Jihočeská univerzita v Českých Budějovicích

Přírodovědecká fakulta

Bakalářská práce

2017 **Vojtěch Koutský**

Jihočeská univerzita v Českých Budějovicích

Přírodovědecká fakulta

Analýza bezpečnosti jednotlivých druhů mobilních telefonů

Bakalářská práce

Vojtěch Koutský

Školitel: Mgr. Jakub Kothánek, LL.M.

České Budějovice 2017

Bibliografické údaje

Koutský, V., 2017: Analýza bezpečnosti jednotlivých druhů mobilních telefonů [Safety analysis of individual types of mobile phones Bc. Thesis, in Czech] – 39 p., Faculty of Science, The University of South Bohemia, České Budějovice, Czech Republic

Anotace

Tato bakalářská práce se zabývá forenzní analýzou jednotlivých druhů mobilních telefonů. V teoretické části jsou popsány dva nejčastější operační systémy - Android a iOS. Dále jsou rozebrány pojmy forenzní analýza a digitální stopy. V praktické části jsou provedeny samotné forenzní analýzy vybraných telefonů a vyhodnoceny získané výsledky. Na základě výsledků byla nalezena bezpečností rizika a jejich možné řešení.

Klíčová slova

Android, iOS, Forenzní analýza, mobilní telefon

Annotation

This bachelor thesis deals with forensic analysis of different kinds of mobile phones. Theoretical part describes two most common mobile operating systems - Android and iOS. Furthermore it contains definition of forensic analysis and digital footprints. Practical part consists of forensic analysis of chosen phones itself and of evaluated results. Based on these results, security risks and their possible solutions were formed.

Keywords

Android, iOS, Forensic analysis, mobile phone

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 Přírodovědeckou 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..…….. ……..

podpis

Poděkování

Chtěl bych velice poděkovat vedoucímu mé bakalářské práce Mgr. Jakubu Kothánkovi LL.M. za cenné rady a čas věnovaný při vypracování mé práce. Dále bych chtěl poděkovat své rodině a přátelům za podporu během mého studia.

Obsah

Seznam zkratek

API – Application Programming Interface

AOT – Ahead of Time

MIDI – Musical Instrument Digital Interface

VPN – Virtual Private Network

UNIX – Uniplexed Information and Computing System

RAM – Random Access Memory

MTK – MediaTek

Seznam pojmů

Open source – mobilní systém s otevřeným zdrojovým kódem

Multitasking – schopnost provádět několik procesů najednou

Peer to peer – počítačová síť klient – klient

Read only přístup – práva pouze ke čtení

Bootloader – zavaděč, nahrává operační systém

1 Úvod

V dnešní době technologií používá mobilní telefon téměř každý, někdo má i dva a více. Tento počet bude v budoucnu neustále narůstat. Důležité je proto vědět, jak takový telefon funguje a jaká může, kromě výhod, představovat rizika. Mnozí uživatelé přitom vůbec nevědí, kolik osobních informací mají v mobilním telefonu uložených, natož aby věděli, jakým způsobem ho nejlépe zabezpečit. Mnoho lidí mění telefon velmi často, protože se stále objevují jejich nové a lepší verze a například pro děti ve škole se značka telefonu stala až prestižní záležitostí. Vůbec si přitom neuvědomují, kolik v něm zůstane souborů a informací o nich a jejich životě, když ho například prodají.

Tato bakalářská práce se bude zabývat analýzou bezpečností mobilních telefonů a to u dvou největších operačních systémů na trhu - Androidu a iOS. Hlavním cílem práce je testování jednotlivých systémů, porovnání jejich bezpečnosti a doporučení pro uživatele, jak by měli zodpovědně a co nejbezpečněji zacházet se svými daty.

1.1 Cíle práce

- Popis operačních systému iOS a Android;
- Popis forenzní analýzy a forenzních nástrojů;
- Provedení a vyhodnocení forenzních analýz;
- Nalezení bezpečnostních rizik;
- Doporučení základního zabezpečení mobilních telefonů.

2 Druhy operačních systémů mobilních telefonů

Tato bakalářská práce se bude zabývat pouze hlavními operačními systémy, které používá většina uživatelů mobilních telefonů, tedy operačními systémy Android a iOS.

2.1 Android

Android je mobilní operační systém založený na jádru Linuxu a je dostupný jako open source. Je používán převážně pro smartphony a tablety. Operační systém vlastní firma Google, která jej v roce 2005 odkoupila od společnosti Android Inc., která byla založena v roce 2003. Android je velice oblíbený a má největší zastoupení jako operační systém u mobilních telefonů. V roce 2016 měly mobilní telefony s operačním systémem Android dokonce 86% podíl ze všech prodaných mobilních telefonů [1].

2.1.1 Architektura OS Android

Architekura OS Android je dělena do následujících vrstev.

Linux Kernel

Základem Androidu je jádro Linuxu. Použití jádra Linuxu umožňuje Androidu využívat klíčových funkcí jeho zabezpečení a umožňuje výrobcům zařízení vyvinout ovladače hardwaru pro dobře známé jádro [2].

Hardware Abstraction Layer

Hardware Abstraction Layer poskytuje standardní rozhraní, které vystavují schopnosti hardwaru zařízení do vyšší úrovně rozhraní Java API. Modul Hardware Abstraction Layer se skládá z několika knihovních modulů, z nichž každý implementuje rozhraní pro konkrétní typ hardwarových komponent, jako je například kamera nebo modul bluetooth. Když rozhraní API Framework vyvolá přístup k hardwaru zařízení, systém Android načte knihovní modul pro tuto hardwarovou komponentu [2].

Android Runtime

U zařízení se systémem Android verze 5.0 nebo vyšší se každá aplikace spouští ve svém vlastním procesu a z vlastní instance aplikace Android Runtime. Android Runtime je napsán pro spouštění více virtuálních strojů na zařízení s malou pamětí při spouštění souborů DEX, což je formát bytecode navržený speciálně pro Android, který je optimalizován pro minimální paměť. Vytvoření nástrojových řetězců, jako je Jack, kompiluje zdroje Java do DEX bytecode, které mohou běžet na platformě Android.

Mezi hlavní rysy Android Runtime patří následující:

- předběžná (AOT) a just-in-time kompilace;
- optimalizovaný sběr odpadu;
- lepší podpora při ladění, včetně specializovaného profilu odběru vzorků, podrobných diagnostických výjimek a hlášení o selhání a možnost nastavit hlídání konkrétních polí.

Před verzí Android verze 5.0 byl Dalvik Android Runtime. Pokud aplikace běží spolehlivě na Android Runtime, pak by měla pracovat na Dalvik stejně, ale obráceně už to platit nemusí. Android také obsahuje sadu základních knihoven Runtime, které poskytují většinu funkcí programovacího jazyka Java [2].

Native C/C++ Libraries

Mnoho základních komponent a služeb systému Android, jako například Android Runtime a Hardware Abstraction Layer, je postaveno z nativního kódu, který vyžaduje nativní knihovny napsané v programovacích jazycích C a C ++. Platforma Android poskytuje rozhraním API rozhraní Java Framework, které vystavují funkce některých nativních knihoven aplikacím. Je možné například přistupovat k aplikaci OpenGL ES prostřednictvím Java OpenGL API rámce Android a přidat podporu pro kreslení a manipulaci s 2D a 3D grafikou v konkrétní aplikaci [2].

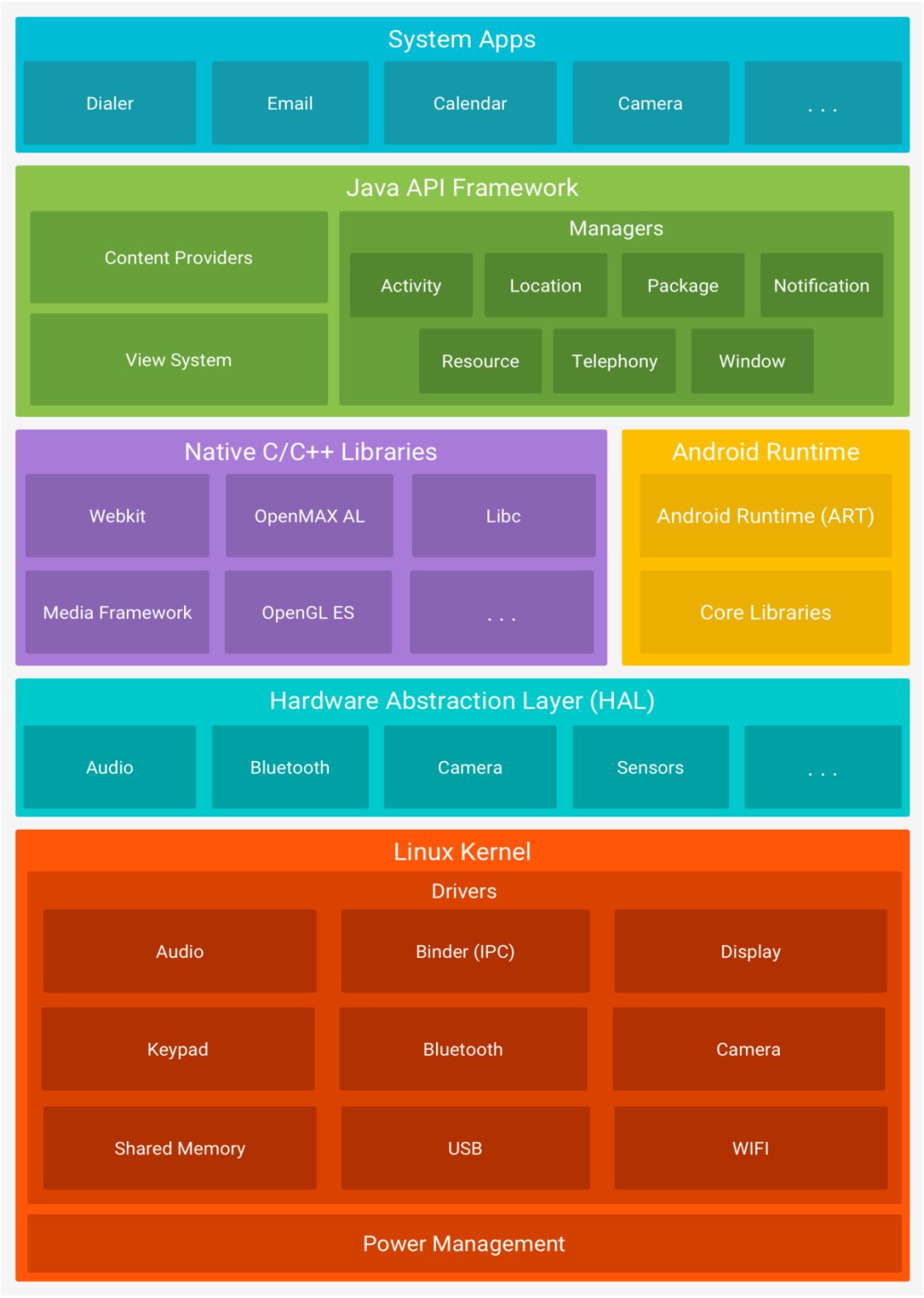
Java API Framework

Celá sada funkcí operačního systému Android je k dispozici prostřednictvím rozhraní API napsaných v jazyce Java. Tato rozhraní API vytvářejí stavební bloky, které jsou potřeba k vytváření aplikací pro Android, a to zjednodušením opětovného použití jádrových a modulárních součástí systému a služeb, které zahrnují následující:

- bohatý a rozšiřitelný systém zobrazení, který je možné použít k vytvoření uživatelského rozhraní aplikace, včetně seznamů, mřížky, textových polí, tlačítek a dokonce i vestavěného webového prohlížeče;
- správce zdrojů, který poskytuje přístup k nekódujícím prostředkům, jako jsou lokalizované řetězce, grafika a soubory rozložení;
- správce oznámení, který umožňuje všem aplikacím zobrazovat vlastní upozornění ve stavovém řádku;
- správce aktivit, který řídí životní cyklus aplikací a poskytuje společný zásobník pro navigaci;
- poskytovatelé obsahu, kteří umožňují aplikacím přistupovat k datům z jiných aplikací, například aplikace kontakty, nebo sdílet vlastní data [2].

System Apps

Android obsahuje sadu hlavních aplikací pro e-maily, SMS zprávy, kalendáře, procházení internetu, kontakty a další. Aplikace zahrnuté do platformy nemají žádný zvláštní status mezi aplikacemi, které se uživatel rozhodne nainstalovat. Aplikace třetích stran se tak může stát výchozím webovým prohlížečem, serverem SMS Messenger nebo dokonce i výchozí klávesnicí. Aplikace systému fungují jako aplikace pro uživatele a poskytují klíčové funkce, které mohou vývojáři získat z vlastní aplikace. Pokud by aplikace chtěla například doručit zprávu SMS, nemusí tuto funkci vytvářet sama - může místo toho vyvolat kteroukoli aplikaci SMS, která je již nainstalována, aby doručila zprávu příjemci, který byl zadán [2].

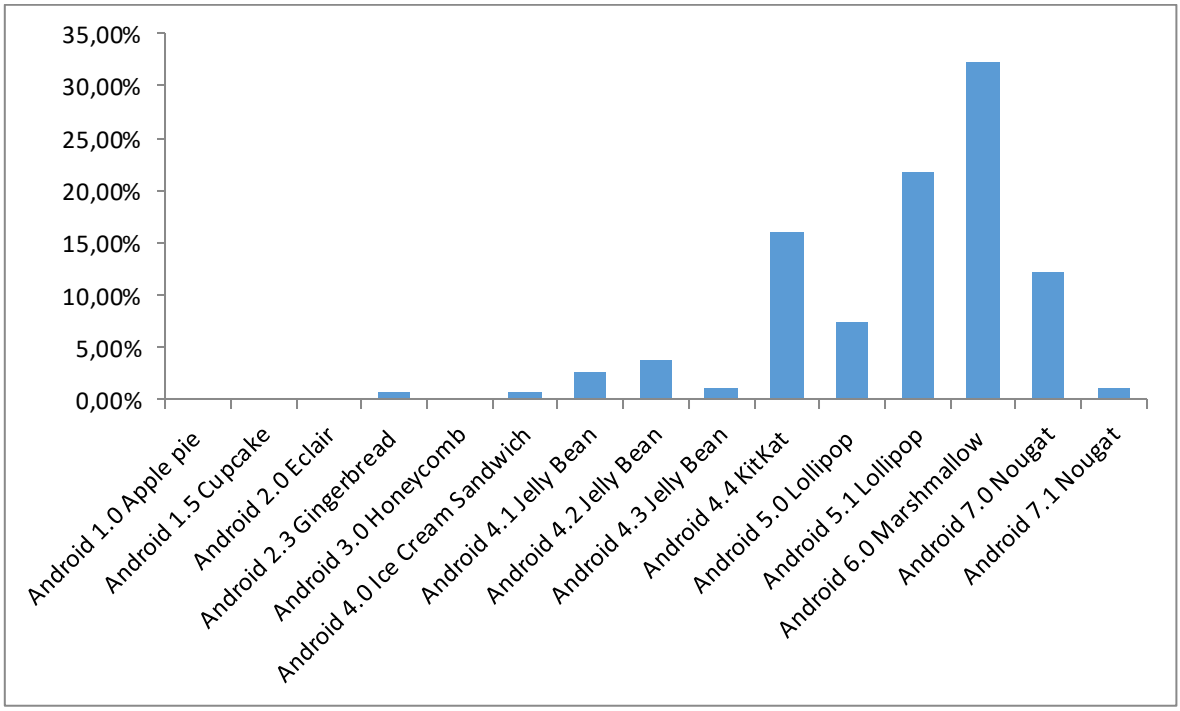


Obrázek 1 Struktura OS Android – převzato z [2]

2.2 Verze systému Android

V roce 2008 byla vydána první verze systému Android. Následovaly další verze, v každé bylo nějaké vylepšení a software se stále vyvíjel. Každá verze si získala jinou popularitu, některé se vůbec nepoužily nebo mají jen omezené množství uživatelů, kteří si je do svých mobilních telefonu nainstalovali úmyslně. Počáteční verze systému se už dnes nepoužívají, protože jsou zastaralé a byly nahrazeny novými vylepšenými verzemi. Zastoupení jednotlivých verzí Android v roce 2017 bylo následující:

- Android 1.0 Apple pie – 0 %;
- Android 1.5 Cupcake – 0 %;
- Android 2.0 Eclair – 0 %;
- Android 2.3 Gingerbread – 0.7 %;
- Android 3.0 Honeycomb – 0 %;
- Android 4.0 Ice Cream Sandwich – 0.7 %;
- Android 4.1 Jelly Bean – 2.7 %;
- Android 4.2 Jelly Bean – 3.8 %;
- Android 4.3 Jelly Bean – 1.1 %;
- Android 4.4 KitKat – 16 %;
- Android 5.0 Lollipop – 7.4 %;
- Android 5.1 Lollipop – 21.8 %;
- Android 6.0 Marshmallow – 32.3 %;
- Android 7.0 Nougat – 12.3 %;
- Android 7.1 Nougat – 1.2 %.



Graf 1 Přehled verzí OS Android v roce 2017 – převzato z [3]

Ze statistiky zastoupení lze vyčíst, že nejoblíbenjší verzí je Marshmallow následovaný verzí Lollipop. Dále je zajímavé, že na nejnovější verzi Nougat přešlo pouze malé množství uživatelů, i když je na trhu již více než rok [3, 4].

2.3 iOS

iOS je mobilní operační systém vytvořený společností Apple Inc. v roce 2007. Původně byl vytvořen pouze pro mobilní telefony, později byl rozšířen i na iPad, iPod Touch a Apple TV. Tento systém je považován v mobilním průmyslu jako průlomový. Díky svému přímému vývoji pouze pro svá zařízení a uzavřenosti softwaru dokázal na svou dobu pracovat daleko efektivněji a lépe než ostatní systémy [5].

2.3.1 Architektura iOS

Architektura je dělená do vrstev. Na nejvyšší vrstvě funguje iOS jako komunikační prostředek mezi hardware a aplikacemi. Aplikace nekomunikují přímo s hardware, ale se sadou systémových rozhraní, která umožňují zápis aplikací. Implementaci technologií systému můžeme považovat za soubor vrstev. Nižší vrstvy obsahují soubor technologií, zatímcovyšší vrstvy systému vycházejí z nižších a poskytují propracovanější služby a technologie [6].

Cocoa Touch Layer

Obsahuje klíčové rámce k vytváření aplikací pro iOS. Tyto rámce poskytují také podporu ke klíčovým technologiím, jako jsou multitasking, dotykový vstup, upozornění push a mnoho dalších systémových služeb.

Technologie využívané v Cocoa Touch Layer jsou následující:

- App Extensions – umožňuje rozšířit vybrané oblasti systému;
- Handoff – umožňuje zahájit činnost na jednom zařízení a pokračovat na jiném, které je přihlášené ke stejné Apple ID;
- Document Picker – umožňuje úpravy dokumentu více aplikacemi a sdílení mezi nimi;
- Air Drop – umožňuje sdílet dokumenty, fotografie, videa a jiná data s nedalekými zařízeními iOS;
- TextKit – umožňuje práci s textem;
- UIKit Dynamics – umožňuje specifikovat dynamické položky;
- Multitasking – umožňuje přesunout aplikace do pozadí a zmrazit je, aby zbytečně nezatěžovaly systém a poté, když jsou znovu potřeba, tak je vrátit zpátky do popředí;
- Auto Layout – použití Auto Layout umožňuje uspořádání prvků v uživatelském rozhraní;
- Storyboards – slouží pro navrhování uživatelského rozhraní aplikace. Umožňuje navrhnout celé uživatelské rozhraní na jednom místě a zároveň vidět, jak spolu všechny vrstvy spolupracují.;
- UI State Preservation – zajišťuje, že se aplikace při spuštění otevře ve stejném stavu, v jakém byla uzavřena;
- Apple Push Notification Service – upozorní uživatele na nové informace i v případě, že je aplikace vypnutá nebo je na pozadí;
- Local Notifications – umožňuje vygenerovat lokální upozornění bez nutnosti připojení k externímu serveru;

- Gesture Recognizers – rozpoznává základní gesta, jako jsou například přejetí a zatlačení prstem;
- Standard System View Controllers – řadiče pro standartní systémové rozhraní [7].

Media

Tato vrstva obsahuje grafické, zvukové a video technologie. Vysoká kvalita grafiky je důležitá část všech aplikací iOS.

Grafické technologie použité v iOS:

- UIKit graphics – podpora pro kreslení obrázků a textového obsahu;
- Core Graphics – pro vytváření 2D tvarů a obrázků;
- Core Animation – základní technologie pro animace v aplikacích;
- Core Image – umožňuje manipulaci s videem a obrázky;
- Open GL ES and GLKit – zpracovává pokročilé vykreslování 2D a 3D, což je využíváno hlavně při tvorbě mobilních her;
- Metal – umožňuje vysoký výkon pro lepší vykreslování a výpočetní úlohy;
- TextKit and Core Text – pro typografii a správu textu;
- Image I/O – rozhraní pro čtení a zápis obrazových formátů;
- Photos Library – usnadňují přístup k fotografiím, videím a mediím uživatele.

Zvukové technologie použité v iOS:

- Media Player framework – pro snadné přehrávaní skladeb;
- AV Foundation – pro správu nahrávání a přehrávání zvuků a videa;
- OpenAL – pro poskytování pozičního zvuku;
- Core audio – rozhraní pro záznam a přehrávání zvuku a obsahu MIDI.

Video technologie použité v iOS:

- UIImagePickerController – pro výběr mediálních souborů a zachycení nového obsahu;
- AVKit – pro přehrávání videa;

- Core Media – pro definici datových typů [8].

Core Services

Obsahuje základní služby systému pro aplikace. Tato vrstva také obsahuje technologie pro podporu funkcí iCloud, sociální média a vytváření sítí.

Funkce dostupné v Core Services:

- Peer to Peer Services – poskytuje peer to peer připojení přes Bluetooth;
- iCloud Storage – umožňuje ukládat dokumenty a data na centrální místo a přistupovat k nim z různých zařízení;
- Block Objects – jazykové konstrukce;
- Data Protection – umožnuje šifrování citlivých dat;
- File - Sharing Support – umožnuje vytvářet uživatelské datové soubory v programu iTunes;
- Grand Central Dispatch – technologie ke správě úkolů v aplikacích;
- In - App Purchase – umožnuje finanční transakce pomocí účtu uživatele v iTunes;
- SQLite – umožňuje vkládání databází;
- XML Support – umožňuje podporu formátů XML [9].

Core OS

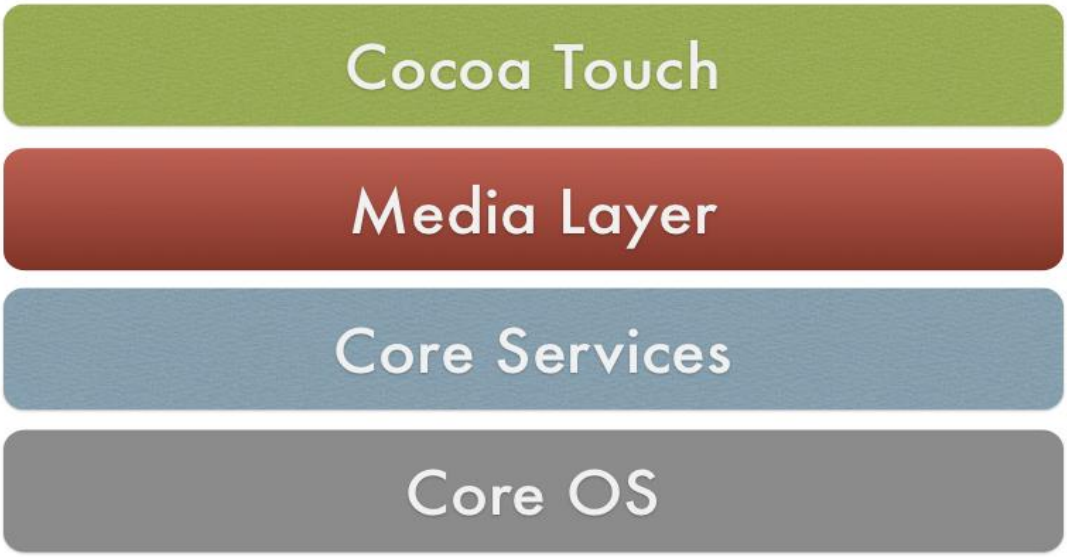
Tato vrstva obsahuje funkce na nízké úrovni. Tyto technologie nejsou využívány přímo při práci s aplikacemi, ale jsou nezbytnou součástí pro funkčnost celého operačního systému.

Funkce dostupné v Core OS:

- Accelerate Framework – pro zpracování digitálního signálu a lineární algebry;
- Core Bluetooth Framework – umožňuje pracovat s Bluetooth;
- External Accessory Framework – umožňuje komunikaci s hardwarovým příslušenstvím připojeným k zařízení s iOS;
- Generic Security Services – poskytuje služby pro zabezpečení systému iOS;

- Local Authentication Framework – umožňuje používat dotykové ID pro autentizaci uživatele;
- Network Extension Framework – poskytuje podporu pro konfiguraci a řízení VPN;
- Security Framework – pro správu certifikátů a veřejných klíčů;
- System – zahrnuje prostředí jádra, ovladače a rozhraní UNIX;
- 64 - Bit Support – podpora 64 bitové architektury od iOS 7.0 [10].

Strukturu operačního systému iOS zobrazuje následující obrázek:



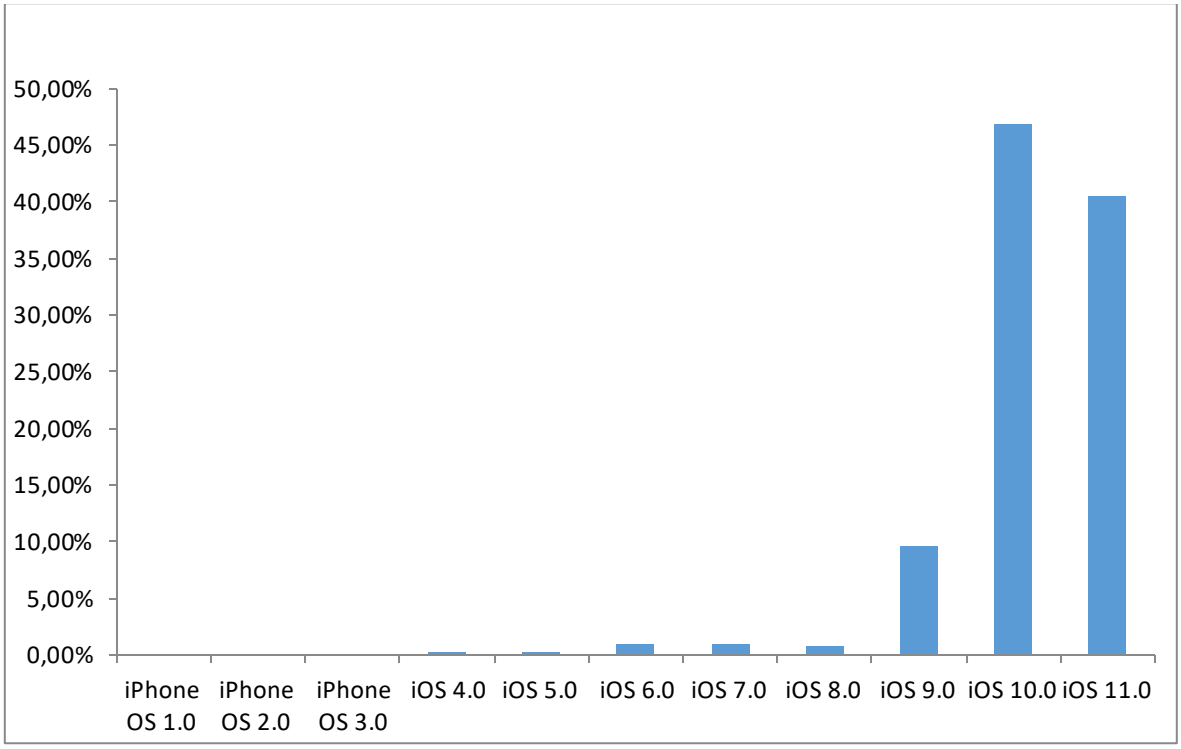
Obrázek 2 Architektura iOS – převzato z [6]

2.3.2 Verze systému iOS

V roce 2007 byla vydána první verze systému iOS, tehdy ještě nazývaného iPhone OS. Následovaly další verze, které průběžné rozšiřují funkce a možnosti tohoto operačního systému. Níže je uveden aktuální přehled jednotlivých verzí a jejich zastoupení mezi mobilními telefony.

- iPhone OS 1.0 – 0 %;
- iPhone OS 2.0 – 0 %;
- iPhone OS 3.0 – 0 %;
- iOS 4.0 – 0.1 %;

- iOS 5.0 – 0.2 %;
- iOS 6.0 – 1 %;
- iOS 7.0 – 1 %;
- iOS 8.0 – 0.7 %;
- iOS 9.0 – 9.6 %;
- iOS 10.0 – 46.9 %;
- iOS 11.0 – 40.5 %;



Graf 2 Přehled verzí iOS z roku 2017 – převzato z [11]

Ze statistiky můžeme vyčíst, že nejrozšířenější je verze iOS 10.0 s 46.9 procentním zastoupením. Lze ale předpokládat, že se poměr zastoupení brzy změní, protože tvůrci systému iOS usilují o to, aby všichni uživatelé měli na svých zařízeních nainstalovány co nejaktuálnější verze tohoto operačního systému. V nových verzích jsou totiž odstraněné chyby předchozích verzí a zároveň přidaná různá vylepšení pro uživatele. Mobilní telefon po vydání nové verze operačního systému upozorní uživatele, že je k dispozici novější verze a toto upozornění se objevuje do té doby, dokud uživatel operační systém neaktualizuje [11].

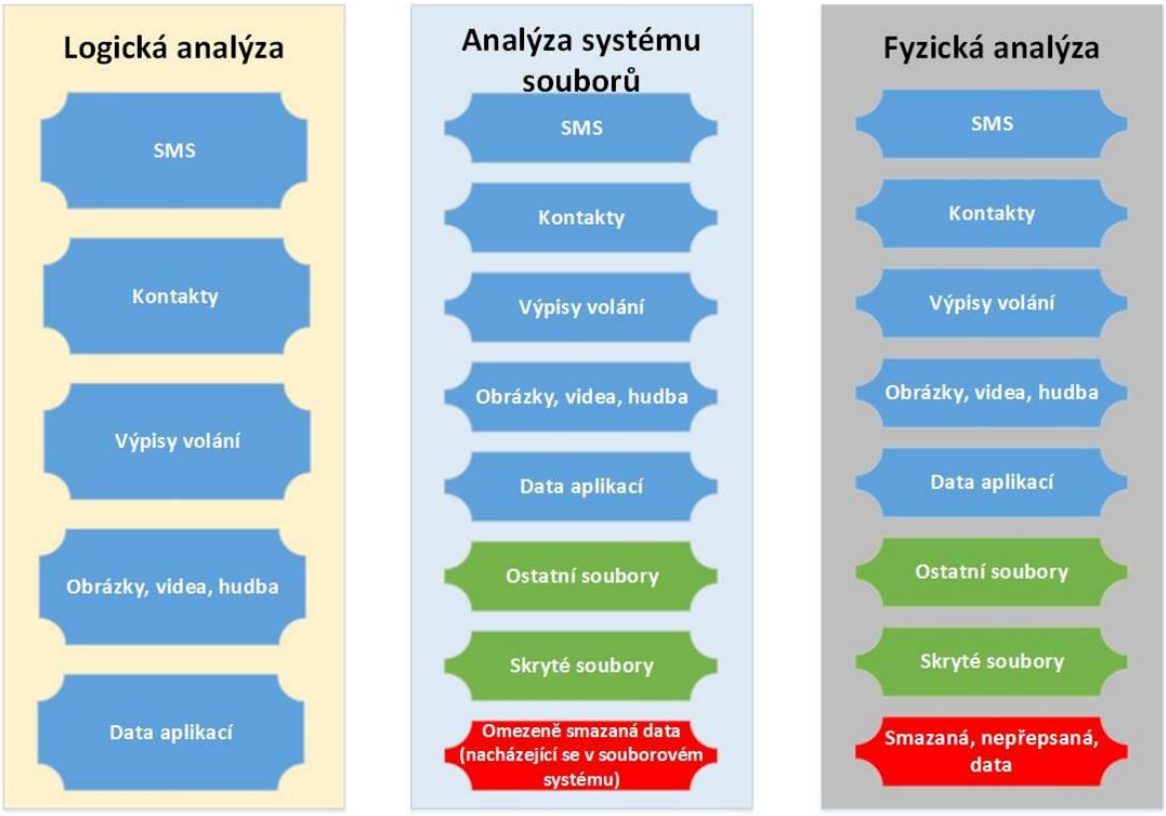
3 Forenzní analýza

Forenzní analýza digitálních dat je vědní obor zabývající se zjišťováním dat z digitálních zařízení. Nalezená data musí být přísně chráněna a nesmí s nimi být manipulováno z důvodu jejich využívání například při objasňování trestných činů.

Forenzní analýza má několik částí. První je ochrana důkazů, které mají být forenzně zkoumány, aby nedošlo k manipulaci nebo poškození dat. Další částí je provedení samotné analýzy dat. Následuje vyhodnocení získaných informací a jejich interpretace ve srozumitelné podobě tak, aby mohly být použity jako důkazy při odhalování trestné činnosti. Velice důležité je také důsledné zdokumentování celého procesu, aby nemohl být v budoucnu nikým zpochybněn a zjištěné informace a důkazy tak mohly být plnohodnotně použity v rámci důkazního řízení. U mobilních telefonů, kterými se budu dále zabývat, je možno aplikovat několik verzí forenzních analýz, které budou popsány v následujících kapitolách. [12].

3.1 Druhy forenzních analýz

Existují tři hlavní druhy forenzních analýz - logická analýza, analýza systémových souborů a fyzická analýza. Na obrázku níže jsou seřazené od nejjednodušší analýzy po nejsložitější. Jednotlivé druhy analýz nejsou použitelné pro všechny druhy mobilních telefonů. Při výběru varianty forenzní analýzy je potřeba zvolit nejvyšší možnou variantu proveditelnou pro konkrétní mobilní telefon. Při volbě varianty forenzní analýzy je potřeba dále zohlednit možnost provedení analýzy bez zapínání telefonu, zadávání kódu telefonu a také riziko zásahu do dat. Před zahájením analýzy je doporučováno vyjmout SIM a paměťovou kartu. Ty jsou zkoumány samostatně, aby nedošlo ke vzdálenému smazání dat. Paměťová karta je vyjmuta hlavně z toho důvodu, že jinak není možné zajistit smazané soubory z této karty [13].



Obrázek 3 Druhy forenzních analýz – převzato z [20]

3.1.1 Logická analýza

Logická analýza je nejnižší úroveň analýzy, přístupná pro většinu mobilních telefonů. V této analýze je využita interakce s mobilním telefonem prostřednictvím Application Programing Interface, dále API, který specifikuje, jak by aplikace a firmware měly spolu fungovat. Při provádění logické analýzy forenzním nástrojem UFED (podrobněji popsáno v kapitole 3.2.1) po načtení API zažádá o read-only přístup do API a po potvrzení začne extrahovat určená data. Nelze při ní zajistit smazané soubory, lze zajistit jen uživatelsky přístupné soubory. Je nutné mít telefon zapnutý, případně vložit kód k odblokování a provést potřebné úkony uvnitř mobilního telefonu. Z logické analýzy lze získat například SMS, kontakty, výpisy volání, obrázky, videa, hudbu a data z aplikací. Veškerá v minulosti smazaná data již nelze pomocí tohoto druhu analýzy zajistit [13].

3.1.2 Analýza systémových souborů

Tato analýza také využívá API a interakci s mobilním telefonem. Rozdíl je ve využití jiných metod extrakce za pomoci API. Funguje na podobném principu jako logická analýza, kdy UFED pošle dotaz API, zda může vytěžit souborový systém a po kladné

odpovědi začne s extrakcí. UFED poté musí ještě dekódovat data, která se nacházela v systémových souborech. Ve většině případů je nutné zapnout mobilní telefon, zadat kód a provést potřebné úkony uvnitř mobilního telefonu. Tato analýza vytěží celý souborový systém. Je možné extrahovat i skryté soubory operačního systému a také některé smazané soubory, které ještě nebyly přepsány jinými. Stejně jako u logické analýzy je možno nalézt SMS, kontakty, výpisy volání, obrázky, videa, hudbu a data aplikací, ale navíc také ostatní soubory, skryté soubory a smazaná data, která se nacházejí uvnitř souborového systému [13].

3.1.3 Fyzická analýza

Fyzická analýza je nejvyšší úrovní forenzní analýzy. Extrahuje vnitřní obraz paměti telefonu. Ve většině případů nemusí být telefon zapnutý. Využívá se takzvaný bootloader, což je kód, který je uložený v RAM paměti a během zapínání mobilního telefonu umožní forenznímu nástroji přístup a kopírovaní dat z mobilního telefonu. Jen u některých mobilních telefonů HTC je nutné mobilní telefon zapnout, zadat kód a provést potřebné úkony uvnitř mobilního telefonu. Z obrazu paměti telefonu lze dekódovat smazané nepřepsané soubory. Tento druh analýzy podporuje nejméně zařízení a je nejvíce náchylný na změny v operačním systému a aktualizace. Tak jako u předchozích analýz je možné vytěžit SMS, kontakty, výpisy volání, obrázky, hudbu, videa, data aplikací. Stejně jako u analýzy systémových souborů lze nalézt ostatní soubory, skryté soubory a také smazaná nepřepsaná data. Fyzická analýza provádí bitovou kopii celého telefonu. Podle posledního vyjádření firmy Cellebrite, která vlastní forenzní nástroj UFED, lze fyzickou analýzu použít na 90 procentech zařízení s operačním systémem Android. Nutné je před analýzou propojit počítač s mobilním telefonem, nastavit telefon, nahrát aplikaci z forenzního nástroje UFED a poté udělat extrakci na předem zvolené úložiště [13].

3.2 Druhy forenzních nástrojů

Pro provedení forenzní analýzy je potřeba použít konkrétní forenzní nástroj. Některé mobilní telefony lze vytěžit pouze specifickým forenzním nástrojem. V současné době existuje celá řada forenzních nástrojů. V této bakalářské práci jsou testovány mobilní telefony pouze nástrojem UFED firmy Cellebrite. Popsány jsou i některé další forenzní nástroje jako jsou MobilEdit! Forensic, Oxygen Forensic Suite či MSAB XRY.

3.2.1 Cellebrite UFED

Tento forenzní nástroj je používán k extrakci dat z mobilních telefonů, paměťových karet a disků. Podporuje více než šestnáct tisíc mobilních zařízení. Dokáže obejít hesla, přístupové kódy nebo gesta u velkého množství telefonů. Je schopen prolomit „rootované“ i „nerootované“ Android telefony. Vytěží data i ze zakódovaného telefonu iPhone 4 nebo 5. Je také možná fyzická extrakce dat a hesel z telefonů vybavených čínskými chipsety MTK, Spreadtrum, Infineon. Tento forenzní nástroj je dostupný ve dvou formách - 4PC a Touch2. Obě dvě formy jsou v podstatě stejné, jen verze 4PC je nainstalovaná v počítači a Touch2 je pro tablet určený přímo pro tento nástroj [14].

3.2.2 MobilEdit! Forensic

Jedná se o extraktor mobilních telefonu a cloudů, datový analyzátor a generátor zpráv. Využívá jak fyzické tak logické metody. Je schopen analyzovat aplikace, obnovit smazaná data na široké škále mobilních telefonů a zvládne prolomit některá hesla [15].

3.2.3 Oxygen Forensic Suite

Forenzní nástroj k vytěžení dat z mobilních telefonů, jejich záloh, dronů nebo cloudových služeb. Podporuje více než šestnáct tisíc druhů mobilních zařízení. Existuje v několika verzích, nejvíce využívaná jsou Analyst, která slouží k analyzování zařízení a ostatních věcí, a Detective, která hledá hesla, obrázky, zálohy u zařízení a lokace a historii dronů [16].

3.2.4 MSAB XRY

Digitální forenzní nástroj, který se používá k analýze a obnově mobilních zařízení. Skládá se z hardwarového zařízení, přes které je připojen mobilní telefon k počítači a softwaru. Software je dostupný pro orgány činné v trestném řízení, vojenské a zpravodajské agentury. XRY umožňuje jak logické, tak fyzické analýzy mobilních zařízení [17].

4 Digitální stopy

Digitální stopa je jakákoliv informace s vypovídající hodnotou pro danou relevantní událost, uložená, nebo přenášená v digitální podobě. V kriminalistice a forenzních vědách se jedná o důkazní materiál. V tomto případě to mohou být digitální data nalezená přímo na místě spáchání trestného činu, nebo jakýkoliv jiný důkaz, který má vazbu na trestný čin. Digitální stopy vznikají působením člověka na počítač, mobilní telefon, tablet nebo jakékoliv jiné digitální zařízení. Někteří lidé si ani neuvědomují, kolik digitálních stop za svůj život zanechají. Digitální stopy jsou například jakékoliv fotografie, videa, dokumenty nebo zprávy a volání z mobilního telefonu [19].

4.1 Zajištění digitálních stop

Zajišťovaní digitálních stop musí provádět vyškolený technik a to přímo na místě nálezu. Tento technik musí být seznámen se všemi nalezenými médii, na kterých se vyskytují digitální stopy, protože digitální stopy jsou samy o sobě nehmotné. Technika by měla zajímat jak uložená data, například na mobilním telefonu, tak i data přenášená nebo zpracovávaná. Zajištěné digitální stopy jsou poté expertizně zkoumány a použity jako důkazní materiál při soudním řízení. Fyzické a datové stopy se stávají důkazy teprve, když jsou akceptované orgány činnými v trestném řízení. Samozřejmě je nutné akceptovat legislativu dotčených zemí, případně obecně platné smlouvy mezinárodního práva. Datové objekty mohou mít různé formáty, ale nikdy se nesmí změnit původní informace. Fyzické prvky jsou například disky, CD, DVD a paměťové karty [18].

4.2 Specifikace digitálních stop

Digitální stopy mají své obecné druhové charakteristiky a vlastnosti, které mají negativní i pozitivní důsledky, patří mezi ně:

- nehmotnost – samy o sobě nehmotné, nutné medium pro jejich uložení;
- latentnost – pro většinu uživatelů neviditelné, neznalý uživatel zanechá stopy, aniž si to uvědomí. Ke zviditelnění digitálních stop je používán různý aplikační, systémový nebo specializovaný forenzní systém;

- časová trasovatelnost – velmi často jsou digitální stopy přímo spojeny s časovým údajem a nejčastěji má každá digitální stopa nějakou časovou známku;
- vysoká obsažnost – díky vysoké obsažnosti digitálních stop s nimi lze pracovat mnoha způsoby. Důkazní digitální stopy slouží jako věcný důkaz. Dále existují indikativní digitální stopy, ty obsahují nepřímé informace, které samy o sobě neprokazují trestný čin. Dalším druhem jsou profilové digitální stopy, což jsou informace, se kterými člověk pracoval jakoukoliv formou a jsou uložené na digitálních zařízeních a discích;
- velmi nízká životnost – rozhodující je rychlost, s jakou jsou digitální stopy získány. Ty se mohou nacházet v operační paměti, běžícím serveru nebo na discích, které se dají snadno přepsat;
- uchovávání a kvalita je ovlivněna řadou faktorů – dobře nastavené legislativní a interní předpisy a odbornost administrace mohou zajistit úspěšné získání digitálních stop;
- velký datový objem – velké množství informací na datových mediích v dnešní době znamená obtížnější objevení digitálních stop;
- datová hustota v čase s rozvojem nových technologii neustále klesá – kvůli velkokapacitním mediím se digitální stopy stále hůře nalézají;
- extrémní dynamičnost prostředí – nelze přerušit například chod serveru, a proto je obtížnější z něj digitální stopy získat;
- heterogennost a komplexnost prostředí – v dnešní době je prostředí velmi rozmanité a heterogenní, a proto je možné najít digitální stopy, i když byly zničeny na jiných zdrojích;
- velký geografický rozsah prostoru – některé útoky jsou vedeny přes více serverů a tudíž jsou hůře dohledatelné, je potřeba vždy respektovat legislativu daných zemí viz výše;
- vysoký stupeň ochrany dat – zašifrovaná a zakódovaná data neobsahují v této formě žádnou použitelnou informaci;
- automaticky identifikovatelné – některé digitální stopy vznikají samy nezávisle na uživateli a můžeme je nezávisle vyhledat pomocí specializovaného softwaru;

- vysoká úroveň zahlazování stop pachatelem – schopný pachatel dokáže nejen napáchat rozsáhlé škody, ale také je po sobě velice dobře zahladit;
- restaurovatelnost – některé digitální stopy, které byly smazané je možno obnovit;
- originálnost – datové záznamy a jejich nosiče lze snadno duplikovat, aniž by došlo ke změně obsahu nebo vlastností digitálních stop [19].

5 Forenzní analýza jednotlivých zařízení

K testování bylo použito sedm mobilních telefonů, dva se systémem iOS a pět se systémem Android. Telefony byly vybrány tak, aby byly zastoupeny nejčastější verze obou operačních systémů. U operačního systému Android byly vybrány verze Android 4.4 KitKat, Android 6.0 Marshmallow a Android 7.0 Nougat. U operačního systému iOS byly vybrány verze iOS 7.1 a iOS 11.0 - verze 7.1 z důvodu, že byla nainstalována na iPhone 4, na kterém lze provést fyzickou analýzu. Během testování byly použity všechny druhy forenzních analýz, takže lze vidět rozdíly mezi nimi. Všechny telefony byly testované na forenzním nástroji UFED od firmy Cellebrite na verzi 4PC. Dále je popsán průběh analýzy, konkrétně na mobilních telefonech Lenovo K5 Note se systémem Android, iPhone 6s se systémem iOS a iPhone 4 se systémem iOS. Pro ostatní telefony se systémem Android probíhala analýza stejným způsobem jako u telefonu Lenovo K5 Note, a proto již nejsou znovu popisovány.

5.1 Analýza mobilního telefonu s operačním systémem Android

Analýza mobilního telefonu s operačním systémem Android bude podrobně popsána na příkladu telefonu Lenovo K5 Note. Odlišnosti analýz ostatních telefonů budou popsány na konci kapitoly.

Na začátku je třeba telefon vyhledat ve forenzním nástroji Cellebrite UFED. Je zde možná autodetekce nebo je také možné vybrat z historie, pokud již byla analýza na tento typ telefonu v minulosti prováděna. Doporučuje se ale vyhledat telefon ručně, jelikož program může někdy zvolit špatnou verzi daného telefonu. Dále se u daného telefonu objeví výběr z analýz, které jsou k tomuto zařízení dostupné. U většiny případů se nabízí logická, fyzická nebo analýza systémových souborů. Vždy by měla být vybrána nejvyšší možná, kterou je v tomto případě analýza fyzická. Po zvolení vybrané analýzy nástroj UFED upozorní na další kroky, které je potřeba provést předtím, než lze analýzu spustit. Před zahájením analýzy je potřeba prověřit, že je zařízení dostatečně nabité, aby vydrželo po dobu celé analýzy, a že je dostatek paměti na paměťové kartě, která musí být vložena

uvnitř. Dále je potřeba v telefonu zapnout možnosti pro vývojáře a také režim ladění a zůstat vzhůru. Následně povolit Media Transfer Protocol a neznámé zdroje v zabezpečení a poté pokračovat samotnou analýzou. Nástroj UFED si nahraje svojí aplikaci přímo do telefonu a pomocí ní udělá bitovou kopii na vloženou paměťovou kartu. Na konci tuto aplikaci smaže a analýza je hotova. Na paměťové kartě lze nalézt soubor .ufd, ve kterém jsou všechna data, která forenzní nástroj UFED nalezl a také aplikaci, která umožní přístup do UFED Readeru. Zde je možné veškerá data prohlédnout a analyzovat.

Postup analýzy byl u ostatních telefonů s operačním systémem Android podobný, pouze u telefonu Samsung Galaxy A3 s verzí Android 7.0 byla použita logická analýza. Fyzická analýza by u tohoto telefonu byla také možná, provádějí jí však pouze v sídle firmy UFED a je zpoplatněná. V našich podmínkách není tuto analýzu možné provést. U telefonu Huawei Ascend P6 byla použita fyzická analýza stejně jako u telefonu Lenovo K5 Note.

Výše popsaný postup není běžně používaný v praxi. Běžná fyzická analýza by měla být prováděna na vypnutém telefonu pomocí takzvaného bootloaderu, neboli zavaděče, aby nedocházelo ke změnám dat. Tato možnost analýzy se už u novějších typů telefonů nepoužívá z důvodu většího zabezpečení od výrobců. Právě z tohoto důvodu se derou do popředí právě fyzické analýzy prováděné na zapnutém telefonu.

5.2 Analýza mobilního telefonu iPhone 6s s operačním systémem iOS

Začátek analýzy je stejný jako u telefonu se systémem Android, je potřeba vyhledat telefon ve forenzním nástroji UFED. Poté se objeví všechny dostupné forenzní analýzy. U iPhone 6s verze 11.0.3 jsou možné všechny analýzy, pouze fyzická nelze provést v našich podmínkách a je potřeba pro její provedení odeslat zkoumaný telefon do firmy Cellebrite. Byla tedy zvolena druhá nejvyšší možná varianta forenzní analýzy a to analýza systémových souborů. Dále je potřeba zvolit složku, do které se budou vytěžené soubory z mobilního telefonu ukládat. Poté je nutné nastavit mobilní telefon, který je zkoumán, a to následujícím způsobem: v nastavení telefonu zvolit uzamčení telefonu na nikdy a ověřit dostatečné nabití telefonu. Nakonec se spustí začátek forenzní analýzy na telefonu a zvolí se možnost důvěřovat zařízení UFED, čímž se spustí celá analýza. Výsledek celé analýzy je v předem zvolené složce. Uvnitř této složky lze nalézt soubor .ufd, ve kterém jsou

všechna vytěžená data a také zástupce aplikace UFED Reader, ve kterém jsou data setříděna do jednotlivých kategorií, a je možné s nimi pracovat.

5.3 Analýza mobilního telefonu iPhone 4 s operačním systémem iOS

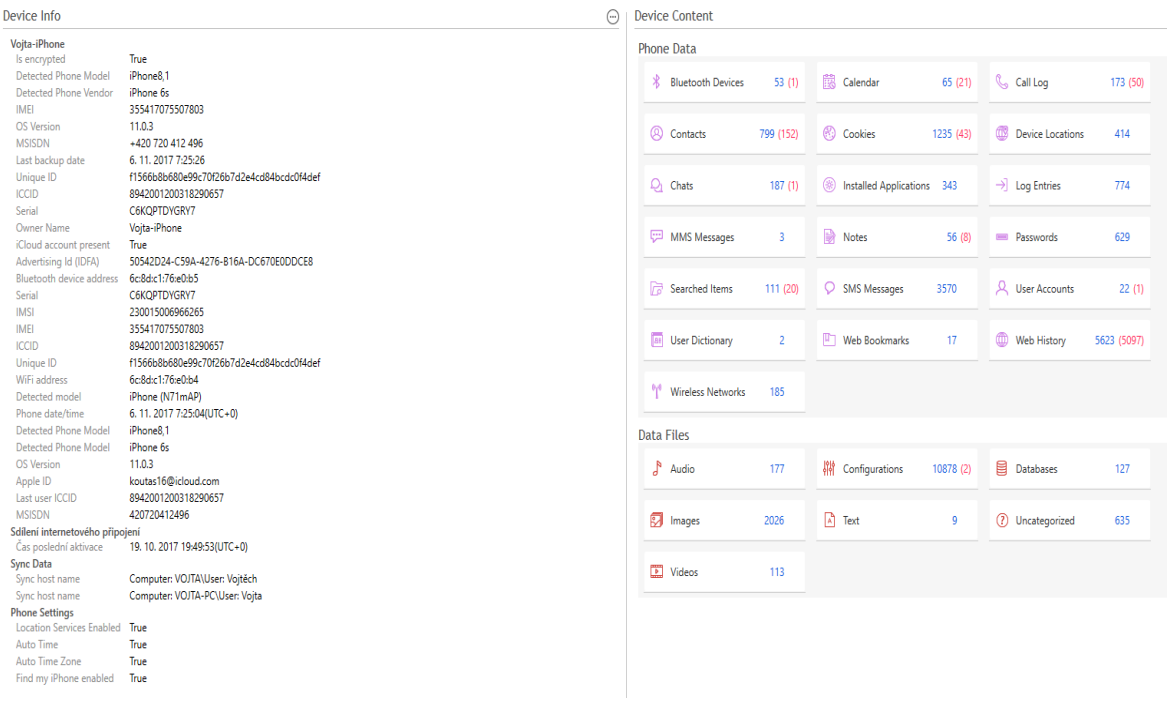
Stejně jako u předchozích analýz je potřeba nejdříve mobilní telefon vyhledat ve forenzním nástroji UFED a poté zvolit nejvyšší možnou forenzní analýzu, kterou tento nástroj nabízí. U tohoto mobilního telefonu je možno provést nejvyšší stupeň forenzní analýzy tedy fyzickou, aniž bychom museli mobilní telefon kamkoli posílat. Dále je zvolena složka, do které se uloží vytěžená data. Od tohoto okamžiku se postup obou analýz liší. Je potřeba mobilní telefon nejdříve vypnout, poté připojit jednu část kabelu T-110 do počítače. Poté stisknout tlačítko domů na telefonu iPhone a zároveň připojit druhou část kabelu do mobilního telefonu. Tlačítko domů je potřeba držet tak dlouho, dokud nezmizí obrázek na ploše telefonu. Tímto je zařízení připojeno v režimu obnovy. Dále je potřeba zároveň stisknout tlačítko na vypnutí a tlačítko domů a poté zapnout analýzu. Následně uvolnit tlačítko na vypínání a nakonec, když se celá analýza rozběhne, pustit i tlačítko domů. Forenzní nástroj nejdříve prolomí čtyřmístný kód na telefonu a potom provede samotnou analýzu celého telefonu. Výsledek analýzy se opět objeví v předem definované složce. Zde jsou znovu dva soubory - první je soubor .ufd se všemi daty a druhý je zástupce aplikace UFED Reader, pomocí kterého lze analyzovat všechna vytěžená data.

6 Vyhodnocení výsledků

V této kapitole jsou vyhodnoceny a porovnány výsledky všech forenzních analýz u jednotlivých mobilních telefonů. Výsledky jednotlivých analýz získáme otevřením souboru .ufd daného mobilního telefonu v programu UFED Reader. Vznikne tak report, ve kterém je možno nalézt vše, co bylo možno vytěžit z mobilního telefonu. Je důležité zmínit, že do všech mobilních telefonů byl během zkoumání umožněn přístup.

6.1 iPhone 6s se systémem iOS

Následující obrázek znázorňuje výsledek analýzy systémových souborů po otevření reportu v UFED Readeru. Verze operačního systému tohoto mobilního telefonu je 11.1.3.



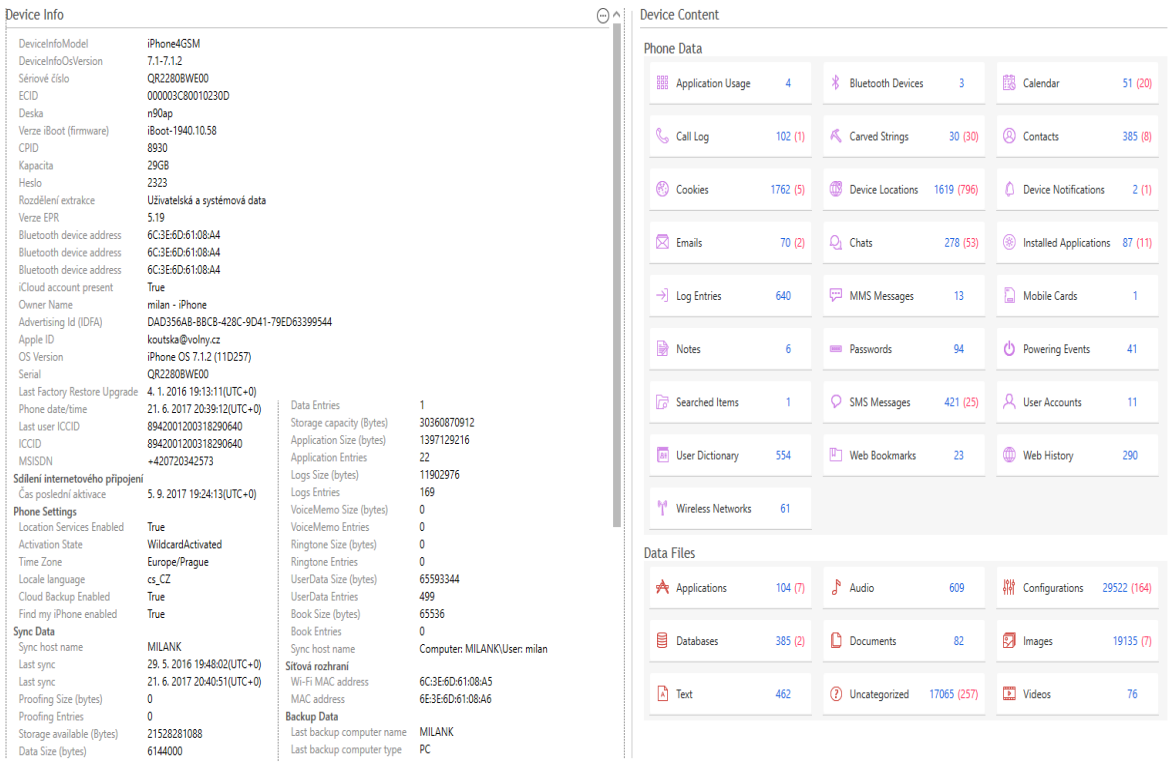
Obrázek 4 Výsledek forenzní analýzy iPhone 6s - Screenshot

Vlevo je možné vidět všechna data o telefonu. Mezi nejdůležitější patří model telefonu a jeho verze, dále IMEI a verze operačního systému iOS. Je zde možno nalézt jméno držitele mobilního telefonu, datum poslední zálohy, existenci iCloud účtu, Apple ID, telefonní číslo, objeví se zde i informace o tom, zda je aktivovaný režim vyhledávání iPhone a také s jakým počítačem je mobilní telefon spárovaný. Vpravo jsou vidět veškerá vytěžená data. U některých kategorií se objevují hodnoty modrými a červenými čísly. Modrá znázorňují data, která se stále nacházejí v mobilním telefonu a červená pak data

smazaná, která se během forenzní analýzy podařilo obnovit. Lze vidět data z kalendáře, kontaktů, umístění zařízení, hesla, zprávy včetně SMS a chatů jako je Messenger a WhatsApp, dále historii webového prohlížeče, připojené WiFi sítě, obrázky, videa, hudbu, poznámky. Forenzní analýza také odhalila rozšifrovaná hesla z některých webových stránek nebo WiFi sítí, které nemají svá hesla dostatečně zašifrovaná.

6.2 iPhone 4 se systémem iOS

Stejně jako u předchozího telefonu jsou výsledky znázorněny v reportu znázorněném prostřednictvím UFED Readeru. U tohoto mobilního telefonu byla použita fyzická analýza a verze jeho operačního systému je 7.1.3.



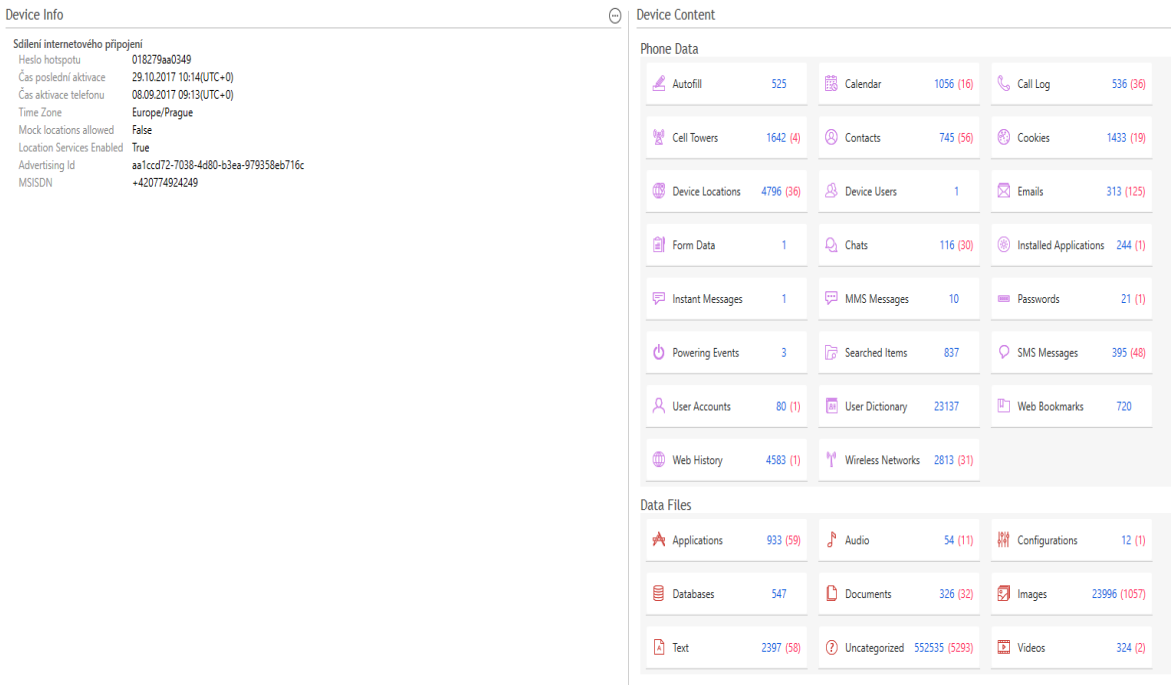
Obrázek 5 Výsledek forenzní analýzy iPhone 4 - Screenshot

Vzhledem k tomu, že bylo možné u tohoto telefonu použít fyzickou analýzu, byly získány daleko rozsáhlejší informace o tomto zařízení. Na obrázku vlevo jsou uvedeny základní informace o mobilním telefonu, například jeho verze i typ, verze operačního systému, iCloud účet, Apple ID, telefonní číslo, zda jsou zapnuté polohové služby, počítač s kterým byl telefon spárován, na jaký počítač a kdy byla provedena poslední záloha: Navíc bylo možné díky analýze zjistit přístupový kód do telefonu či velikost úložiště v zařízení. V pravé části obrázku jsou podobná data jako u předchozí analýzy - výpis

z kalendáře, kontaktů, lokací zařízení, zpráv a jiných chatů, nainstalované aplikace, poznámky, hesla stejně, jako v předchozím telefonu, dále také uživatelské účty, SMS a MMS zprávy, videa, fotky, hudba, historie a záložky z webu a také všechny WiFi sítě, na které byl telefon připojen. Navíc jsou zde uvedeny emaily, logy ze zapínání a vypínaní mobilního telefonu, dokumenty a také větší množství smazaných souborů.

6.3 Lenovo K5 Note se systémem Android

V reportu UFED Readeru je možno vidět výsledek této forenzní analýzy u mobilního telefonu Lenovo K5 Note s verzí operačního systému 6.0, na který byla použita fyzická forenzní analýza.

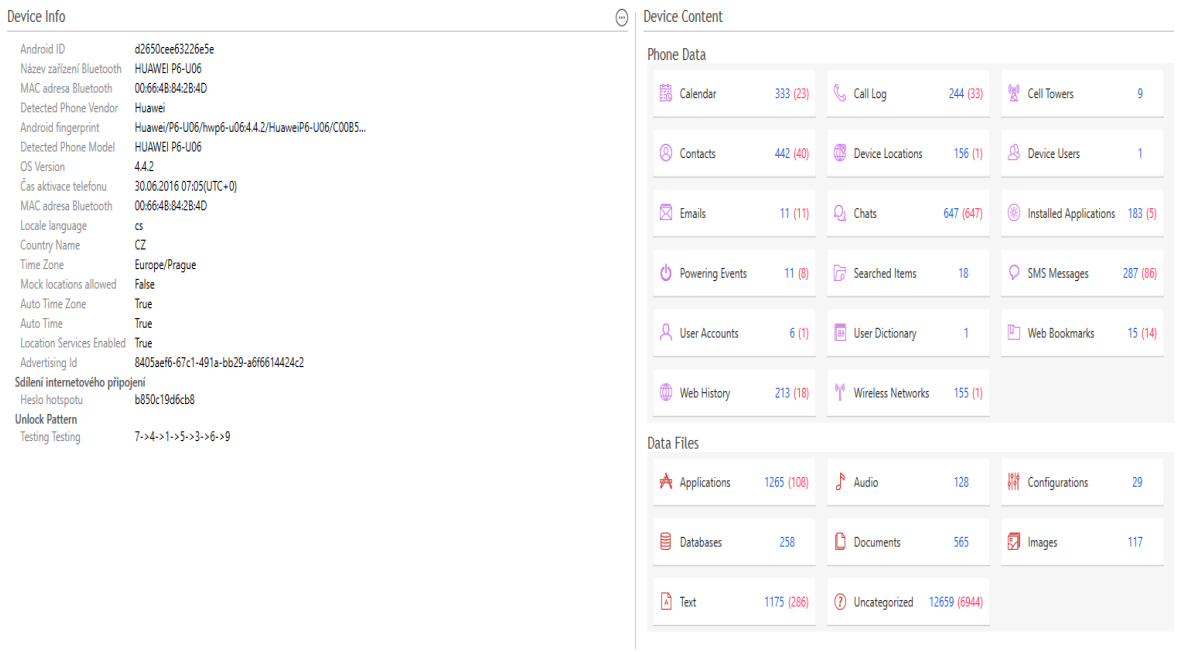


Obrázek 6 Výsledek forenzní analýzy Lenovo K5 Note - Screenshot

Obrázek opět znázorňuje výsledek forenzní analýzy. V levé části jsou zobrazeny systémové údaje a telefonní číslo tohoto mobilního telefonu, v pravé části pak data, která jsou roztříděná do kategorií. Jsou zde údaje z kalendáře, kontakty, uživatelské účty, emaily, chaty, hesla, zprávy a webová historie společně se záložkami z webu, dále jsou zde také fotky, videa, hudba a textové soubory z tohoto mobilního telefonu.

6.4 Huawei Ascend P6 se systémem Android

Na obrázku níže vidíme výsledek forenzní analýzy mobilního telefonu Huawei Ascend P6 s verzí operačního systému 4.4, na který byla použita fyzická analýza.

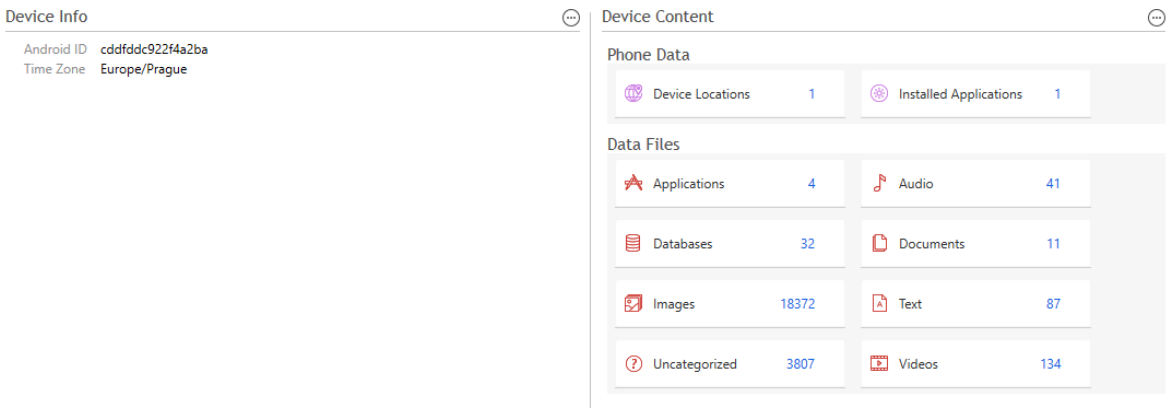


Obrázek 7 Výsledek forenzní analýzy Huawei Ascend P6 - Screenshot

Vlevo jsou opět vypsány údaje o mobilním telefonu, který byl analyzován. Je zde Android ID, název, model, země a verze operačního systému, vpravo pak data, která byla vytěžena. Jsou zde SMS, MMS, výpisy z kalendáře, kontakty, chaty, zapnutí a vypnutí telefonu, webové záložky a historie, dále také fotky, videa, hudba, dokumenty a aplikace z mobilního telefonu.

6.5 Samsung Galaxy A3 se systémem Android

Na telefonu Samsung Galaxy A3 s verzí operačního systému Android 7.0 byla použita logická analýza. Na obrázku jsou opět znázorněna data z reportu po otevření UFED Readeru.



Obrázek 8 Výsledek forenzní analýzy Samsung Galaxy A3 - Screenshot

Z obrázku je zřejmé, že pomocí této analýzy nebylo nalezeno takové množství informací jako v přechozích případech. Nebyly nalezeny téměř žádné informace o zařízení jako takovém a ani množství vytěžených dat není nijak velké. Jsou zde pouze pozice mobilního telefonu, nainstalované aplikace, hudba, databáze, dokumenty, obrázky a videa. Analýza nenalezla ani žádné smazané soubory, kontakty čizprávy.

6.6 Xiaomi 3s se systémem Android

Telefon Xiaomi 3s s verzí operačního systému Android 6.0 je jedním ze dvou telefonů, na kterém se forenzní analýza v našich podmínkách nepodařila provést. U mobilního telefonu Xiaomi nešlo před provedením analýzy mobilní telefon spárovat s nástrojem UFED. Možností proč tomu tak je může být mnoho. Může to být vadný USB konektor nebo upravený systém mobilního telefonu, či jiné neznáme komplikace.

6.7 HTC Incredible S se systémem Android

Poslední mobilní telefonem, který byl analyzován je telefon HTC Incredible S s verzí operačního systému Android 4.4. Tento telefon měl rozbitý displej, a proto se jej nepodařilo analyzovat. U telefonů HTC je totiž pro úspěšné provedení forenzní analýzy potřeba provést konkrétní úkony uvnitř telefonu, konkrétně je potřeba potvrdit USB vstup přímo na displeji telefonu, což nebylo s rozbitým displejem možné. Naproti tomu například telefony Samsung se starší verzí operačního systému Android než je 7.0 pro provedení analýzy displej nepotřebují a analýza by tedy mohla být i přes tuto překážku provedena.

6.8 Shrnutí výsledků

Po vyhodnocení výsledku všech analýz bylo zjištěno, že nejméně bezpečný je iPhone 4, jelikož UFED dokázal prolomit i jeho heslo. Hlavním důvodem je zejména to, že firma Apple tento mobilní telefon přestala podporovat a nelze na něj nainstalovat novější verze operačního systému iOS, která by zajistila jeho větší bezpečnost, a proto je velice náchylný na jakékoliv útoky. Naopak nejlepšího výsledku dosáhl telefon Samsung, ve kterém nebyla po použití logické analýzy nalezena téměř žádná důležitá data. Je to zapříčiněno jednak vyšším zabezpečením telefonu a zároveň druhem použité analýzy.

U všech telefonů je velkým problémem nešifrování hesel z různých internetových stránek nebo WiFi sítí. Tato hesla by se dala využít například pro přístup do firemních sítí, kam má držitel mobilního telefonu přístup nebo také do jeho vlastních účtů na internetu. Dalším velkým problémem jsou nezašifrované zprávy a e-maily, takže si útočník může přečíst veškerou komunikaci oběti a najít z ní potřebná data. Dalším potenciálním problémem jsou kontakty uvnitř mobilního telefonu. Pro některé firmy, které mají velkou konkurenci, by například zcizení seznamu jejich zákazníků mohlo mít velmi negativní následky na jejich podnikání. V tabulce níže jsou shrnuté výsledky všech analýz a přehledně popsaná data, která byla nalezena u jednotlivých telefonů.

	iPhone 6s	iPhone 4	Lenovo K5 Note	Huawei Ascend P6	Samsung Galaxy A3
Operační systém	iOs	iOs	Android	Android	Android
Verze operačního systému	11.1.3.	7.1.3.	6.0.	4.4.	7.0.1.
Typ forenzní analýzy	Systémvých souborů	Fyzická	Fyzická	Fyzická	Logická
Údaje o telefonu	Ano	Ano	Částečně	Ano	Ne
Uživatelský účet	Ano	Ano	Ano	Ano	Ne
Kalendář	Ano	Ano	Ano	Ano	Ne
Kontakty	Ano	Ano	Ano	Ano	Ne
Místa kde bylo zařízení	Ano	Ano	Ano	Ano	Ne
E-mail	Ne	Ano	Ano	Ano	Ne
Zprávy	Ano	Ano	Ano	Ano	Ne
Web	Ano	Ano	Ano	Ano	Ne
WiFi sítě	Ano	Ano	Ano	Ano	Ne
Obrázky	Ano	Ano	Ano	Ano	Ano
Hudba	Ano	Ano	Ano	Ano	Ano
Videa	Ano	Ano	Ano	Ano	Ano
Hesla	Ano	Ano	Ano	Ano	Ne
Přístupové heslo	Ne	Ano	Ne	Ne	Ne
Smazaná data	Částečně	Ano	Ano	Ano	Ne

Tabulka 1 Výsledky forenzních analýz

7 Doporučení k základnímu používání mobilních telefonů

V dnešní době používá mobilní telefon v podstatě každý, od dětí po důchodce. Každý by měl mít mobilní telefon úměrný tomu, za jakým účelem ho chce používat. Pokud se v něm nachází například důležité pracovní nebo osobní informace, měl by uživatel tohoto telefonu důsledně dbát na zajištění jeho bezpečnosti. Vždy je samozřejmě výhodou vlastnit novější typ mobilního telefonu, který je vybaven nejnovějšími technologiemi. Velmi důležité je pravidelně aktualizovat operační systém telefonu a dbát doporučení výrobců.

Každý uživatel by měl dodržovat základní bezpečnostní pravidla, jako například neukládat si hesla do telefonu, nevolit si kód nebo gesto na telefonu takové, které se dá snadno prolomit. Také by neměl zapisovat svoje hesla například do poznámek nebo různých textových editorů, protože jak vyplynulo z výsledků, všechna tato data jsou přístupná po provedení forenzní analýzy. Útočník by tak byl schopen zjistit i velice složité heslo.

Dále je možné sledovat polohu a pohyb mobilního telefonu, pokud jsou zapnuté polohové služby. Doporučuje se tyto služby vypnout, pokud nejsou nezbytně nutné, například kvůli používání map nebo navigace.

Co se týče mobilního prohlížeče, je z výsledků analýzy patrné, že je možné zjistit historii vyhledávání. Útočník tak může zjistit konkrétní informace o uživateli, například jakou využívá banku nebo jiná citlivá data. Řešením v tomto případě může být průběžné odstraňování historie vyhledávání v mobilním prohlížeči.

Mobilní telefony jsou často využívány pro různé chaty, messengery, iMessage a jiné zprávy, které slouží ke komunikaci s jinými uživateli mobilních telefonů nebo jiných komunikačních zařízení. Z důvodu soukromí uživatelů, kteří mobilní telefon poskytli na forenzní analýzy, nebyly zprávy obsaženy v těchto telefonech zveřejněny, ale po provedení forenzní analýzy byly všechny zprávy z mobilních telefonů k přečtení a nebyly nijak zašifrované. Doporučuje se tedy Messenger nebo jiné chatovací aplikace občas smazat a nainstalovat znovu. Zprávy je možné v budoucnu kdykoli znovu stáhnout ze serveru, ale po reinstalaci této aplikace již nebudou uloženy ve sledovaném zařízení.

Někteří uživatelé provádějí root u telefonu se systémem Android nebo jailbreak u telefonů se systémem iOS. Znamená to, že tento uživatel získá administrátorská práva u daného telefonu a má přístupnou veškerou paměť telefonu a je schopen nainstalovat aplikace dostupné mimo Google Play nebo App Store. U Androidu je pak viditelný režim pro vývojáře s režimem ladění. Tyto zásahy mohou být vzhledem k bezpečnosti telefonu velice rizikové a nedoporučují se provádět.

Další rizikovou činností může být přeinstalovaní operačního systému od výrobce za jiný, který například tolik nezatěžuje mobilní telefon. Existuje riziko, že tento software není tolik bezpečný jako předchozí, proto by si měl každý uživatel tento krok velmi důkladně rozmyslet.

8 Závěr

Tato bakalářská práce se zabývá bezpečností dvou hlavních operačních systémů Android a iOS. Teoretická část se zabývala architekturou obou těchto systémů a principem forenzní analýzy. Dále bylo v práci vybráno a popsáno několik forenzních nástrojů, které se používají k forenzní analýze mobilních telefonů.

Praktická část obsahuje provedené forenzní analýzy hlavních verzí těchto operačních systémů na mobilních telefonech iPhone 6s, iPhone 4, Lenovo K5 Note, Huawei Ascend P6 a Samsung Galaxy A3.

Po vyhodnocení výsledků těchto analýz bylo nalezeno několik bezpečnostních rizik u testovaných verzí operačních systémů. Nejméně bezpečným byl iPhone 4, jelikož forenzní nástroj UFED dokázal prolomit i jeho heslo. Hlavním důvodem je zejména to, že firma Apple tento mobilní telefon přestala podporovat a nelze na něj nainstalovat novější verze operačního systému iOS. Naopak nejlepšího výsledku dosáhl telefon Samsung Galaxy A3, ve kterém nebyla po použití logické analýzy nalezena téměř žádná důležitá data, což mohlo být zapříčiněno jednak vyšším zabezpečením telefonu a zároveň druhem použité analýzy.

Jedním z velkých problémů u všech telefonů bylo nešifrování hesel z různých internetových stránek nebo WiFi sítí. Tato hesla by se dala využít pro přístup do firemních sítí nebo také do účtů vlastníka telefonu. Dalším velkým problémem jsou nezašifrované zprávy, kontakty a e-maily uvnitř mobilního telefonu, ze kterých si potencionální útočník může zjistit vše, co potřebuje.

Poslední kapitola bakalářská práce obsahuje základní doporučení k zabezpečení mobilních telefonů. Mezi nejdůležitější patří neukládaní hesel v internetových prohlížečích a aplikacích telefonu nebo nezapisování hesel do poznámek. Poté je důležité mazat historii webového prohlížeče, aby útočník nemohl zjistit vyhledávaná data. Z důvodu snížení bezpečnosti mobilního telefonu se nedoporučuje provádět root a jailbreak.

Každý uživatel mobilního telefonu by měl zvážit bezpečnostní rizika související s jeho používáním a vyhnout se jednání, které by mohlo ohrozit jeho nebo jeho okolí.

Seznam literatury

[1] *Android (operační systém).* [online]. [cit. 14. 10. 2017] Dostupné z: https://cs.wikipedia.org/wiki/Android_(opera%C4%8Dn%C3%AD_syst%C3%A9m).

[2] *Platform Architecture*.[online]. [cit. 14. 10. 2017]. Dostupné z: https://developer.android.com/guide/platform/index.html#system-apps.

[3] *Android 7 Nougat posiluje minimálně. Další verze přitom klepe na dveře*.[online]. 2017. [cit. 18. 10. 2017]. Dostupné z: https://www.svetandroida.cz/android-7-nougat-posiluje-minimalne-201708/.

[4] *Android platform*.[online]. 2017. [cit. 18. 10. 2017]. Dostupné z: http://socialcompare.com/en/comparison/android-versions-comparison.

[5] *Kompletní historie iOS: od prvního iPhonu až po iOS 9*.[online]. 2016. [cit. 19. 10. 2017]. Dostupné z: https://www.letemsvetemapplem.eu/2016/03/06/kompletni-historie-ios/.

[6] *iOS Architecture*. [online]. [cit. 19. 10. 2017]. Dostupné z: https://intellipaat.com/tutorial/ios-tutorial/ios-architecture/.

[7] *Cocoa Application Layer*. [online]. [cit. 19. 10. 2017]. Dostupné z: https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/OSX_Technology_Overview/CocoaApplicationLayer/CocoaApplicationLayer.html#//apple_ref/doc/uid/TP40001067-CH274-SW1.

[8] *Media Layer*. [online]. [cit. 19. 10. 2017]. Dostupné z: https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/OSX_Technology_Overview/MediaLayer/MediaLayer.html#//apple_ref/doc/uid/TP40001067-CH273-SW1.

[9] *Core Services Layer*. [online] [cit. 19. 10. 2017]. Dostupné z: https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/OSX_Technology_Overview/CoreServicesLayer/CoreServicesLayer.html#//apple_ref/doc/uid/TP40001067-CH270-BCICAIFJ.

[10] *Core OS Layer*. [online]. [cit. 19. 10. 2017]. Dostupné z: https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/OSX_Te

chnology_Overview/CoreOSLayer/CoreOSLayer.html#//apple_ref/doc/uid/TP40001067-CH9-SW1.

[11] *iOS Version Stats*. [online]. Poslední změna 10. 10. 2017. [cit. 19. 10. 2017]. Dostupné z: https://david-smith.org/iosversionstats/.

[12] KADLEC, Bc. Josef. *Forenzní analýza unixových systémů*. Hradec Králové, 2006. Diplomová práce. Univerzita Hradec Králové. Fakulta informatiky a managementu. Katedra informačních technologií.

[13] *What happens when you press that button?*. [online]. [cit. 25. 10. 2017]. Dostupné z: http://smarterforensics.com/wp-content/uploads/2014/06/Explaining-Cellebrite-UFED-Data-Extraction-Processes-final.pdf.

[14] *10 důvodů proč si vybrat UFED.* [online]. [cit. 25. 10. 2017]. Dostupné z: http://www.ufed.cz/.

[15] *MOBILedit Forensic Express*. [online]. [cit. 25. 10. 2017]. Dostupné z: http://www.mobiledit.com/forensic-express.

[16] *OXYGEN FORENSIC® DETECTIVE*. [online]. [cit. 25. 10. 2017]. Dostupné z: https://www.oxygen-forensic.com/en/.

[17] *XRY (software)*. [online]. [cit. 25. 10. 2017]. Dostupné z: https://en.wikipedia.org/wiki/XRY_(software).

[18] *Digitální stopy v kriminalistice a forenzních vědách*. [online]. [cit. 26. 10. 2017]. Dostupné z: http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf.

[19] *Vlastnosti digitálních stop a jejich dopady na forenzní šetření*. [online]. [cit. 26. 10. 2017] Dostupné z: http://www.sinz.cz/archiv/docs/si-2005-04-183-192.pdf.

[20] KOTHÁNEK, Jakub. *Analýza cloudových služeb v českém protředí.* 2017.

Seznam obrázků

Seznam grafů

Seznam tabulek