FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Untersuchen und Analysieren von Android-Apps auf Modifikation

Sebastian Becker, B. Sc.

Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik

IT Forensik
FH Aachen

Gliederung

- Einleitung
- Problemstellung
- Das Programm: Malware Detection
  - Das Archiv
  - Der Downloader
  - Die Analyse
- Probleme der Analyse
- Zusammenfassung

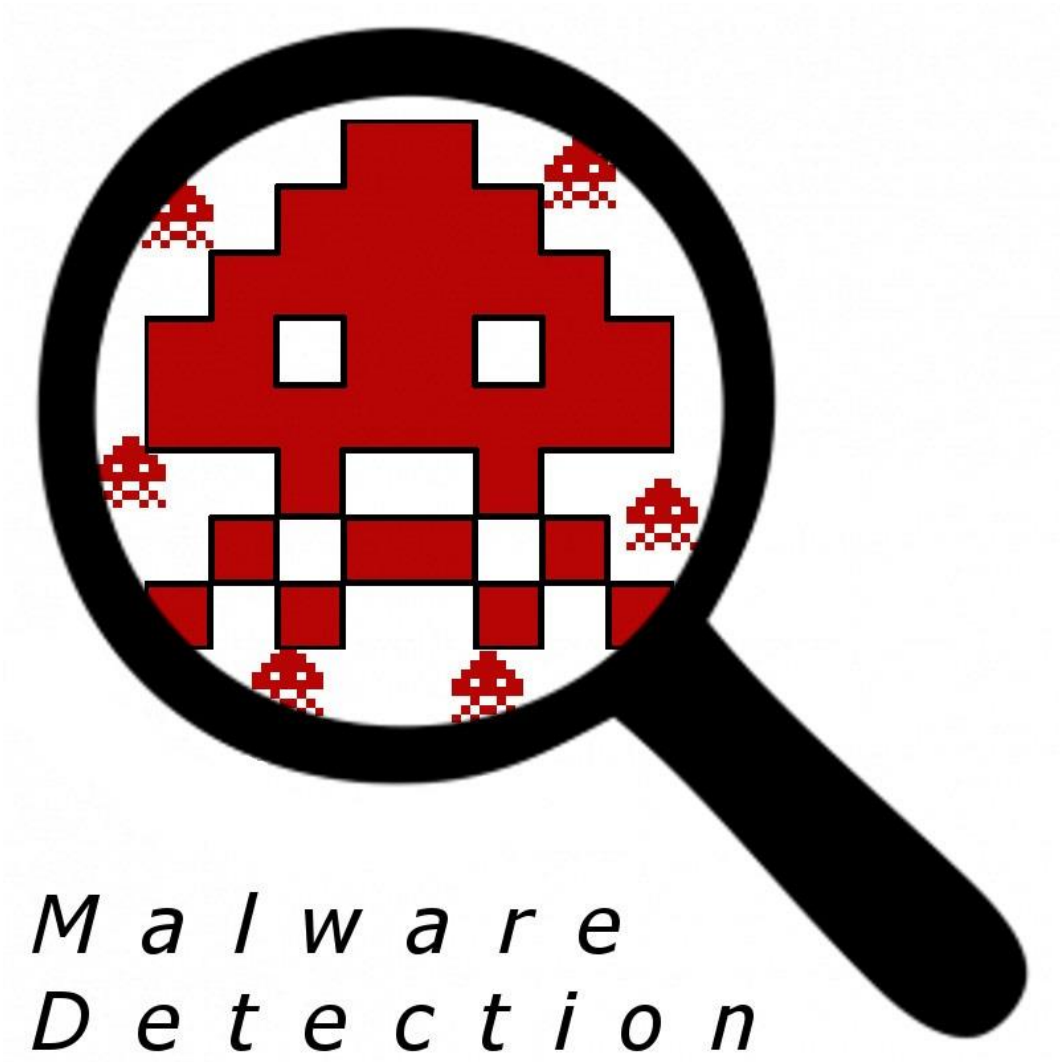
Einleitung

- 46 Millionen Bundesbürger besitzen ein Smartphone (Tendenz steigend)
- Android ist mit 71,6% Markführer
- 97% aller Malware wird für Android hergestellt

Problemstellung

- Anwender laden Apps aus dem Internet:
  - App nicht im Google Play Store (Flappy Bird)
  - App kostet im Google Play Store (Navigon)
- Benutzer akzeptieren App-Berechtigungen ohne diese zu lesen
- Folgen: Hohe Handyrechnungen, Datendiebstahl
- Identifizieren von modifizierten Apps nur händisch möglich

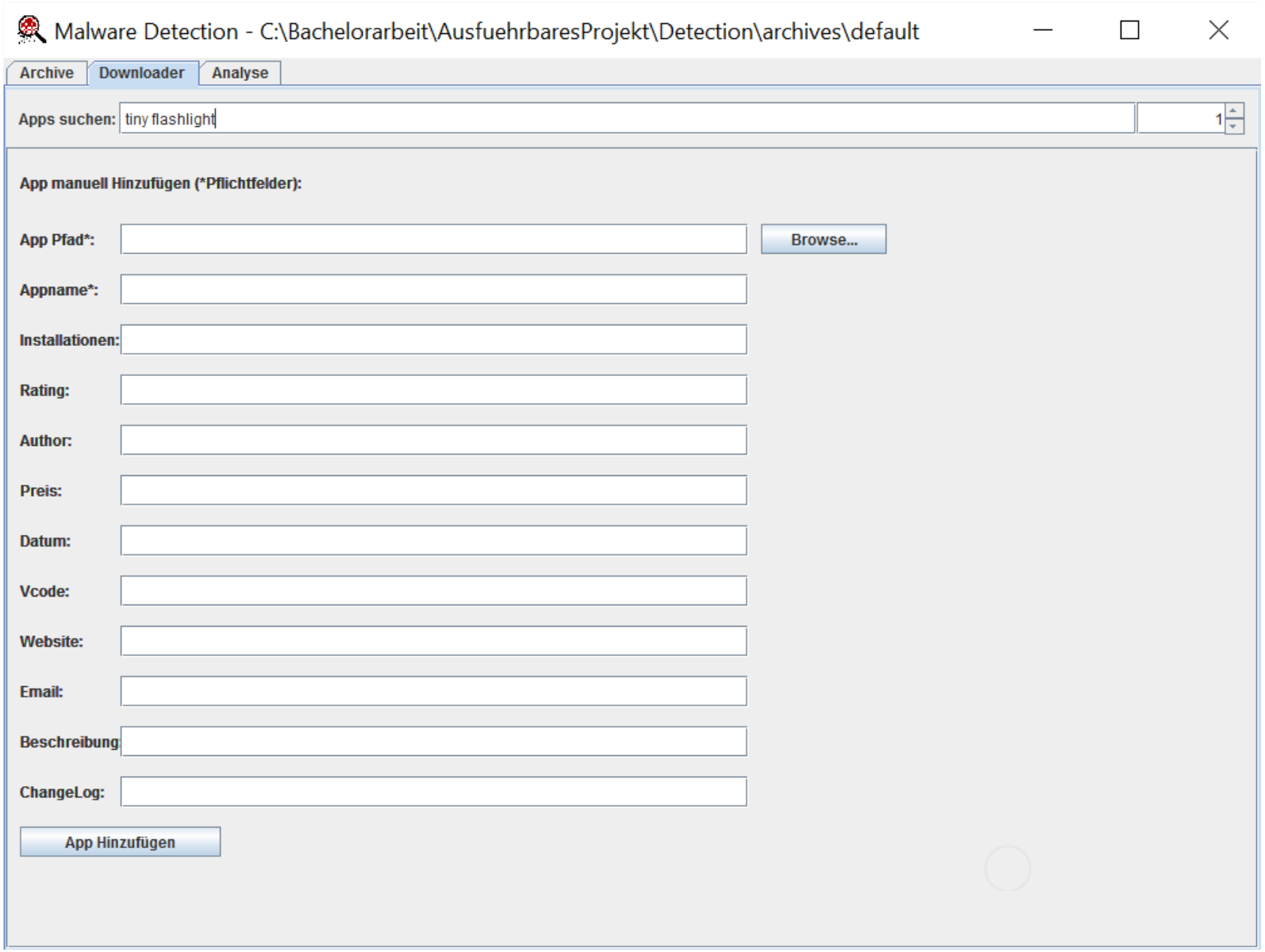
Das Programm: Malware Detection



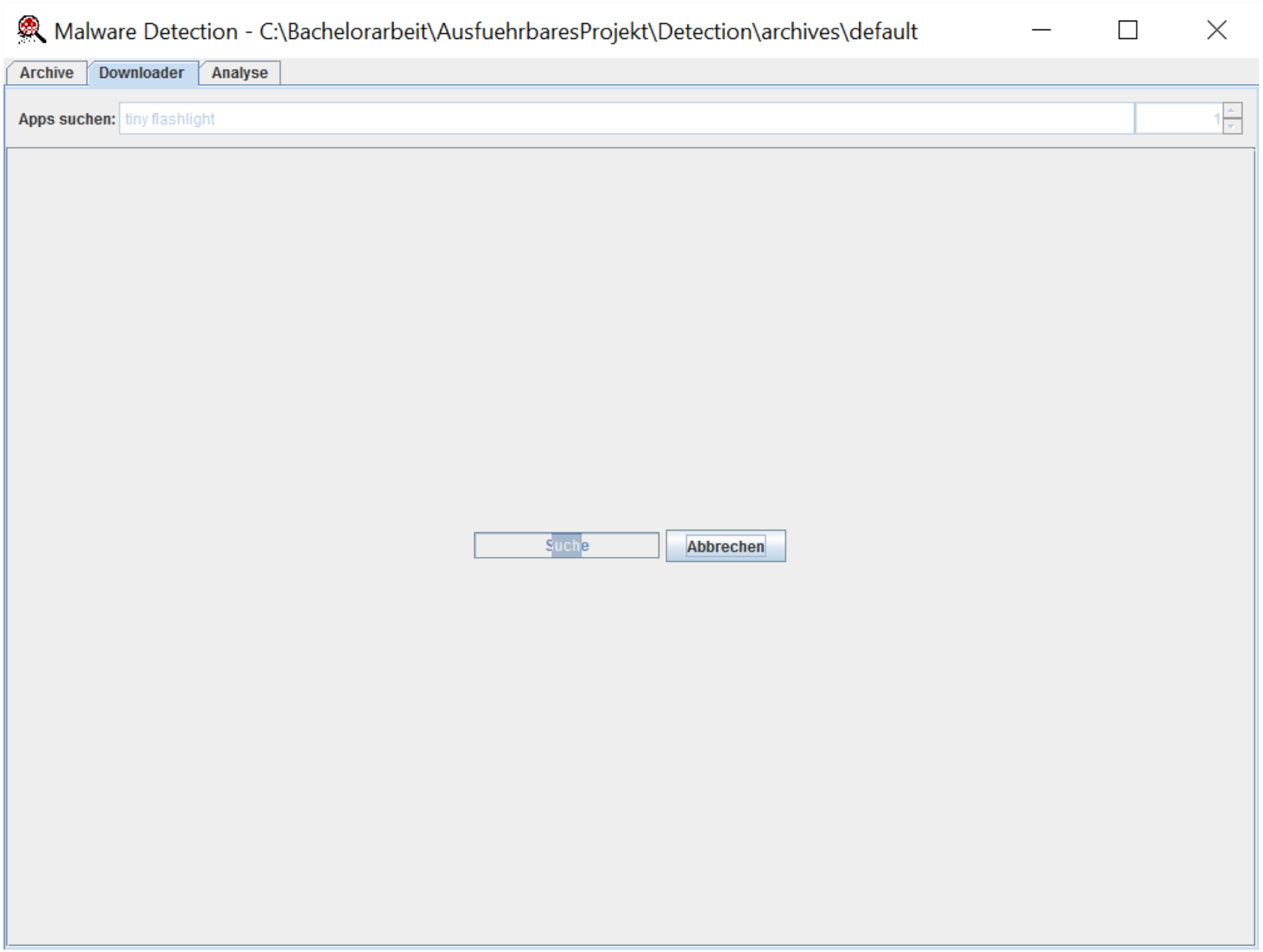
Das Programm – Der Aufbau

- Programm unterteilt sich in:
  - Downloader
  - Archiv (Datenbank)
  - Analyse
- Vorstellung am Beispiel: Tiny Flashlight

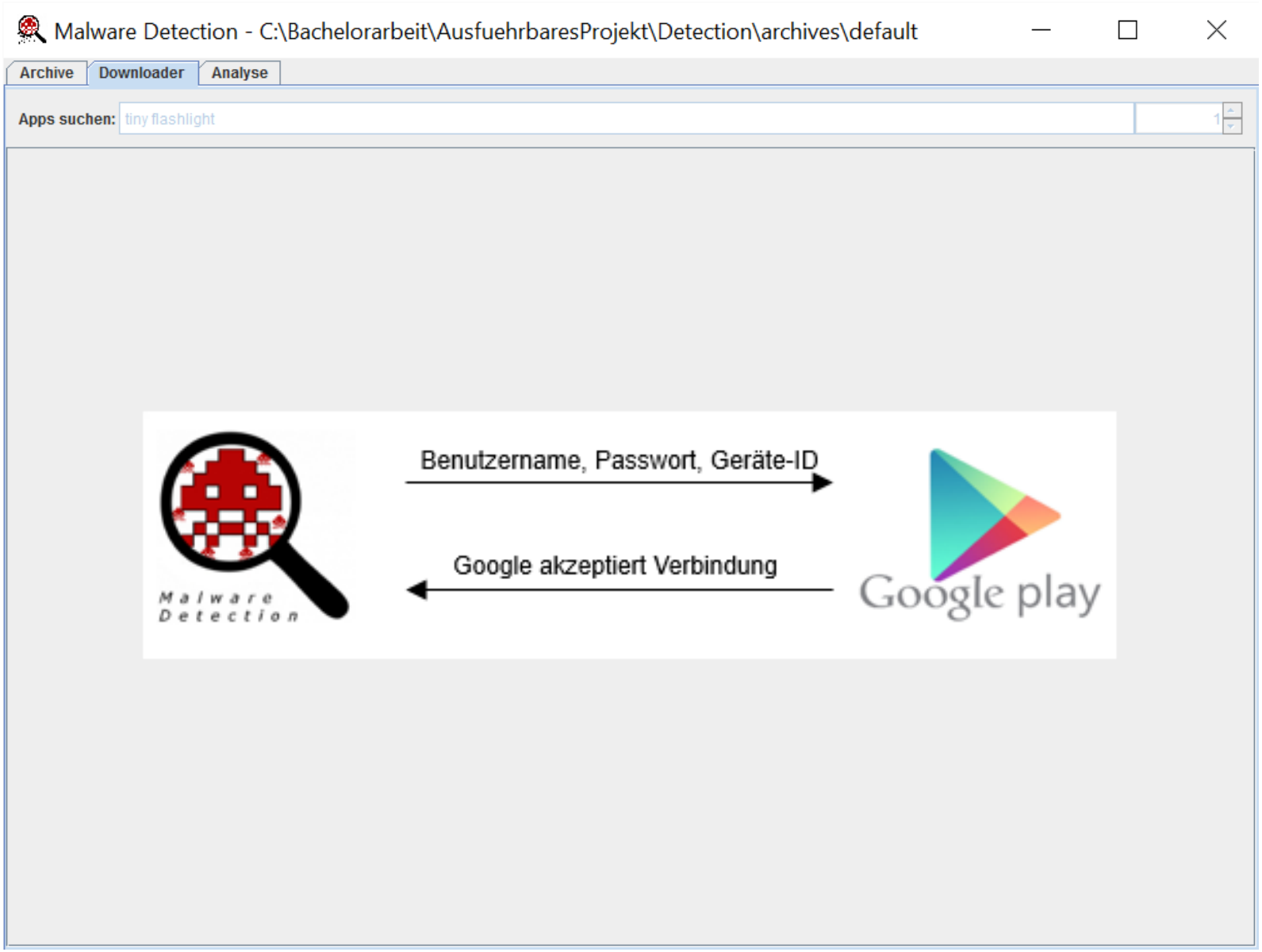
Der Downloader - Benutzeroberfläche



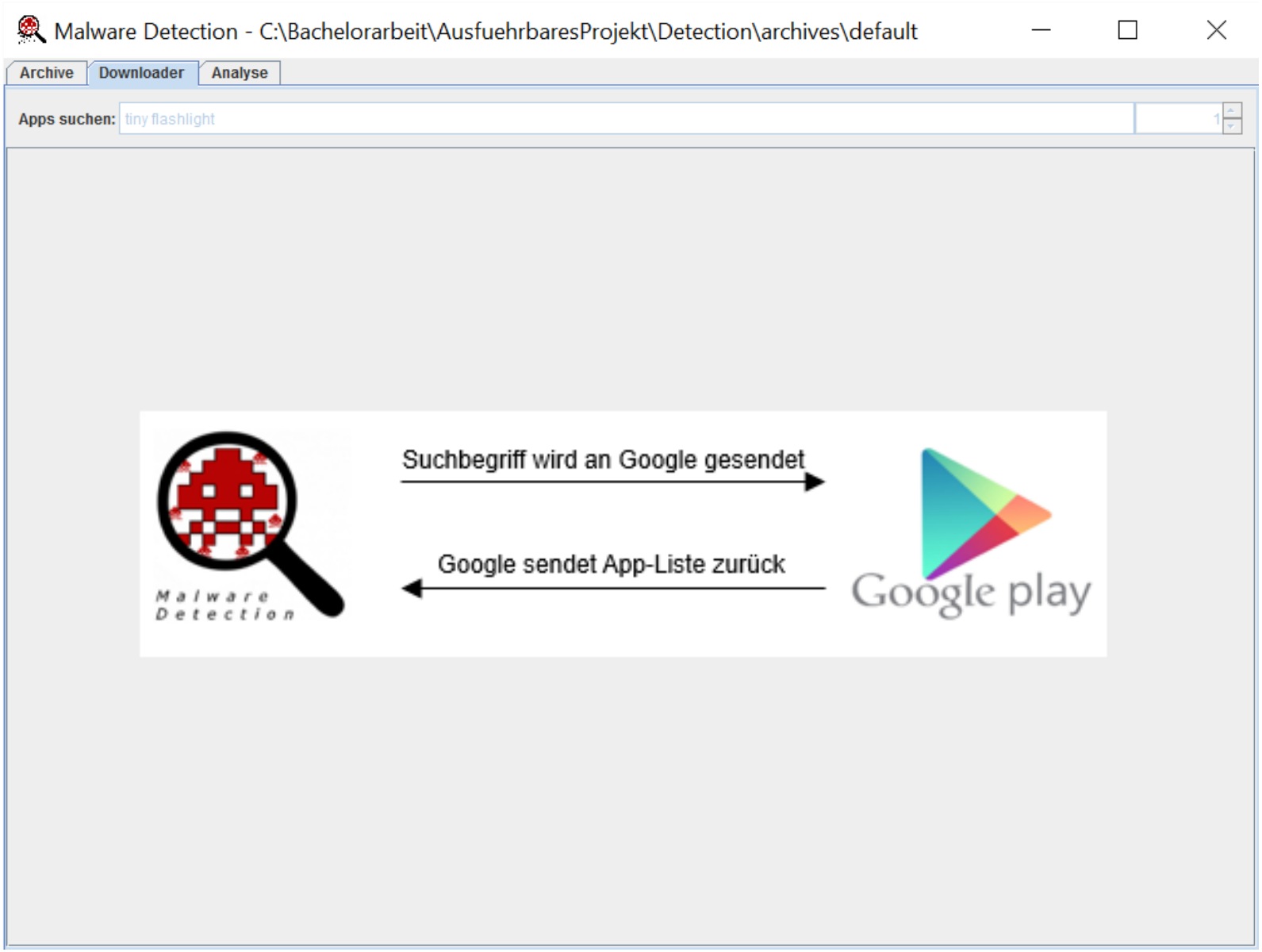
Der Downloader – Online herunterladen



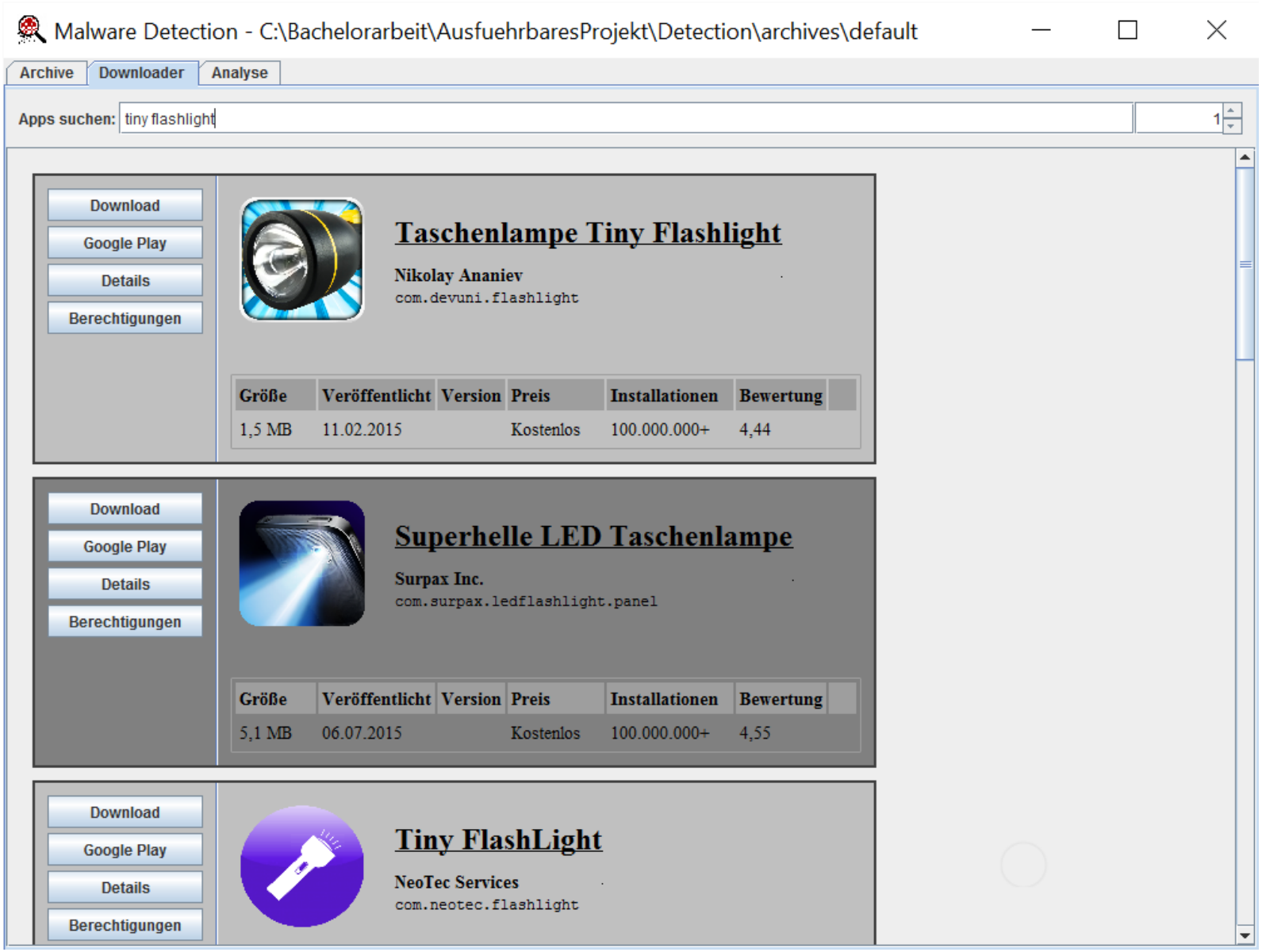
Der D. – Verbindungsaufbau(1/2)



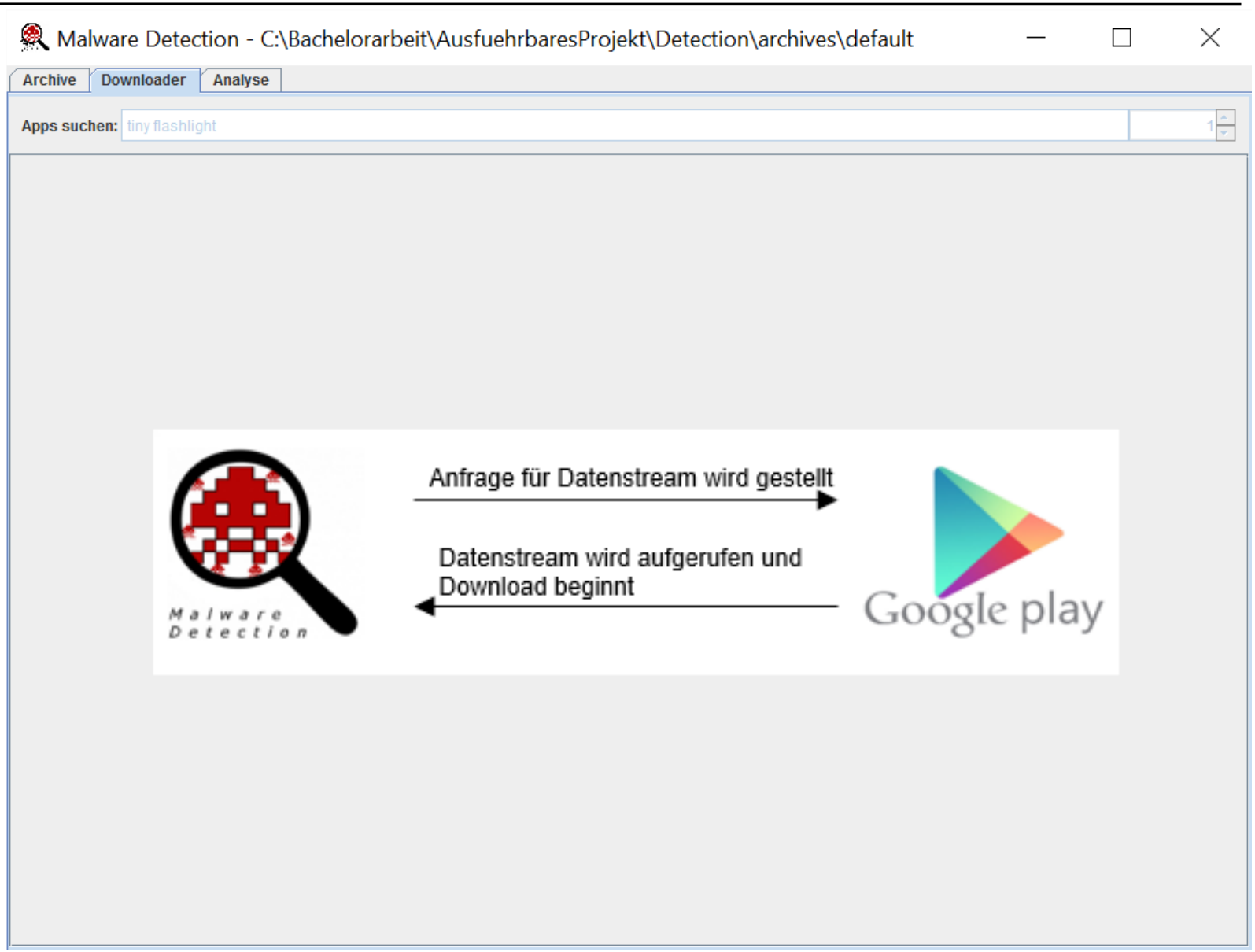
Der D. – Verbindungsaufbau(2/2)



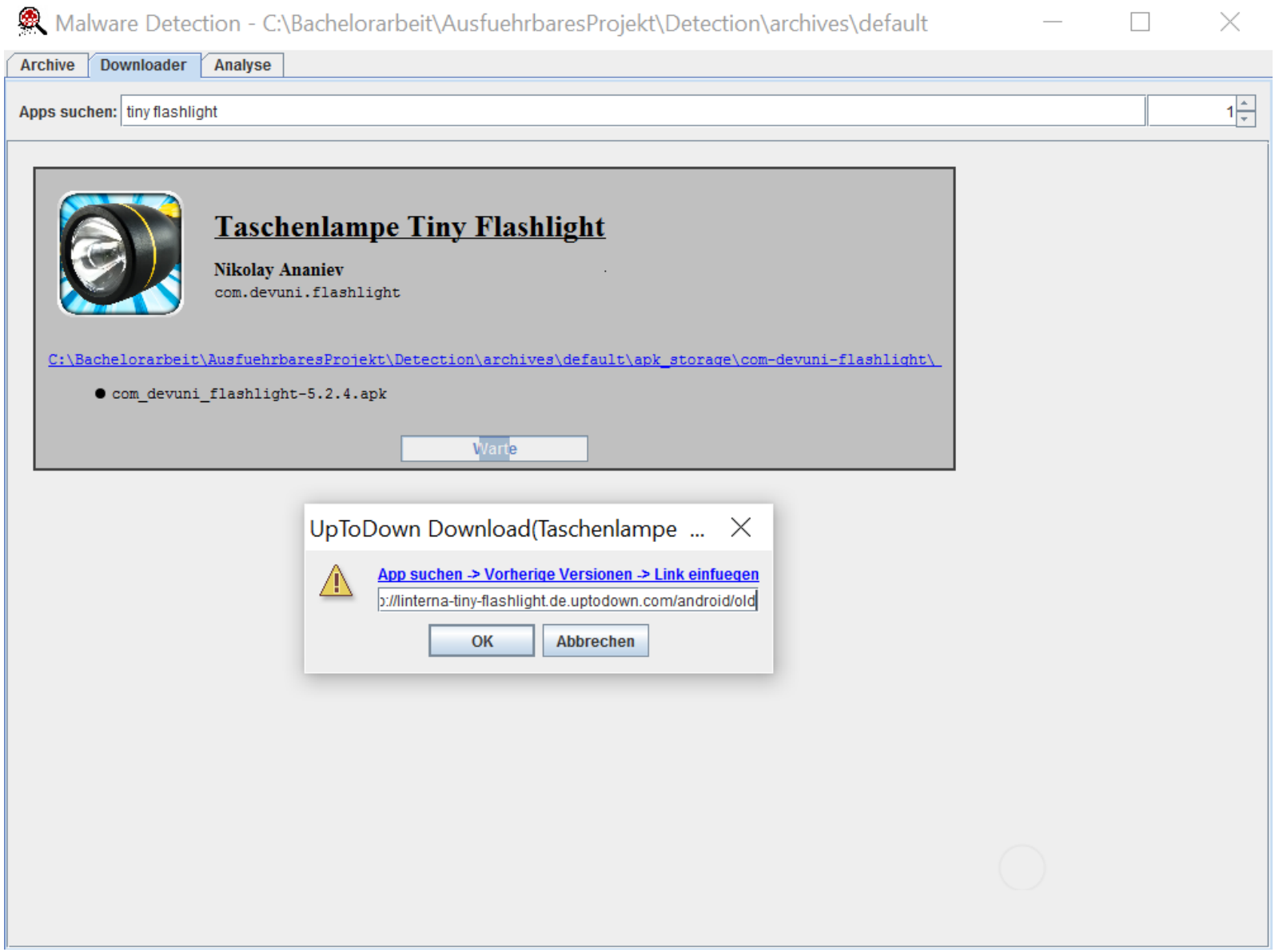
Der D. – Google Play Store



Der D. – Der Download(1/5)

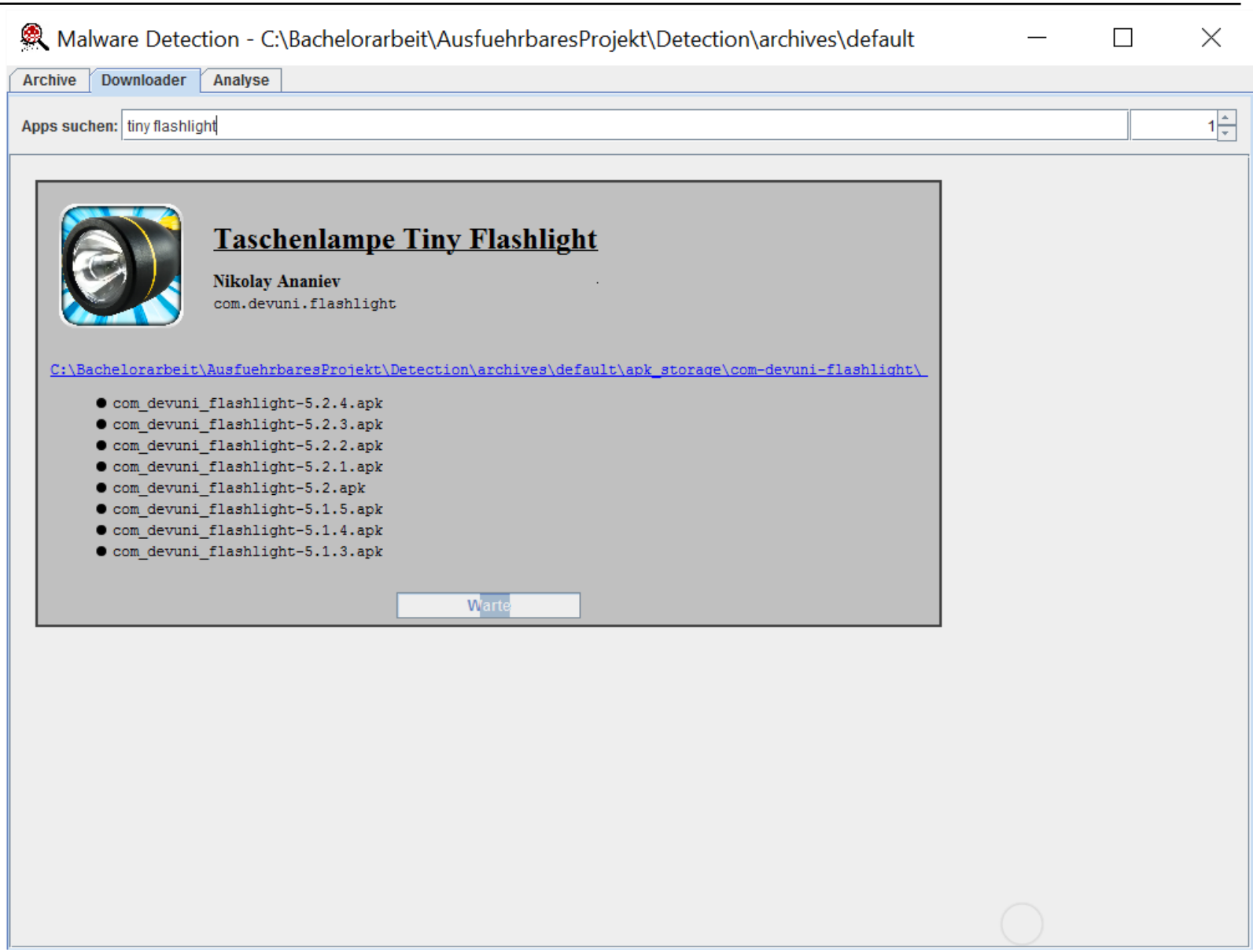


Der D. – Der Download(2/5)

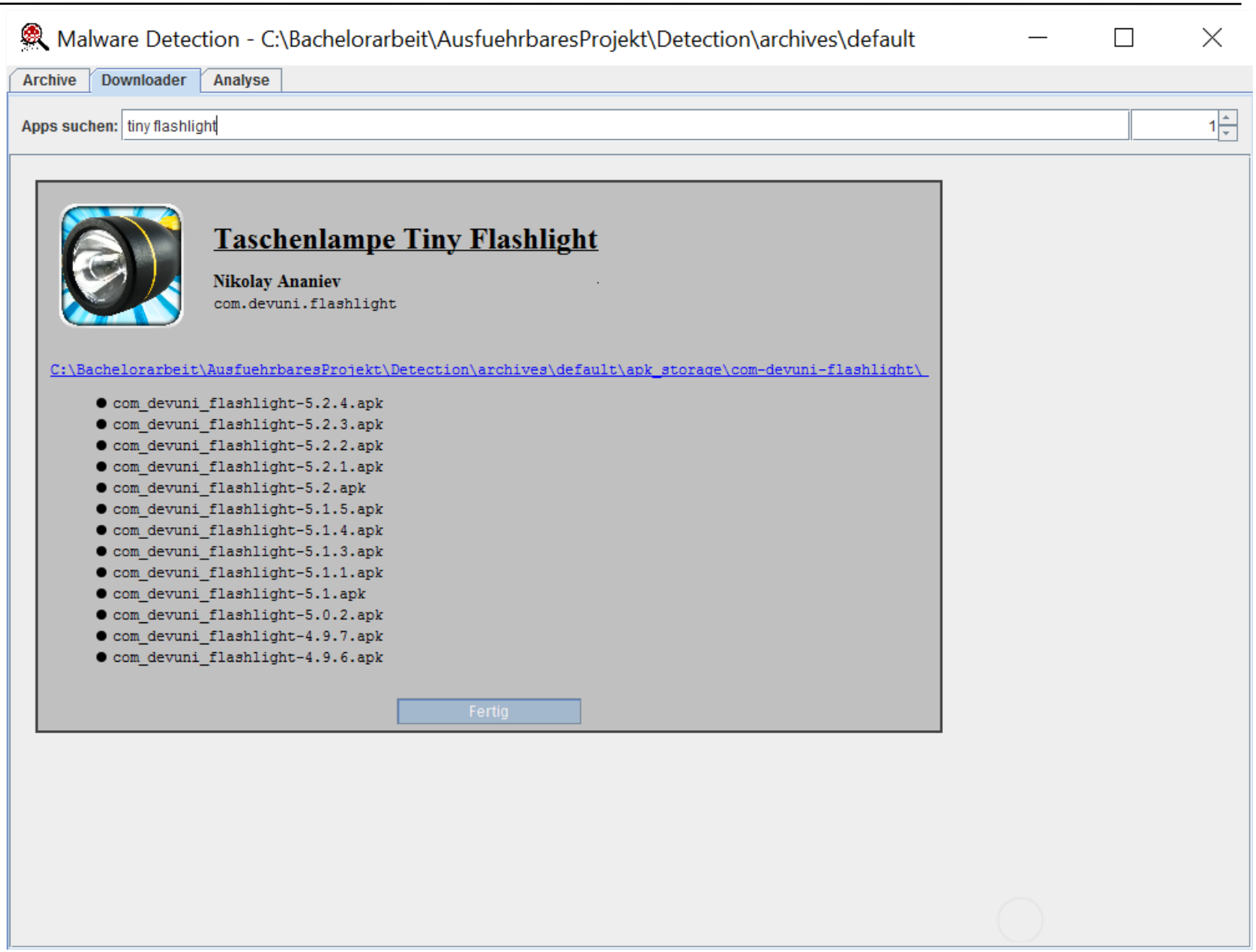


Der D. – Der Download(3/5)

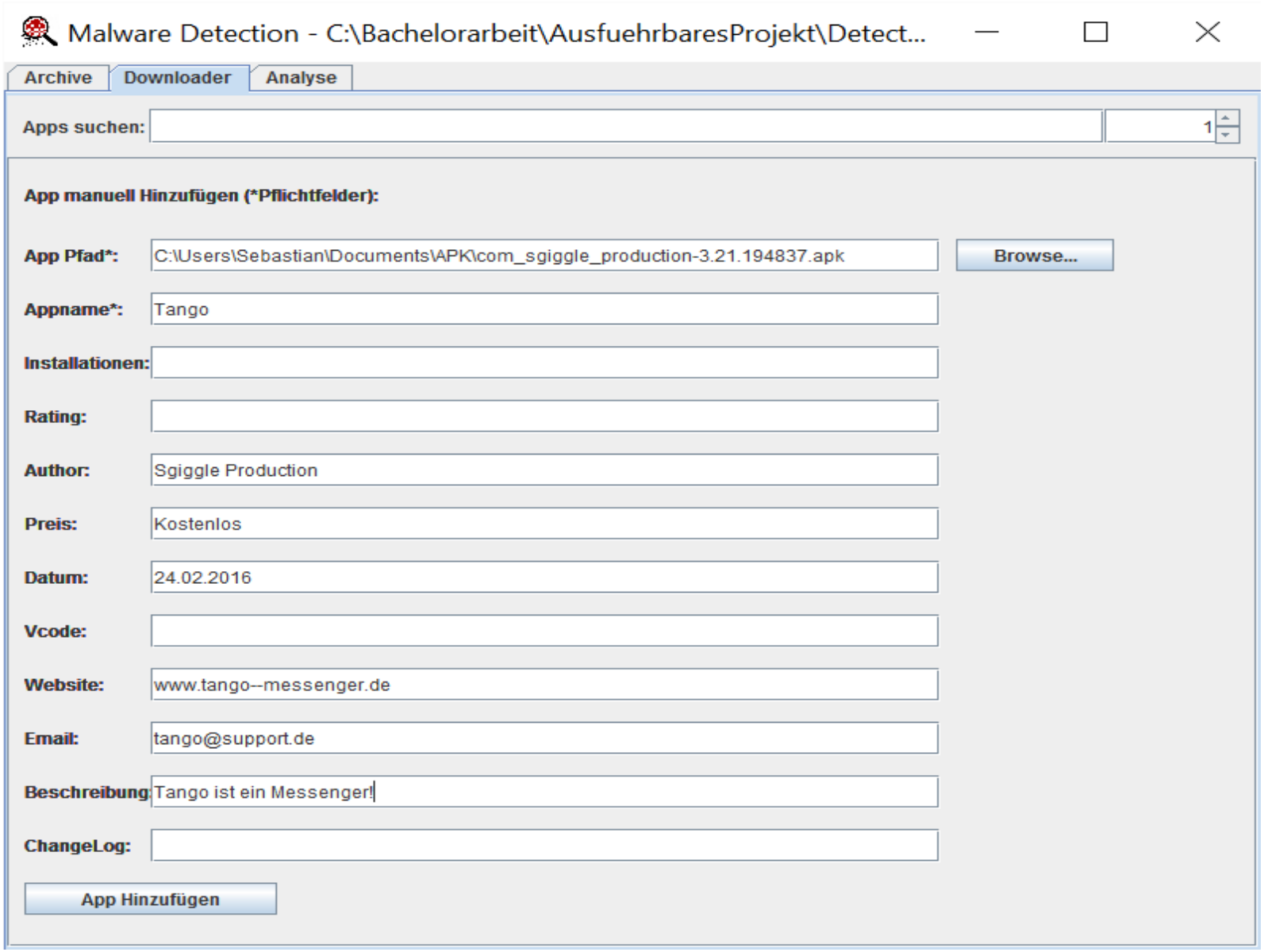
Der D. – Der Download(4/5)



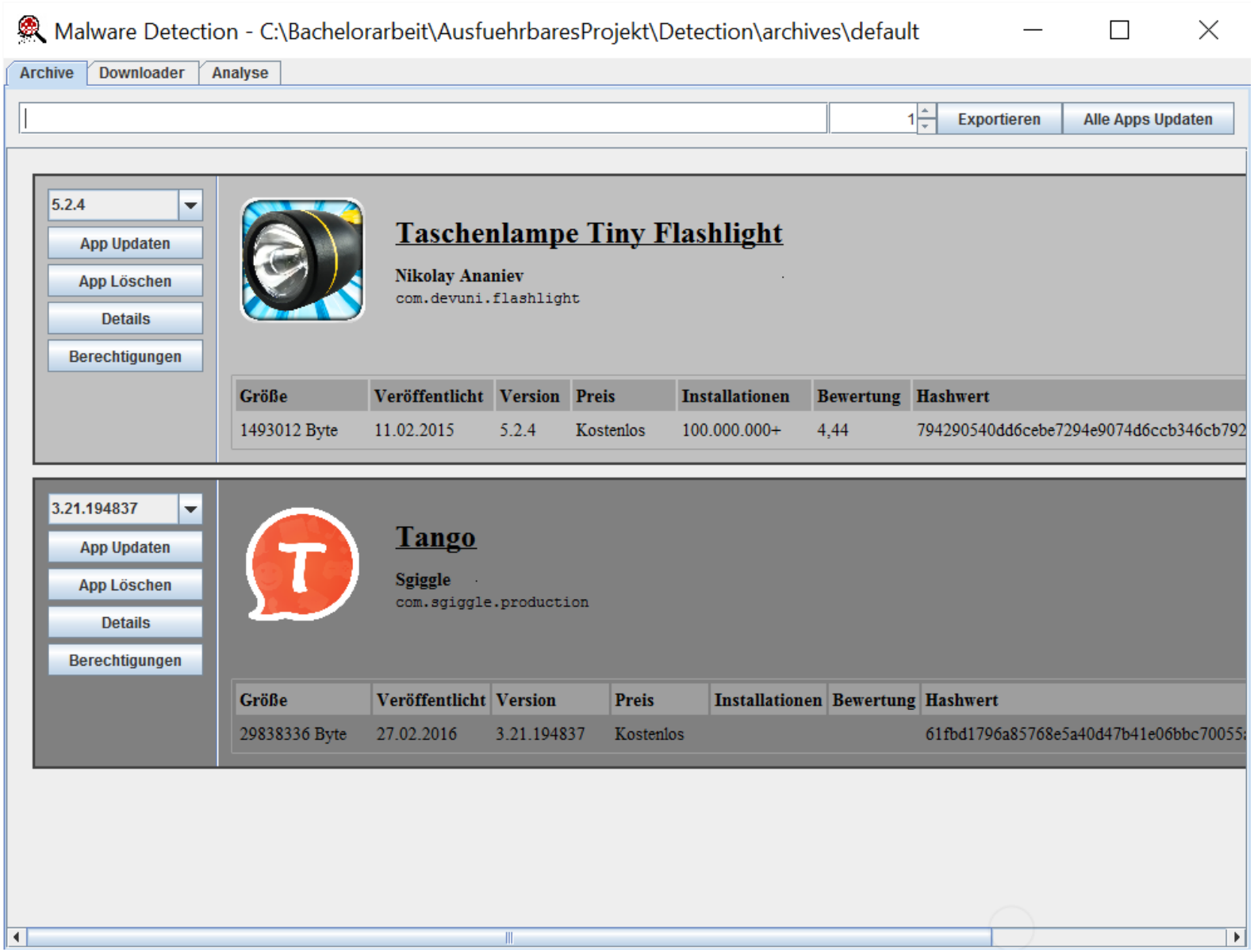
Der D. – Der Download(5/5)



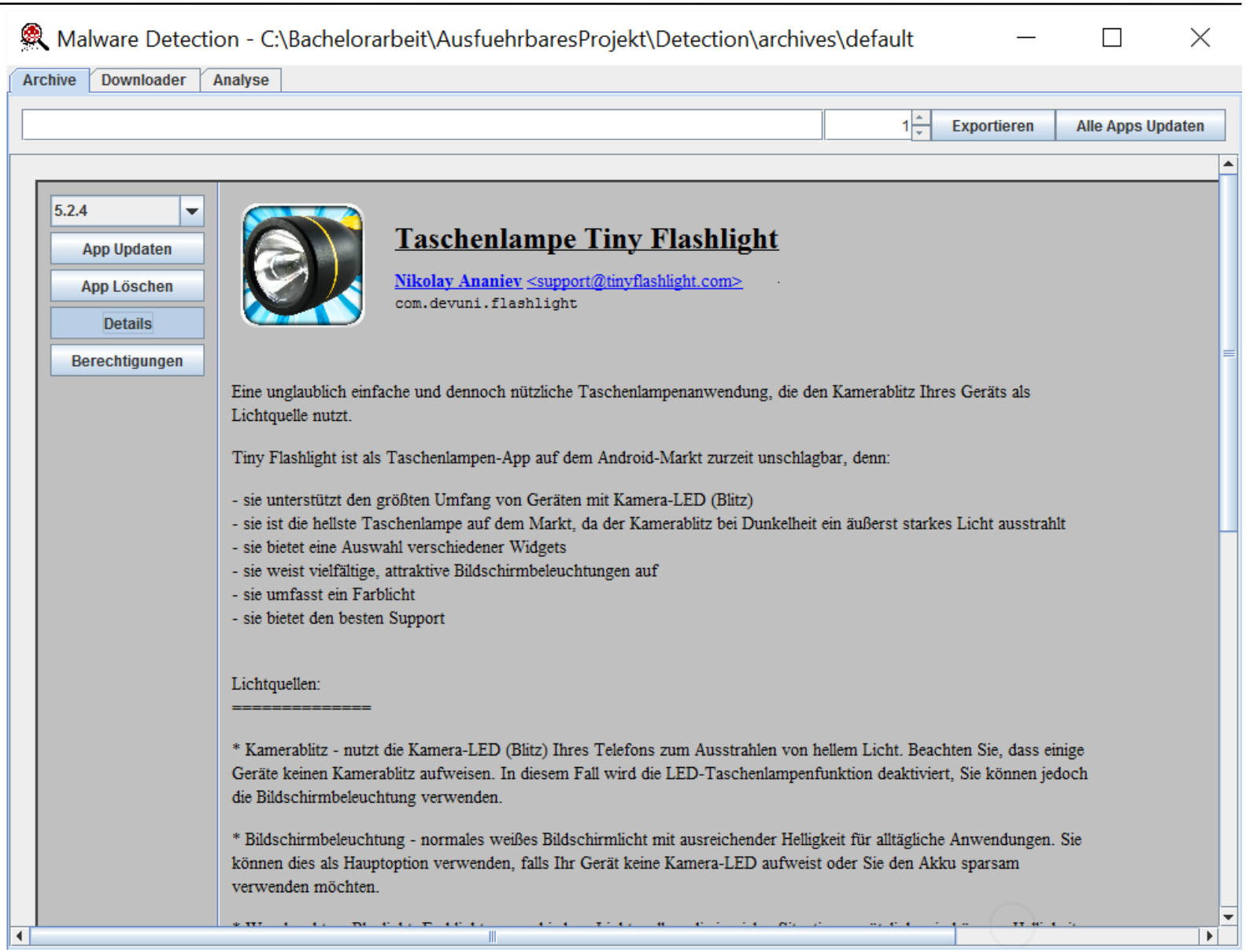
Der D. – Manuell hinzufügen



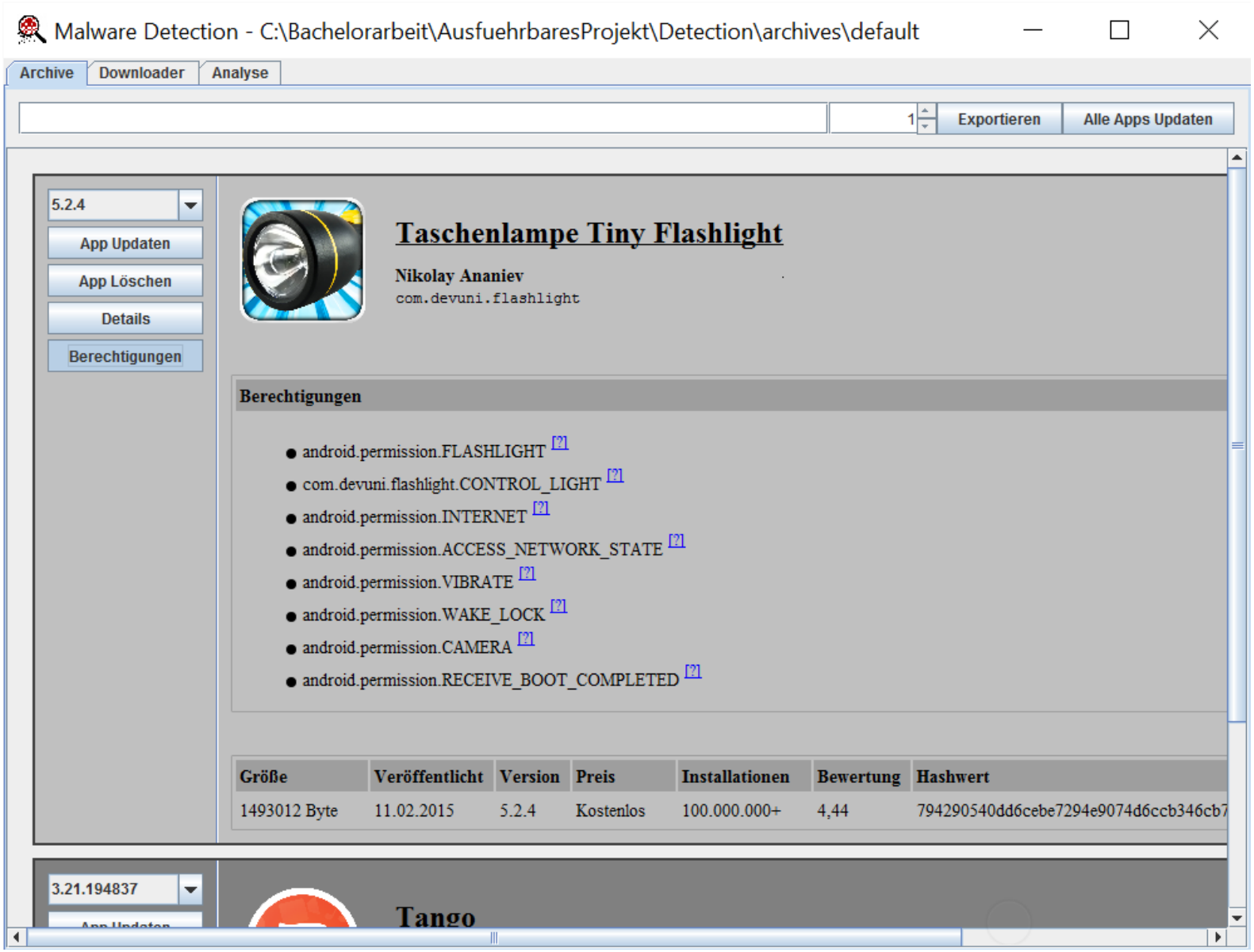
Das Archive - Benutzeroberfläche



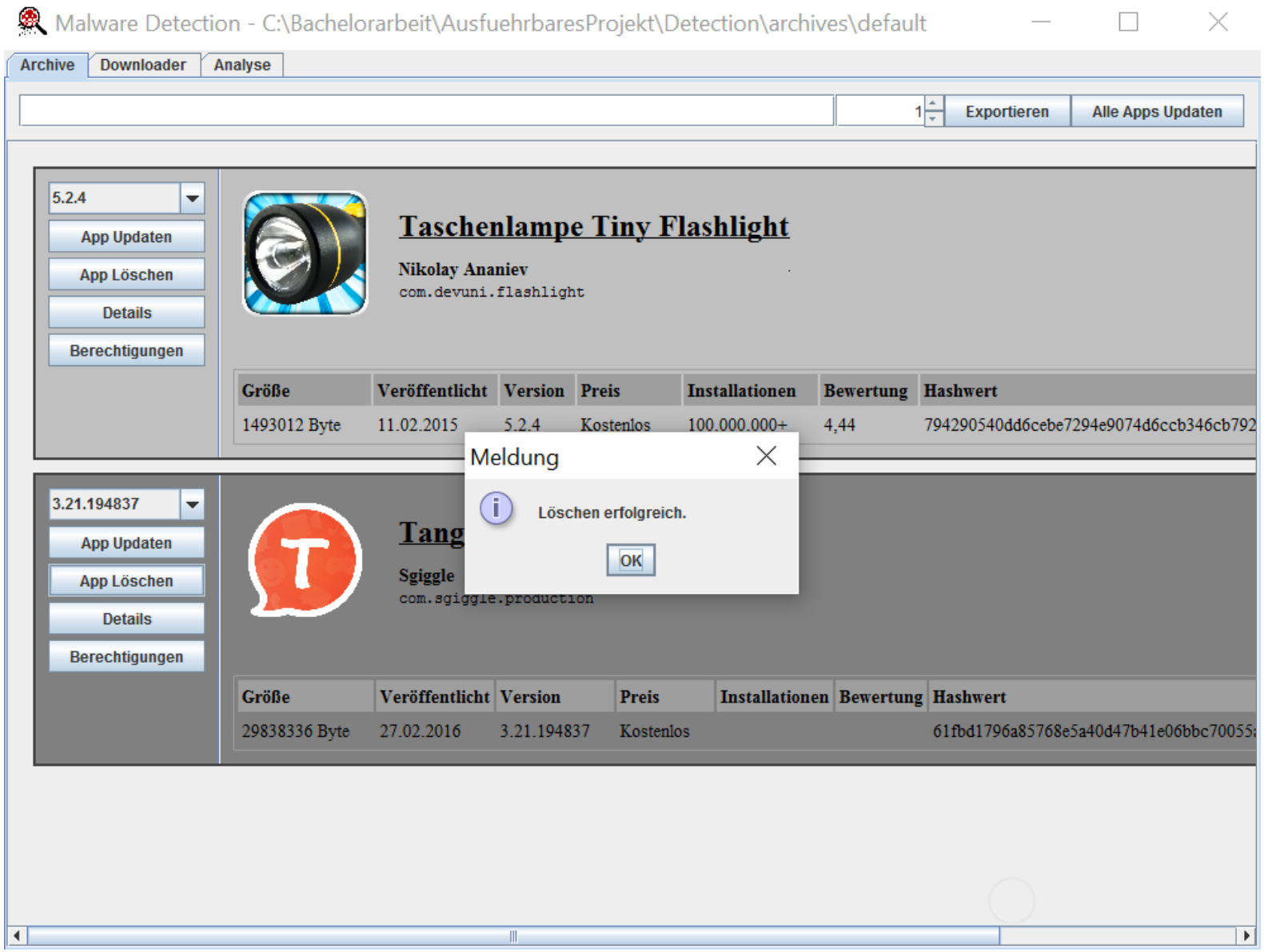
Das Archive - Details



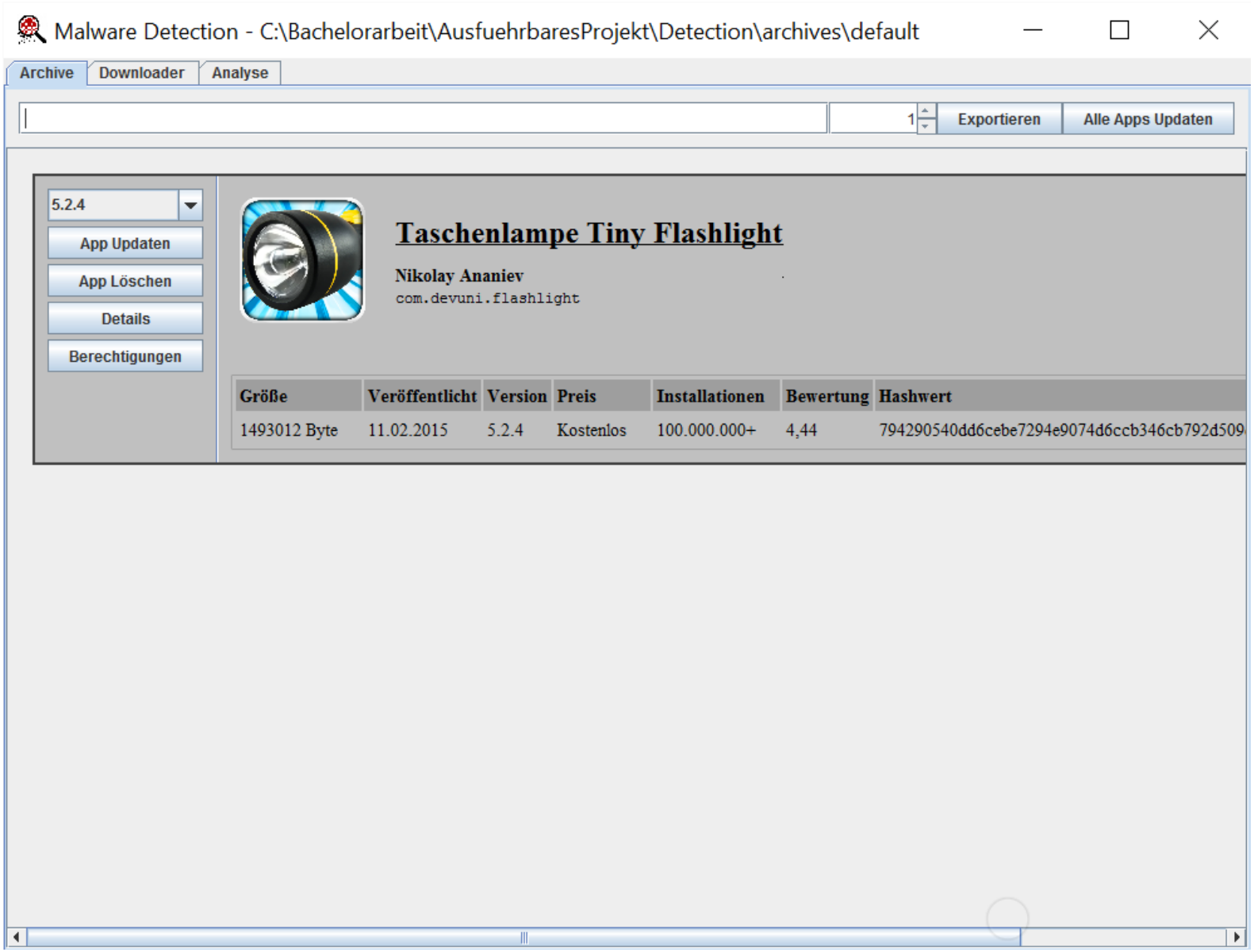
Das Archive - Berechtigungen



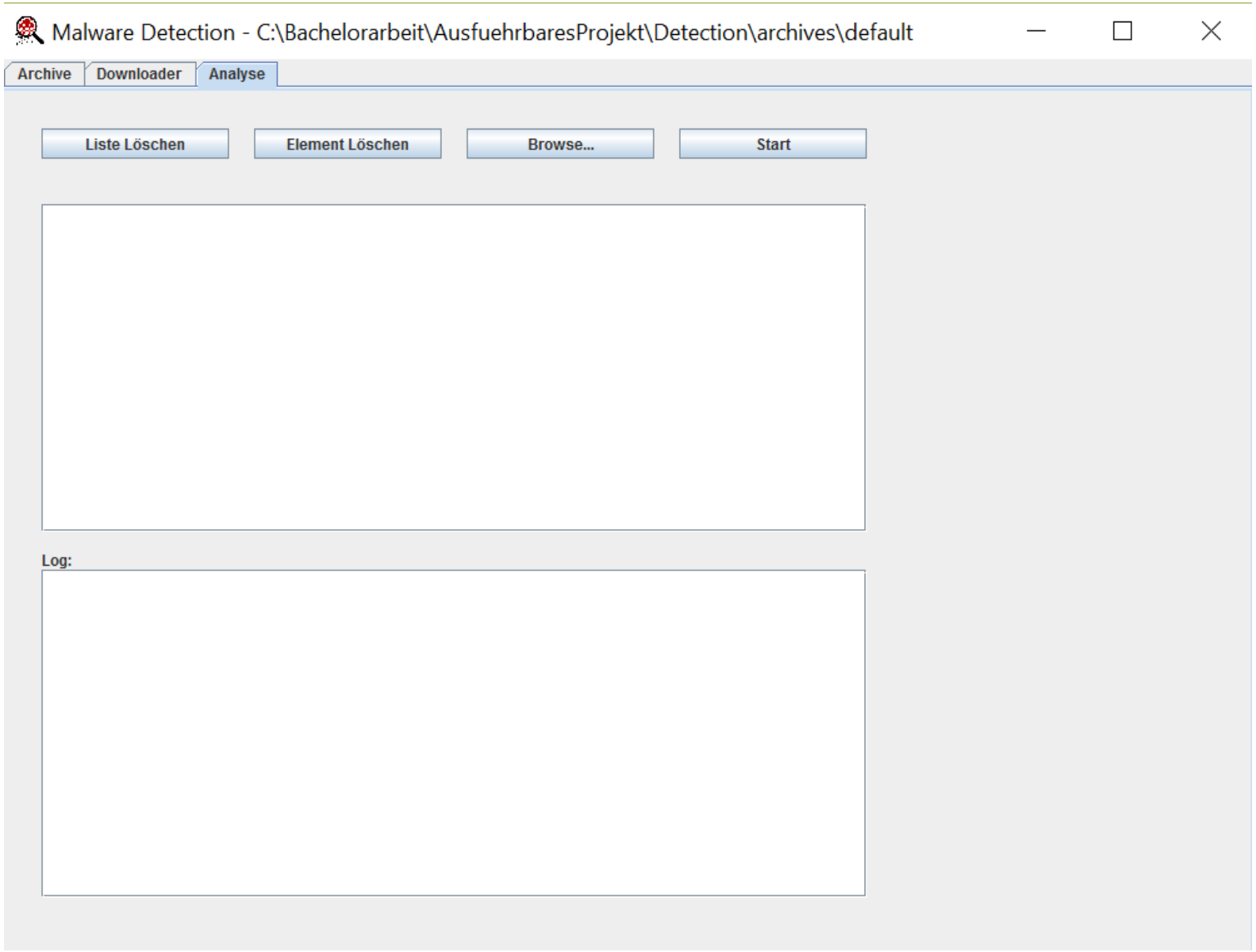
Das Archive – Löschen



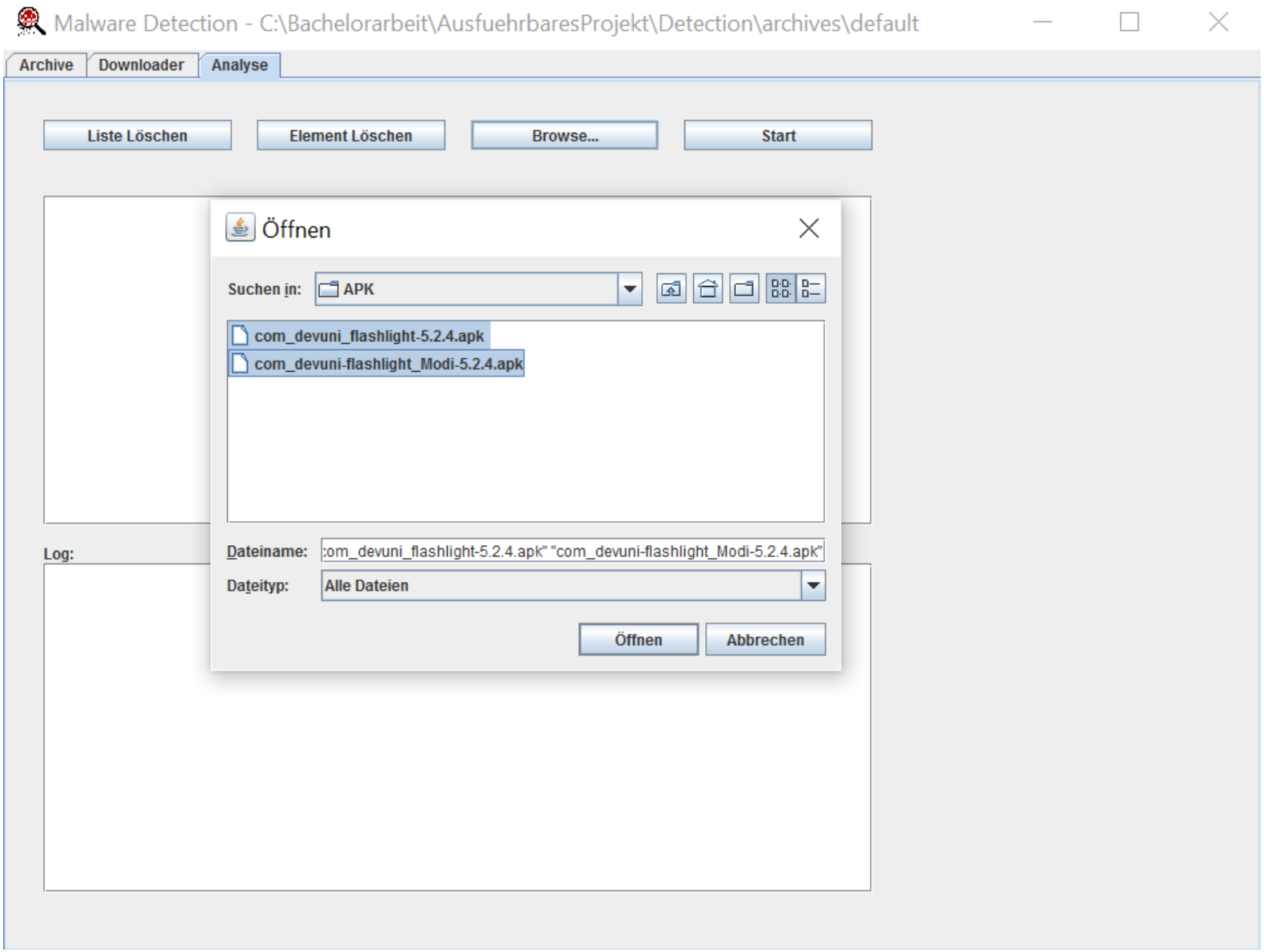
Das Archive – Nach dem Löschen



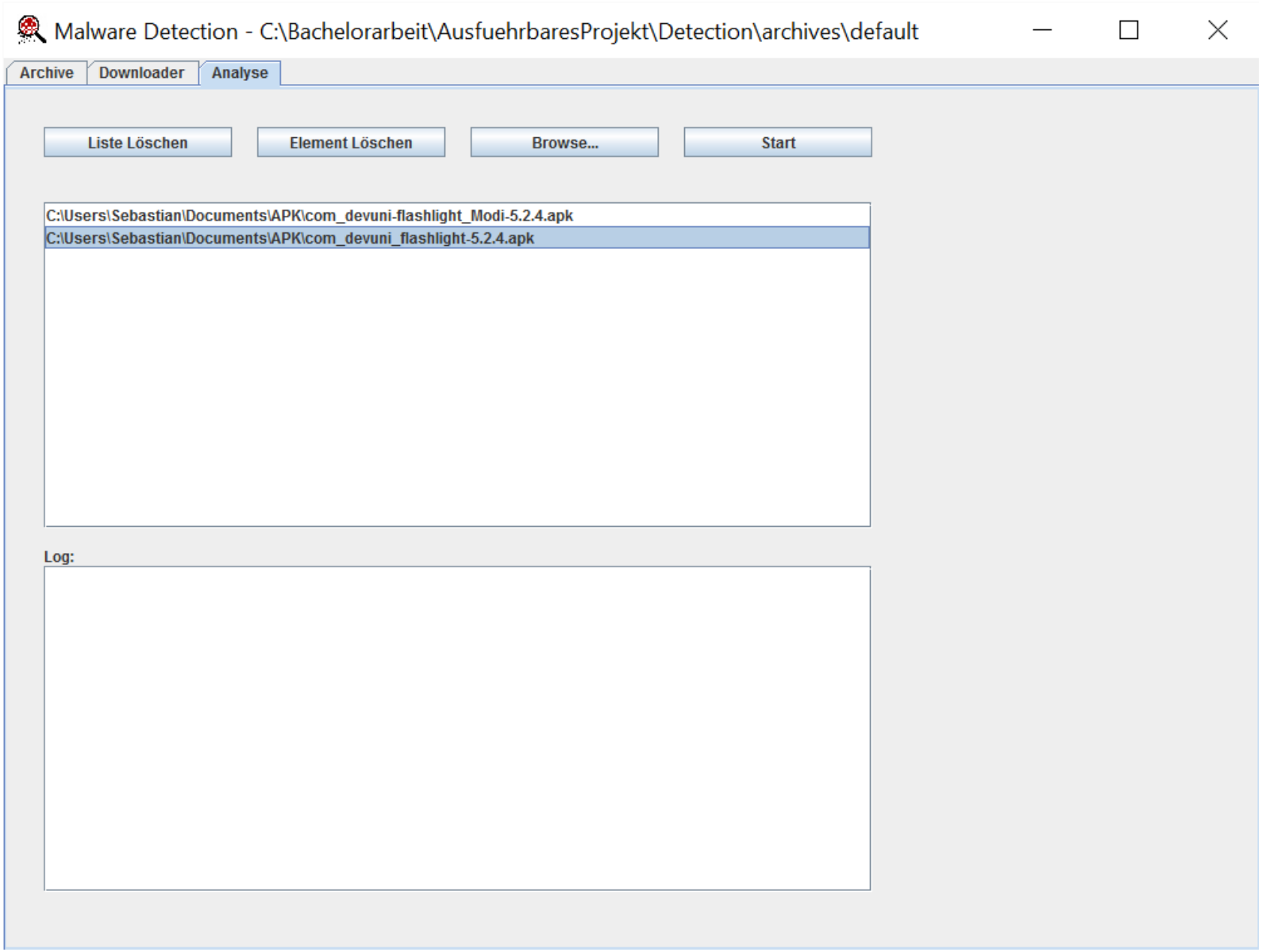
Die Analyse - Benutzeroberfläche



Die Analyse – App-Auswahl



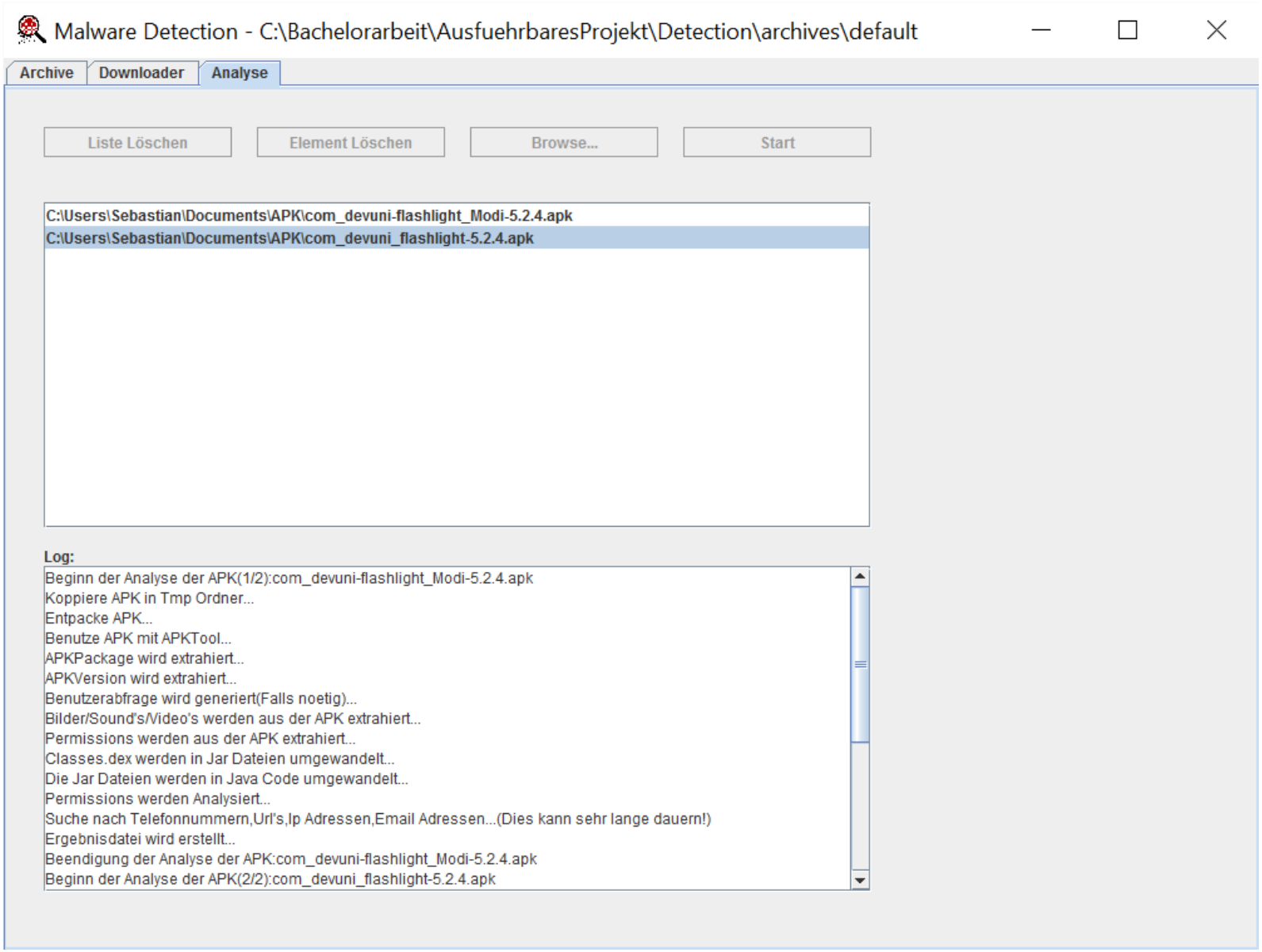
Die Analyse - Benutzeroberfläche



Die Analyse - Zwischenschritte

- Verifikation des Hashwertes (Archiv)
- APKTOOL: Zerlegt APK-Datei
  - Androidmanifest.xml wird decodiert
- 7ZipCore: Entpackt APK-Datei
  - Bilder, Videos, Sound können gefiltert werden
  - Classes.dex kann verwendet werden
- DexToJar: Jar-Datei wird erstellt
- JD-Core: Konvertiert Jar-Datei in Java-Code
- Alle wichtigen Informationen werden aus den generierten Dateien gefiltert.

Die A. – Analysieren der Testapps



Ergebnisse(1/2)

Testprotokoll

POLIZEI Nordrhein-Westfalen Landeskriminalamt

FH AACHEN UNIVERSITY OF APPLIED SCIENCES

App Daten:

AppName	com_devuni_flashlight-5.2.4.apk	**AppVersion**	5.2.4
AppPackage	com.devuni.flashlight	**HashWert**	794290540dd6cebe7294e9074

Das Risiko, dass diese App Malware enthält, liegt bei: 30 %

Es wurden 10 Permissions & Packages gefunden...

Hohes Risiko: (10%):

android.permission.CAMERA

Normales Risiko (60%):

Unbekannte Permissions & Packages: (30%)

Der Quellcode wurde durchlaufen und folgende Elemente gefunden:

Mögliche URL Adressen:

Es gab keinen Unterschied zwischen der Datenbank und der auszuwertenden App.

Ergebnisse(2/2)

Testprotokoll

POLIZEI Nordrhein-Westfalen Landeskriminalamt

App Daten:

AppName	com_devuni_flashlight_Modi-5.2.4.apk	**AppVersion**	5.2.4
AppPackage	com.devuni.flashlight	**HashWert**	7294f2c1c3e7db53ad84dac39194

Das Risiko, dass diese App Malware enthält, liegt bei: 32,727 %

Es wurden 11 Permissions & Packages gefunden...

Hohes Risiko: (18,182%):

android.permission.SEND_SMS

android.permission.CAMERA

Normales Risiko (54,545%):

Unbekannte Permissions & Packages: (27,273%)

Der Quellcode wurde durchlaufen und folgende Elemente gefunden:

Mögliche Telefonnummern:

/com/devuni/flashlight/d.java: +49123456789

Mögliche Ip-Addressen:

/com/google/android/gms/ads/b/a.java: 192.168.178.2

Mögliche URL Adressen:

Mögliche Email Adressen:

Es gab einen Unterschied zwischen der Datenbank und der auszuwertenden App:

Die Datei: res\drawable\screen_icon.png wurde in der zu Überprüfenden APK gelöscht!

Die Datei: res\drawable\test.txt wurde in der zu Überprüfenden APK hinzugefügt!

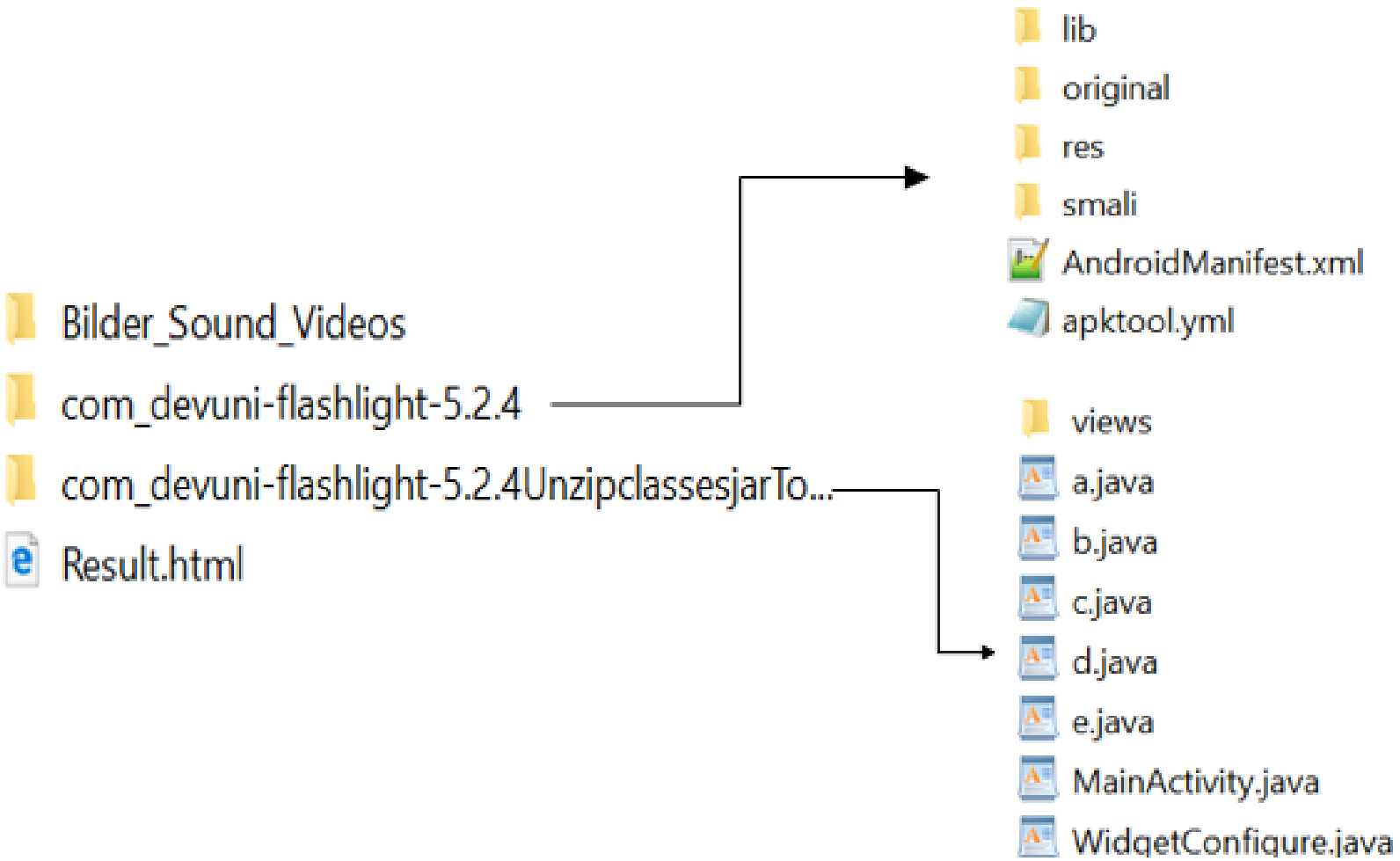
Die Datei: com\devuni\flashlight\b.javawurde verändert!

Die Datei: com\devuni\flashlight\d.javawurde verändert!

Die Datei: com\devuni\flashlight\MainActivity.javawurde verändert!

Die Datei: com\google\android\gms\ads\b\a.javawurde verändert!

Ergebnisordner



Probleme der Analyse

- Verschlüsselung erschwert das Finden von Informationen
- Informationen können dynamisch aufs Handy gelangen
- Obfuskierung des Quellcodes

Zusammenfassung

- Apps können auf Modifikationen geprüft werden
- Modifikationen werden angezeigt
- Nicht alle Informationen können aus der App gefiltert werden
- Ergebnisordner ermöglicht weitere Untersuchungen

FRAGEN?