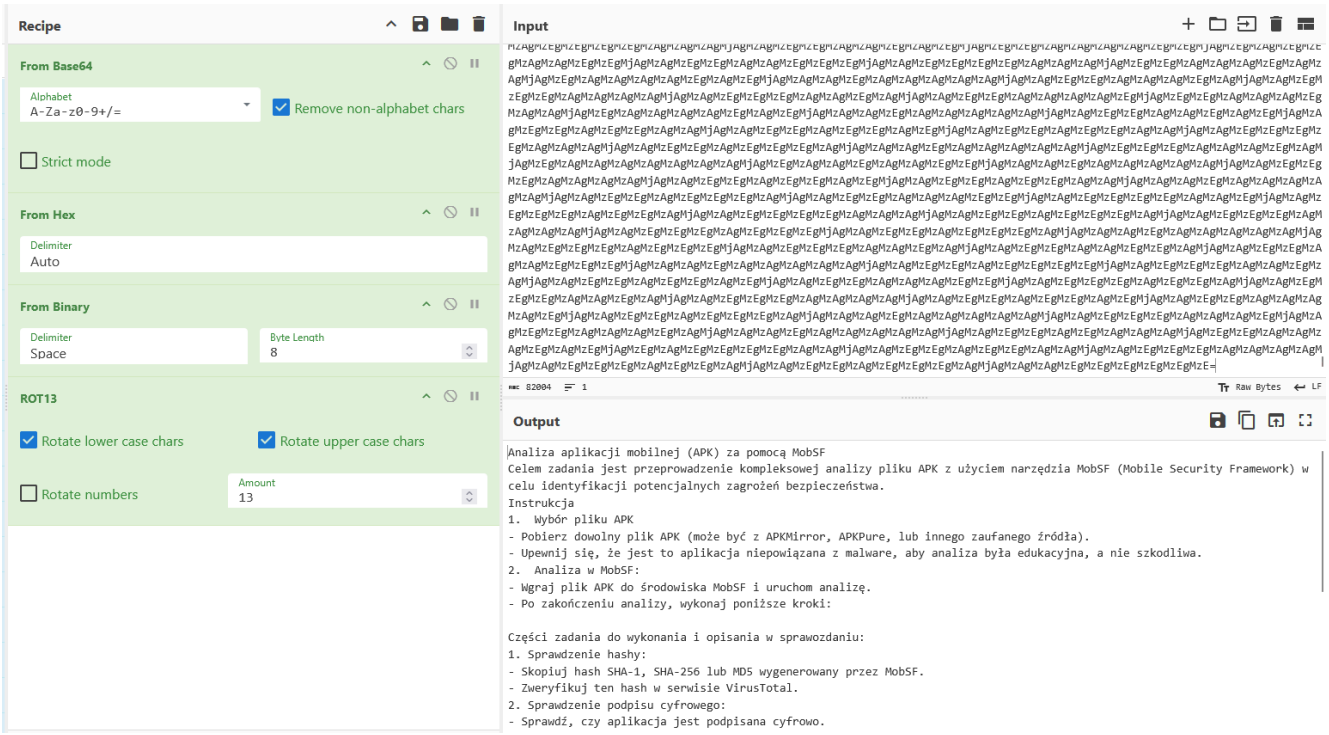
POLITECHNIKA WROCŁAWSKA Wydział Informatyki i Telekomunikacji	Wydział: Informatyki i Telekomunikacji Kierunek: Cyberbezpieczeństwo Rok Akademicki: 2024/2025 Rok studiów, semestr: 2, 4 Grupa: 1 Termin: pon., 7:30
CBESI0053G Informatyka śledcza – Laboratorium 11	
Prowadzący: mgr inż. Adrian Florek	Autor: 1. Gerard Błaszczyk
Data wykonania ćwiczenia: 19.05.2025	
Data oddania sprawozdania: 25.05.2025	

1. Cel ćwiczenia

Przeprowadzenie kompleksowej analizy pliku APK z użyciem narzędzia MobSF (Mobile Security Framework) w celu identyfikacji potencjalnych zagrożeń bezpieczeństwa

2. Rozszyfrowanie instrukcji laboratoryjnej

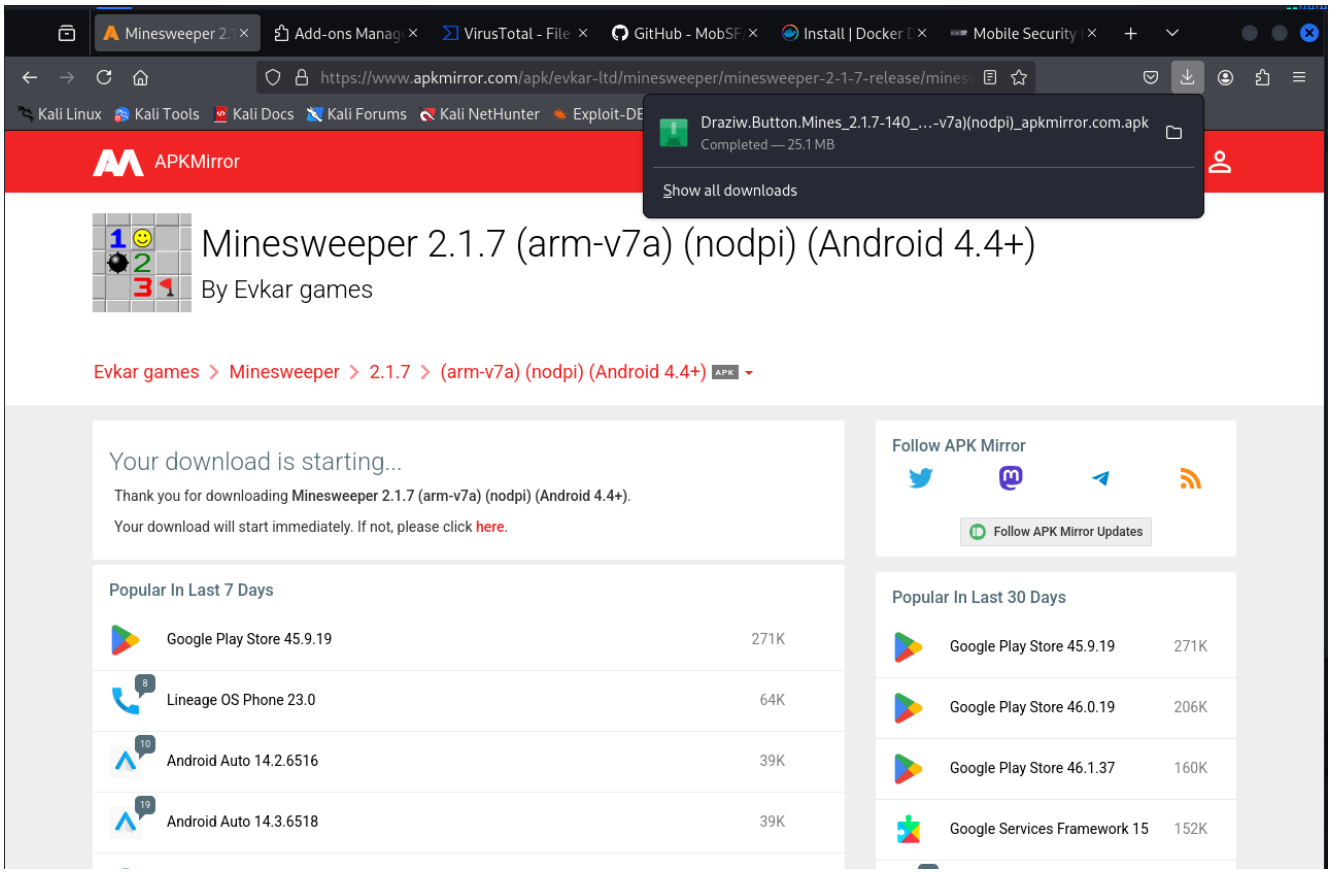


Rysunek 1: rozszyfrowanie instrukcji; CyberChef

3. Realizacja zadań laboratoryjnych

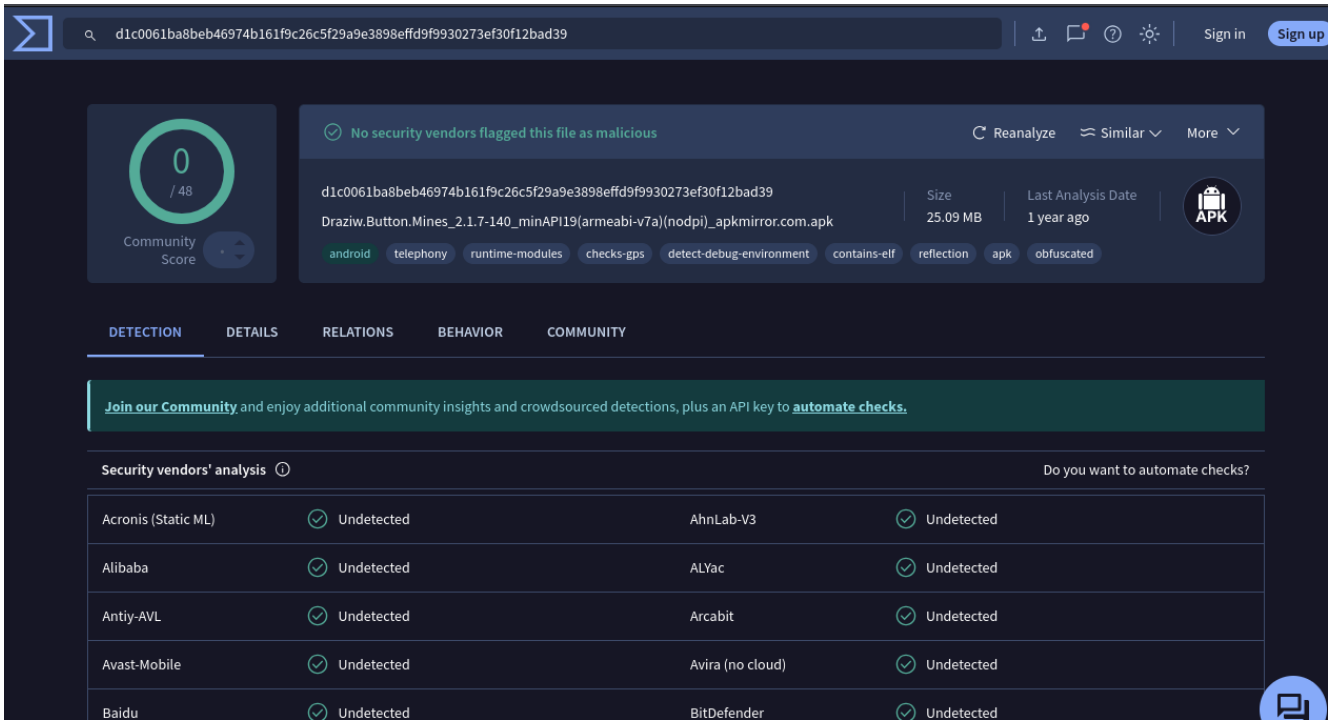
Zadanie 1. Wybór pliku APK

- Pobierz dowolny plik APK (może być z APKMirror, APKPure, lub innego zaufanego źródła).



Rysunek 2: instalacja pliku APK; APKMirror

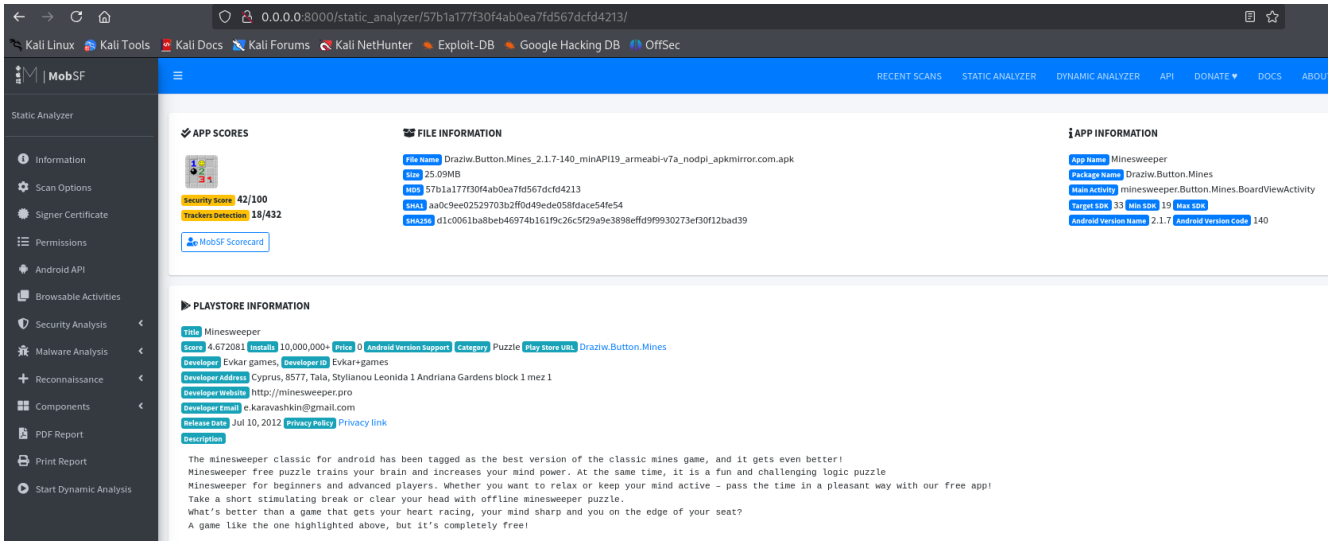
- Upewnij się, że jest to aplikacja niepowiązana z malware, aby analiza była edukacyjna, a nie szkodliwa.



Rysunek 3: Analiza bezpieczeństwa; VitusTotal

Zadanie 2. Analiza w MobSF:

- Wgraj plik APK do środowiska MobSF i uruchom analizę.



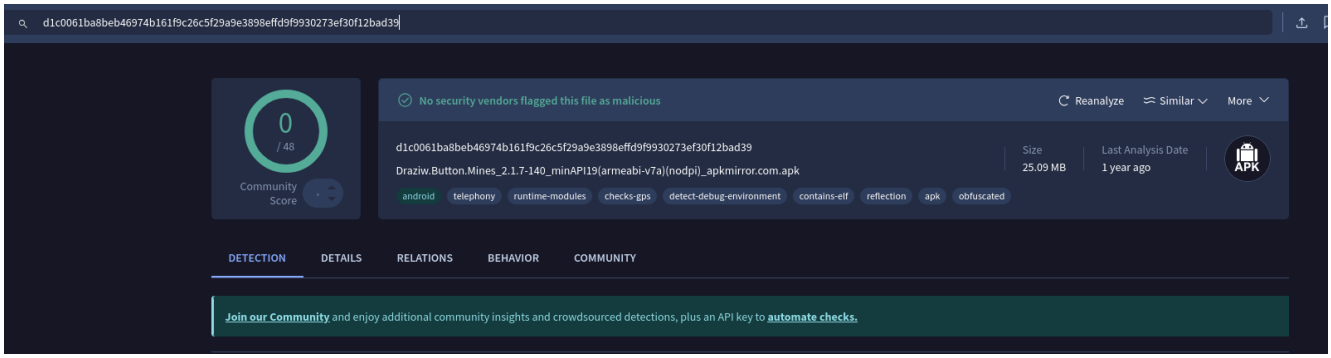
Rysunek 4: analiza pliku APK; MobSF

- Po zakończeniu analizy, wykonaj poniższe kroki:
Części zadania do wykonania i opisania w sprawozdaniu:

1. Sprawdzenie hashy:

- Skopiuj hash SHA-1, SHA-256 lub MD5 wygenerowany przez MobSF.

- Zweryfikuj ten hash w serwisie VirusTotal.



Rysunek 5:

2. Sprawdzenie podpisu cyfrowego:

- Sprawdź, czy aplikacja jest podpisana cyfrowo.

- Oceń wiarygodność podpisu – czy pochodzi od znanego wydawcy?

SIGNER CERTIFICATE

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=RU, ST=Sverdlovskaya, L=Verhniya Pishma, CN=Evgeny Karavashkin
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-07-10 15:08:56+00:00
Valid To: 2041-07-03 15:08:56+00:00
Issuer: C=RU, ST=Sverdlovskaya, L=Verhniya Pishma, CN=Evgeny Karavashkin
Serial Number: 0x1c30482
Hash Algorithm: sha256
md5: 8d7fb9f4ba421a04c7426bf838bcfad6
sha1: 479cb12a4ccd7736146d6097942cdda527922237
sha256: ca6b9f44f27831ce11620dc65d7b156c3226aa4d4d5390bc1f0cb7007e5321f9
sha512: 4099f429360657854a13eaf42e4b140bdcb7a643e82740d5eb063cd02e82b57e14bbb8cac1fb705f5fe4b8f679266580f8b68496f83745e78344dee2a2ca71fc
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 472473d76a7a8e9a093ec4917da95e671bf82a19a87d1b06347da5a4e2b9d1ca
Found 1 unique certificates
```

Rysunek 6: podpis pliku

Komentarz: Podpis z kraju: Rosja. Ważny do 2041, (29 lat), co jest niestandardowym okresem ważności, Podpis jest na imię i nazwisko a nie nazwę znanego producenta. Te informacje nie przesądzają o niebezpieczeństwie, ale nie jest to znany i zaufany producent aplikacji, należy zachować ostrożność.

3. Weryfikacja uprawnień aplikacji:

- Wypisz wszystkie żądane uprawnienia.

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.	
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.	
android.permission.ACCESS_ADSERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.	
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.	Show Files
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.	Show Files
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.	Show Files
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.	Show Files
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.	Show Files
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.	Show Files
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.	Show Files

Rysunek 7: żądane uprawnienia

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.	
com.applovin.array.apphub.permission.BIND_APPHUB_SERVICE	unknown	Unknown permission	Unknown permission from android reference	
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.	Show Files
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.	Show Files
Draziw.Button.Mines.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference	

Rysunek 8: żądane uprawnienia

- Wybierz 3 najbardziej podejrzane lub nadmiarowe.

android.permission.WRITE_EXTERNAL_STORAGE

android.permission.ACCESS_NETWORK_STATE

android.permission.INTERNET

- Uzasadnij, czy aplikacja rzeczywiście potrzebuje tych uprawnień – np. „kalkulator proszący o dostęp do SMS” budzi podejrzenia.

Komentarz: Prosta gra taka jak „saper” z pewnością nie potrzebuje uprawnienia do zapisywania jakichkolwiek danych na zewnętrzny dysk. Uprawnienia dotyczące internetu zakładam, że są wykorzystywane do wyświetlania reklam, jednakże jest ich kilka – pytanie czy wszystkie na pewno są potrzebne. Ponadto gra ma wbudowany system *in-app-purchases* więc pytanie czy reklamy są absolutnie konieczne do uzyskania zysku.

4. Analiza domen i konfiguracji sieci:

- Zidentyfikuj domeny i adresy URL obecne w aplikacji - zwróć uwagę na podejrzane lub nietypowe domeny.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
a.applovin.com	ok	**IP:** 34.117.147.68 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
a.applvn.com	ok	**IP:** 34.117.147.68 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
adc-ad-assets.adtilt.com	ok	**IP:** 151.101.195.52 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
adc3-launch-staging.adcolony.com	ok	No Geolocation information available.
adc3-launch.adcolony.com	ok	**IP:** 34.36.45.50 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498

Rysunek 9: domeny

URLS

Search:

URL	FILE
data:{ https://www	com/safedk/android/utils/g.java
data:,	com/applovin/impl/sdk/ae.java
data::from	com/smaato/sdk/core/gdpr/SomaGdprV2Utils.java
data::new	com/smaato/sdk/core/gdpr/SomaGdprData.java
data:a.data)};function data:d),c)}	com/inmobi/media/m9.java
data:auto=	com/safedk/android/analytics/brandsafety/BannerFinder.java
data:d),c)}function data:a.data)};function	com/bytedance/sdk/openadsdk/core/g/e.java
data:d),c)}function data:a.data)};function	com/yandex/mobile/ads/impl/su0.java

Rysunek 10: URL's

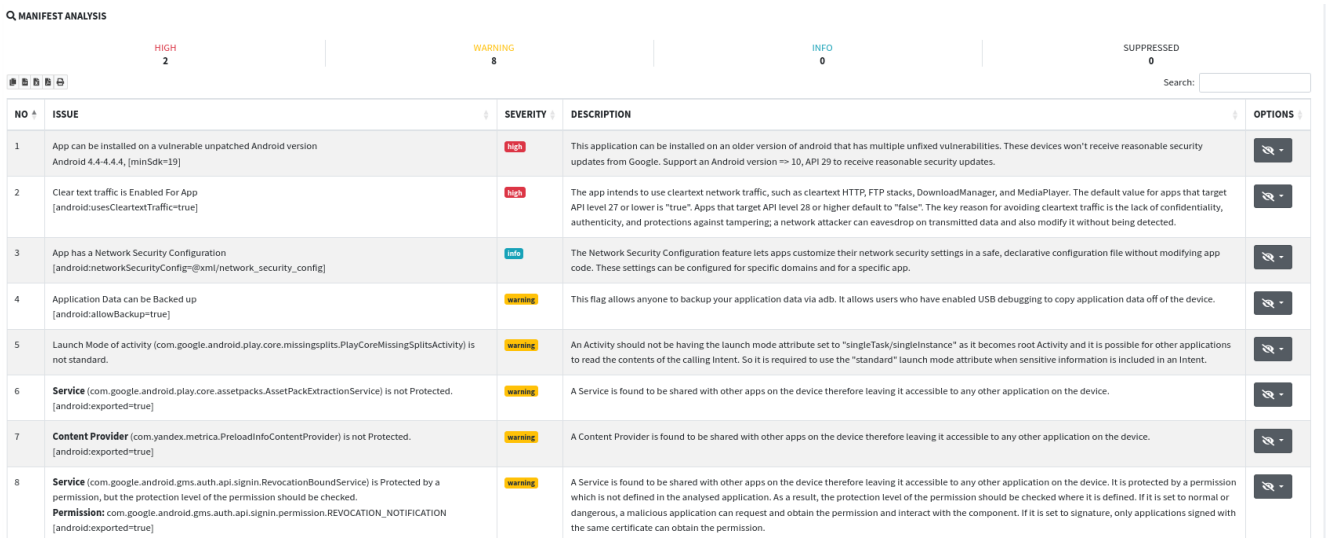
Komentarz: nie znalazłem podejrzanych ani nietypowych adresów ani domen.

- Sprawdź, czy aplikacja komunikuje się po HTTPS, czy zawiera niezabezpieczone połączenia.

Komentarz: odpowiedź w kolejnym podpunkcie.

5. Analiza pliku AndroidManifest.xml:

- Otwórz zakładkę z manifestem i wypisz najważniejsze informacje



MANIFEST ANALYSIS

HIGH 2 | WARNING 8 | INFO 0 | SUPPRESSED 0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable unpatched Android version Android 4.4-4.4.4, [minSdk=19]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.	
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.	
3	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.	
4	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.	
5	Launch Mode of activity (com.google.android.play.core.missingsplits.PlayCoreMissingSplitsActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.	
6	**Service** (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
7	**Content Provider** (com.yandex.metrica.PreloadInfoContentProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
8	**Service** (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. **Permission:** com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.	

Rysunek 11: zakładka manifest analysis

Komentarz: najważniejsze – ostrzeżenia o indeksach 1 i 2.

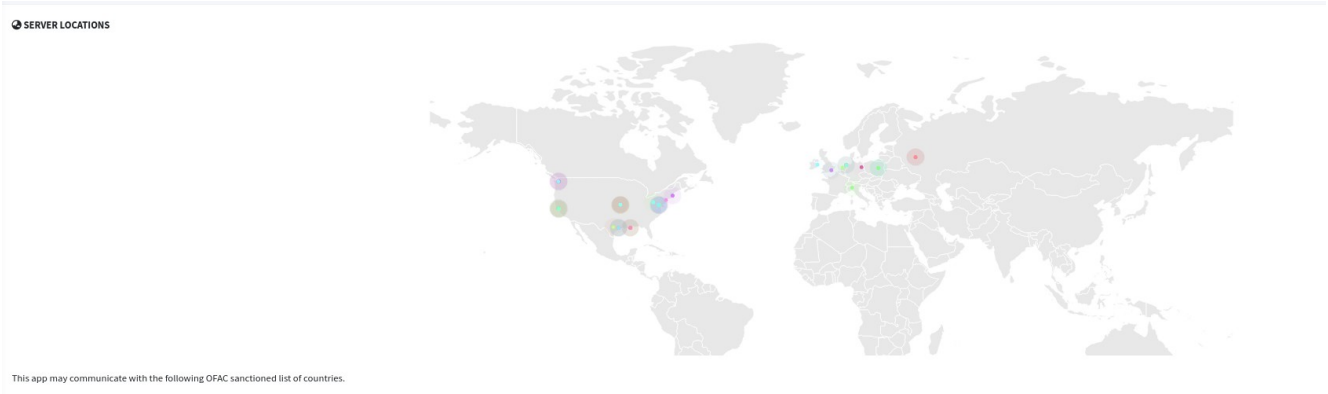
- Opisz, co mogą one sugerować o funkcjonalności aplikacji.

1. – ostrzeżenie zwraca uwagę, że aplikacja może być instalowana ma starsze wersje androida, co jest niebezpieczne samo w sobie, ponieważ starsze wersje systemu mają znane luki w zabezpieczeniach. Korzystanie z zdezaktualizowanego oprogramowania nie jest dobrą praktyką.

2. – ostrzeżenie mówi o wykorzystywaniu komunikacji „cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer”. Korzystanie z nieszyfrowanych protokołów do przesyłania danych nie jest bezpieczną praktyką.

6. Sprawdzenie lokalizacji serwerów:

- Używając znalezionych domen/IP spróbuj ustalić geolokalizację serwerów (np. przez iplocation.net).



Rysunek 12: sekcja server locations

- Czy aplikacja komunikuje się z serwerami w podejrzanych lokalizacjach (np. obce kraje, nieznane hostingi)?

W zdecydowanej większości nie ma tutaj podejrzanych lokalizacji – głównie Stany Zjednoczone oraz Europa. Podejrzane jest łączenie się z serwerem w Rosji, natomiast według opisanych wcześniej danych jest to kraj pochodzenia autora aplikacji.

7. Podsumowanie wyników i wnioski:

- Oceń ogólny poziom bezpieczeństwa aplikacji.

Ogólny poziom bezpieczeństwa aplikacji określam jako dobry, poza nieznacznymi odchyłami od standardów nie zauważam poważnych naruszeń bezpieczeństwa.

- Wypisz wszystkie potencjalnie niebezpieczne artefakty, np.:

* Nieszyfrowana komunikacja sieciowa,

* Zbyt szerokie uprawnienia odnośnie dostępu do sieci,

* Ogólne powiązania z Rosją,

* Za duża ilość trackerów reklamowych.

- Zakończ krótką oceną ryzyka – czy aplikacja jest bezpieczna do użycia?

Moim zdaniem aplikacja jest bezpieczna do użycia. Dla zapewnienia całkowitego bezpieczeństwa zawsze można podjąć dodatkowe środki ostrożności np. zabronić uruchamiania się tej aplikacji w tle, nie przyznawać dostępu do internetu, korzystać z niej tylko w trybie samolotowym – natomiast nie sądzę aby ta prosta gra naruszała znacząco bezpieczeństwo urządzenia ani użytkownika.