



MATEMATIKAI ÉS INFORMATIKAI INTÉZET

Kliens-szerver kommunikáció Android platformon

Készítette

Balajti-Tóth Kristóf

Programtervező Informatikus BSc

Témavezető

Tajti Tibor

Egyetemi adjunktus

EGER, 2019

Tartalomjegyzék

1. Fejlesztői környezetek	5
1.1. Android Studio	5
1.2. Pycharm Professional Edition	5
1.3. Postman	6
2. Platformok	7
2.1. A szerver kiválasztása és felépítése	7
2.2. Mobil platform választása	8
3. Felhasznált technológiák	10
3.1. Verzió kezelés	10
3.2. Folyamatos integrálás	11
3.3. Szerveren használt technológiák	12
3.3.1. Flask	12
3.3.2. SQLite	12
3.3.3. Pusher Beams (Python Server SDK)	13
3.3.4. Docker	14
3.3.5. jd-cmd	14
3.3.6. Apktool	14
3.3.7. dex2jar	15
3.3.8. JSON	15
3.4. Androidon használt technológiák	16
3.4.1. AndroidX	16
3.4.2. OkHttp	17
3.4.3. Pusher Beams (Java Client SDK)	17
3.4.4. Firebase Messaging	18
3.4.5. Room	18
3.4.6. CodeView	18
3.4.7. Espresso	19
3.4.8. Material Design 2.0	21

4. Teszteléshez felhasznált eszközök és források	23
4.1. Sérülékeny Android alkalmazások	23
5. Megvalósított funkciók	24
5.1. Regisztráció	24
5.2. Bejelentkezés	24
5.3. Kijelentkezés	24
5.4. Adatok törlése	24
5.5. Fájl feltöltés	24
5.6. Fájl letöltés	25
5.7. Navigáció a fájlrendszerben	25
5.8. Értesítések	26
6. Továbbfejlesztési lehetőségek	27
7. Tapasztalatok	28

Bevezetés

Az szoftver fejlesztés egy nagyon komplex folyamat és rengeteg részletre oda kell figyelni. Az elkészült programnak hatékonynak, hibamentesnek és gyorsnak kell lennie. Természetesen, mindezt határidőn belül kell teljesíteni. Sajnos a biztonság nem egy első számú szempont egy megrendelő szemében, csak akkor ha már valami baj történt. Inkább a gyorsaságon és a folyamatok automatizálásán van a hangsúly, ezért nem meglepő, hogy a fejlesztés életciklusának tervezési szakaszában kevés figyelem fordul a szoftver biztonságossá tételére.

A statista.com [1] kutatása szerint 2020-ra több mint 4.78 billió telefon lesz használatban. Ezzel a cégek is tisztában vannak és tudják, hogy ha még több emberhez szeretnék eljuttatni a szolgáltatásukat, akkor rendelkezniük kell saját mobilos app -al.

A mobilos eszközöket célzó támadások száma hatalmas ütemben nő. Mindez azért lehetséges, mert figyelmen kívül marad a „secure coding”-nak nevezett gyakorlat. Egy alkalmazásnak a sebezhetőségét különböző támadási vektoron is ki lehet aknázni. Az elején, bennem többek között az a kérdés merült fel, hogy honnan tudható hogy ez alkalmazás ebezhető-e vagy sem.egy kérdés merült fel. Honnann tudhatom, hogy egy adott alkalmazás sebezhető-e vagy sem és ha igen milyen súlyos a hiba. A leghatékonyabb módszer ha visszafejtjük az alkalmazást forráskódra. Ezt angolul „reverse engineering”-nek nevezik. A visszaállított fájlok olvashatósága nem lesz tökéletes, főleg ha obfuscált¹ kóddal állunk szemben, de egy tapasztalt szem így is kitudja szűrni a gyakori hibákat.

A szakdolgozatomban Android platformra készült alkalmazások forrás fájlkká való visszaállításáról írok, valamint bemutatom hogyan valósítható meg a kliens-szerver kommunikáció egy REST API és egy Android platforma készült kliens segítségével. A felhasználó egy egyszerű autentikáció után képes lesz .apk fájlok feltöltésére, letöltésére és az elkészült projekteben való navigálásra. Hosszabb ideig tartó folyamatok állapotról és elkészültéről értesítést kap és lehetősége lesz a forrás kód alkalmazáson belüli megtekintésére és megosztására. A projektet „Reverse Droid”-nak neveztem el.

¹ Az obfuscáció célja röviden, hogy megnehezítse a visszafejtett kód olvashatóságát.

1. fejezet

Fejlesztői környezetek

1.1. Android Studio

Az Android Studio jelenleg az egyetlen jól támogatott és minőségi fejlesztői környezet Android fejlesztéshez. Régebben sok panaszt hallottam az emulátorára, hogy nagyon lassú és körülményes a használata. Mára már egy pillanat alatt lehet futtatni a programunk és abszolút kényelmes lett a használata. Az emulátor állapota menthető, ezáltal indításkor ott folytathatjuk ahol abba hagytuk. Azon kívül, hogy használatával több különböző eszközön tesztelhetjük az alkalmazásunk, lehetőséget ad a szenzorok, hálózati és GPS kapcsolat szimulálására. Rendelkezik APK elemzővel, vizuális felhasználó felület szerkesztővel és intelligens kód szerkesztővel is. Az egyik kedvenc funkcióm a valós idejű profilozó, ami segítségével megtudjuk nézni valós időben, milyen erőforrásokat használ az alkalmazásuk. Ez különösen hasznos, ha megakarunk találni egy memória szivárgást vagy egy olyan részt, ami a kelleténél jobban meríti az akkumulátorunk. Említésre méltó még a flexibilis build rendszere is, a Gradle. Használatával megtehetjük, hogy külön build típusokat hozunk létre a különböző eszközökre. Az *instant run* funkció segítségével egyből tudjuk futtatni a kódban véghez vitt kisebb változtatásokat, anélkül hogy újraindítanánk az Activity -t vagy újra buildelnénk az egész projektet és új APK -t telepítenénk. [2]

1.2. Pycharm Professional Edition

A PyCharm is egy IDE ¹, mint az Android Studio. Dolgozhatunk webes technológiákkal vagy mesterséges intelligenciával, a PyCharm megfelelő választás lehet bármilyen területen programozó számára. A Pycharm mögött is a *Jetbrains* cég áll. Ezt azért fontos megemlíteni, mert már 15 éve azon dolgoznak, hogy a legjobb és leghatékonyabb fejlesztői környezetek állítsanak elő. Véleményem szerint ez sikerült is nekik. Az Android

¹ Integrated Development Environment (integrált fejlesztői környezet)

Studio-n és a Pycharm-on is látszik, hogy minőségi termékek és rengeteget segítenek a fejlesztők mindennapjaiban. Én a *PyCharm Professional Edition*-t használtam, amihez a diákok ingyenesen hozzájuthatnak. Mivel adatbázissal is dolgoznak, ezért a *Community Edition* nem lett volna megfelelő. Nem csak az adatbázis támogatást nyújt, hanem webes keretrendszer támogatást és profilozót is. A távoli fejlesztés funkció is rendkívül praktikus. A fejlesztés közben egyszerűen tudtam feltölteni a szerverre a változtatásaimat. A verzió kezelőknek is egyesített felületet nyújt, amivel jelentős időt spórolhatunk meg. Ez a lehetőség mindkettő fejlesztői környezetben elérhető.[8]

1.3. Postman

Jelenleg a Postman a legnépszerűbb API² tesztelésben használt eszköz. A Postman kollekciók futtatható leírásai egy API-nak és sarok kövei a Postman beépített eszközeinek. Ezeknek a beépített eszközöknek köszönhetően futtathatunk hálózati kéréseket, teszteket, debuggolhatunk és csinálhatunk mock szervereket is. Ráadásul automatizáltan futtathatjuk a teszteket és egyszerűen elkészíthetjük és publikálhatjuk az API dokumentációját. Én csak dokumentáció készítésre és a végpontok tesztelésére használtam. Ettől természetesen sokkal több lehetőség rejlik benne. A 1.1 képen látható egy kérés, ami tartalmaz egy *Authorization Header*-t. Attól függően, hogy helyes-e a felhasználó név és jelszó páros a szerver visszaad egy választ JSON formátumban, amit a kép alján láthatunk.



1.1. ábra. Egy GET kérés és válasz a Postman alkalmazásban.

² Application Programming Interface

2. fejezet

Platformok

2.1. A szerver kiválasztása és felépítése

Olyan szerverre volt szükségem, ami nem túl költséges, de mégis megfelelően testreszabható és gyors tárhelyet biztosít. A választásom a Digital Ocean felhő szolgáltatására esett. Az oldal felületén lehetőségünk van több, úgynevezett *droplet*-et létrehozni, amik nem mások mint virtuális szerverek. Megadhatjuk milyen disztribúciót szeretnénk telepíteni, jelen esetben én az Ubuntu Linux 18.10-es verzióját telepítettem.

The screenshot shows the Digital Ocean admin interface for a project named 'InfoSec Adventures'. The 'Resources' tab is active, displaying a list of 'DROPLETS (1)'. A single droplet named 'reversedroid' is shown with the following details:

Image	Size	Region	IPv4	IPv6	Private IP
Ubuntu 18.10 x64	1 vCPUs 1GB / 25GB Disk (\$5/mo) Resize	FRA1	207.154.198.244	Enable	Enable

Below the droplets, the 'DOMAINS (1)' section shows a domain 'reversedroid.infosecadventures.com' with '1 A / 3 NS / 1 SOA' records.

2.1. ábra. Droplet a Digital Ocean admin felületén.

A projecthez készítettem egy subdomain-t és telepítés után a droplet IP címét hozzárendeltem ehhez a subdomain-hez. Ezzel biztosítottam, hogy domain név alapján is elérhető legyen a szerver. Ez a 2.2 képen jól látható.

A kész projektben nem ezt a folyamatot választottam, hanem a Digital Ocean által nyújtott „one-click apps” menüben egyszerűen kiválasztottam a Docker alkalmazást és

Type	Host	Value	TTL	
A Record	@	185.199.108.153	Automatic	
A Record	@	185.199.109.153	Automatic	
A Record	@	185.199.110.153	Automatic	
A Record	link	52.72.49.79	Automatic	
A Record	reversedroid	207.154.198.244	Automatic	

2.2. ábra. DNS rekordok a domain beállításában.

az elkészült képfájlt ezen futtattam. Így automatizálva a szerver telepítésének folyamatát és megspórolva magának a Docker-nek a telepítését és konfigurálását. Erről még a Szerveren használt technológiák fejezet Docker alfejezetében bővebben írok.

2.2. Mobil platform választása

A mobilos operációs rendszerek közül az Androidot választottam. Bevallom őszintén, nem volt nehéz a döntés. Android platform rengeteg olyan lehetőséget biztosít, amivel a többi platform nem szállhat versenybe. Itt gondolok az egyszeri és nem megújuló fizetésre a fejlesztői fiókért, valamint az iOS-el ellentétben a fejlesztői környezete elérhető mind a három fő operációs rendszerre (Linux, macOS, Windows). Számomra ezek elég nyomós érvek voltak, ezért döntöttem úgy, hogy Android platformra fog először elkészülni a program. A Windows Phone a Microsoft cégnek volt egy próbálkozása, ami végül kudarcba fulladt, ezért ez az opció nem jöhetett szóba.

A többi mobilos operációs rendszerrel ellentétben az Android nyílt forráskódú és a piac jelentős részét uralja. Engem különösen megfogott az általa nyújtott szabadság és testre szabhatóság. Az iOS ezzel ellentétben arról híres, hogy egyszerű és megbízható a használata. Viszont jelen vannak olyan megkötések, amik mind a végfelhasználókat és mind a fejlesztőket limitálják. Gondolok itt a minimális testre szabhatóságra és a nagy részt zárt forráskódra. Itt most nyilván nem szeretném részletezni, hogy melyik

operációs rendszer a jobb vagy éppen rosszabb, mert mindegyik rendszernek megvan az előnye, illetve a hátránya. Inkább csak a személyem érveimet és tapasztalataimat sorakoztatom fel, amik alapján platformot választottam.

Fontos megemlíteni, hogy az Android rendszer nem csak mobil telefonok terjedt el. Jelen van az okos televíziókban (Android TV), autókban (Android Auto), okos órákban (Wear OS) és IoT¹-ben is (Android Things). Ezek az Android által úgymond eredmények annak is köszönhetőek, hogy a Google felvásárolta az Android céget és azóta ők tartják karban.

Természetesen nem csak jó tulajdonságokkal rendelkezik, hanem bizony van néhány hátránya is. Ide tartozik például a gyártóktól függő frissítések. Tegyük fel, hogy új biztonsági rést fedeztek fel az Android operációs rendszerben. A Google általában ezekre meglehetősen gyorsan reagál és néhány napon belül frissítést ad ki az eszközeire (Nexus, Pixel). Azoknak a gyártóknak akiknek saját testre szabott rendszerük van, jóval tovább tart orvosolni a hibát. Ez az időtartam a mai napig hónapokban mérhető, de persze ez függ az adott cégtől és a hiba súlyosságától.

Számomra ezek voltak a legnyomósabb érvek a rendszer kiválasztásában. A mai napig úgy gondolom, hogy ebben a platformban van a legnagyobb potenciál a fejlesztők és felhasználók számára egyaránt.

¹ Internet of Things

3. fejezet

Felhasznált technológiák

3.1. Verzió kezelés

Egy verzió kezelő rendszer képes kezelni egy fájl vagy akár több fájl módosításait olyan módon, hogy lehetőségünk legyen időben „visszamenni” és megnézni egy fájl bizonyos verzióját. A Linux kernel forráskódja óriási méretű és a Git verzió kezelőt használják a fejlesztéshez. Ez azért érdekes, mert nagyon sok ember dolgozik egy óriási kódbázissal és a Git mégis képes hatékonyan kezelni a változásokat. A alábbi listában látható, hogy miért bíznak meg benne egy ilyen nehéz feladat esetében és hogyan teljesíti a Git minden elvárásukat:

- Atomosság
- Teljesítmény
- Biztonság

Az atomosság biztosítja, hogy az adatok ne vesszenek el és ne történjen verzió eltérés részlegesen befejezett műveletek miatt. A gyorsasága mellett nem használ fel jelentős mennyiségű tárhelyet, ellentétben a többi verzió kezelő rendszerrel. Ha Git-et használunk biztosra mehetünk, hogy senki sem módosítja a fájlok tartalmát. Ez a SHA-1 kivonatolásnak köszönhető.[5]

A fentiek fényében nyilvánvaló, hogy a Git mellett döntöttem, ami széles körben elterjedt a szoftver fejlesztők között. A Git egy ingyenes és nyílt-forráskódú elosztott verzió kezelő rendszer. Úgy készült, hogy gyorsan és hatékonyan tudjon kezelni kis és nagy projekteket is egyaránt. Már a projekt kezdetekor készítettem egy privát Github repository-t, hogy nyomon tudjam követni a változtatásaimat és esetleges hiba esetén visszaállítani egy korábbi verzióra.

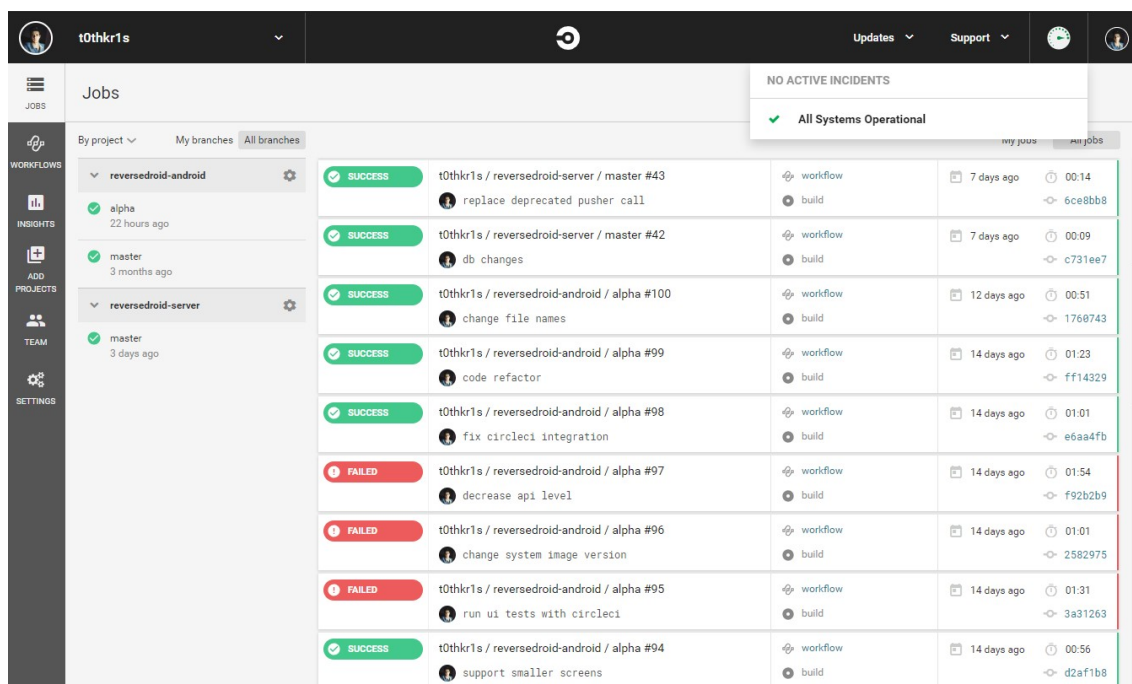
A Github nem összetévesztendő a Git-el, mert a Git a forráskód változtatásainak kezelésére szolgál (lokálisan), a Github pedig egy tárhelyet nyújt a verzió kezelt könyvtárak és fájlok tárolására. A projekt fejlesztése alatt több gépről dolgoztam és Github

a segítségével biztosítani tudtam, hogy mindenhol elérjen a projektek legfrissebb változtatásait. Lényegében egy központi szerverként szolgált számomra.

3.2. Folyamatos integrálás

A folyamatos integrálás egy szoftver fejlesztési gyakorlat, ahol a csapat tagjai sűrűn integrálják a munkájukat általában napi rendszerességgel. Ez naponta több integrációhoz vezet. Pontosabban megfogalmazva a folyamatos integrálás egy extrém programozási gyakorlat. A folyamatos integrálás arról szól, hogy ha egy feladat elkészült akkor azt egyből beintegráljuk a rendszerbe. Minden integráció hitelesítve van egy automatikus build rendszer által (egység tesztekkel együtt) annak érdekében, hogy minél hamarabb észrevegyük az integrációs hibákat. A beintegrálás után természetesen minden egység tesztnek sikeresen le kell futnia. Sok csapat úgy gondolja, hogy ez a megközelítés jelentősen kevesebb integrációs problémához vezet és meggyorsítja a fejlesztés menetét.[3]

Több nagy cég is a CircleCi szolgáltatását használja a folyamatos integráláshoz, ilyen például a *Facebook*, *Spotify* és a *GoPro*. A CircleCi összeköthető a Github-al, így kényelmesen tudjuk csatolni az ott tárolt projektjeinket. A konfigurációs fájl létrehozása pedig végtelenül egyszerű, ha követjük a dokumentációt. A 3.1 képen látható, hogy minden egyes változtatáskor lefutnak a tesztek. Ezek a tesztek minden alkalommal egy tiszta konténerben vagy virtuális gépen futnak. Jelen esetben az Android program egy Docker konténerben fut, aminek a neve *circleci/android:api-28-alpha*. Az eredményről mindig értesítést kapunk, így egyből tudhatjuk azt is, ha egy build nem volt sikeres.



Jobs		NO ACTIVE INCIDENTS	
		All Systems Operational	
By project	My branches	All branches	
reversedroid-android	alpha	22 hours ago	
reversedroid-server	master	3 months ago	
reversedroid-server	master	3 days ago	
SUCCESS	t0thkr1s / reversedroid-server / master #43	replace deprecated pusher call	workflow build 7 days ago 00:14 c6e8bb8
SUCCESS	t0thkr1s / reversedroid-server / master #42	db changes	workflow build 7 days ago 00:09 c731ee7
SUCCESS	t0thkr1s / reversedroid-android / alpha #100	change file names	workflow build 12 days ago 00:51 1760743
SUCCESS	t0thkr1s / reversedroid-android / alpha #99	code refactor	workflow build 14 days ago 01:23 ff14329
SUCCESS	t0thkr1s / reversedroid-android / alpha #98	fix circleci integration	workflow build 14 days ago 01:01 e6aa4fb
FAILED	t0thkr1s / reversedroid-android / alpha #97	decrease api level	workflow build 14 days ago 01:54 f92b2b9
FAILED	t0thkr1s / reversedroid-android / alpha #96	change system image version	workflow build 14 days ago 01:01 2582975
FAILED	t0thkr1s / reversedroid-android / alpha #95	run ui tests with circleci	workflow build 14 days ago 01:31 3a31263
SUCCESS	t0thkr1s / reversedroid-android / alpha #94	support smaller screens	workflow build 14 days ago 00:56 d2af1b8

3.1. ábra. Project buildek követése a CircleCi felületén.

3.3. Szerveren használt technológiák

3.3.1. Flask

A szervert a Flask webes mikro keretrendszer felhasználásával készítettem el. Attól, hogy mikro keretrendszer még nem jelenti azt, hogy kevesebb tud mit a többi keretrendszer. Erős alapot nyújt az alapvető szolgáltatásokkal, miközben a kiegészítők nyújtják a többit. Azzal a lehetőséggel, hogy kitudjuk választani magunknak a kiegészítő csomagokat, képesek vagyunk egy olyan programok felépíteni, ami pontosan azt tartalmazza amire szükségünk van és nem tartalmaz semmi fölöslegeset.

A Flask nem támogatja natívan az adatbázis elérést, web formok validálását, felhasználói autentikációt és egyéb magas szintű feladatokat. Ezek és más egyéb kulcs szolgáltatások, amikre egy webes applikációnak szüksége van kiegészítőkön keresztül elérhető. Fejlesztőként lehetőségünk van egyesével kiválogatni vagy éppen magunktól megírni azokat a kiegészítőket, amik az aktuális projekthez kellenek. [6]

Úgy gondolom, hogy sokkal hatényobban programot lehet írni, ha csak azt építjük bele a szoftverbe, amire tényleg szükségünk van. Nekem csak kettő kiegészítőre volt szükségem, mivel a többi funkcionalitást alapból nyújtja a keretrendszer.

Flask-Testing

Az egyik ilyen a „Flask-Testing” csomag, amire az egység tesztek miatt volt szükségem. Segítségével rendkívül egyszerűen és hatékonyan tudjuk tesztelni az alkalmazás található végpontokat.

Flask-Bcrypt

Mivel alapból a Flask keretrendszer nem biztosít titkosítás, keresnem kellett egy külső megoldást. A másik ilyen csomag amit felhasználtam, a „Flask-Bcrypt” volt. Nagyon rossz gyakorlat, ha a jelszavakat titkosítás nélkül tároljuk az adatbázisban. Ennek elkerülése érdekében választottam a bcrypt algoritmust szolgáltató csomagot, ami kifejezetten erre a célra készült.

3.3.2. SQLite

Az SQLite egy nyílt forráskódú szoftver csomag, ami relációs adatbázis kezelő rendszert biztosít. Relációs adatbázis rendszereket arra használjuk, hogy a felhasználó által meghatározott rekordokat nagy méretű táblákban tároljunk. Az adat tárolás és kezelés mellett, az adatbázis motor komplex lekérdezéseket dolgoz fel. Néhány meghatározó funkciója az SQLite adatbázisnak:

1. **Szerver mentes.** Az SQLite-nak nincs szüksége külön szerver folyamatra vagy rendszerre a működéshez. Az SQLite könyvtár közvetlenül kezeli a tárhely fájlokat.
2. **Nulla konfiguráció.** Ha nincs szerver, nincs konfiguráció sem. Úgy csinálhatunk SQLite adatbázist, mintha fájlt hoznánk létre.
3. **Platform független.** Az egész adatbázis példány egy darab platform független fájl, ami semmilyen adminisztrációt nem igényel.
4. **Önálló.** Egy darab könyvtár tartalmazza az egész adatbázis rendszert, ami közvetlenül az alkalmazásba integrálódik.
5. **Tranzakciós.** Lehetővé teszi a biztonságos hozzáférést más szálakból vagy folyamatokból.
6. **Kifejezetten megbízható.** A SQLite fejlesztői csapata nagyon komolyan veszi a forrás kód tesztelését.

Összességében az SQLite egy funkcionális és flexibilis relációs adatbázis környezet, ami csak minimális erőforrást igényel. [7] Nem mellesleg ez a legtöbbet használt adatbázis motor a világon. Számtalan alkalmazás használja és Android platformon is ez az alapértelmezett adatbázis. Ha többet szeretnénk megtudni róla, akkor azt megtehetjük a <https://www.sqlite.org/index.html> oldalon.

3.3.3. Pusher Beams (Python Server SDK)

A szerverről való értesítés küldéshez a Pusher Beams SDK¹-jét használtam. A Beams SDK lehetővé teszi, hogy egyszerűen küldjünk push értesítést „érdeklődési” körök alapján és platformtól függetlenül. Ingyenesen és korlátlanul küldhetjük ezeket az értesítéseket. Erről bővebben olvashatunk a <https://docs.pusher.com/beams> oldalon. Ha kimondottan a szerver oldali python dokumentációt szeretnénk elolvasni, azt megtehetjük itt: <https://docs.pusher.com/beams/reference/server-sdk-python>. A szerver és kliens is oldal implementációja is nagyon egyszerű és jól dokumentált, de ha mégis problémánk támadna az online ügyfélszolgálatuk is végtelenül segítőkész.

Bevallom, amikor implementáltam a szerverről való üzenetküldést nem ment minden simán. Az volt a probléma, hogy csak azt az értesítést kaptam meg amelyik nem tartalmazott plussz adatot az értesítés címén és leírásán kívül. Fel kellett keresnem őket, mert hiába követtem a dokumentációkat nem értettem a hiba okát. Az üzenetemre kifejezetten gyorsan (egy napon belül) válaszoltak és kérték, hogy küldjek több

¹ Software Development Kit

információt. Hamar kiderült, hogy a problémát az FCM² okozza, ami nem engedi, hogy egyszerre küldjünk értesítést és adatot. Itt kiegészítésként fontos megemlíteni, hogy a Pusher a Firebase Cloud Messaging által küldi az értesítéseket. Miután rávilágítottak a hiba okára, egyből megoldást ajánlottak és frissítették a dokumentációjukat. Úgy sikerült kikerülni ezt a limitációt, hogy kettő darab értesítést kell küldeni. Az első csak magát az értesítést tartalmazza, a második pedig csak az adatok küldéséért lesz felelős. Természetesen a második értesítésnek nem lesz vizális reprezentációja a kliens oldalon.

3.3.4. Docker

A Docker az egy nyílt forráskódú motor, ami automatizálja az alkalmazások üzembe helyezését konténereken belül. Úgy lett tervezve, hogy egy helyi súlyú és gyors környezetet nyújtson, amiben hatékonyan tudjuk futtatni a kódunk. Célja még, hogy hordozhatóvá és könnyen buildelhetővé tegye az alkalmazásunk. Ösztönzi a szolgáltatás orientált architektúrát és azt ajánlja, hogy minden konténerben csak egy alkalmazás fusson.

Képfájlok

Konténerek

A szerverhez készítettem egy Dockerfile-t és csatoltam a projekt Github-os repository-ját. Ezzel elérve, hogy minden egyes változtatásnál a Docker Hub újra buildelje a képfájlt.

3.3.5. jd-cmd

Szükségem volt egy parancssorból használható Java Decompiler-re is.

<https://github.com/kwart/jd-cmd>

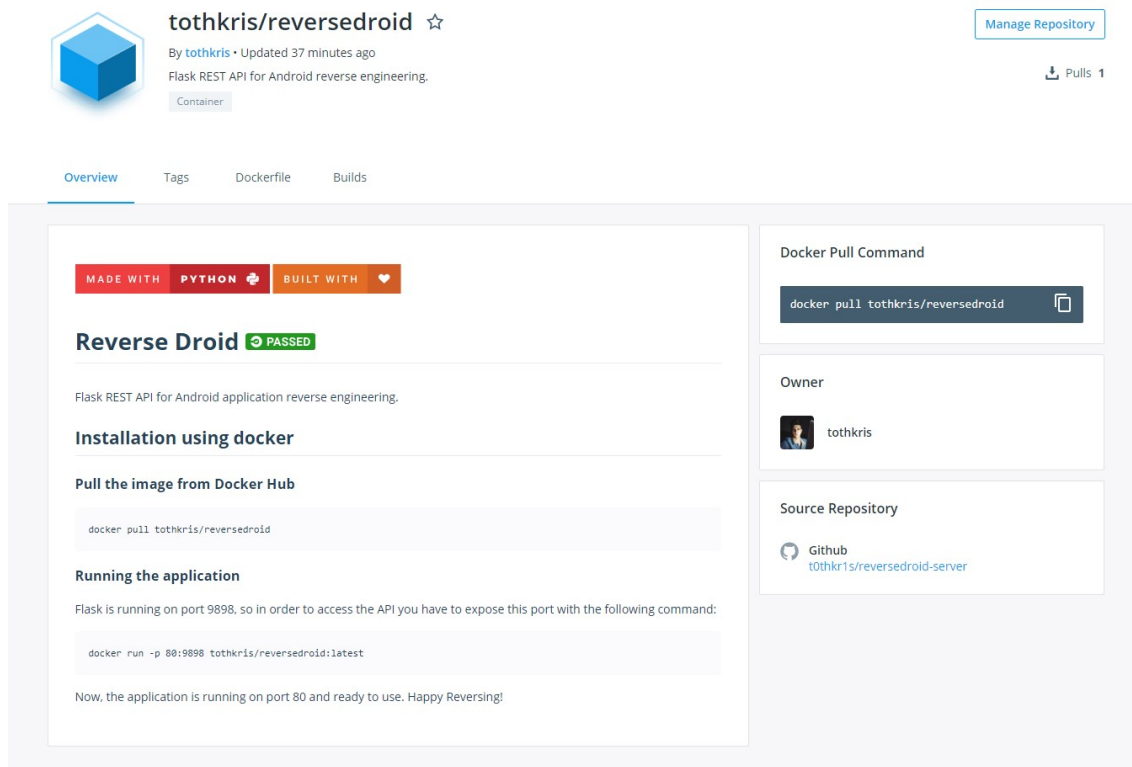
3.3.6. Apktool

Az Apktool egy olyan eszköz, aminek a segítségével vissza tudjuk fejteni a harmadik féltől származó, zárt forrású, bináris Android alkalmazásokat. Majdnem eredeti az állapotukba tudja dekódolni a forrásokat és újra buildeni őket néhány módosítással.

Funkciók:

<https://github.com/iBotPeaches/Apktool>

² Firebase Cloud Messaging



3.2. ábra. Az applikáció Docker Hub-on is elérhető.

3.3.7. dex2jar

Android .dex és .class fájlokkal való dolgozáskor kulcs szerepet játszott a *dex2jar*. Jelen esetben nem csak egy programról beszélünk, mert valójában több eszközt foglal magába. Az Android telepítő fájl kitömörítése után, az alkalmazás forráskódja egy *classes.dex* fájlban található meg. Ez a fájl byte kódot tartalmaz az ART számára és ezt kellett átalakítani .jar formátumba, amivel már a decompiler dolgozni tud.

<https://bitbucket.org/pxb1988/dex2jar>

3.3.8. JSON

A JSON³ egy platformok közötti adatátvitelre szolgáló formátum. Az adatátviteli formátum egy olyan szöveges formátum, amit különböző platformok közötti adat cserére használnak. Egy másik széles körben használt adatátviteli formátum az XML⁴. Ezek biztosítják a nagyon eltérő rendszerek közötti adatváltást. A JSON egy olyan formátum, amin megegyeztek ezek a rendszerek adat kommunikáció céljából. [9] Kettő struktúrára épül:

1. **Kulcs-érték párok.** Ez a koncepció nagyon elterjedt a számítástechnikában és több programozási nyelvben van megfelelője.

³ JavaScript Object Notation

⁴ Extensible Markup Language

2. **Listába rendezett értékek.** A legtöbb nyelvben megfelel a tömböknek, vektoroknak és listának.

Ezek olyan univerzális adatszerkezetek, amiket gyakorlatilag minden programozási nyelv támogat ilyen vagy olyan formában. Ésszerűnek tűnik tehát, hogy az az adatformátum, amelyet programozási nyelvek kommunikációjához kívánunk használni, szintén ezekre a szerkezetekre épüljön.[10]

```
1 {  
2   "result": "APK_uploaded_successfully_and_reverse_engineering_started!"  
3 }
```

3.1. Listing. Egy nagyon egyszerű példa a szerverről érkező JSON válaszra.

Emberek számára is könnyen olvasható és írható, ahogy ez a 3.1 példán is látszik. A szakdolgozatomban is fontos szerepet tölt be, ugyanis a klien-szerver kommunikáció teljes egészében erre alapul. Véleményem szerint sokkal átláthatóbb és egyszerűbb, mint például az XML társa.

3.4. Androidon használt technológiák

3.4.1. AndroidX

Az AndroidX egy nyílt forráskódú projekt, amit az Android fejlesztői csapata használ library-k fejlesztéshez, teszteléséhez és kiadásához a Jetpack-en belül. Az eredeti support library-hez képest az AndroidX egy jelentős fejlődés. Ahogy a support library-t is, az AndroidX-et is az Android operációs rendszertől függetlenül tudjuk használni és biztosítja a visszafelé kompatibilitást. Az AndroidX teljesen felváltja a support library-t azáltal, hogy azonos funkciókat biztosít és új könyvtárakat. Ezen felül az AndroidX a következő funkciókat tartalmazza:

1. Minden csomag egy konzisztens névtérben van, ami „androidx”-el kezdődik.
2. A support library-vel ellentétben az AndroidX csomagok külön vannak karbantartva és frissítve.
3. Az összes új support library fejlesztés az AndroidX könyvtárban fog történni. Ez magába foglalja az eredeti support library fenntartását és az új Jetpack komponensek bevezetését.

3.4.2. OkHttp

A modern alkalmazások a HTTP ⁵ protokollal dolgoznak. Segítségével adatokat tudunk küldeni és fogadni. Ha hatékonyan használjuk a HTTP protokolt, akkor gyorsabban tudjuk az adatokat betölteni és sávszélességet spórolhatunk meg.

Az OkHttp egy HTTP kliens, ami alapértelmezetten hatékony. Néhány tulajdonsága:

1. Az átlátszó GZIP csökkenti a letöltés méretét.
2. A válaszokat cache-ben tárolja, ezért ismétlődő kéréseknél elkerülhető a hálózat használata.

Akkor sem omlik össze, ha problémás a hálózat, valamint csendben helyreáll a gyakori kapcsolati problémák esetében is. Ha a szolgáltatásunknak több IP címe lenne, akkor az alternatív IP címekkel próbálkozna kapcsolati hiba esetén. Ez szükséges IPv4+IPv6 használatakor és olyan szolgáltatások esetében, amik redundáns adat központokban vannak. Támogatja a modern TLS funkciókat, ami a biztonságos adatátvitelért felelős.

Az OkHttp használata egyszerű. A kérés/válasz API-ja builder tervezési mintára épült, amit nagyon könnyű használni.

Lehetőséget ad szinkronizált (egyidejű) blokkoló hívásokra és aszinkron hívásokra is „callback”-ek segítségével. A könyvtár támogatja az Android 5.0+ (API szint 21+) verziókat és támogatja a Java 8-at, valamint az attól felfelé lévő verziókat. Hamar kiderült, hogy

3.4.3. Pusher Beams (Java Client SDK)

A Beams megkönnyíti az értesítések küldését iOS és Android eszközökre. Bonyodalommentessé teszi az eszköz tokenek kezelését és az interakciót az Apple és a Google által biztosított üzenetküldő szolgáltatásokkal.

A Pusher nagyon sokoldalú API-val és SDK-kal rendelkezik. Ezek közül a Beam egy fejlesztő barát eszköz, aminek a segítségével értesítéseket küldhetünk. Számos mobil automatizálási eszköz javasolja a promóciós értesítések küldését, amiket nem mindig szeretnek a felhasználók és leiratkoznak.

A Beam-mel egyenesen a programból indíthatjuk az értesítések küldését a valós alkalmazásban történő eseményekre alapozva. Így a felhasználók kevésbé fogják megenni az értesítéseket is törölni esetlegesen az appot. Íme néhány példa a felhasználást illetően:

- Étél kiszállítással kapcsolatos folyamatos értesítések

⁵ HyperText Transfer Protocol

- Játékokban pontok alapján való értesítés küldés
- Tranzakciós értesítések

3.4.4. Firebase Messaging

3.4.5. Room

A Room egy absztrakciós réteget nyújt az SQLite adatbázishoz, ezzel lehetővé téve az egyszerűbb és hatékonyabb adatbázis elérést. A Room segítségével sokkal egyszerűbben tudtam kezelni az SQLite adatbázist, mert nem kellett adatbázist leíró osztályt és hosszú lekérdezéseket írnom. Ami külön tetszett benne, hogy az SQL utasításokat fordítási időben ellenőrzi. Annotációk segítségével tudjuk összekötni a Java POJO⁶ osztályokat az SQLite adatbázissal.

3.4.6. CodeView

A forrás kód megjelenítését nem lett volna célszerű nulláról felépíteni, ezért inkább kész megoldások után néztem. Kutatásaim során, nem találtam megfelelő natív Android komponenst, amivel kivitelezhető lett volna a forrás kód megjelenítése. Ezt úgy értem, hogy a kijelölést nem lehet megoldani egy egyszerű *TextView* osztállyal. Mindenképpen kellett egy olyan könyvtár, ami megbízható és elegendő funkcionalitást és testreszabhatóságot nyújt. Jó pár könyvtárat végig kellett próbálnom, mire ráakadtam az igazira. Találkoztam olyannal, amelyik nem megfelelően töltötte be a kódot és nem is volt megbízható. Voltak olyanok is, amelyeket nagyon régóta nem voltak karban tartva és elavult kód bázissal rendelkeztek. Találtam aktív fejlesztés alatt lévőket is, de azok többnyire még kiforratlan állapotban voltak és nem rendelkeztek elegendő funkcióval.

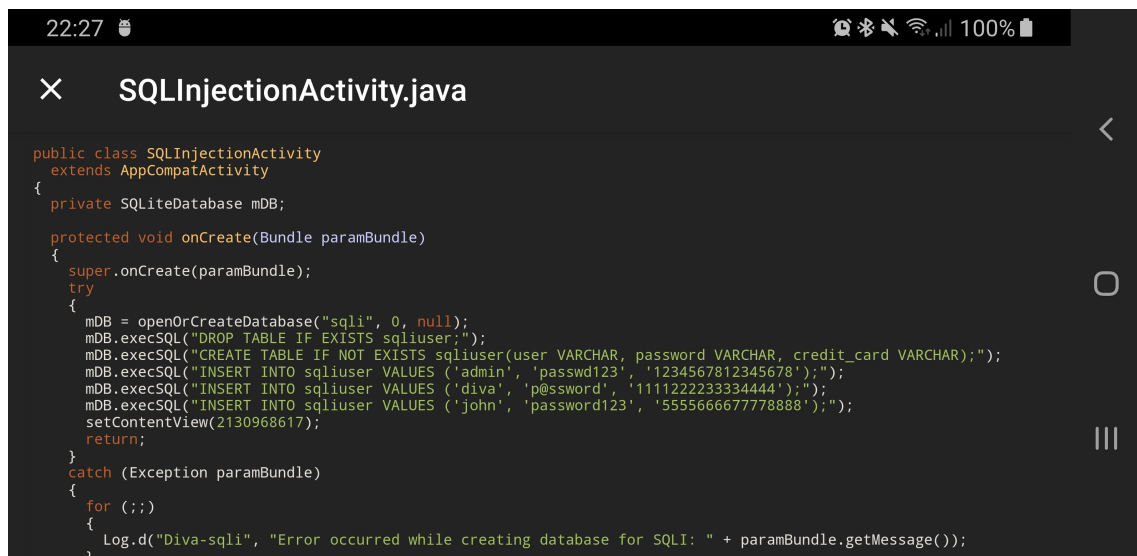
A megvalósítást ezek a könyvtárak, úgy végezték el, hogy lényegében egy *WebView* komponensbe töltötték be a forrás kódot, amit aztán különböző JavaScript keretrendszerek segítségével színezték ki. A választásom egy olyan könyvtárra esett, ami a *highlight.js* keretrendszert használja. Ez biztosít több különböző témát szintaktikai kijelölésre és amit még fontosabbnak tartok, hogy automatikusan felismeri a domináns programozási nyelveket, mint a *Java*, *Python* vagy *Ruby*. Így sokkal kényemesebb a használata, mert nem kellett kiterjesztés alapján megadni az adott nyelvet. Néhány funkció hiányzott ugyan, mint például a két ujjal való nagyítás, kicsinyítés és a kezdő betű méret beállítása. Ezeknek a támogatását sikerült viszonylag egyszerűen megoldani, hiszen a *CodeView* a *WebView* osztályból származik és rendelkezik a megfelelő metódusokkal. A 3.2 kódrészletben a *CodeView* megvalósítása és kiegészítése látható, alatta pedig a 3.3 képen látható a forrás kód megjelenítése az alkalmazásban.

⁶ Plain Old Java Object

A választott könyvtár elérhető: <https://github.com/Thereisnospon/CodeView>

```
1 codeView = view.findViewById(R.id.codeView);
2 codeView.setTheme(CodeViewTheme.RAILSCASTS).fillColor();
3 codeView.getSettings().setBuiltInZoomControls(true);
4 codeView.getSettings().setDisplayZoomControls(false);
5 codeView.getSettings().setTextZoom(50);
6 codeView.setWebViewClient(new WebViewClient() {
7     @Override
8     public void onPageStarted(WebView view, String url, Bitmap favicon) {
9         super.onPageStarted(view, url, favicon);
10        Log.d(Constants.TAG, "onPageStarted:_loading_page");
11    }
12
13    @Override
14    public void onPageFinished(WebView view, String url) {
15        super.onPageFinished(view, url);
16        Log.d(Constants.TAG, "onPageFinished:_page_loaded");
17        loading.setVisibility(View.GONE);
18    }
19 });
```

3.2. Listing. A CodeView könyvtár felhasználása és kiegészítése.



3.3. ábra. A visszafejtett forrás kód megjelenítése szintaktikai kijelöléssel.

3.4.7. Espresso

Az Android Studio rendelkezik jó pár funkcióval, amikről már tettem említést. Amit szándékosan kihagytam, az a UI⁷ tesztek felvétele. Az Espresso Test Recorder funkció

⁷User Interface

által megtehetjük, hogy nem kézzel írjuk a teszteket, hanem felvesszük őket. Feltudjuk venni az interakcióinkat az alkalmazással és ellenőrizni tudjuk az elemeket a felhasználói felületen, valamint biztosítani tudjuk az adott pillant kép helyességét. Az Espresso Test Recorder veszi az elmentett teszt felvételt és automatikusan generál egy hozzátartozó UI tesztet, amit aztán futtatni tudunk az alkalmazásunk tesztelése érdekében.

Espresso Test Recorder az Espresso Testing keretrendszer alapján írja a teszteket, ami egy API az AndroidX Test-ben. Segít megbízható és tömör UI teszteket írni a felhasználói interakcióra alapozva. Állíthatunk elvárásokat és interakciókat anélkül, hogy hozzáférnénk az alkalmazás nézeteihez és activity-jeihez. Ez a struktúra optimalizálja a tesztek futási idejét. [4]

A projektem esetében nem volt ilyen egyszerű a helyzet. Mindenképpen segített, hogy feltudtam venni a teszteket, de vegyük a következő helyzetet. Tegyük fel, hogy a bejelentkezés folyamatára már készen van a teszt. Amikor Espresso-val tesztet veszünk fel, az alkalmazás tiszta állapotról indul. Ez az jelenti, hogy ha bármilyen bejelentkezés utáni interakciót szeretnénk felvenni, akkor a teszt a bejelentkezéssel együtt kezdődik. Az ilyen problémákat manuálisan kell kikerülni. A 3.3 kódrészletben megfigyelhető, hogy egy *@Before* annotációval⁸ ellátott metódusban elmentettem egy teszt felhasználó nevet és jelszót. Ezután pedig egyszerűen egy Intent segítségével elindítottam az Activity-t. Mindez nem volt elegendő ahhoz, hogy sikeresen tovább mehessek ugyanis bejelentkezés után történik a különböző engedélyek ellenőrzése. Az Espresso arra is nyújt megoldást, hogy ezeket az engedély kéréseket automatikusan elfogadjuk a tesztekben a *GrantPermissionRule* osztály segítségével.

```
1 @LargeTest
2 @RunWith( AndroidJUnit4 . class )
3 public class DeleteDataTest {
4
5     @Rule
6     public ActivityTestRule<MainActivity> mActivityTestRule = new
7     ActivityTestRule<>(MainActivity . class );
8
9     @Rule
10    public GrantPermissionRule mGrantPermissionRule =
11    GrantPermissionRule . grant (
12        "android . permission . READ _ EXTERNAL _ STORAGE" ,
13        "android . permission . WRITE _ EXTERNAL _ STORAGE" ) ;
14
15    @Before
16    public void setSharedPref() {
17        SharedPreferencesUtil . saveCredentials ( getInstrumentation () .
```

⁸ Az annotációk a programkód elemeihez rendelhetők (csomagokhoz, típusokhoz, metódusokhoz, attribútumokhoz, konstruktorokhoz, lokális változókhoz), plusz információt hordoznak a Java fordító ill. speciális eszközök számára.[11]

```

17     getTargetContext(), "test", "test");
18     mActivityTestRule.launchActivity(new Intent());
19 }
20
21 @Test
22 public void deleteDataTest() {
23     try {
24         Thread.sleep(5000);
25     } catch (InterruptedException e) {
26         e.printStackTrace();
27     }
28
29     onView(allOf(withId(R.id.delete_data),
30         childAtPosition(
31             childAtPosition(
32                 withId(R.id.action_bar),
33                 1),
34             0),
35         isDisplayed())) .perform(click());
36
37     onView(allOf(withId(android.R.id.button1),
38         childAtPosition(
39             childAtPosition(
40                 withId(R.id.buttonPanel),
41                 0),
42             3))) .perform(scrollTo(), click());
43 }
44 }

```

3.3. Listing. Espresso UI teszt az adatok törléséhez.

3.4.8. Material Design 2.0

Az alkalmazás elkészítésekor próbáltam figyelembe venni a felhasználói interfésszel kapcsolatban támasztott ki nem mondott elvárásokat. Korábbi Play Store-ban publikált alkalmazásaim alapján mondhatom, hogy a felhasználónak az app megjelenése legalább olyan fontos, mint a funkcionalitása. A Google már korábban, az Android 5.0 (API verzió 21) verzióval hozta be az akkoriban még újnak számító Material Design-t és teljesen megreformálta az Android platform felületét. Sok embernek tetszettek az élénk színek és a vetett árnyakok, amik meghatározó részei voltak a komponenseknek. Persze, ez nem volt tökéletes. A nevéből is ered, hogy az anyagokból kiindulva és azok egymásra pakolásával született meg a dizájn. Kicsit pontosabban fogalmazva a Material Design irányelveket foglal össze, amiket nem fontos követni, de ajánlott. A Material Design 2

nem hozott hatalmas eltéréseket elődjéhez képest, inkább csak letisztultabb lett, ami szimplán jobb vizuális élményt nyújt. Az Android platformot tekintve új komponensek érkeztek, ezek közé tartozik a *BottomAppBar* és a *Chip*.

4. fejezet

Teszteléshez felhasznált eszközök és források

4.1. Sérülékeny Android alkalmazások

A teszteléshez keresnem kellett olyan sérülékeny alkalmazásokat, amelyeken jól lehet demonstrálni a visszafejtést. Minden alkalmazás, amit itt megemlítek nyílt forrás kódú és kimondottan erre a célra készítették őket. Ez azért is jó, mert a visszafejtett kódot össze lehet hasonlítani az eredetivel és megnézni mennyire volt hatékony a visszafejtési folyamat. A következő lista tartalmazza a teszteléshez felhasznált szándékosan sérülékeny alkalmazásokat.

- Diva
- Sieve
- Pivaa
- Frida

5. fejezet

Megvalósított funkciók

5.1. Regisztráció

A szolgáltatást nem akartam mindenki számára elérhetővé tenni, csak a regisztrált felhasználóknak.

5.2. Bejelentkezés

Természetesen regisztrálás után a felhasználónak be kell jelentkeznie, hogy hozzáférhessen azokhoz a végpontokhoz, amik bejelentkezéshez vannak kötve.

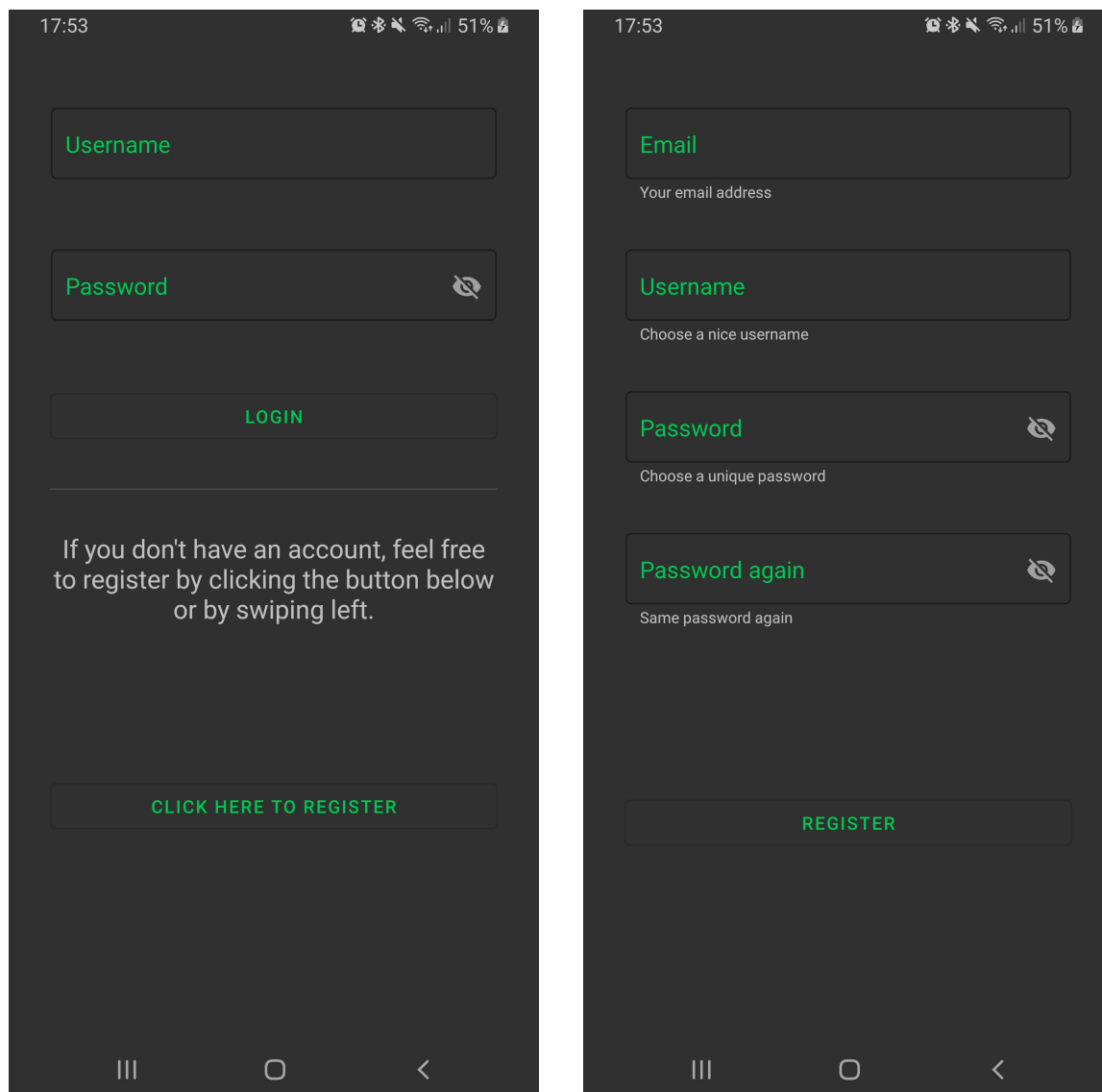
5.3. Kijelentkezés

5.4. Adatok törlése

A kliens oldalon elég sok adat jelenik meg. Ilyen például a feltöltések listája, értesítések és természetesen a letöltött fájlok is ide tartoznak. Az adatok törlése funkcióval biztosítottam, hogy a felhasználónak lehetősége legyen törölni minden adatot és előzményt. Jól jöhet ez a funkció akkor is ha a telefon esetleg nem rendelkezik elég tárhellyel vagy egyszerűen csak helyet szeretnénk felszabadítani.

5.5. Fájl feltöltés

Az alkalmazás egy alapvető funkciója, hogy fel tudjuk tölteni az APK fájlokat. Ezt a funkciót próbáltam a legkézenfekvőbb helyen elhelyezni, mert ezzel indul az egész folyamat és magától értetődőnek kell lennie.



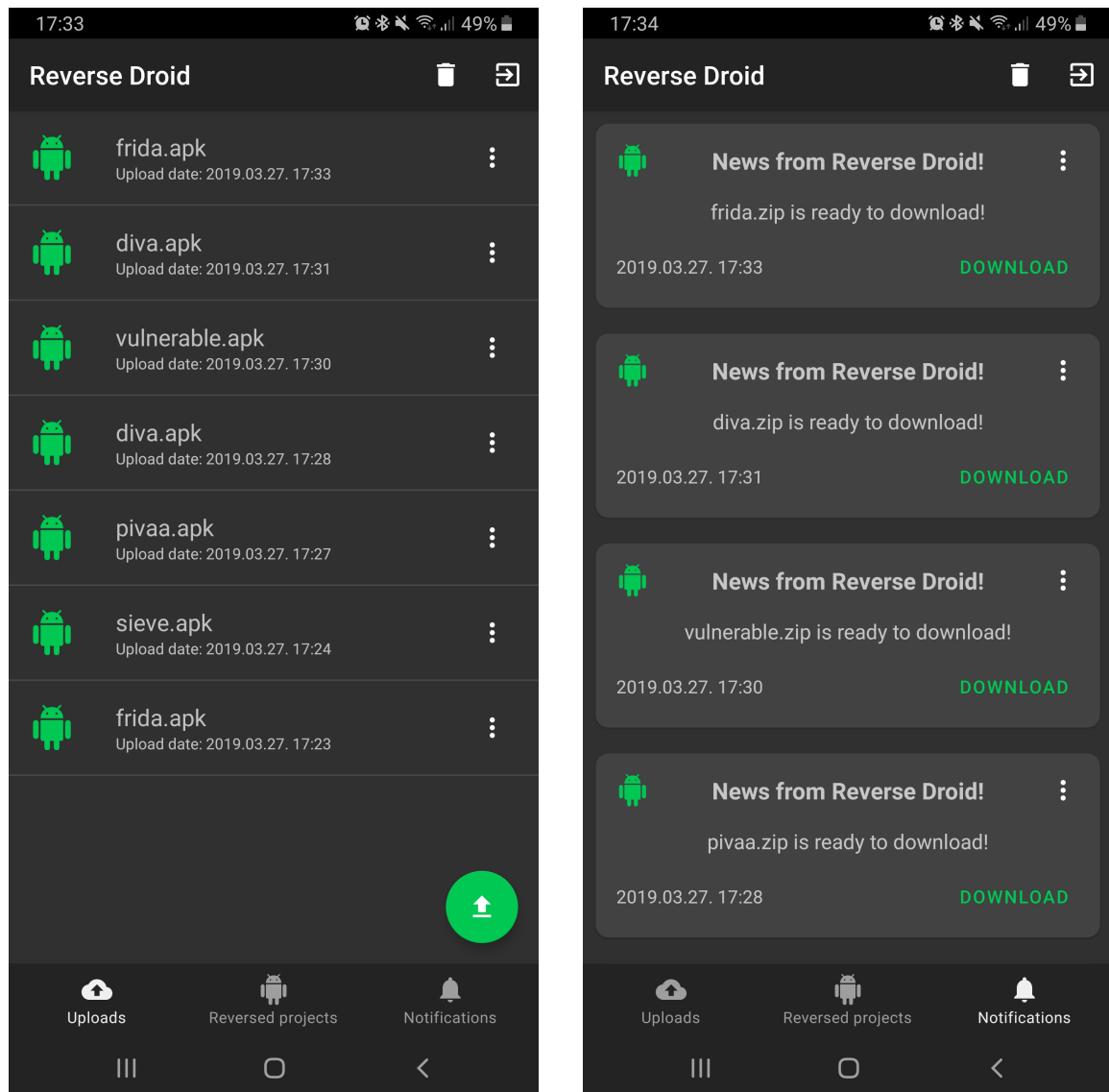
5.1. ábra. A bejelentkezési és regisztrációs felület megvalósítása.

5.6. Fájl letöltés

A fájl letöltés is egy roppant fontos funkció, ugyanis csak így jut el a felhasználóhoz az eredmény. A megvalósítását hozzákötöttem az értesítésekhez, mert a kliens abban kapja vissza a letöltendő fájl nevét.

5.7. Navigáció a fájlrendszerben

A letöltött és kitömörített projektek az alkalmazás mappájában kerülnek. Ezzel alapvetően nincs is semmi probléma, csak ha megszeretnénk nézni a fájlokat, akkor el kellene hagynunk az alkalmazást. Ez pedig rossz felhasználói élményhez vezetett volna. Ennek megoldására megvalósítottam egy nagyon egyszerű fájl rendszer navigációt, de ezt csak az alkalmazás mappájában tettem lehetővé. Így kitömörítés után egyszerűen és gyorsan



5.2. ábra. A feltöltött APK fájlok és értesítések felülete.

elérhetővé válik a projekt a felhasználó számára. Részleteit tekintve csak a fájl nevét, módosítás dátumát és a fájl méretét jelenítettem meg.

5.8. Értesítések

Az értesítések küldése és fogadása szintén egy kulcs fontosságú része az alkalmazásnak. A fájlok letöltése és kitömörítése mérettől, valamint hálózati kapcsolattól függően időt vesz igénybe.

A szerveren történő visszafeltés az a folyamat, ami jelentős időtartamot igényel.

6. fejezet

Továbbfejlesztési lehetőségek

Úgy gondolom, hogy sokkal nagyobb piaci érték rejlik ebben az alkalmazásban, mint amennyit egyedül sikerült megvalósítanom. A jövőben is szeretném folytatni a fejlesztést és esetlegesen nyílt forráskódúvá tenni a projekteket, hogy mások is közre tudjanak működni a fejlesztésben.

Szeretnék több figyelmet fordítani a biztonságra és hatékonyságra. Gondolok itt a biztonságos kommunikációra TLS-es keresztül és a harmadik féltől származó könyvtárak csökkentésére. Azért lenne érdemes minimalizálni a harmadik féltől származó könyvtárakat, mert nem mindig tudjuk milyen kódot tartalmaznak és mennyire tartják karban a kód bázist.

Jelenleg csak a forráskódok megjelentését támogatja az alkalmazás, de jó lenne ha különböző fájl típusokat is megtudna jeleníteni. Például a képek vagy adatbázisok megtekintése is kritikus lehet egy Android alkalmazás elemzésekor. A kód visszafejtése végén egy összegző report is hasznos lehetne a felhasználó számára, ami tartalmazná a feldolgozott fájlok számát és egy gyors áttekintést nyújtana az adott alkalmazással kapcsolatban.

Egy forrás kód elemző integrálása is jelentős előnnyel járhat a többi alkalmazással szemben. Hasonlóan a Google Play Protect-hez, jelezhetnénk a felhasználó számára, ha a feltöltött *apk* malware. Találkoztam több webes *apk* analízálóval, ahol csak az Android komponenseket emelték ki, de az elemzést már a felhasználóra bízták. Nyilván nem lenne célszerű mindent egy algoritmusra bízni, de mindenesetre könnyebbé lehet látok egy átfogó analízisben, ami esetlegesen mestersége intelligenciára alapul.

7. fejezet

Tapasztalatok

Úgy érzem elértem a céloom ezzel a projekttel és sokat sikerült tanulnom az elkészítése alatt. Új technológiákat ismertem meg és használtam. Nem állítom, hogy hibamentes és minden működik, hiszen ez mégis csak egy szoftver, amit folyamatosan karban kell tartani és fejleszteni. A fejlesztés minden fázisában találtam valami kihívást, ami segítette a fejlődésemet és arra ösztönzött, hogy jobban megismerjem az adott technológiát.

Természetesen nem volt minden magától értetődő és jó pár nehézséggel is találkoztam, amiket már korábban meg is említettem. Számomra, ha valami nem sikerült az mindig ösztönzőleg hatott és motivált a tanulásban. Sikerült az idegen technológiák iránt érzett kíváncsiságom is kielégíteni. A reverse engineering világába is betekintést nyertem, ami különösen érdekelt engem.

A fejlesztésnél csak egyetlen kellemetlen dologgal találkoztam. Szerintem sok fejlesztő egyet ért ha azt mondom, hogy a hiányos vagy éppen félre vezető dokumentáció a legnagyobb ellensége. Szerencsére nem sokszor futottam bele, de amikor igen, akkor pár napig álltam a fejlesztéssel. Végül az oldalon egy rendkívül türelmes és segítőkész fiatalember segített a helyes irányba.

Még a problémáival együtt is úgy gondolom, hogy sikerült egy olyan szoftvert készítenem, ami egyedi és megállja a helyét a piacon.

Irodalomjegyzék

- [1] ONLINE: Number of mobile phone users worldwide from 2015 to 2020, <https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide>
- [2] ONLINE: Everything you need to build on Android <https://developer.android.com/studio/features.html>
- [3] FOWLER M, FOEMMEL M. Continuous integration. Thought-Works 2006 May 1 http://www.dccia.ua.es/dccia/inf/asignaturas/MADS/2013-14/lecturas/10_Fowler_Continuous_Integration.pdf
- [4] ONLINE: Create UI tests with Espresso Test Recorder <https://developer.android.com/studio/test/espresso-test-recorder>
- [5] SOMASUNDARAM R. Git: Version control for everyone. Packt Publishing Ltd; 2013.
- [6] GRINBERG M. Flask web development: developing web applications with python. " O'Reilly Media, Inc."; 2018 Mar 5.
- [7] KREIBICH J. Using SQLite. " O'Reilly Media, Inc."; 2010 Aug 17.
- [8] ONLINE: PyCharm Features <https://www.jetbrains.com/pycharm/features/>
- [9] BASSETT L. Introduction to JavaScript Object Notation: A to-the-point Guide to JSON. " O'Reilly Media, Inc."; 2015 Aug 5.
- [10] CROCKFORD, DOUGLAS Introducing JSON. json.org, 2009 May 28.
- [11] ONLINE: Java annotációk https://hu.wikipedia.org/wiki/Java_annot%C3%A1ci%C3%B3k