VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Excel@FIT 2024

Platforma pre automatizované vytváranie odtlačkov mobilných aplikácií

O projekte

Vytvorený systém umožňuje automatizované vytváranie odtlačkov mobilných aplikácií, zložených z odtlačkov TLS a prípadne hodnôt SNI. Systém je dostupný prostredníctvom webového rozrania, ako aj rozhrania API. Cieľom platformy je poskytnúť používateľom centralizovanú databázu odtlačkov mobilných aplikácií, postavených na platforme Android.

Využitie projektu :

- Zefektívnenie práce sieťových administrátorov pri identifikácii komunikácie
- Odhaľovanie potenciálne nebezpečných aplikácií alebo malvérov
- Kontrola používateľov pripojených k spravovanej sieti

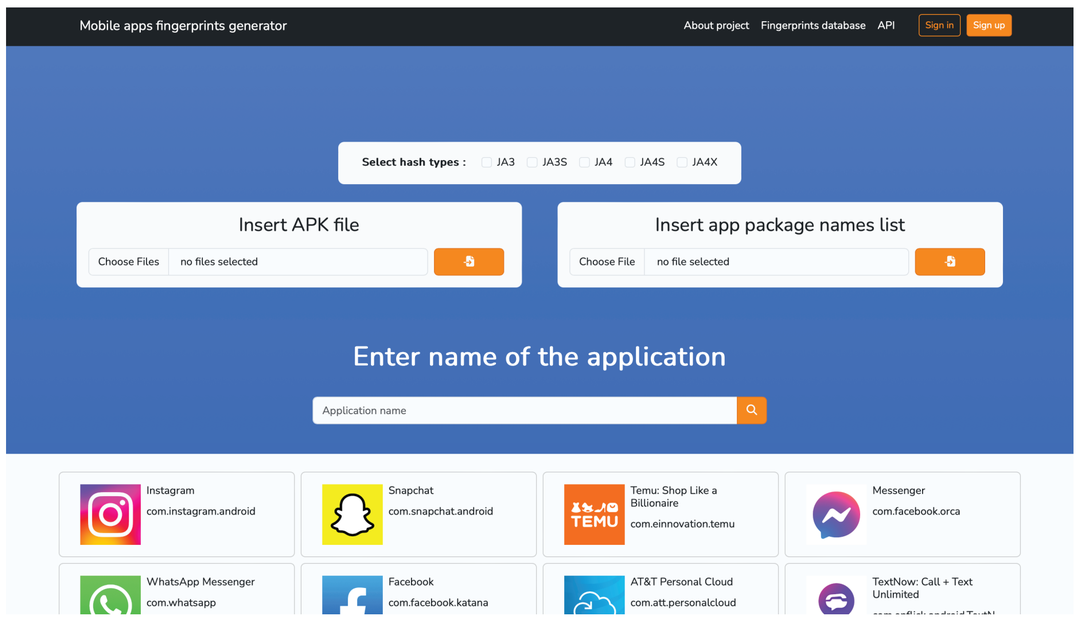
Riešené problémy počas vývoja :

- Získanie zdroja súborov APK a automatizované sťahovanie
- Izolácia a zachytávanie komunikácie android emulátorov
- Súčasné spracovávanie požiadaviek viacerých používateľov
- Možnosť identifikácie malvéru

Podporované typy odtlačkov TLS : **JA3, JA3S, JA4, JA4S, JA4X**

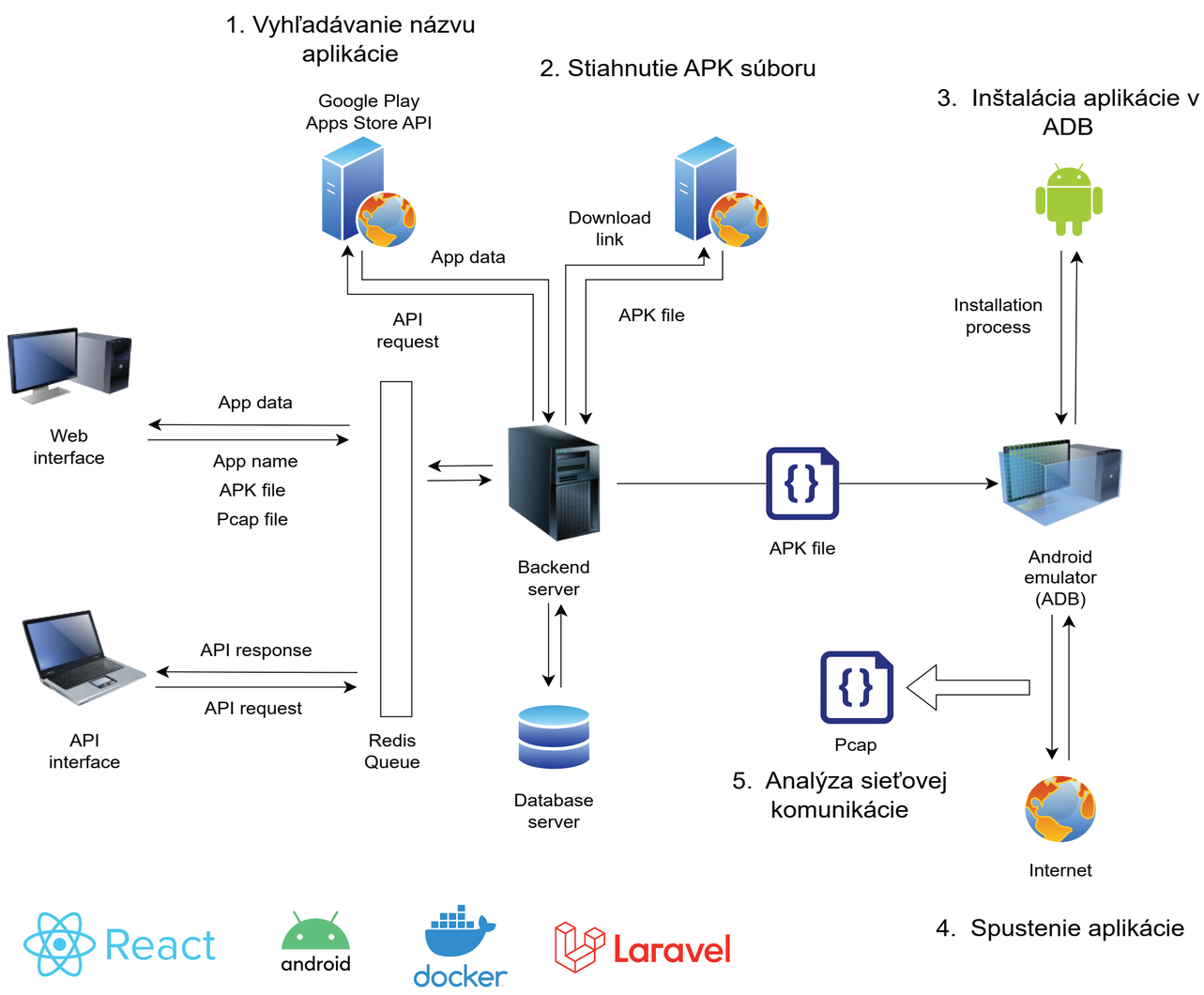
Hlavná stránka

Obrázok 1



Návrh systému

Obrázok 2



Odtlačky aplikácií

JSON 1

Odtlačky aplikácie Microsoft OneDrive : {

```
"app_name" : "Onedrive",
"version" : 7.2.1,
"package_name" : "com.microsoft.skydive",
"sni" : "login.live.com",
"JA3_hash" : "b32309a26951912be7dba376398abc3b",
"JA3S_hash" : "7d8fd34fdb13a7fff30d5a52846b6c4c",
"JA4_hash" : "t13d1515h2_8daaf6152771_de4a06bb82e3",
"JA4S_hash" : "t120400_c030_09f674154ab3",
"JA4X_hash" : "a373a9f83c6b_2bab15409345_2cdf432ec278",
```

}

Odtlačky malvéru A310logger : {

```
"app_name" : "a310logger",
"sni" : "login.live.com",
"JA3_hash" : "28a2c9bd18a11de089ef85a160da29e4",
"JA3S_hash" : "7d8fd34fdb13a7fff30d5a52846b6c4c",
"JA4_hash" : "t12d1909h2_d83cc789557e_7af1ed941c26",
"JA4S_hash" : "t120400_c030_09f674154ab3",
"JA4X_hash" : "a373a9f83c6b_2bab15409345_7bf9a7bf7029",
"issuer" : "CN=DigiCert SHA2 Secure Server CA, ON=Digicert Inc",
"subject" : "CN=login.live.com, ON=Microsoft Corporation",
```

}

Výsledky identifikácie aplikácií

Tabuľka 1

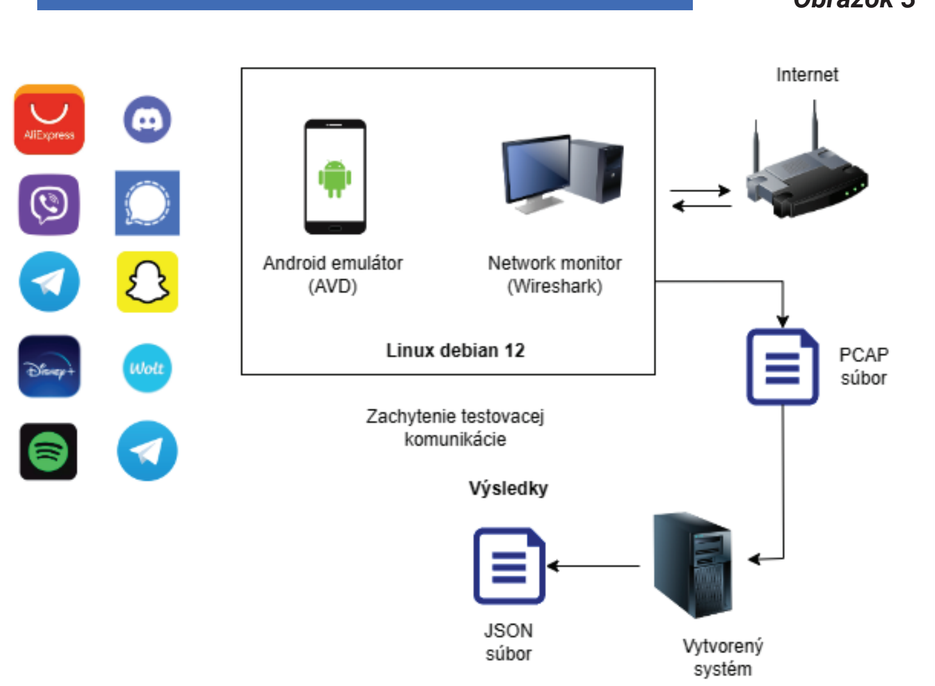
Typ odtlačku	Total	Accurancy	Precision	Recall
JA3	386	63,21%	100,00%	56,04%
JA3_JA3S	386	70,73%	100,00%	65,02%
JA3_JA3S_SNI	386	96,11%	99,04%	96,28%
JA4	386	63,99%	100,00%	56,97%
JA4_JA4S	386	70,98%	100,00%	65,32%
JA4_JA4S_SNI	386	96,11%	99,04%	96,28%
JA3_JA3S_SNI_JA4_JA4S	386	96,11%	99,04%	96,28%

Dataset 1 : Aliexpress (8.90.2), Alza (10.15.1), Signal (6.46.7), Viber (22.0.1.0), Messenger (448.0.0.47.109), Muj vlak (2.11.2), Spotify (8.9.14.543), Wolt (4.52.0), Twitter (10.29.0), TikTok (34.2.2)

Dataset 2 : Telegram (10.8.2), Snapchat (12.75.0.42), Reddit (2024.07.0), Mapy.cz (9.44.1), RegioJet (3.41.2), Netflix (8.106.1), Discord (216.14), Foodora CZ (24.2.0), DisneyPlus (24.02.12.10), Packeta (1.18.10)

Testovacia topológia

Obrázok 3



Autor práce : KRISTIÁN KIČINKA (xkicin02@vutbr.cz)

Vedúci práce : doc. Ing. PETR MATOUŠEK, Ph.D., M.A.