzamčená zařízení představují pro forenzní analýzu velký problém. Není totiž možné získat data z takovýchto zařízení pomocí standardních logických metod, jinými slovy, nelze připojit zařízení k počítači a pomocí forenzního nástroje z něj získat informace. Aby vše šlo tak jak má, musí být zařízení odemknuté nebo musíme mít k dispozici nástroj schopný prolomit heslo.

Jistou alternativou se může zdát být tzv. Bypass uživatelského zámku, tedy technika, která nám umožní přístup k zařízení i bez znalosti hesla. Této problematice se věnuje následující kapitola.



Obrázek 3 Uzamčený iPhone

5.5.1 Bypass uživatelského kódu

Přestože se společnost Apple snaží u svých produktů o co nejvyšší zabezpečení, mezi jednotlivými verzemi iOS je možné při znalosti potřebných technik obejít uživatelské heslo a dostat se tak do části telefonu. Nejde ovšem o plný přístup, který získáme při znalosti kódu, ale spíše o přístup k pár

vybraným funkcím. Postupy se obměňují, jak se je Apple snaží pomocí záplat napravit a spolu s tím i funkce, ke kterým získáme při použití bypassu přístup.

Níže jsou uvedeny postupy pro vybrané verze iOS, spolu s funkcemi, které se nám zpřístupní.

1. **Bypass iOS 4.1**
    - **a.** Zapneme přístroj a přejdeme na obrazovku pro nouzové volání
    - **b.** Napíšeme ###, začneme vytáčet a okamžitě stikneme tlačítko pro uzamčení
    - **c.** Získáváme přístup do kontaktů, odkud můžeme poslat email a MMS, získáváme přístup ke kameře a můžeme uskutečnit hovor.
2. **Bypass iOS 6.1**
    - **a.** Zapneme přístroj a přejdeme na obrazovku pro nouzové volání
    - **b.** Podržíme tlačítko Power tak dlouho, dokud se nám nezobrazí možnost vypnutí zařízení
    - **c.** Jakmile se zobrazí možnost vypnutí, zmáčkneme Cancel
    - **d.** Začneme vytáčet číslo 112, ale před samotným uskutečněním spojení hovor ukončíme.
    - **e.** Zmáčkneme tlačítko Power, abychom zařízení uspali
    - **f.** Zmáčkneme tlačítko Power opět, abychom zařízení probudili
    - **g.** Podržíme tlačítko Power a těsně před tím, než se objeví možnost vypnutí telefonu (přibližně 3 vteřiny), zmáčkneme tlačítko nouzového volání. Tento krok je nejnáročnější a vyžaduje přesné načasování.
    - **h.** Zatímco držíme tlačítko Power, získáváme přístup ke kontaktům a historii volání. Zároveň můžeme také provést telefonní hovor.
3. **Bypass iOS 6.1.3 na iPhone 4**
    - **a.** Zapneme přístroj

b. Před tím, než se dostaneme k obrazovce pro zadáním kódu, podržíme tlačítko Home pro aktivování hlasového vytáčení.

c. Zadáme hlasový příkaz pro vytáčení

d. Jakmile začne telefon vytáčet, rychle vytáhneme SIM kartu.

e. Získáváme přístup ke kontaktům a obrázkům. Poněvadž není SIM karta v telefonu, nebude možné provést hovor.

4. **Bypass iOS 7**

a. Zapneme přístroj

b. Přejdeme do Control Center

c. Otevřeme Budík

d. Podržíme tlačítko Power. Jakmile se nám objeví možnost vypnutí zařízení, stiskneme Cancel a hned na to 2x tlačítko Home

e. Získáváme přístup do obrazovky multitaskingu. Odtud se lze dostat k fotoaparátu, fotkám a můžeme sdílet příspěvky na Twitteru, Facebooku nebo posílat emaily.

Výše zmíněné metody tedy získávají většinou přístup ke kontaktům a obrázkům. Větší část důležitých informací ovšem zůstává nepřístupná, např. historie prohlížeče, sms a další. Přesto se ovšem vyplatí znát metody obcházení přístupového kódu, protože lze díky nim získat alespoň částečný přístup do uzamčeného telefonu, který také může přinést důležité informace.

5.6 Classes

Ke každému nově vytvořenému souboru na zařízení s iOS systémem je přidělena příslušná třída. Každá tato třída používá různé politiky k určení, kdy má přístup k souborům.

5.6.1 Complete Protection

Tento klíč třídy je chráněn klíčem, který je odvozen UID zařízením a uživatelským přístupovým kódem. Jestliže uživatel uzamkne zařízení, všechna data v této třídě se stanou nepřístupna a to do té doby, než uživatel zadá heslo. Do této ochrany spadají například zprávy, přílohy a obrázky.[6]

5.6.2 Protected Unless Open

I když je zařízení uzamčené, některé soubory potřebují mít možnost zapisovat. Příkladem je stahování nových e-mailů. Data Protection vytvoří pár veřejný/soukromý klíč. Dále sdílený tajný klíč je vypočítán pomoci soukromého klíče a pomocí klíče třídy, jehož soukromý klíč je chráněn uživatelským heslem a UID. Takto vytvořený sdílený klíč chrání vytvořený pár. Jakmile je práce se souborem ukončená, sdílený klíč a pár veřejného a soukromého klíče je z paměti vymazán. [6]

5.6.3 Protected Until First User Authentication

Tato třída se chová stejným způsobem jako Complete Protection, nemaže pouze klíč třídy z paměti po uzamčení zařízení.[6]

5.6.4 No Protection

Je to výchozí třída pro všechny soubory, která je chráněna pouze UID. Všechny potřebné klíče k dešifrování souborů jsou uložené na zařízení a tak mohou být vzdáleně vymazány. [6]

5.6.5 Keychain Data Protection

Řada aplikací využívá pro ochranu svých dat hesla nebo přihlašovací údaje, o které se Keychain Data Protection starají. Keychain je implementován jako SQLite databáze a je uložená v souborovém systému. Data Keychain jsou chráněna pomocí struktury třídy, podobné té, kterou používají souborové. Tyto

třídy se chovají podobně jako třídy pro ochranu dat, s tím rozdílem, že používají jiné šifrovací klíče a jsou součástí rozhraní API. Keychain třídy jsou chráněny UID, a díky tomu nemůže dojít k zneužití zálohy na jiném zařízení.[6]

5.7 Keybags

Klíče pro file data protection a keychain data protection jsou uchovávány v keybagu. Systém iOS využívá 4 typy keybagu: system, backup, escrow a iCloud backup.

V System keybagu jsou uchovávány klíče zabalených tříd. Pro představu: pokud uživatel zadá heslo, je načtena třída NSFileProtectionComplete ze systém keychain a rozbalena. Jde o binární plist uložený ve třídě No protection. System keybag je jediný ze zmiňovaných, který je uložený přímo na zařízení.[6]

Backup keybag je vytvořen v okamžiku, kdy je provedena záloha zařízení pomocí iTunes. Tento keybag je chráněný heslem, zadaným v iTunes.[6]

Escrow (podmíněný) keybag je použit pro synchronizování iTunes. Tento keybag umožňuje uživateli, aby prováděl zálohu a synchronizaci s iTunes, aniž by musel zadávat heslo. Je uložen na počítači, který provádí synchronizaci.[6]

iCloud backup keybag je podobný backup keybagu. Všechny třídy klíčů v tomto keybagu jsou asymetrické a tak iCloud backup může být proveden na pozadí.[6]

6 Jailbreak

Jailbreak je technika, která má za cíl nahrazení firmware oddílu zařízení upravenou verzí, umožňující mimo jiné instalaci softwaru pro zkoumání zařízení. S funkčním jailbreakem je tak možné využití například SSH nebo Terminálu. Dále získáváme plný přístup do souborového systému zařízení, kde tak uvidíme všechny lokální soubory. U této problematiky je třeba rozlišovat pojmy jailbreak, root a unlock. Zatímco jailbreak bývá spojovaný s iOS a odemyká na zařízení výše zmíněné možnosti, root bývá na druhou stranu spojován s operačním systémem Android. Nabízí ale velmi podobnou funkcionalitu. Pokud je zařízení určeno pouze pro jednoho operátora (typicky u dotovaných telefonů se smlouvou) a chceme ho používat i pod jiným operátorem, je třeba provést unlock, který tuto možnost odemkne.

6.1 Provedení jailbreak

V současnosti existuje hned několik nástrojů, které umožňují provést jailbreak zařízení. Kvůli pohodlí uživatelů jsou často jednoduché a vyžadují pouze vybrání zařízení a určení verze iOS. Následuje proklikání se instalačním wizardem a jailbreak je proveden.

Pro příklad si uveďme webovou stránku http://www.jailbreak-me.info/, kde se můžeme po vyplnění informací o našem zařízení informovat, zda pro nás existuje jailbreak.

Obrázek 4 Zjištění, zda existuje jailbreak pro naše zařízení

Po stisknutí tlačítka Check your iDevice se provede kontrola, zda existuje vhodný jailbreak a zároveň je nám nabídnut odkaz ke stažení.

Obrázek 5 Odkaz na jailbreak software

Po kliknutí na odkaz se nám stáhne malý downloader, který po spuštění stáhne aplikaci, sloužící pro jailbreak přes počítač.

Obrázek 6 Aplikace pro jailbreak

Jak aplikace sama hlásá, je silně doporučeno před samotným jailbreakem provést zálohu pomocí iTunes. Pokud by instalace selhala nebo bychom se chtěli v budoucnu vrátit zpět do stavu před jailbreakem, musíme mít zálohu. Pokud využíváme heslo pro zálohu v iTunes nebo uživatelský kód, je doporučeno před započetím jailbreaku je vypnout. Poté už stačí jen stisknout tlačítko Jailbreak a sledovat postup, který probíhá automaticky bez nutnosti další interakce uživatele. V případě, že během provádění jailbreaku se proces

zasekne, je bezpečné aplikaci restartovat, restartovat i zařízení (podržením tlačítka Power a Home, dokud se zařízení nevypne) a proces zvrátit, případně využít iTunes a zálohu, pokud všechny pokusy o zprovoznění selžou.

6.2 Výhody jailbreak na zařízení

Jak již bylo zmíněno, jailbreak sebou přináší řadu výhod. Je možné například instalovat nová témata a přizpůsobit si tak vzhled zařízení podle svého, zvolit si vlastní vyzvánění, využívat program iFile, který slouží jako průzkumník ve Windows, přístup k aplikacím ze Cydie, která je alternativou App Store pro jailbreaknuté telefony a provedení unlock telefonu, umožňující ho používat se všemi operátory.

Pro potřeby forenzní analýzy je ale nejdůležitější fakt, že jailbreaknuté zařízení umožňuje přístup do všech jeho částí a tedy forenzní nástroje dokážou z přístroje získat více informací.

6.3 Dopady jailbreak na zařízení

Jailbreak má ovšem i své stinné stránky. Zatímco se dá na přístup ke všem souborům obecně pohlížet jako na výhodu, pro méně zkušeného uživatele, který ať už úmyslně, či neúmyslně smaže nebo poškodí systémový soubor, může tato „výhoda“ znamenat nutnost obnovy ze zálohy. Další nevýhodou může být snížená výdrž baterie, protože některé programy, nutné pro chod jailbreaku, musí být stále spuštěné. Jailbreak může také zpomalit spouštění aplikací, protože na některých zařízeních bylo evidováno vyšší využití RAM paměti. Pokud je na zařízení jailbreak, přicházíme také o možnost aktualizace iOS metodou Over the air, která nevyužívá počítač ke stažení aktualizace, ale data jsou stahována přímo do zařízení. Dále, pokud bychom chtěli zařízení reklamovat, prodejce nebo servis nemusí zařízení přijmout z důvodu přítomnosti jailbreaku. Zařízení by se tedy muselo dát do továrního nastavení.

Pro potřeby forenzního zkoumání je situace složitější. Jak již bylo zmíněno, jednou z podmínek forenzního zkoumání je nutnost integrity dat, tzn., že data nesmí být pozměněna. Pokud by ovšem znalec pro potřeby zkoumání chtěl využít jailbreak, dojde k jejich pozměnění. Záleží pak už na situaci, zda je jailbreak skutečně pro potřeby zkoumání třeba. Druhým problémem je povinnost uvést zařízení do stavu, ve kterém bylo před začátkem zkoumání. Pokud bychom se totiž rozhodli aplikovat jailbreak, nelze ho po zkoumání jednoduše odstranit, ale zařízení by se muselo obnovit ze zálohy nebo uvést do továrního nastavení.

7 Metody získávání dat

Pro potřeby forenzního zkoumání je třeba nejprve data získat. Ty se získávají z disku nebo paměti zařízení a jsou uloženy v externím souboru, který může být prozkoumán forenzním nástrojem. Důvodem tvorby obrazu dat je mít kopii, se kterou se může bezpečně pracovat bez rizika poškození originálních dat. „Nejvyšší metou“ forenzního získávání dat je metoda bitové kopie originálu, která má za následek vytvoření identického obrazu. Zatímco tyto metody jsou velmi dobře známé a relativně snadno proveditelné u počítačů, u mobilních zařízení a tabletů se setkáváme s řadou překážek. Pevné disky z počítačů snadno vyndáme, můžeme využít nabootování do forenzního prostředí. U mobilů a tabletů ovšem těžko vyndáme paměť, protože je připájená na desce a omezení operačních systémů neumožňují nabootování do jiného prostředí.

7.1 Backup metoda

Tato metoda se využívá v případě, že již nemáme k dispozici fyzické zařízení. Spočívá ve využití zálohy, která byla uložena na počítači. Poněvadž zdrojem dat jsou zálohované soubory určené synchronizačním protokolem, získáme přístup pouze k nim. Existuje řada forenzních nástrojů, schopných získat data ze zálohy. Jde například o Oxygen Forensic Suite nebo iPhone Analyzer.

Když dojde k vytvoření zálohy zařízení pomocí iTunes, data jsou uložena v defaultním adresáři v závislosti na používaném operačním systému (více v sekci 8.2). Soubory status.plist, info.plist a manifest.plist jsou konfigurační soubory, které uchovávají informace o zařízení, zálohách a stavu zálohy. Pro naše potřeby jsou nejdůležitější soubory *.mddata a *.mdinfo. Ty obsahují uživatelská data.

7.2 Logická metoda

Logická metoda získávání dat znamená kopírování aktivního souborového systému zařízení do jiného souboru. Díky této metodě je možné získat alokovaná data, která mohou být později analyzována. Tento přístup bývá často prvním a také jediným způsobem získávání dat, protože je jednoduchý a poskytuje dostatečné množství dat. Fyzické metody sice mohou poskytnout mnohem více dat, ale jsou také mnohem náročnější na úspěšné provedení a vyžadují více času na analýzu. Logická metoda jde aplikovat pouze na odemčená zařízení.

Řada forenzních nástrojů podporujících logické metody jako svůj výstup nabízí report, který obsahuje často otevírané soubory. Problémem bývá, že znalec sice vidí data, ale nevidí jejich zdroj, např., report může sdělovat, že byla navštívena určitá webová adresa, ale už neříká kdy. Pro tyto případy pak musí mít znalec přístup ke zdrojovým datům, aby si chybějící informace dohledal.

Obecný postup pro získání dat pomocí logické metody je následující:

1. Spustit vybraný forenzní nástroj
2. Připojit zařízení
3. Začít získávat data. Postup bude velmi podobný jako u Backup metody, s tím rozdílem, že nebudeme získávat data ze zálohy, ale z fyzického zařízení.

7.3 Fyzická metoda

Fyzická metoda je už řadu let využívána ve forenzním zkoumání, ale je relativně nová pro mobilní telefony a tablety. Bohužel u neupraveného zařízení nám brání bezpečnostní mechanismy v provedení forenzní analýzy fyzickou

metodou. Avšak existuje několik metod sloužících k získání potřebných práv na vytvoření obrazu NAND paměti.

Fyzická metoda vytváří bitovou kopii souborového systému zařízení, podobně jako to můžeme znát u harddisku. Tento přístup má největší úspěch v množství získaných dat a to i proto, že je schopný získat také smazaná data. Pokud by zařízení bylo uzamčeno a my chtěli získat všechny data, musí nástroj obsahovat funkci prolomení hesla. Tuto funkci obsahuje například UFED Physical Analyzer.

Vydání zařízení s čipem A5 přineslo řadu problému pro forenzní analýzu. Na zařízeních s tímto čipem (iPhone 4S, iPad2 a vyšší) se vyskytuje hardwarové šifrování, které způsobí, že ač je možné vytvořit bitovou kopii zařízení, tak data budou stále šifrována. Toto šifrování se musí následně prolomit. V současnosti fyzické nástroje plně podporují mobilní telefony do verze iPhone 4 a první verzi iPadu. U těchto zařízení lze provést úspěšně fyzickou analýzu. Novější zařízení tuto metodu neumožňují, pokud nejsou jailbreaknutá.
Pro vytvoření a následné prolomení šifrování u podporovaných zařízení je několik způsobů. První je Zdziarskiho metoda, která nahrazuje software RAM paměti verzí, umožňující vytvoření bitové kopie. Tato metoda ovšem není pro veřejnost dostupná. Dalším způsobem je využití aplikace Lantern 2. Ta umožňuje jak vytvoření bitové kopie, tak i prolomení hardwarového šifrování. Je možné taky využít aplikaci iXam, která se nesnaží modifikovat NAND paměť ani neupravuje jádro systému, jako v případě jailbreakingu. Další možností je využití aplikace UFED Physical Analyzer, která je schopná pracovat kromě iOS i s BlackBerry a Androidem.

7.4 Jailbreak metoda

Pro potřeby forenzní analýzy se dá využít ještě jedna metoda získání dat ze zařízení. Pokud budou práva upravená pomocí jailbreaku a zařízení se bude

vyskytovat ve stejné síti jako počítač, je možné využít vzdálenou extrakci obrazu paměti. Na stanici, kterou využíváme pro analýzu dat, stačí zadat tento příkaz k zahájení procesu extrakce dat:

```
ssh root@192.168.0.1 dd if=/dev/rdisk0 bs=1M | dd
of=ios_obraz.img
```

Toto je ovšem možné pouze v případě, že se na zařízení vyskytuje běžící SSH server. IP adresu zařízení v příkladu je pak třeba nahradit reálnou adresou, kterou můžeme vyčíst z nastavení WiFi. Příkaz `dd` říká, že má dojít k bitovému kopírování. Zdrojem tohoto kopírování je celá NAND paměť, ne pouze určitý oddíl. Parametr `bs` (block size) určuje, po jak velkých kusech se mají data načítat. Poté pomocí „roury“ (pipe) přesměrujeme vstup na další příkaz, jehož výsledkem je po provedení na počítači soubor ios_obraz.img, obsahující obraz paměti zařízení. S tímto obrazem lze pracovat pomocí forenzních nástrojů.

Je ovšem třeba mít na paměti, že jak již bylo zmíněno v sekci 7.3, zařízení s čipem A5 (iPhone 4S, iPad2 a vyšší) s sebou přináší hardwarové šifrování. Jailbreak ovšem není schopen toto šifrování prolomit a tak výsledkem výše zmíněného příkazu na novějších zařízeních bude zašifrovaný obraz. Pokud bychom chtěli obraz dešifrovat, museli bychom použít vhodný nástroj. Příklady těchto nástrojů jsou uvedeny v předchozí podkapitole. Tato metoda má tedy smysl pouze u starších zařízení. U novějších je pro bitovou kopii vhodnější fyzická metoda s nástrojem schopným dešifrovat obraz paměti.

8 Nástroje

V této kapitole bude čtenář seznámen s důležitými nástroji pro forenzní analýzu iOS zařízení. Je třeba upozornit, že řada z níže zmíněných nástrojů je placených a pro účely této práce byly zvoleny jejich bezplatné verze. Dá se předpokládat, že jejich možnosti se budou lišit od placených verzí, které jsou určeny především pro profesionály.

8.1 Find My iPhone / iPad

Služba Find My iPhone / iPad je jednou ze součástí služeb iCloud. Tato služba slouží jako bezpečnostní pojistka při ztrátě nebo odcizení zařízení a může Vám jej pomoci nalézt, poslat na něj zprávu, vzdáleně uzavřít nebo zcela vymazat.

Tyto bezpečnostní prvky zařízení nám mohou znepříjemnit a následně omezit forenzní zkoumání. V této kapitole budou dané postupy použité ke zmírnění ztráty dat a přístupu k zařízení.

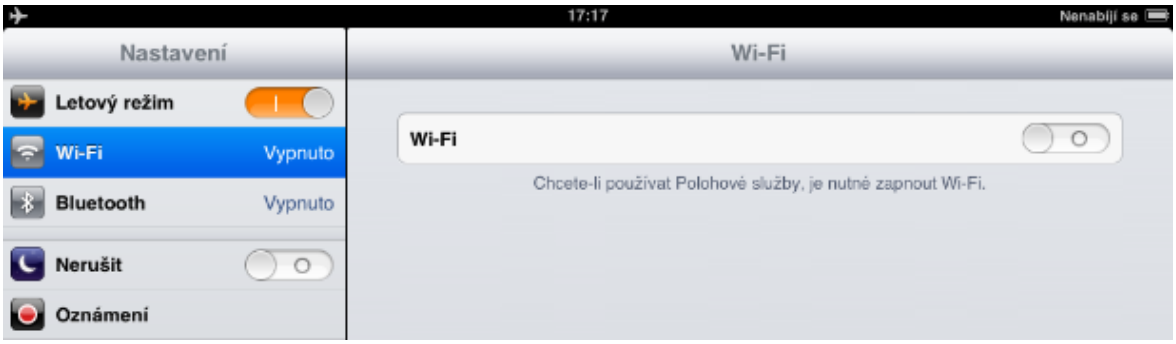
Obrázek 7 Zapnutí funkce Hledat iPad

Jakmile tyto kroky byly dokončeny, každý, kdo má přístup k on-line iCloud účtu, může vzdáleně vymazat nebo uzamknout zařízení.

Izolace zařízení

Ke zmírnění ztráty dat, když narazíme na iOS zařízení, a heslo není aktivní, použijeme následující kroky k izolaci zařízení od Cellular a Wi-Fi sítě.

1. Klepněte na ikonu Nastavení. 
2. Klepněte na horní nastavení, Letový režim
3. Přepneme z vypnuto na zapnuto.
4. Někdy Letový režim může být aktivní a Wi-Fi bude stále aktivní. V nastavení přepneme zapnuto na vypnuto, jak je znázorněno na obrázku 8.
5. Na iPod touch a Wi-Fi iPad, stačí vypnout pouze Wi-Fi. (neplatí pro verze s Cellularem)



Obrázek 8 Nastavení Letový režim, Wi-Fi vypnuto

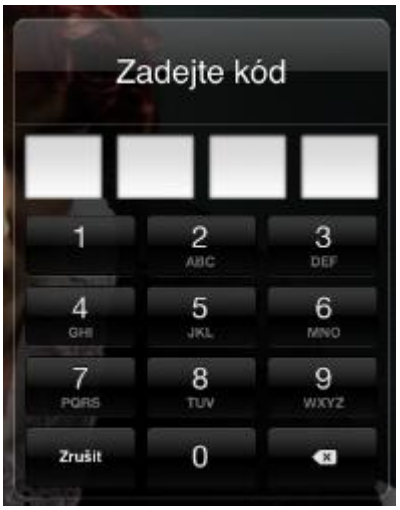
Další krokem je vysunutí SIM karty nebo mini-SIM karty z iPhonu nebo iPadu. Pomocí kancelářské sponky nebo nástrojem pro vysunutí SIM karty, který je dodáván se zařízením, můžete vysunout SIM kartu z horní nebo boční strany přístroje.

Pokud zařízení má aktivovaný kódový zámek a je uzamčené, můžeme rychle a bezpečně izolovat zařízení pomocí staniolu.

Passcode

Dále musíme zjistit, zda přístupový kód zámku byl aktivován. Chceme-li to zjistit, postupujeme takto:

Pokud po probuzení zařízení nám vyskočí na obrazovku Enter Passcode (Zadejte kód), viz obrázek 9, přístupový kód je aktivní. Šance na získání kódů bez speciálního nástroje je nulová.



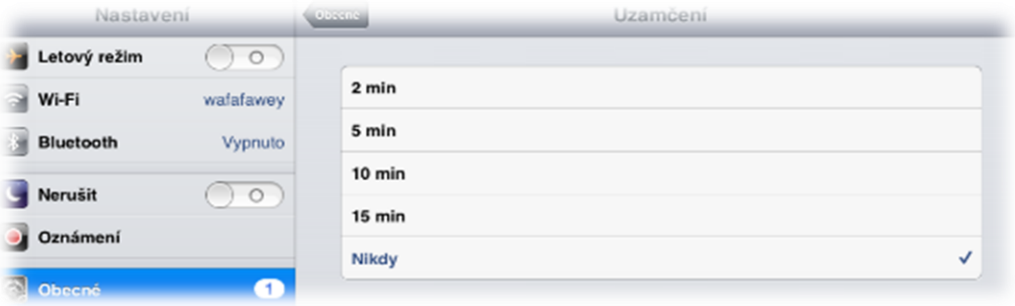
Obrázek 9 Zadejte přístupový kód

Můžeme také narazit na iOS zařízení, které má kódový zámek aktivní a Auto-Lock (Uzamčení) nebylo zakázané. V takovém případě postupujeme následovně.

1. Klepněte na ikonu Nastavení. 
2. Klepněte Obecné.
3. Pokud narazíme na obrazovku, viz obrázek 10, zařízení má heslo.

Obrázek 10 Kódový zámek aktivní

1. Klepněte na Auto-Lock (Uzamčení)
2. Změníme nastavenou hodnotu 10 min na hodnotu Nikdy, jak je znázorněno na obrázku 11.
3. Tyto úpravy nám ulehčí práci při dalším zkoumaní. Zařízení bude mít pořad aktivní kód zámku, ale zkoumající bude mít plný přístup k zařízení. Proto nesmíme zapomenout na příslušenství daného zařízení, jako je USB kabel nebo napájení. A hlídat stav baterie daného zařízení.



Obrázek 11 Změna hodnoty na Nikdy

8.2 Backup iTunes

Forenzní analýzu lze provádět ze záloh z iTunes nebo přímo ze živého zařízení. Tato metoda je nejméně náchylná na ztrátu dat. Analýza na živém zařízení je časově náročnější a především obnáší technické problémy spojené s restartováním zařízení a změnou informaci uloženích v daném zařízení. Proto

v kritických případech forenzní analytik spoléhá na zálohy získané přes iTunes. iTunes používá AFC (Apple file connection) protokol, který provádí zálohy dat, aniž by to nějak změnilo obsah daného zařízení.

V této kapitole se budu věnovat především analýze z iTunes. Vysvětlím technické postupy a analýzy spojené s extrahováním dat ze záloh iPad. Pochopení forenzní analýzy spojené s iTunes je také užitečné v případech, kdy se získá fyzický přístup k počítači podezřelého místo iOS zařízení přímo. Pokud podezřelý používá počítač pro synchronizaci se svým zařízením, většina informací, dat, bude právě zálohována v počítači. Získáme-li přístup k danému počítači, je pravděpodobné získat i přístup k datům mobilních zařízení.

Forenzní analýza byla provedena na iPad mini s iOS 6.1 Zálohy uvedené v této kapitole byly pořízené pomocí iTunes 11.0

iTunes záloha:

Jak bylo zmíněno, iTunes slouží k synchronizaci iOS zařízení s počítačem. Pokud je iOS zařízeni připojené k počítači poprvé a synchronizuje se s iTunes, iTunes automaticky vytvoří složku se zařízením UDID (unikátní ID zařízení - 40 hexadecimálních znaků), jako jméno a zkopíruje obsah zařízení do nově vytvořené složky.

iOS zařízení lze synchronizovat pomocí iTunes přes Wi-Fi nebo připojeným USB kabelem. Během první synchronizace iTunes vyžaduje úplnou zálohu zařízení. Při dalším zálohování iTunes pouze přepíše data, která jsou upravená na zařízení. Umístění záloh vytvořených pomocí iTunes se liší pro různé operační systémy.

Přesné cesty k adresářům pro různé operační systémy jsou znázorněné níže.

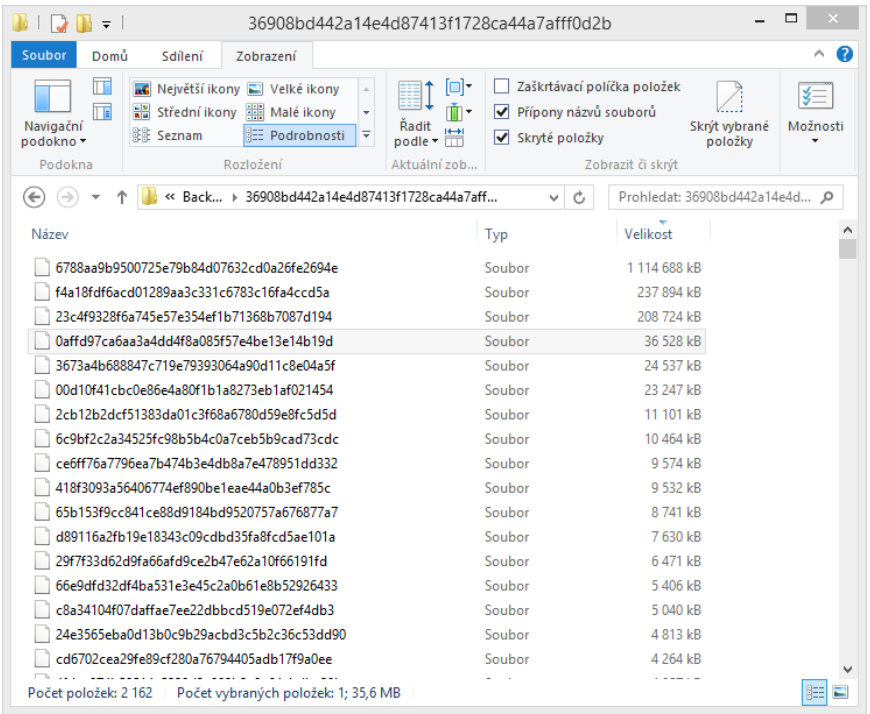
Windows XP	%HOMEPATH%\ApplicationData\AppleComputer\MobileSync\Backup\{UDID}

Windows Vista/7/8	%HOMEPATH%\AppData\Roaming\Apple
OS X	~/Library/Application Support/MobileSync/Backup/{UDID}

Tabulka 2 Cesty k zálohám zařízení

Zálohované informace zahrnují nakoupenou hudbu, televizní pořady, aplikace a knihy, fotky a videa ve složce Fotoaparát; nastavení zařízení (například oblíbené položky telefonu, tapetu a účty pošty, kontaktů a kalendářů); data aplikací; uspořádání aplikací na výchozí obrazovce; zprávy (iMessage, SMS a MMS), zvonění a další. Soubory médií synchronizované z počítače nejsou zálohovány, ale lze je obnovit synchronizací s iTunes.

Složka obsahuje seznam souborů, které nejsou v čitelném formátu, a skládají se z jedinečně pojmenovaných souboru s 40místným alfanumerickým HEXa názvem bez jakékoliv přípony souboru.

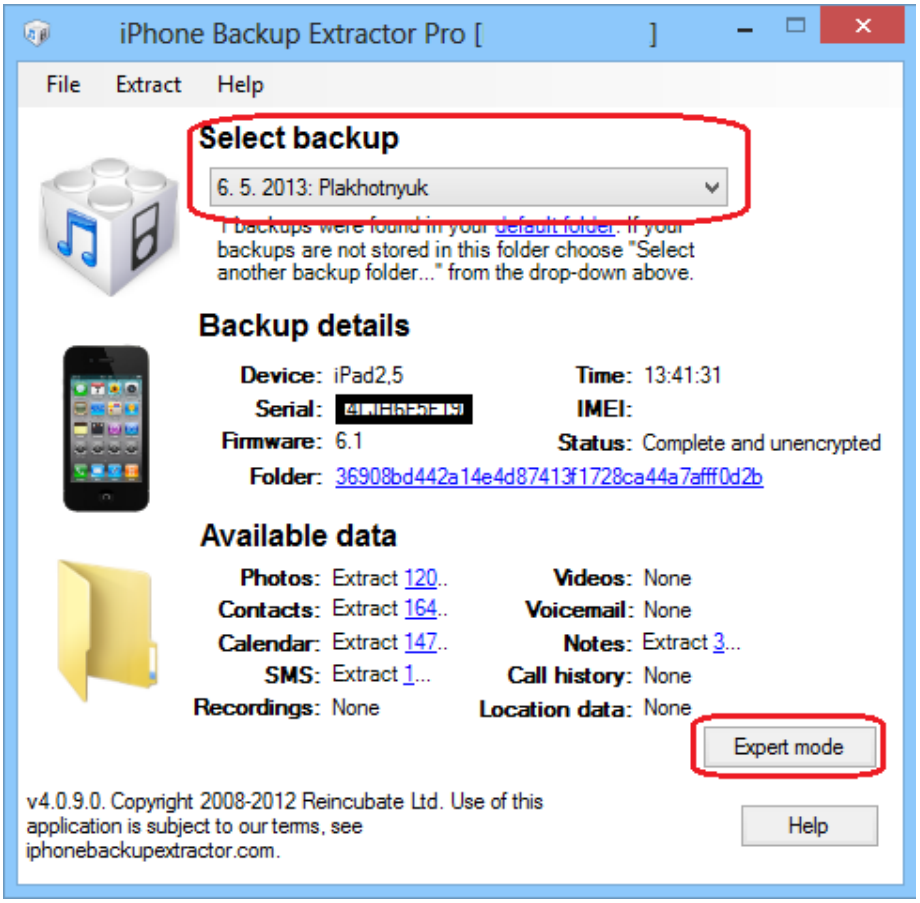


Obrázek 12 Seznam souborů s HEXa názvem

8.3 iPhone Backup Extractor

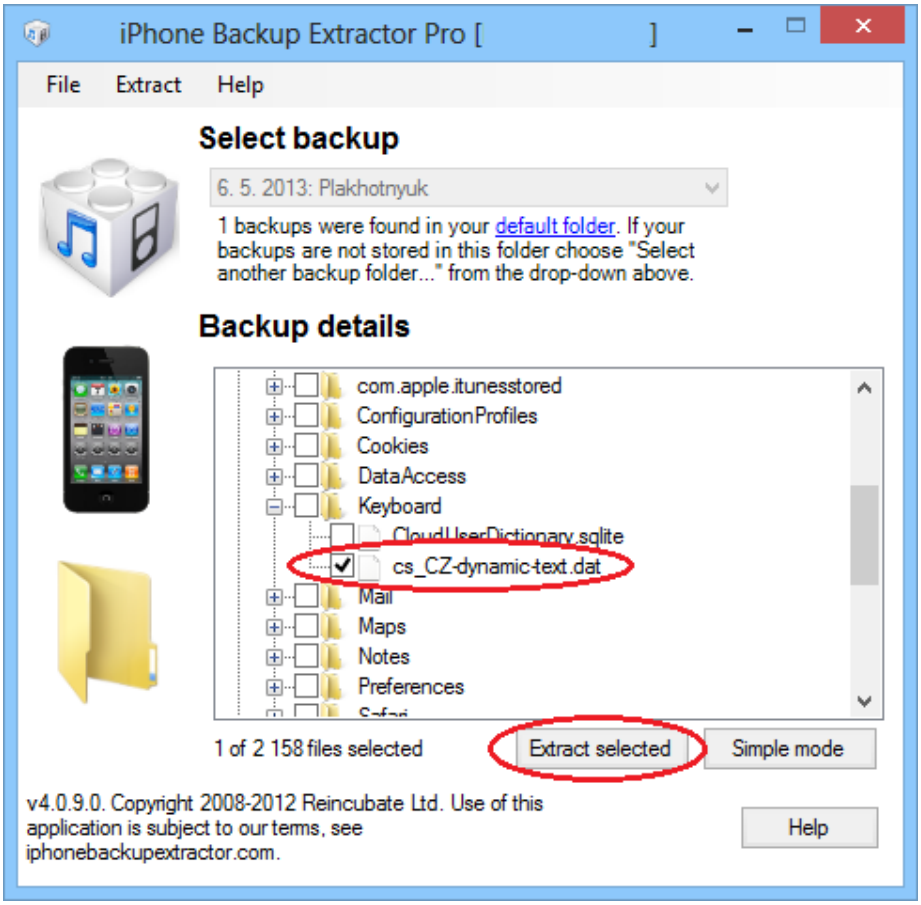
Pro analýzu dat ze záloh můžeme použít několik speciálních nástrojů. V tomto případě byl zvolen iPhone Backup Extractor a to přímo pro analýzu Keyboard (klávesnice). iOS zařízení zaznamenává většinu slov, co uživatel zadává na klávesnici, to aby bylo možné zajistit funkce, jako jsou automatické opravy chyb a vyplňování formulářů. Rovněž mohou být uložené i citlivé údaje. Téměř každé nečíselné slovo je uložené v mezipaměti klávesnice a to v takovém pořadí, v jakém bylo napsané. Mezipamět klávesnice není vázaná na mezipamět dané aplikace a tak data nemohou být odstraněna. Údaje napsané do textových polí pro prakticky libovolnou aplikaci, mohou zůstat v mezipaměti po dobu delší než jeden rok, pokud sám uživatel pravidelně neobnovuje nastavení.

Po spuštění iPhone Backup Extractor máme základní informace o dané záloze, z jakého zařízení byla záloha provedená, sériové číslo zařízení, v jakém čase byla záloha provedená. A hlavně samotná data. Po výběru zálohy přejdeme na Expert mode.



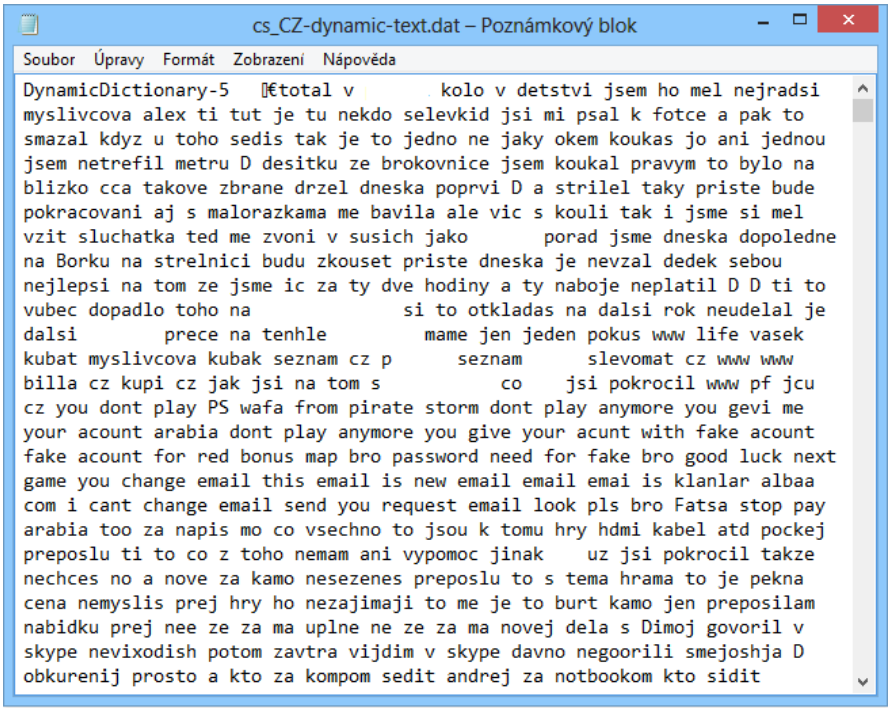
Obrázek 13 Informace z iPhone Backup Extractor

V expert modu máme detailní přehled o zálohovaných souborech: Application (aplikace), Library (knihovna), Media, SystemConfiguration (systémové nastavení). Nás bude především zajímat Library a v ní složka Keyboard (klávesnice). V které se nachází cs_CZ-dynamic-text.dat, jak je znázorněno níže. Zvolíme Extract selected a vybereme místo uložení.

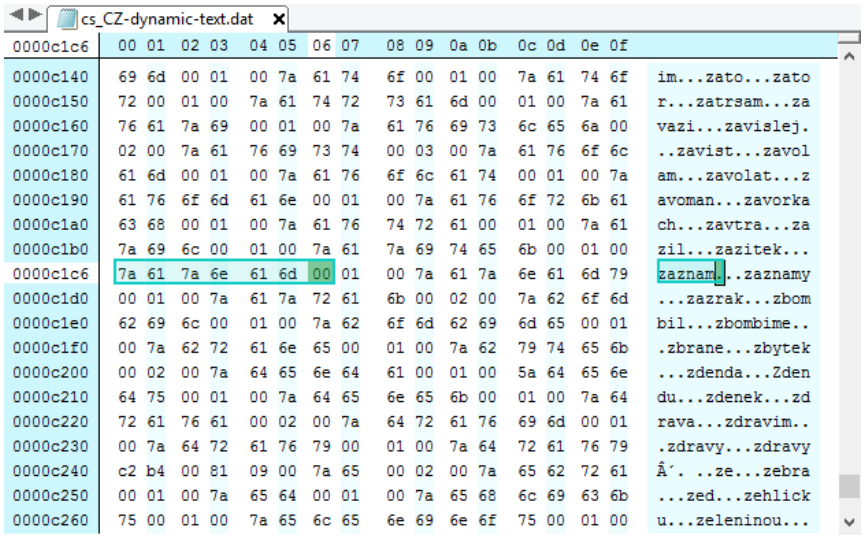


Obrázek 14 Výběr požadovaných informací pro extrakci

V konečné fázi máme složku \Library\Keyboard\cs_CZ-dynamic-text.dat. Soubor cs_CZ-dynamic-text.dat je binárního typu, který obsahuje text zadaný uživatelem. Text je často zobrazen v takovém pořadí, v jakém byl psán a to nám umožní dát dohromady fráze nebo věty při řešení daného incidentu.



Obrázek 15 Zobrazení dynamického textu v poznámkovém bloku



Obrázek 16 Zobrazení dynamického textu v Hex Editoru Neo

8.4 MOBILedit! Forensics

MOBILedit! Forensics je jedním z nejpoužívanějších vyšetřovacích nástrojů mobilních zařízení, který umožňuje získat přehled o obsahu mobilního zařízení. Tento produkt je vysoce hodnocený Národním institutem standartu a technologií a jako primární nástroj pro vyšetřování se používá ve více než 70 zemích světa. [7]

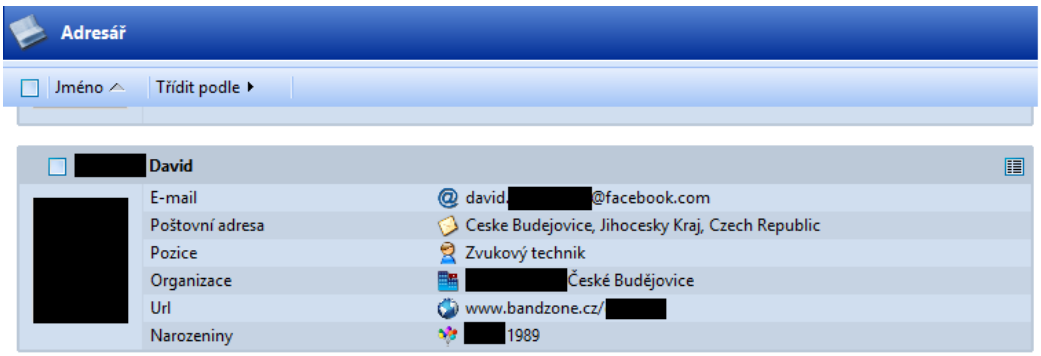
MOBILEdit! Forensic je forenzní logický nástroj, určený pro analýzu mobilních zařízení. Jeho výhodou je jednoduché připojení, ať už pomocí USB kabelu, Wi-Fi, Bluetooth nebo IrDA. MOBILedit! Forensics je komerční nástroj a k jeho plnému užívání je třeba vlastnit platnou licenci, která stojí téměř jedenáct tisíc korun. Pro potřeby testování byla zvolena nekomerční verze MOBILedit! Lite. Po získání nástroje a jeho jednoduché instalaci bylo připojeno zařízení k počítači pomocí USB kabelu, do zkoumaného zařízení bylo zapotřebí nainstalovat MOBILedit! Connector. Posléze nástroj sám vyhledal zařízení a umožnil jeho okamžité prohlížení.

MOBILedit! Forensics dokázal ze zařízení (iPad mini a iPhone 4S) získat:

- Základní informace o zařízení
- Adresář
- Zmeškané hovory
- Volaná čísla
- Přijaté hovory
- Zprávy
- Data aplikací
- Schůzky
- Poznámky

Adresář

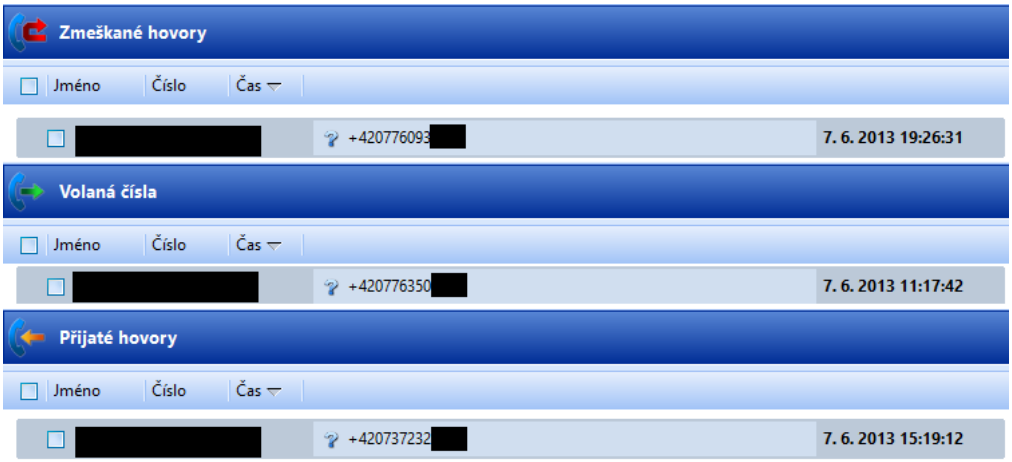
V seznamu uložených kontaktů se objevily nejenom jména a telefonní čísla, ale také další informace jako e-mail, poštovní adresa, pozice, organizace, URL (webová stránka) a narozeniny.



Obrázek 17 Položka Adresář z MOBILedit! Forensics

Zmeškané hovory, volaná čísla, přijaté hovory

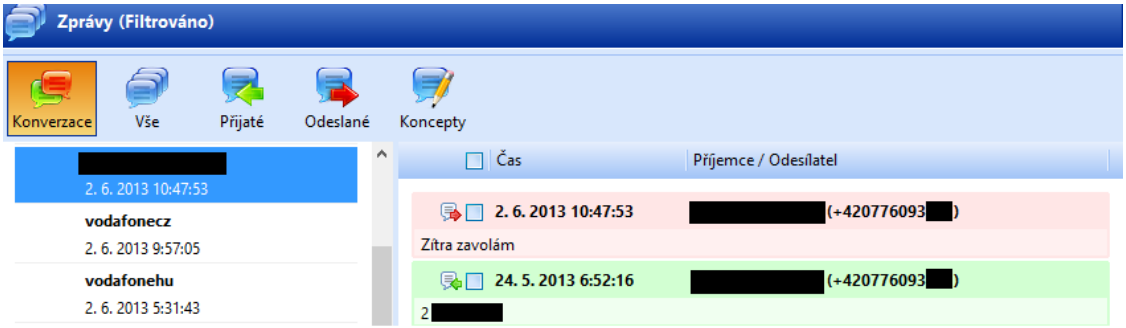
V testovacím případě se jednalo o přehled zmeškaných, přijatých a volaných čísel, s informací, jakého dne se hovor uskutečnil, v kolik hodin a o jaké telefonní číslo šlo. Pokud je telefonní číslo obsaženo v adresáři, je u telefonních čísel uvedeno i jméno.



Obrázek 18 Položka Zmeškané hovory z MOBILedit! Forensics

Zprávy

Pro lepší přehlednost jsou zprávy rozděleny pomocí filtru na konverzace, všechny, přijaté, odeslané a koncepty. Je zde uveden datum, čas, jméno, telefonní číslo a obsah konverzace.



Obrázek 19 Položka Zprávy z MOBILedit! Forensics

Pomocí MOBILedit! Lite byly dále získány základní informace o telefonu, jsou-li využívány schůzky (kalendář), lze také zjistit jeho přesný obsah. V poznámkách je vidět jednoduché shrnutí obsahu. Data aplikací obsahují veškeré informace o aplikacích na daném zařízení. Na testovaném zařízení iPhone 4S jsem měl přístup ke CameraRollDomain, ve které jsem viděl veškeré fotografie pořízené tímto zařízením. Daly se vyčíst názvy fotografií, velikost, datum a čas vytvoření a jejich změny.

8.5 iPhone Analyzer

iPhone Analyzer je dalším z logických nástrojů, který nám umožňuje analyzovat nebo obnovit data ze záloh zařízení. Ke své práci používá zálohy vytvořené pomoci iTunes. Vzhledem k tomu, že pracuje se zálohami, práce s ním je bezpečná a nedochází ke změně dat.

iPhone Analyzer je dostupný pro všechny, jedna se o open-source nástroj a k jeho práci není potřeba žádná licence nebo aktivační klič. Je to multi-platformní Java nástroj, který je podporován na Linuxu, Mac i Windows. Ke stažení je na http://sourceforge.net/projects/iphoneanalyzer/.

Po stažení není třeba žádná instalace, stačí pouze otevřít JAR soubor a přistoupit k analýze. Nástroj nám dává možnost pracovat s celou zálohou anebo s jejími částmi. K dispozici je také možnost přístupu k živému zařízení pomocí SSH, ovšem pouze s jailbreakem. Tato možnost je v beta verzi a nepodporuje všechny verze iOS.

Při testování jsem používal zálohy ze zařízení iPad mini (iOS 6) a iPhone 4S (iOS 6). Po načtení záloh se zobrazily tyto informace:

- Informace o zařízení
- Adresář
- Zvukové zprávy
- Textové zprávy (všechny, přijaté, odeslané)
- Volání (všechny, přijaté, odchozí)
- Všechna média
- Koncepty
- Adresář souborového systému

Informace o zařízení

Obsahovaly informace, kdy byla záloha vytvořena, identifikační číslo zálohy, verze iOS systému, typ zařízení, sériové číslo zařízení, verze iTunes.

Adresář

Pří testování se zobrazil seznam kontaktů, kdy pomocí dalších záložek máme možnost vidět tyto informace v SQL databázi, textové, a v hexadecimální podobě. Nejdůležitější záložkou však zůstávají odstraněné fragmenty, které nástroj dokázal ze záloh dostat. Smazané fragmenty můžeme vidět na obrázku 20.

Obrázek 20 Smazané fragmenty Adresáře v iPhone Analyzer

Zvukové zprávy

Ani na jedné testované záloze nebyly zvukové zprávy, testování nepřineslo žádné výsledky.

Textové zprávy

Zde vidíme všechny odchozí a přijaté SMS zprávy. Zobrazují se i MMS zprávy, ale jejich obsah je nečitelný. Zobrazení zpráv je celkově nepřehledné, pro lepší přehled můžeme využít třídění. Jako u adresáře máme i zde možnost zobrazit informace v SQL databázi, textové, a v hexadecimální podobě. Dostupnost smazaných fragmentu je zde také. Smazané fragmenty zpráv můžeme vidět na obrázku 21.

Obrázek 21 Smazané fragmenty Textových zpráv v iPhone Analyzer

Volaní

Zde máme přehled o všech příchozích, odchozích a zmeškaných hovorech. Pro lepší a rychlejší analýzu můžeme třídit informace podle telefonního čísla, data, kdy hovor byl proveden, délky trvaní a typu hovoru. Možnost vidět smazané fragmenty máme i zde.

Všechny media

Zde se nachází všechny dostupné fotografie a videa. Jejích přehled je zobrazen v miniaturách. Po rozkliknutí se fotografie zvětší a zobrazí se nám EXIF souboru.

Adresář souborového systému

Nachází se zde Dokumenty, Knihovna, Media a Systémové nastavení. Při testování se z dokumentu daly získat fotografie, které byly přijaté pomocí aplikace Skype. V adresáři souborového systému lze zobrazit libovolný SQLite a plist soubor a proto není potřeba dalších nástrojů pro jejích zobrazení.

Nástroj disponuje také vyhledáváním a exportem souborů. Pro zařízení s iOS 5 a nižší je dostupné online a offline mapovaní, nástroj podporuje také geolokaci.

8.6 Oxygen forensic Suite 2013

Oxygen Forensic Suite 2013 je forenzní software, který používá pokročilé proprietární protokoly, díky kterým dokáže extrahovat mnohem více dat, než obvykle umožňují ostatní logické forenzní nástroje.[8]

Instalace a práce je s ním jednoduchá. Po stažení a instalaci nástroje stačí připojit mobilní zařízení k počítači, v programu nastavit připojení pomocí USB a posléze je mobilní zařízení automaticky identifikované. Na testovaných zařízeních doba trvaní získávání informací trvala od 2-4 hodin. Příčinou takového rozdílu v čase bylo zaplnění pamětí na daných zařízeních. Velkou výhodou tohoto nástroje je to, že po získání všech dostupných informací není potřeba mít nadále zařízení k dispozici.

Oxygen Forensic Suite 2013 dokázal ze zařízení iPhone 4S (iOS6) bez jailbreaku získat následující informace:

- Základní informace o zařízení

- Výpis volaní
- Adresář
- Kalendář
- Poznámkový blok
- Zprávy
- Adresář souborového systému
- Aplikace

Dále byla provedena analýza dat na zařízení iPad mini (iOS6) s jailbreakem. Postup při této analýze byl stejný jako s právy běžného uživatele. Oxygen Forensic Suite 2013 dokázal získat navíc následující informace:

- Více dat o aplikacích
- Data z Google Chrome
- Data z Google Mail
- Data z Opera Mini
- Data z Facebook
- Data z Instagram
- Data z Twitter
- Data z Dropbox
- Data z YouTube
- Data z Apple Maps

8.7 iFunBox

iFunBox je nástroj, pomocí kterého se zařízení chová jako vyměnitelný disk. Pomocí tohoto nástroje můžeme vidět všechny uživatelské a systémové aplikace, které jsou nainstalované na zařízení, máme přehled i o kameře, ve které vidíme všechny fotografie a videa, která se na daném zařízení nachází. Prostředí nástroje je podobné Průzkumníku Windows. Práce s ním je velice jednoduchá a rychlá. Hlavním znakem tohoto nástroje je možnost prohlížení

adresáře souborového systému. K zobrazení všech dostupných informací je potřeba jailbreak.

8.8 UFED Physical Analyzer 3

Od založení v roce 1999, je společnost Cellebrite známa pro své technologické průlomy na poli mobilních přístrojů a zařízení. Coby světový lídr a autorita v technologiích mobilních dat, Cellebrite založil svou forenzní divizi v roce 2007 uvedením přístroje UFED (Universal Forensic Extraction Device). Škála mobilních forenzně-analytických produktů série UFED umožňuje extrakci dat bit po bitu a hloubkové analýzy dat z tisíců mobilních přístrojů, včetně starších mobilních telefonů, nových, tzv. chytrých telefonů, přenosných GPS zařízení, tabletů a telefonů vyrobených s čínskými "chipsety".“

UFED Physical Analyzer 3 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 a pomoci průvodce vybrat typ extrakce dat. Na výběr máme dva typy extrakce - rozšířenou logickou a fyzickou.

Rozšířená logická extrakce dokáže ze zařízení získat telefonní seznam, záznamy o volání, SMS zprávy, iMessage zprávy, MMS zprávy, kalendář, data aplikací, obrázky, audio, video a další. A to pouze ze zařízení s odstraněnou ochranou. Při extrakci dat zařízení musí být zapnuto.

Při pokusu o fyzickou extrakci se ovšem objevil problém, který znemožňoval provést získání dat na testovaných zařízeních, protože nebyly podporovány. Fyzickou extrakci dat je možné provést pouze na zařízeních Iphone 4 a starších a Ipad 1. Pro potřeby testu byl tedy zakoupen ještě jeden mobilní telefon, konkrétně Iphone 3GS, který již byl plně podporován.

Po výběru možnosti fyzické extrakce dat je nám nabídnuto získání přístupového hesla pomocí metody brute force, která zkouší postupně všechny kombinace. V případě, že je zvoleno jednoduché heslo, složené ze 4 čísel, je vyluštění rychlé. V mém případě, kdy heslo bylo „8804“, trvalo odhalení 16 minut. Pokud by ovšem bylo nastaveno neomezené heslo složené z čísel a písmen, bylo by rozluštění prakticky nemožné. Znalost hesla ovšem není podmínkou pro úspěšnou fyzickou extrakci dat. Tato možnost je tu především proto, že některé soubory spojené s emaily jsou šifrované a bez znalosti hesla i zašifrované zůstanou. Pro přístup k ostatním souborům pak heslo není třeba. Druhou výhodou této funkce je fakt, že při znalosti hesla může znalec nahlédnout do zařízení přímo, pokud bude potřebovat.

Poté následuje samotné zahájení fyzické extrakce. V závislosti na velikosti paměti se může potřebný čas lišit, ale na testovaném 16GB zařízení vytvoření obrazu dat trvalo 33 minut. Jailbreak pro tuto metodu není třeba a na výsledek nemá žádný vliv.

Po dokončení extrakce nám program nabídne zobrazení získaných dat. Obsahuje jak část uživatelskou, kde jsou uloženy aplikace, fotky, emaily, atd., tak i část systémovou, kde jsou uloženy soubory operačního systému.

Podle očekávání se zde objevilo největší množství informací v porovnání s ostatními přístupy. Šlo především o:

- Emaily
- Obrázky
- Videa
- Historie safari
- SMS
- Kontakty
- Poznámky
- Kalendář

- Výpis volání

Nespornou výhodou fyzické extrakce dat je ovšem získání již smazaných souborů. Na testovaném zařízení se touto metodou podařilo obnovit obrázek, který byl smazaný před začátkem zkoumání.

8.9 Internet Evidence Finder

Nástroj Internet Evidence Finder je zajímavým počinem firmy Magnet Forensics. K dispozici je 30 denní trial verze zdarma, o kterou lze požádat na http://www.magnetforensics.com/. Po schválení žádosti je odeslán email s odkazem ke stažení a aktivačním klíčem. Tento nástroj neslouží pouze na analýzu mobilních zařízení, ale může být užitečný i pro potřebu analýzy počítačů s operačním systémem Windows a OS X. Pokud se ovšem zaměříme pouze na mobilní telefony, je zde podpora systému iOS, Windows phone a Android, včetně Kindle Fire. Co ovšem nástroj neumí, je práce s živým zařízením. Nelze tedy jednoduše připojit mobilní telefon k počítači a získat informace pomocí Internet Evidence Finder. Místo toho nástroj pracuje se zálohami, s výpisem souborů (file dump) a bitovou kopií obrazu. U těchto zdrojů dat je schopen Internet Evidence Finder vyhledat širokou škálu informací, přičemž pátrá i po smazaných souborech.

Při testování jsem používal zálohy ze zařízení iPad mini (iOS 6). Po načtení záloh se objevily tyto informace:

- Data ze Skype
- Obrázky
- Torrentové soubory
- Safari historie
- Emaily
- Poznámky

Poté jsem zkusil použít file dump, který vygeneroval nástroj UFED Physical Analyzer. Internet Evidence Finder dokázal získat mnohem více obrázků a dat ze Skypu. K tomu ještě přibyly položky:

- Zprávy z AIM
- Zprávy z KIK Messengeru
- Zprávy z Viber

9 Vyhodnocení softwaru

Tato sekce je věnována vyhodnocení nástrojů, které byly dříve zmíněny. U každého nástroje je pohlíženo na jeho silné a slabé stránky, a pokud to jde, je porovnán s konkurencí. Pro přehlednost je hodnocení rozděleno na 2 části. První se věnuje samotným forenzním nástrojům, které lze použít pro zkoumání zařízení. Druhá část se zabývá nástroji, které sice ke zkoumání přímo neslouží, ale předchází mu nebo ho usnadňují.

9.1 Forenzní nástroje

Tato část se věnuje vyhodnocení forenzních nástrojů, použitých při zpracovávání praktické části práce. Bylo využito hned 5 nástrojů, mezi nimiž jsou MOBILedit! Forensics, iPhone Backup Extractor, iPhone Analyzer, Oxygen Forensic Suite a UFED Physical Analyzer. Každý se v něčem lišil a umožňoval dosáhnout jiných výsledků.

9.1.1 MOBILedit! Forensics

MOBILedit! Lite dokáže získat ze zařízení základní informace, které jsou přehledně zobrazeny. Použití je velice jednoduché a analýza zařízení byla hotova během několika minut. Verze MOBILEdit! Lite je k dostání zdarma, avšak s omezeními. Vygenerování dokumentace je možné pouze v placené verzi. Cena přibližně 11 tisíc za plnohodnotnou verzi je ovšem přijatelná investice. Výhodou může být široká škála možností připojení zařízení k počítači. Za nevýhodu se dá ale považovat nutnost přítomnosti Connectoru, byť automaticky instalovaného a po dokončení analýzy i automaticky smazaného. Dochází zde totiž k zásahu do paměti zařízení. Při analýze iPhone 4S s omezenými právy a iPad mini s jailbreakem jsem docílil stejných výsledku. Toto zjištění považuji za největší nevýhodu tohoto nástroje. Jailbreak tedy pro tento nástroj nepřináší žádné nové informace.

9.1.2 iPhone Backup Extractor

iPhone Backup Extractor slouží k analyzování záloh, které tvoří iTunes. Jeho výhodou je jednoduchost, se kterou se lze dostat k informacím, jako jsou například údaje napsané do textových polí. Verze zdarma dokáže získat mnoho informací a má i omezenou možnost dešifrování zaheslovaných záloh. Pro potřeby základní forenzní analýzy záloh zařízení jde o vhodného kandidáta.

9.1.3 iPhone Analyzer

iPhone Analyzer dokáže získat ze záloh veškeré dostupné informace, které jsou přehledně zobrazeny. Instalace a použití je velice jednoduché. Použitá verze nástroje neumožňovala využít některých funkcí pro iOS 6. Vhodným doporučením je zde vyhledat nejaktuálnější verzi, umožňující využití maxima funkcí. Výhodou je bezplatnost programu, která sebou ale přináší i nižší četnost výskytu aktualizací. Za velkou výhodu se dá považovat schopnost získat i některá smazaná data, kterou konkurenční iPhone Backup Extractor nemá. Při testovaní nástroj několikrát "zamrznul". Chybí funkce exportu jednotlivých souboru. Tyto zjištění povazují za největší nevýhody tohoto nástroje.

9.1.4 Oxygen forensic Suite 2013

Oxygen Forensic Suite 2013 je vynikající forenzní nástroj, který dokáže ze zařízení získat velké množství informací, přehledně roztříděných do kategorií. Nástroj také disponuje možností vygenerovat dokumentaci o zkoumaném zařízení a to hned v několika formátech. Jak testování ukázalo, po aplikaci Jailbreaku je program schopen získat ze zařízení více informací. Bez něj se jeho výstup velmi podobá konkurenčnímu MOBILedit! Forensics. Jeho největší nevýhodou je cena, která se pohybuje okolo 50 tisíc. Zde ho konkurence výrazně poráží.

9.1.5 UFED Physical Analyzer 3

Tento nástroj obsahuje širokou škálu funkcí. Má nástroje jak pro logickou extrakci dat, tak i pro fyzickou. Navíc umožňuje získání zabezpečovacího hesla ze zařízení. Díky těmto funkcím se dá získat ze zařízení maximum informací. Za nevýhodu by se dalo považovat nepodporování fyzické extrakce u novějších zařízení, ale tuto schopnost nemá žádný konkurenční produkt. Jediný nástroj Elcomsoft Forensic Toolkit dokáže provést fyzickou extrakci u novějších zařízení, ale pouze pokud je zařízení předem jailbreaknuté. Tento nástroj ovšem není v trial verzi k vyzkoušení, proto nemohl být zařazen do testování. UFED ovšem k vyzkoušení byl na 30 dní a za tu dobu se ukázal být nejlepším z použitých nástrojů. Je přehledný, jednoduchý, podporuje širokou škálu zařízení a je schopný získat velké množství informací.

9.1.6 Internet Evidence Finder

Nástroj Internet Evidence Finder je velmi užitečný, pokud neprovádíme pouze forenzní analýzu mobilních zařízení, ale pracujeme také s počítači a jejich pevnými disky. Tím, že dokáže sloučit tyto 2 kategorie, má navrch oproti iPhone Analyzeru. Jeho nevýhodou je ovšem cena. Zatímco trial verze na 30 dní je zdarma, placená začíná na 1000 $. Nástroj ani nepodporuje přístup k živému zařízení, který má iPhone Analyzer ve vývoji. Chybí zde i podpora dešifrování záloh, takže pokud záloha je šifrovaná, Internet Evidence Finder si s ní neporadí. Celkově jde tedy o nástroj, který má sice dobře zvládlou analýzu počítačů, ale u mobilní části se setkáváme s překážkami, kvůli kterým by se vyplatilo šáhnout po jiném nástroji.

9.2 Ostatní nástroje

Předchozí sekce byla věnována forenzním nástrojům. Zde přichází na řadu vyhodnocení nástrojů, které analýze předchází, konkrétně jde o službu Find My iPhone / iPad, Backup iTunes a iFunBox. Každý ze zmíněných slouží

k něčemu jinému a proto je nemožné je mezi sebou porovnat. Místo toho se tato sekce snaží o vystižení silných a slabých stránek.

9.2.1 Find My iPhone / iPad

Tato služba je mocným spojencem, ale ve špatných rukách dokáže znalci velmi ztížit práci. Umožňuje lokalizovat zařízení, poslat na něj zprávu, uzamknout ho nebo ho smazat. Pokud jako majitel ztratíte své zařízení, určitě oceníte možnost ho lokalizovat a v případě potřeby ho i uzamknout. To vše na dálku. Pokud je ovšem zařízení zadrženo pro forenzní zkoumání, může se jeho majitel pokusit o vzdálené smazání dat a tak i případných důkazů. Pro majitele zařízení jde tedy o výhodu, pro znalce o hrozbu. V každém případě je to ale důležitá služba, o které musí mít znalec povědomí.

9.2.2 Backup iTunes

Jde o velmi známý nástroj, který slouží k vytváření záloh zařízení přes iTunes. Jde o oficiální produkt Apple a to sebou přináší řadu výhod, jako jsou časté aktualizace, podpora všech zařízení a stabilita. Pokud se navíc dostane znalci do ruky počítač, na kterém byly prováděny zálohy zařízení pomocí tohoto nástroje, nepotřebuje nutně k samotnému zkoumání zařízení. Pro potřeby vytváření záloh jde o dobrý nástroj a není třeba jeho alternativ.

9.2.3 iFunBox

Největší výhodou tohoto nástroje je fakt, že aniž by zařízení muselo mít upravená práva prostřednictvím jailbreaku, lze s ním spravovat obsah zařízení a použít zařízení jako flash paměť. Umožňuje maximální přenosovou rychlost 20MB/s, tedy dvojnásobek rychlosti iTunes. Nabízí také snadný import a export multimédií a instalaci aplikací a her. Navíc existuje i portable verze, u které není třeba nic instalovat. Přestože je zdarma, nemůže nahradit iTunes, protože neobsahuje vytváření záloh a navíc pro svůj běh vyžaduje přítomnost iTunes. Přesto ale jde o velmi zajímavý nástroj, který stojí za povšimnutí.

10 Důležité adresáře

Adresářová struktura iOS je společná pro všechny iOS zařízení. Některé soubory jsou uložené v textové podobě a jsou snadno čitelné. Všechny ostatní soubory jsou uložené do SQLite databází a XML.

Aplikace ukládají svá data do složky private/var/mobile/Library. Která zahrnuje Adresář, Mail, Kalendář, Mapy, Poznámky, YouTube, Safari, Zprávy, Počasí, Zvukové záznamy a jiné. Níže je popsáno, co přesně v tomto adresáři nalezneme. Pro potřeby forenzní analýzy je toto místo hlavním zdrojem dat.

10.1 Fotografie

Fotografie se nachází v private/var/mobile/media/DCIM. V této složce se nachází fotografie pořízené přímo zařízením nebo pomocí synchronizace jiných aplikací. Fotografie nebo obrázky v této složce mají časové razítko. Fotografie ve složce 100APPLE jsou pořízené přímo zařízením, kdy aplikace fotoaparátu má tendenci fotografie pojmenovávat IMG_0001. První pořízený snímek má název IMG_0001. Další pořízené fotografie pokračují v číslování. Nehledě na to, jestli předchozí fotografie byla odstraněna nebo ne. Pro zkoumajícího je to důležitým faktorem. Pokud jsou v číslování mezery, lze předpokládat, že fotografie byla odstraněna.

10.2 Klávesnice

V /private/var/mobile/Library/Keyboard se nachází cs_CZ-dynamic-text.dat. Je to dynamický slovník, který zaznamenává slova napsaná uživatelem. Slovník ukládá slova z aplikací Facebook, Zprávy, Safari a jiných, které využívají textové pole. Funkce slovníku je používaná pro automatické opravy chyb a vyplňování formulářů. Díky tomuto slovníku máme možnost vidět a zkoumat veškerá nečíselná slova, používaná uživatelem na zařízení. Slovník neobsahuje žádné časové razítko.

10.3 Hesla

Spousta iOS aplikací používá pro správu hesel Keychain, který se nachází v /private/var/Keychains. Soubor key-chain-2.db obsahuje několik tabulek (cert, genp, inet, keys, tversion), které obsahují účty a hesla používané zařízením v minulosti. Zde se také nachází přihlašovací jména a hesla, která byla použitá při připojení k bezdrátové síti. V některých případech budou hesla šifrovaná a bude třeba je dešifrovat. Šifrování závisí na typu zařízení a verzi iOS. Pomocí nástroje Elcomsoft's iPhone Password Breaker můžou být hesla dešifrována.

10.4 Poznámky

Poznámky mohou obsahovat důležité informace o uživateli, které mohou být při vyšetřování klíčovými. Nachází se v /private/var/mobile/Library/Notes. Je zde SQLite databáze notes.sqlite, která obsahuje devět tabulek. Pro vyšetřovatele nejdůležitější tabulkou je ZNOTE, která obsahuje časové razítko k dané poznámce. V tabulce ZNOTEBODY máme možnost vidět obsahy všech poznámek.

10.5 Zprávy

SMS zprávy mohou být jedním z nejdůležitějších důkazů při vyšetřování. Najít je můžeme v /private/var/mobile/Library/SMS. Je zde SQLite databáze sms.db, která obsahuje 8 tabulek. Pro vyšetřovatele jsou nejdůležitější tabulky message a msq_pieces které obsahují cenné informace.

10.6 Historie prohlížeče

Soubor History.plist, využívá mobilní prohlížeč Safari k ukládání historie prohlížení. Najdeme ho v private/var/mobile/Library/Caches/Safari. Tento plist soubor je ve formátu XML. Dokážeme ho přečíst pomocí poznámkového bloku nebo pro lepší přehlednost pomocí XML Viewer. Po otevření souboru

dokážeme vyčíst název webové stránky, adresu, čas poslední návštěvy a kolikrát byla stránka navštívená.

10.7 Adresář kontaktů

Adresář kontaktů obsahuje telefonní kontakty, kontakty z Facebook které uchovávají velké množství informací. Všechny tyto kontakty jsou uložené v SQLite databázi AddessBook.sqlitedb, která se nachází v /private/var/mobile/Library/AddressBook. V databázi je několik tabulek, z toho dvě jsou pro nás důležité. Tabulka ABPerson obsahuje jméno, příjmení, název organizace, ve které osoba pracuje, datum narození, přezdívku a jiné. Tabulka ABMultiValue obsahuje e-mail a telefonní číslo.

10.8 Historie volaní

Historie volání je obsažena v SQLite databázi call_history.db která se nachází v /private/var/Library/CallHistory. Tato SQLite databáze má čtyři tabulky, z kterých dokážeme vyčíst telefonní číslo, datum a čas, kdy hovor byl proveden, dobu trvání a referenční číslo kontaktu.

11 Doporučený postup forenzní analýzy

Po seznámení se zabezpečením dat na zařízeních s iOS, metodách, jak můžeme získat data, a nástrojích, které tyto metody provádějí, lze navrhnout doporučený postup, který je vhodný pro forenzní analýzu dat.

11.1 Postup před forenzní analýzou

Před tím, než vůbec můžeme pomyslet na získávání dat ze zařízení, je třeba se postarat o to, aby data nemohly být podezřelým nebo jinou osobou vzdáleně smazány nebo zařízení uzamčeno. Tento bod je důležitý a měl by být jako první hned při zajišťování stop.

Pokud není na zařízení aktivní heslo, vypneme WiFi a mobilní data. V případě, že je zařízení uzamčené a heslo je aktivní, můžeme ho odstínit pomocí zabalení do staniolu. Jestliže zjistíme, že zařízení má aktivní heslo, uzamčení není zakázané, ale máme k němu přístup, je vhodné zakázat uzamčení. Takto bude mít znalec v případě potřeby přístup k systému, dokud se zařízení nevypne. Proto je dobré zajistit napájení. Také je vhodné vyjmout SIM kartu, pokud ji zařízení obsahuje.

Tímto jsme zabránili tomu, aby do zařízení někdo zasahoval zvenčí. Jak již bylo zmíněno, iPady i iPhony provádějí zálohy prostřednictvím softwaru iTunes na počítači. Pokud podezřelý vlastnil zkoumané zařízení, je pravděpodobné, že vlastnil i počítač. Proto při forenzní analýze kopie disku počítače je dobré i pátrat po zálohách zařízení, které mohou obsahovat důležité informace.

11.2 Postup při forenzní analýze

V této fázi máme zařízení, ke kterému není přístup zvenčí a případnou zálohu zařízení, získanou z počítače. Pro určení postupu forenzní analýzy si musíme odpovědět na několik otázek.

1. **Jaké zařízení zkoumáme?**

Možnosti zkoumání vychází často ze samotného zařízení. Pokud budeme zkoumat starší zařízení od Applu, nebudeme se potýkat s hardwarovým šifrováním a to nám usnadní přístup k bitové kopii. Pokud ovšem budeme zkoumat novější zařízení, tak máme omezené možnosti a nástroje nemusí být s naším modelem plně kompatibilní. Např. většina programů na vytvoření bitové kopie nemá podporu zařízení iPhone 5, iPad 2, iPad mini. U těchto modelů dokážeme vytvořit nejvýše file dump.

2. **Je zařízení uzamčené?**

Velké procento uživatelů se do určité míry snaží chránit svá data. Proto je pravděpodobné, že se na forenzní analýzu dostane zařízení, které je uzamčené. Pokud se tak stane, můžeme na nástroje jako je MobilEdit Forensics! nebo Oxygen Forensics zapomenout, protože nedokážou získat data z uzamčeného zařízení a ani heslo prolomit. To ovšem dokážou některé nástroje pro fyzickou analýzu. Pokud bychom se spokojili s menším množstvím informací, můžeme využít Bypass uživatelského kódu, zmíněný v sekci 5.5.1.

2. **Jaké jsou možnosti znalce?**

Možnosti znalce vychází ze dvou faktorů. Prvním jsou jeho znalosti, druhým je software k dispozici. Zkoumání mobilních telefonů je často velmi limitováno operačním systémem a liší se od zkoumání PC. Znalec musí být seznámen s verzemi operačního systému a jejich změnami, aby mohl zvolit vhodný postup. Finanční stránka je také velmi limitující. Software pro zkoumání nebývá levný a často je to určující prvek výběru forenzního nástroje. Mezi nejlevnější se řadí MOBILedit! Forensics, který je pro většinu případů dostatečný. Pokud bychom ovšem chtěli hlubší analýzu, museli bychom šáhnout jinam, např. k dražšímu UFED Physical Analyzer.

3. **Je třeba provést bitovou kopii?**

Bitová kopie je „svatým grálem“ forenzního zkoumání, schopná přinést maximum informací. U operačního systému iOS ale představuje výzvu, protože u zařízení s čipem A5 je bitová kopie šifrovaná a nástroje pro dešifrování jsou finančně i časově nákladné. Záleží tedy na znalci, zda situace vyžaduje vytvoření bitové kopie a zda má pro tento proces potřebné vybavení.

4. **Je třeba provést jailbreak?**

Pokud zařízení již jailbreak má, logické nástroje z něj dokážou často získat více informací. Pokud znalec nemůže využít fyzickou metodu s dešifrováním, je jailbreak bezplatnou variantou, kterou se dá získat více informací. Je ovšem na zvážení znalce, zda se pro jailbreak rozhodnout, protože jde o zásah do zařízení a přínos nemusí převážit rizika.

Po zvážení všech otázek by se daly navrhnout následující doporučené postupy v závislosti na situaci:

- **Doporučená varianta - Máme možnost vytvoření bitové kopie s dešifrováním. Zařízení může být uzamčené.**
    1. Vypneme zařízení
    2. Podržíme tlačítko Home a připojíme zařízení k PC
    3. Stiskneme a podržíme tlačítka Home a Power
    4. Po zčernání obrazovky počkáme 3 vteřiny
    5. Uvolníme tlačítko Power. Tlačítko Home držíme do té doby, než jsme vyzváni k uvolnění.
    6. Dešifrujeme uživatelské heslo např. pomocí UFED Physical Analyzer
    7. Pomocí vhodného nástroje, např. UFED Physical Analyzer, provedeme vytvoření bitové kopie zařízení
    8. Provedeme analýzu dešifrovaných dat

- **Alternativní varianta – Nemáme možnost vytvoření bitové kopie, ale můžeme vytvořit file dump. Zařízení může být uzamčené.**
    1. Zapneme zařízení
    2. Připojíme zařízení k PC
    3. Dešifrujeme uživatelské heslo např. pomocí UFED Physical Analyzer
    4. Pomocí vhodného nástroje, např. UFED Physical Analyzer, provedeme vytvoření file dump souboru
    5. Provedeme analýzu souboru
- **Dostatečná varianta - Nemáme možnost bitové kopie s dešifrováním ani file dump, ale můžeme provést logickou analýzu dat. Zařízení nesmí být uzamčeno** – použití jailbreaku pouze v situacích, kdy nám získaná dat nestačí, jinak nepoužívat, protože nelze odstranit.
    1. Zapneme zařízení
    2. Připojíme zařízení k PC
    3. Pomocí vhodného nástroje, např. MOBILedit! Forensics, získáme informace ze zařízení
    4. Provedeme analýzu informací

Ve všech výše zmíněných postupech se doporučuje provést navíc ještě analýzu zálohy, pokud je k dispozici a není šifrovaná. Analýza zálohy by ovšem neměla být jedinou prováděnou analýzou, protože zařízení může obsahovat důležité informace, které v záloze nejsou obsažené. Také se doporučuje získání zabezpečovacího hesla od majitele, pro snazší práci se zařízením.

12 Závěr

Tato bakalářská práce se zabývá problematikou forenzního zkoumání zařízení s operačním systémem iOS. Obsahuje možnosti a omezení, které přináší zabezpečení tohoto systému, spolu se způsoby, jak získat potřebné informace. Tyto zmíněné způsoby byly otestované na živých zařízeních, konkrétně iPad Mini, iPhone 4S a v případě fyzické metody i na iPhone 3GS. Díky získaným zkušenostem bylo možné navrhnout doporučené postupy, jak provést forenzní analýzu zařízení, v závislosti na možnostech znalce, situaci a zkoumaném zařízení.

Přes omezení, přinášející operační systém iOS, se podařilo dosáhnout všech vytčených cílů a navrhnout doporučený postup forenzní analýzy, který může sloužit jako návod pro správný výběr metody a jejího provedení.

13 Terminologický slovník

Termín	Význam
AES	Advanced Encryption Standard. Symetrická bloková šifra
API	Application Programming Interface. Je to rozhraní pro programování aplikací
App store	Prostředí pro stahování a nákup softwaru
DFU	Device Firmware Upgrade. Umožňuje zařízením obnovení dřívějšího stavu
Firmware	Software pro řízení určitého systému
iOS	Operační systém od společnosti Apple
Framework	Struktura, která slouží jako podpora při programování, vývoji a organizaci jiných projektů
NAND paměť	Paměť používaná např. u flash disků. Jejich základním prvkem je tranzistor s plovoucím hradlem
SDK	Software Development Kit. Software pro vývoj aplikací
SSH	Secure Shell. Komunikační protokol v počítačových sítích
SQL	Standard Query Language. Dotazovací jazyk pro práci s relačními databázemi

UID	Unique identifier. Způsob, jakým se rozlišují uživatelé
XML	Extensible Markup Language. Značkovací jazyk určený především pro výměnu dat mezi aplikacemi
XNU	Jádro operačního systému iOS

14 Použitá literatura

[1] Češi se už nehodlají dělit o počítač. Počet PC v rodinách roste – Živě.cz. *Živě.cz – O počítačích, IT a internetu* [online]. 2013 [cit. 2014-03-11]. Dostupné z: http://www.zive.cz/bleskovky/cesi-se-uz-nehodlaji-delit-o-pocitac-pocet-pc-v-rodinach-roste/sc-4-a-170140/default.aspx

[2] Statistické údaje pro Kraj Vysočina - podklady pro analýzu vývoje kriminality. *Kraj Vysočina* [online]. [cit. 2014-03-11]. Dostupné z: http://www.kr-vysocina.cz/VismoOnline_ActionScripts/File.ashx?id_org=450008&id_dokumenty=4050248

[3] Android má 75% podíl na trhu se smartphony | CDR.cz. *CDR.cz - Vybráno z IT* [online]. 2013 [cit. 2014-03-11]. Dostupné z: http://cdr.cz/clanek/android-ma-75-podil-na-trhu-se-smartphony

[4] HFS+ Overview. *NTFS.com: Data Recovery Software, File Systems, Hard Disk Internals, Disk Utilities* [online]. 2013 [cit. 2014-03-11]. Dostupné z: http://www.ntfs.com/hfs.htm

[5] IOS Technology Overview: About the iOS Technologies. *Apple Developer* [online]. 2013 [cit. 2014-03-11]. Dostupné z: https://developer.apple.com/library/ios/documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/Introduction/Introduction.html#//apple_ref/doc/uid/TP40007898-CH1-SW1

[6] iOS Security. *Apple* [online]. 2014 [cit. 2014-03-11]. Dostupné z: http://images.apple.com/iphone/business/docs/iOS_Security_Feb14.pdf

[7] MOBILedit Forensic. *MOBILedit – PC Suite For All Phones* [online]. 2014 [cit. 2014-03-11]. Dostupné z: http://www.mobiledit.com/forensic

[8] Oxygen Forensic® Suite - Mobile forensics solutions: software and hardware. [online]. 2014 [cit. 2014-03-11]. Dostupné z: http://www.oxygen-forensic.com/en/

[9] Mixpanel | Mobile Analytics. [online]. [cit. 2014-03-13]. Dostupné z: https://mixpanel.com/trends/#report/ios_frag/from_date:-432,to_date:-225