

Untersuchen und Analysieren von Android- Apps auf Modifikation

Sebastian Becker, B. Sc.

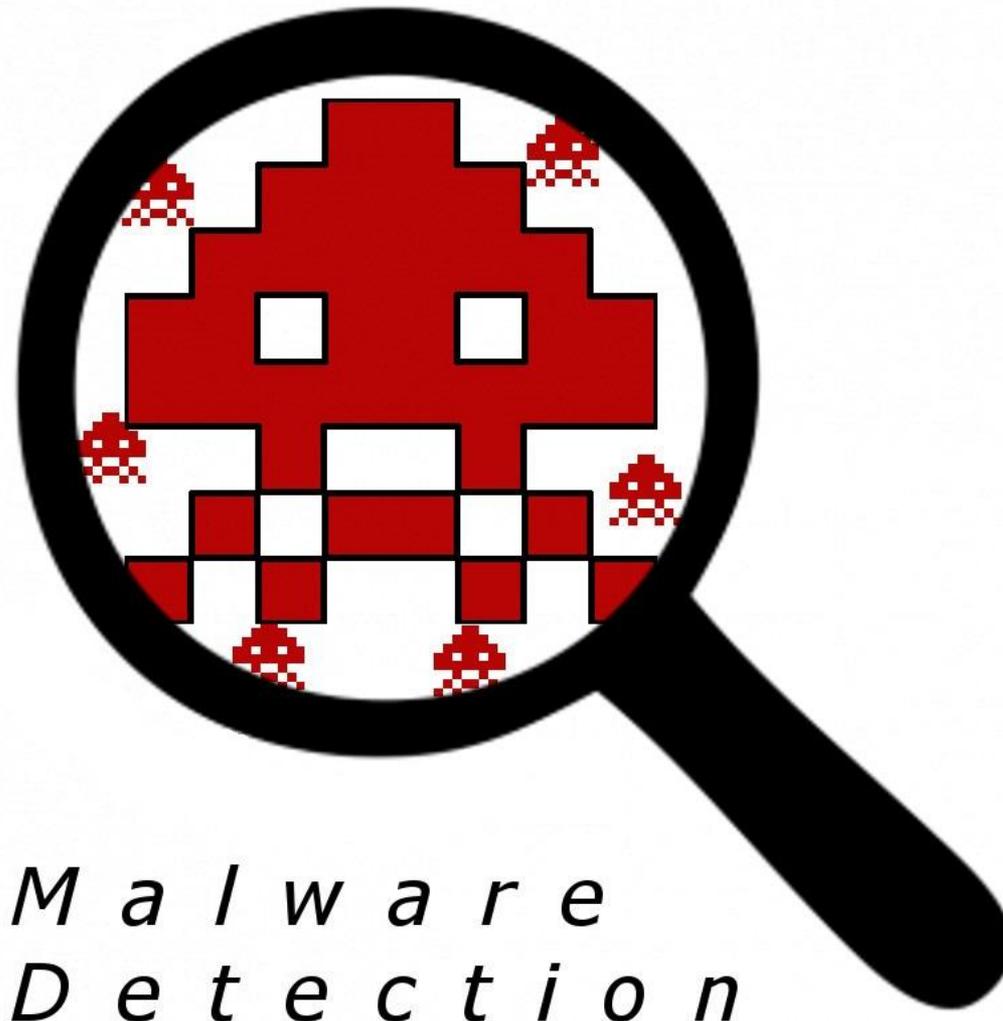
Lehrgebiet Datennetze, IT-Sicherheit
und IT-Forensik



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

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

- 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



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

Malware Detection - C:\Bachelorarbeit\AusfuehrbaresProjekt\Detection\archives\default

Archive Downloader Analyse

Apps suchen: tiny flashlight 1

App manuell Hinzufügen (*Pflichtfelder):

App Pfad*: Browse...

Appname*:

Installationen:

Rating:

Author:

Preis:

Datum:

Vcode:

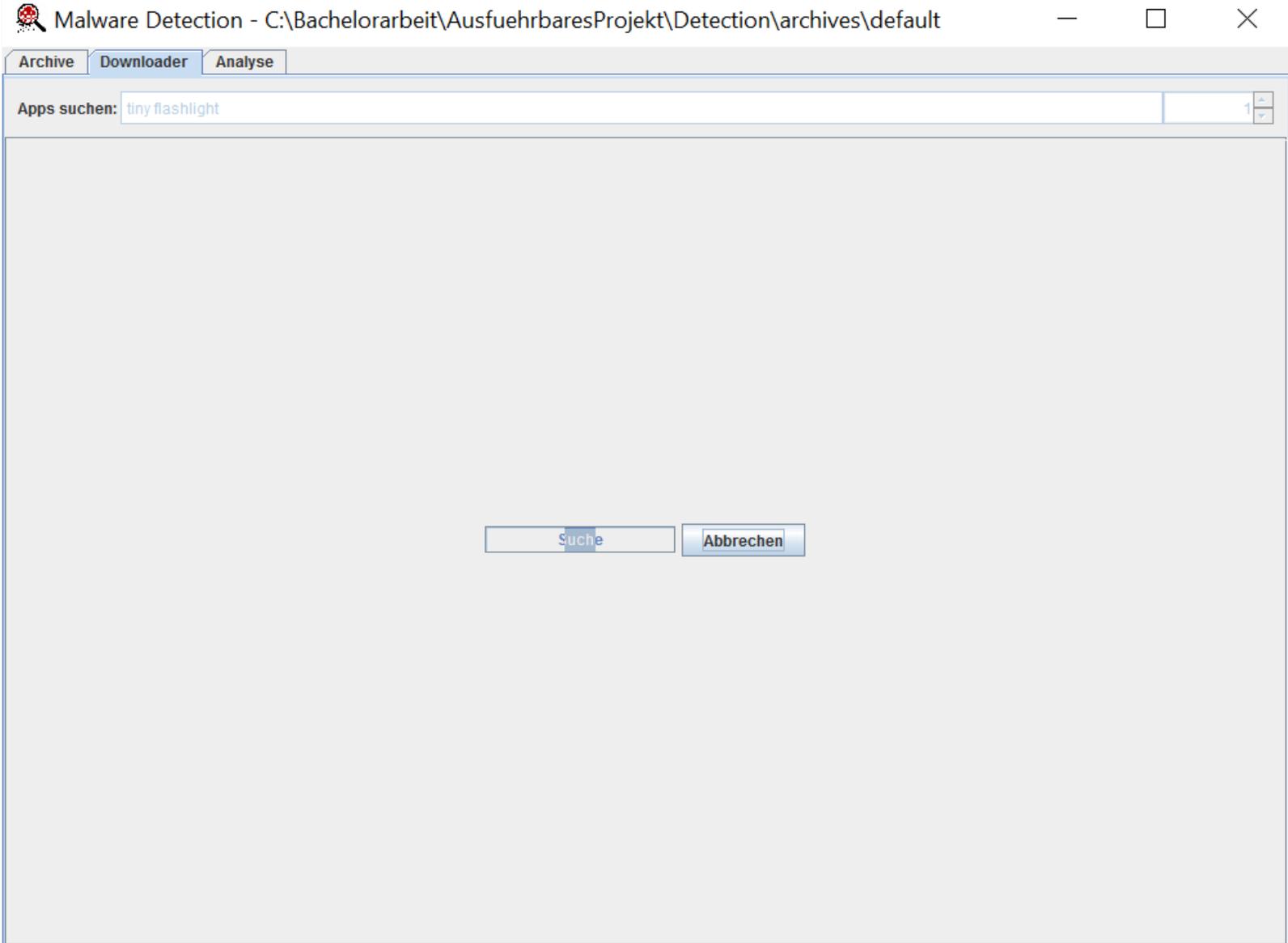
Website:

Email:

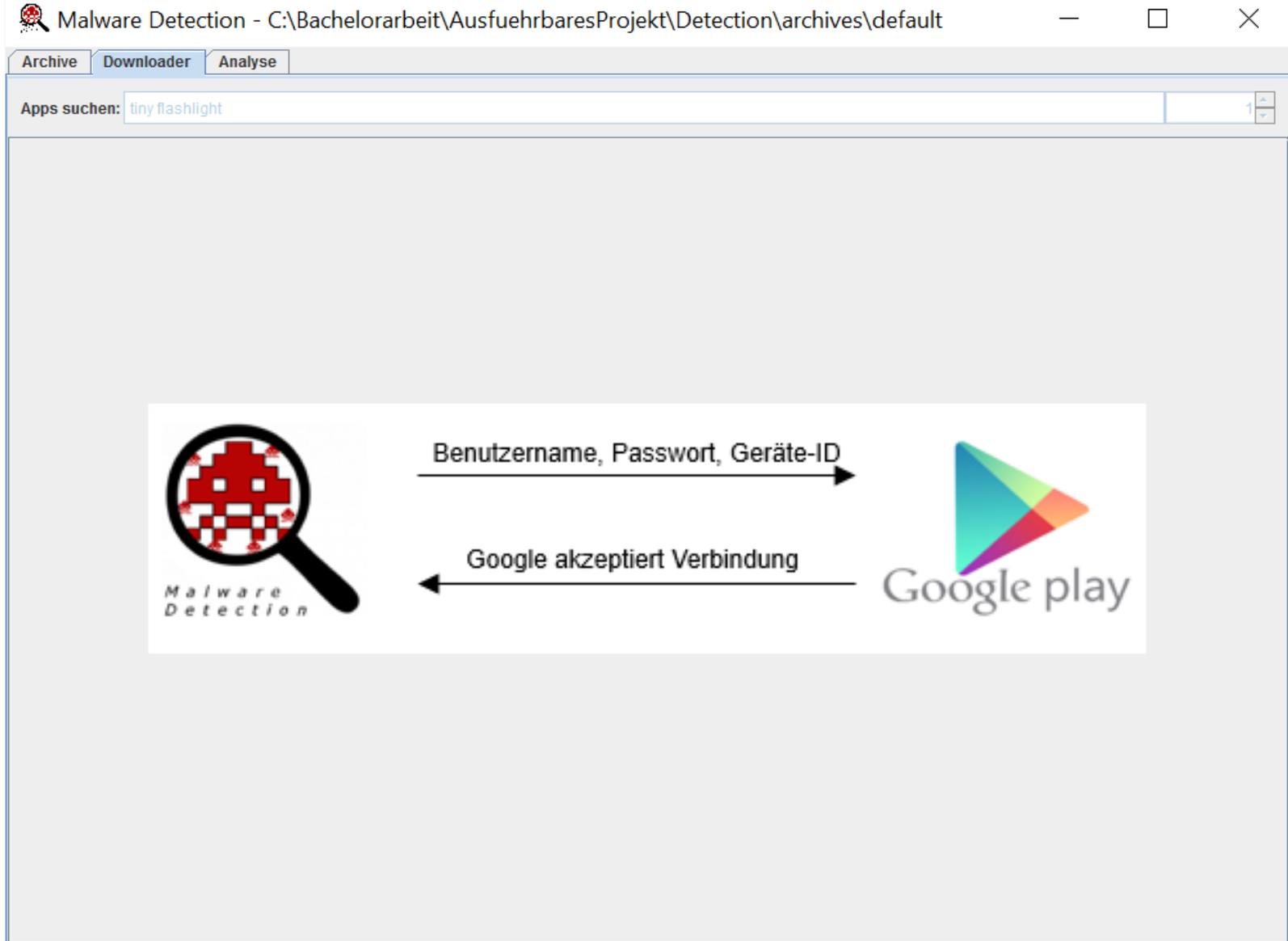
Beschreibung:

ChangeLog:

App Hinzufügen



Der D. – Verbindungsaufbau(1/2)



Malware Detection - C:\Bachelorarbeit\AusfuehrbaresProjekt\Detection\archives\default

Archive Downloader Analyse

Apps suchen: tiny flashlight

Suchbegriff wird an Google gesendet

Google sendet App-Liste zurück

Malware Detection - C:\Bachelorarbeit\AusfuehrbaresProjekt\Detection\archives\default

Archive | Downloader | Analyse

Apps suchen:

Download
Google Play
Details
Berechtigungen



Taschenlampe Tiny Flashlight
Nikolay Ananiev
com.devuni.flashlight

Größe	Veröffentlicht	Version	Preis	Installationen	Bewertung
1,5 MB	11.02.2015		Kostenlos	100.000.000+	4,44

Download
Google Play
Details
Berechtigungen



Superhelle LED Taschenlampe
Surpax Inc.
com.surpax.ledflashlight.panel

Größe	Veröffentlicht	Version	Preis	Installationen	Bewertung
5,1 MB	06.07.2015		Kostenlos	100.000.000+	4,55

Download
Google Play
Details
Berechtigungen



Tiny FlashLight
NeoTec Services
com.neotec.flashlight

Der D. – Der Download(1/5)

Malware Detection - C:\Bachelorarbeit\AusfuehrbaresProjekt\Detection\archives\default

Archive Downloader Analyse

Apps suchen: tiny flashlight

The diagram illustrates the interaction between Malware Detection and Google Play. On the left is the Malware Detection logo, which features a magnifying glass over a red pixelated character. On the right is the Google Play logo. Two horizontal arrows connect them: the top arrow points from Malware Detection to Google Play and is labeled 'Anfrage für Datenstream wird gestellt'; the bottom arrow points from Google Play back to Malware Detection and is labeled 'Datenstream wird aufgerufen und Download beginnt'.

Der D. – Der Download(2/5)

Malware Detection - C:\Bachelorarbeit\AusfuehrbaresProjekt\Detection\archives\default

Archive | **Downloader** | Analyse

Apps suchen: tiny flashlight



Taschenlampe Tiny Flashlight

Nikolay Ananiev
com.devuni.flashlight

C:\Bachelorarbeit\AusfuehrbaresProjekt\Detection\archives\default\apk_storage\com-devuni-flashlight\com_devuni_flashlight-5.2.4.apk

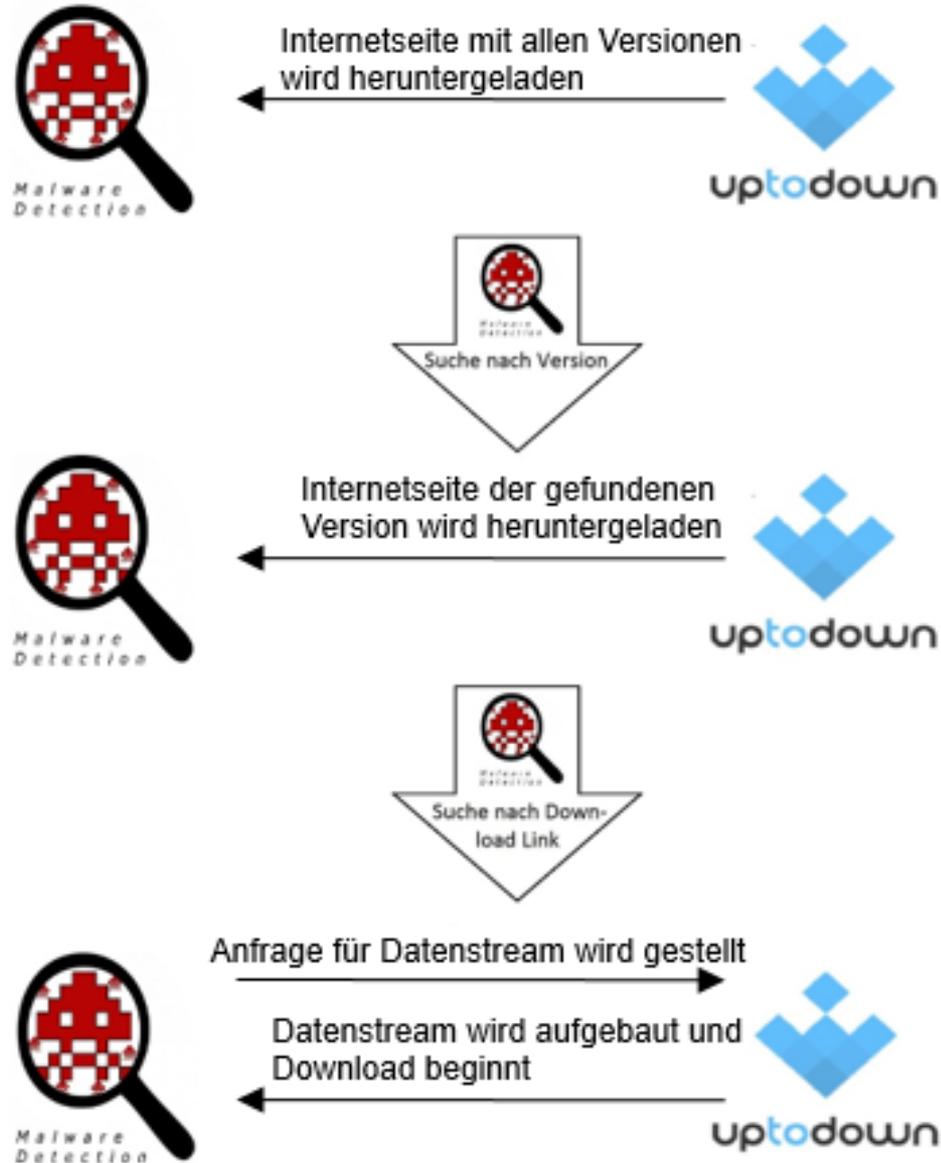
Warte

UpToDown Download(Taschenlampe ...)

 [App suchen -> Vorherige Versionen -> Link einfuegen](#)
<p://interna-tiny-flashlight.de.uptodown.com/android/old>

OK | Abbrechen

Der D. – Der Download(3/5)



Malware Detection - C:\Bachelorarbeit\AusfuehrbaresProjekt\Detection\archives\default

Archive Downloader Analyse

Apps suchen: tiny flashlight 1



Taschenlampe Tiny Flashlight

Nikolay Ananiev
com.devuni.flashlight

C:\Bachelorarbeit\AusfuehrbaresProjekt\Detection\archives\default\apk_storage\com-devuni-flashlight\

- com_devuni_flashlight-5.2.4.apk
- com_devuni_flashlight-5.2.3.apk
- com_devuni_flashlight-5.2.2.apk
- com_devuni_flashlight-5.2.1.apk
- com_devuni_flashlight-5.2.apk
- com_devuni_flashlight-5.1.5.apk
- com_devuni_flashlight-5.1.4.apk
- com_devuni_flashlight-5.1.3.apk

Warte

Malware Detection - C:\Bachelorarbeit\AusfuehrbaresProjekt\Detection\archives\default

Archive Downloader Analyse

Apps suchen: tiny flashlight 1



Taschenlampe Tiny Flashlight

Nikolay Ananiev
com.devuni.flashlight

C:\Bachelorarbeit\AusfuehrbaresProjekt\Detection\archives\default\apk_storage\com-devuni-flashlight\

- com_devuni_flashlight-5.2.4.apk
- com_devuni_flashlight-5.2.3.apk
- com_devuni_flashlight-5.2.2.apk
- com_devuni_flashlight-5.2.1.apk
- com_devuni_flashlight-5.2.apk
- com_devuni_flashlight-5.1.5.apk
- com_devuni_flashlight-5.1.4.apk
- com_devuni_flashlight-5.1.3.apk
- com_devuni_flashlight-5.1.1.apk
- com_devuni_flashlight-5.1.apk
- com_devuni_flashlight-5.0.2.apk
- com_devuni_flashlight-4.9.7.apk
- com_devuni_flashlight-4.9.6.apk

Fertig

Der D. – Manuell hinzufügen

Malware Detection - C:\Bachelorarbeit\AusfuehrbaresProjekt\Detect... — □ ×

Archive **Downloader** Analyse

Apps suchen: 1

App manuell Hinzufügen (*Pflichtfelder):

App Pfad*:

Appname*:

Installationen:

Rating:

Author:

Preis:

Datum:

Vcode:

Website:

Email:

Beschreibung

ChangeLog:

Das Archive - Benutzeroberfläche

Malware Detection - C:\Bachelorarbeit\AusfuehrbaresProjekt\Detection\archives\default

Archive | Downloader | Analyse

1 | Exportieren | Alle Apps Updaten

5.2.4

App Updaten

App Löschen

Details

Berechtigungen



Taschenlampe Tiny Flashlight

Nikolay Ananiev
com.devuni.flashlight

Größe	Veröffentlicht	Version	Preis	Installationen	Bewertung	Hashwert
1493012 Byte	11.02.2015	5.2.4	Kostenlos	100.000.000+	4,44	794290540dd6cebe7294e9074d6ccb346cb792

3.21.194837

App Updaten

App Löschen

Details

Berechtigungen



Tango

Sgiggle
com.sgiggle.production

Größe	Veröffentlicht	Version	Preis	Installationen	Bewertung	Hashwert
29838336 Byte	27.02.2016	3.21.194837	Kostenlos			61fbd1796a85768e5a40d47b41e06bbc70055

Malware Detection - C:\Bachelorarbeit\AusfuehrbaresProjekt\Detection\archives\default
— □ ×

Archive Downloader Analyse

1 Exportieren Alle Apps Updaten

5.2.4

App Updaten

App Löschen

Details

Berechtigungen



Taschenlampe Tiny Flashlight

[Nikolay Ananiev](mailto:support@tinyflashlight.com) <support@tinyflashlight.com>
com.devuni.flashlight

Eine unglaublich einfache und dennoch nützliche Taschenlampenanwendung, die den Kamerablitz Ihres Geräts als Lichtquelle nutzt.

Tiny Flashlight ist als Taschenlampen-App auf dem Android-Markt zurzeit unschlagbar, denn:

- sie unterstützt den größten Umfang von Geräten mit Kamera-LED (Blitz)
- sie ist die hellste Taschenlampe auf dem Markt, da der Kamerablitz bei Dunkelheit ein äußerst starkes Licht ausstrahlt
- sie bietet eine Auswahl verschiedener Widgets
- sie weist vielfältige, attraktive Bildschirmbeleuchtungen auf
- sie umfasst ein Farblicht
- sie bietet den besten Support

Lichtquellen:

* Kamerablitz - nutzt die Kamera-LED (Blitz) Ihres Telefons zum Ausstrahlen von hellem Licht. Beachten Sie, dass einige Geräte keinen Kamerablitz aufweisen. In diesem Fall wird die LED-Taschenlampenfunktion deaktiviert, Sie können jedoch die Bildschirmbeleuchtung verwenden.

* Bildschirmbeleuchtung - normales weißes Bildschirmlicht mit ausreichender Helligkeit für alltägliche Anwendungen. Sie können dies als Hauptoption verwenden, falls Ihr Gerät keine Kamera-LED aufweist oder Sie den Akku sparsam verwenden möchten.

Malware Detection - C:\Bachelorarbeit\AusfuehrbaresProjekt\Detection\archives\default

Archive Downloader Analyse

1 Exportieren Alle Apps Updaten

5.2.4

App Updaten

App Löschen

Details

Berechtigungen



Taschenlampe Tiny Flashlight

Nikolay Ananiev
com.devuni.flashlight

Berechtigungen

- android.permission.FLASHLIGHT [\[?\]](#)
- com.devuni.flashlight.CONTROL_LIGHT [\[?\]](#)
- android.permission.INTERNET [\[?\]](#)
- android.permission.ACCESS_NETWORK_STATE [\[?\]](#)
- android.permission.VIBRATE [\[?\]](#)
- android.permission.WAKE_LOCK [\[?\]](#)
- android.permission.CAMERA [\[?\]](#)
- android.permission.RECEIVE_BOOT_COMPLETED [\[?\]](#)

Größe	Veröffentlicht	Version	Preis	Installationen	Bewertung	Hashwert
1493012 Byte	11.02.2015	5.2.4	Kostenlos	100.000.000+	4,44	794290540dd6cebe7294e9074d6ccb346cb7

3.21.194837

App Updaten



Tango

Malware Detection - C:\Bachelorarbeit\AusfuehrbaresProjekt\Detection\archives\default

Archive | Downloader | Analyse

1 | Exportieren | Alle Apps Updaten

5.2.4

App Updaten

App Löschen

Details

Berechtigungen



Taschenlampe Tiny Flashlight

Nikolay Ananiev
com.devuni.flashlight

Größe	Veröffentlicht	Version	Preis	Installationen	Bewertung	Hashwert
1493012 Byte	11.02.2015	5.2.4	Kostenlos	100.000.000+	4,44	794290540dd6cebe7294e9074d6ccb346cb792

3.21.194837

App Updaten

App Löschen

Details

Berechtigungen



Tang

Sgiggle
com.sgiggle.production

Größe	Veröffentlicht	Version	Preis	Installationen	Bewertung	Hashwert
29838336 Byte	27.02.2016	3.21.194837	Kostenlos			61fbd1796a85768e5a40d47b41e06bbc70055

Meldung

 Löschen erfolgreich.

OK

Malware Detection - C:\Bachelorarbeit\AusfuehrbaresProjekt\Detection\archives\default

Archive Downloader Analyse

1 Exportieren Alle Apps Updaten

5.2.4

App Updaten

App Löschen

Details

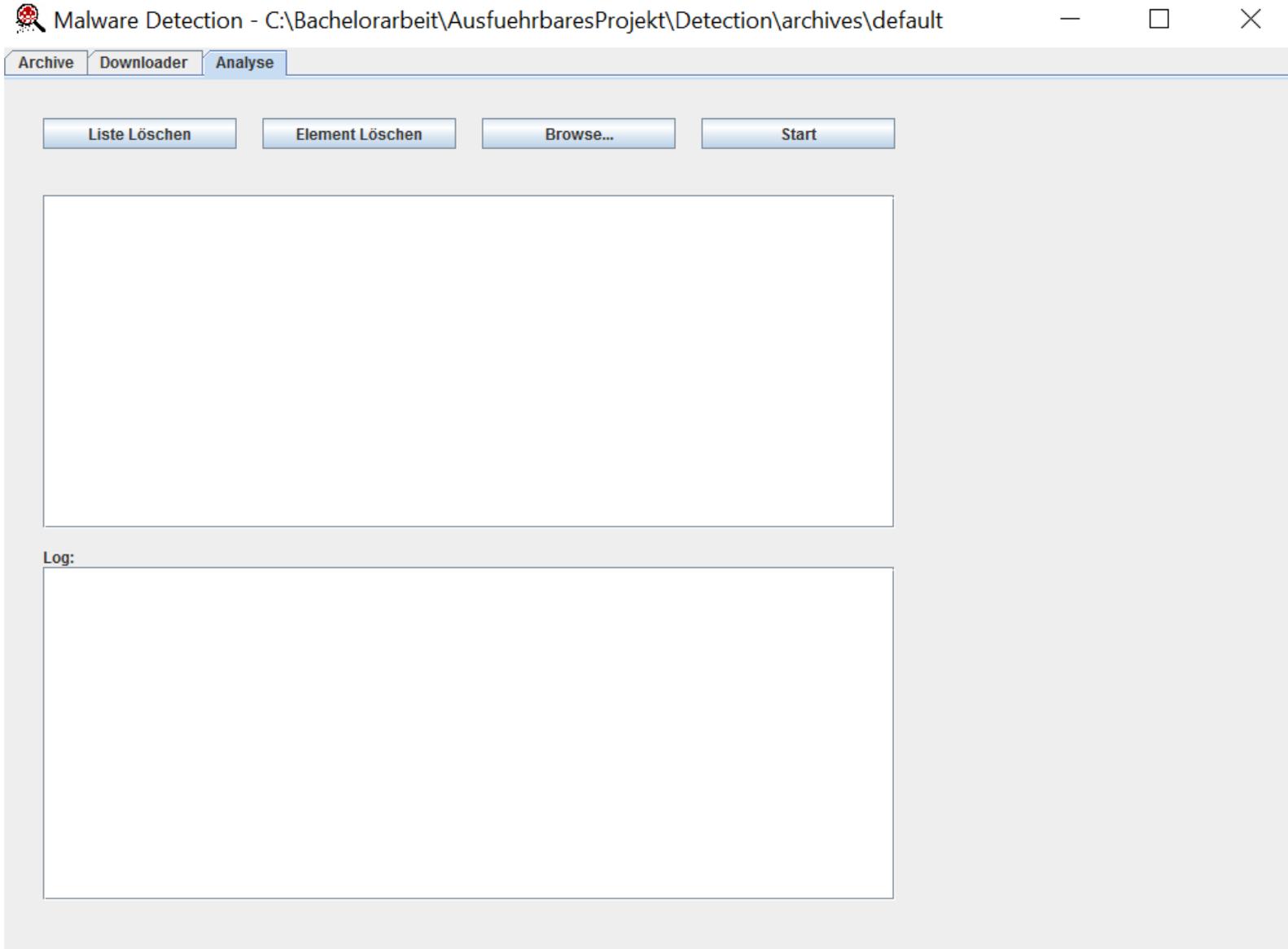
Berechtigungen

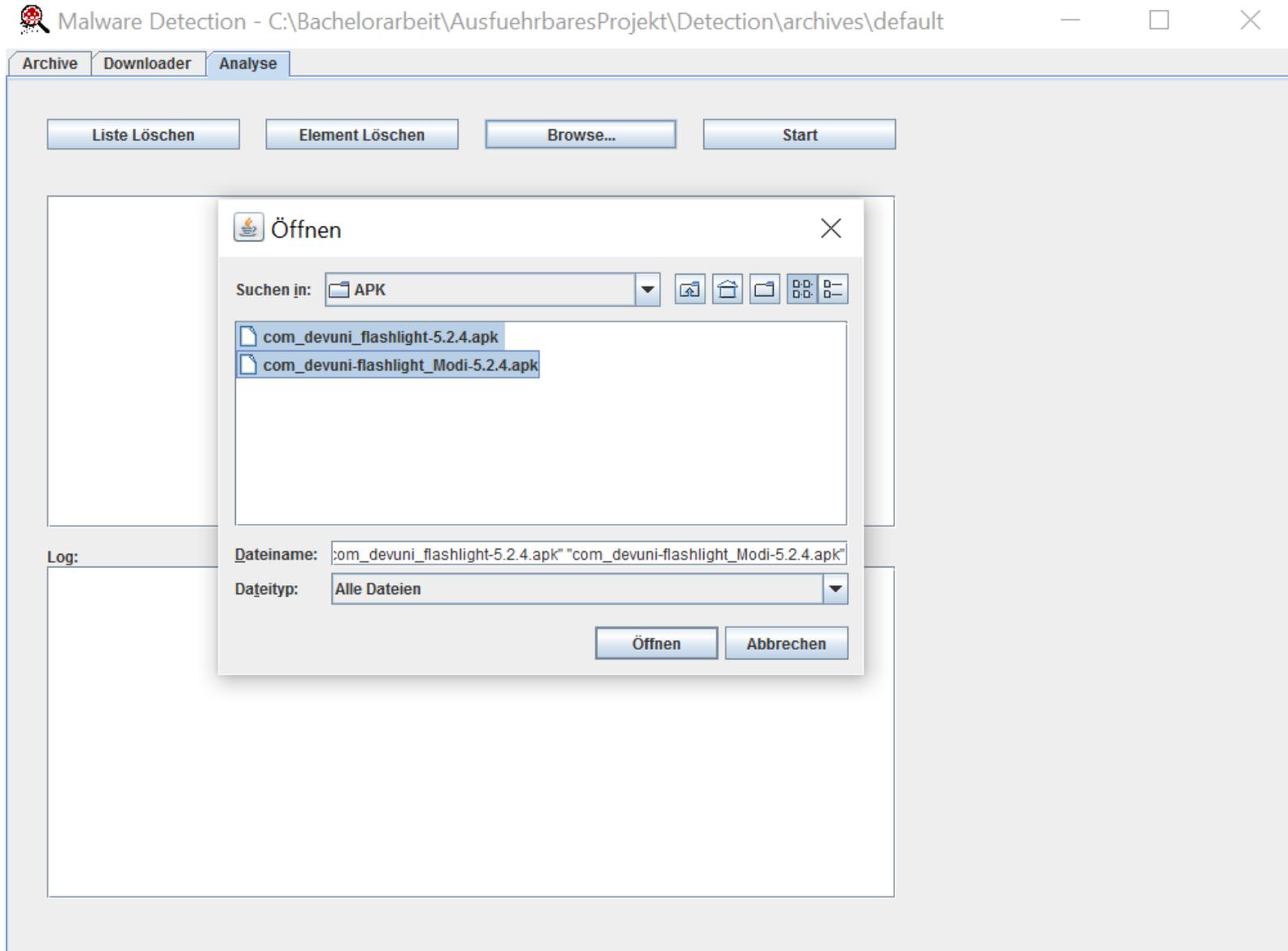


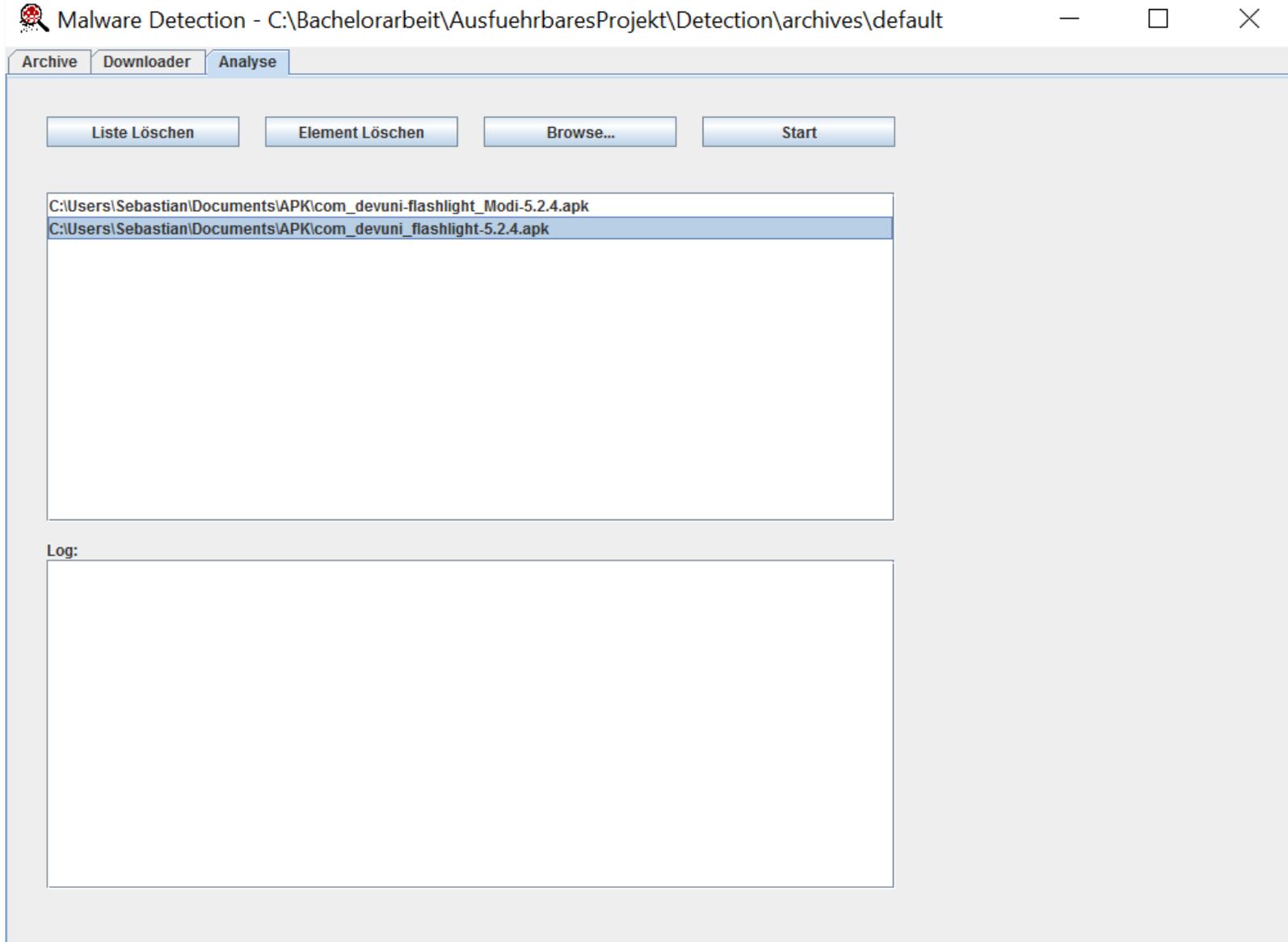
Taschenlampe Tiny Flashlight

Nikolay Ananiev
com.devuni.flashlight

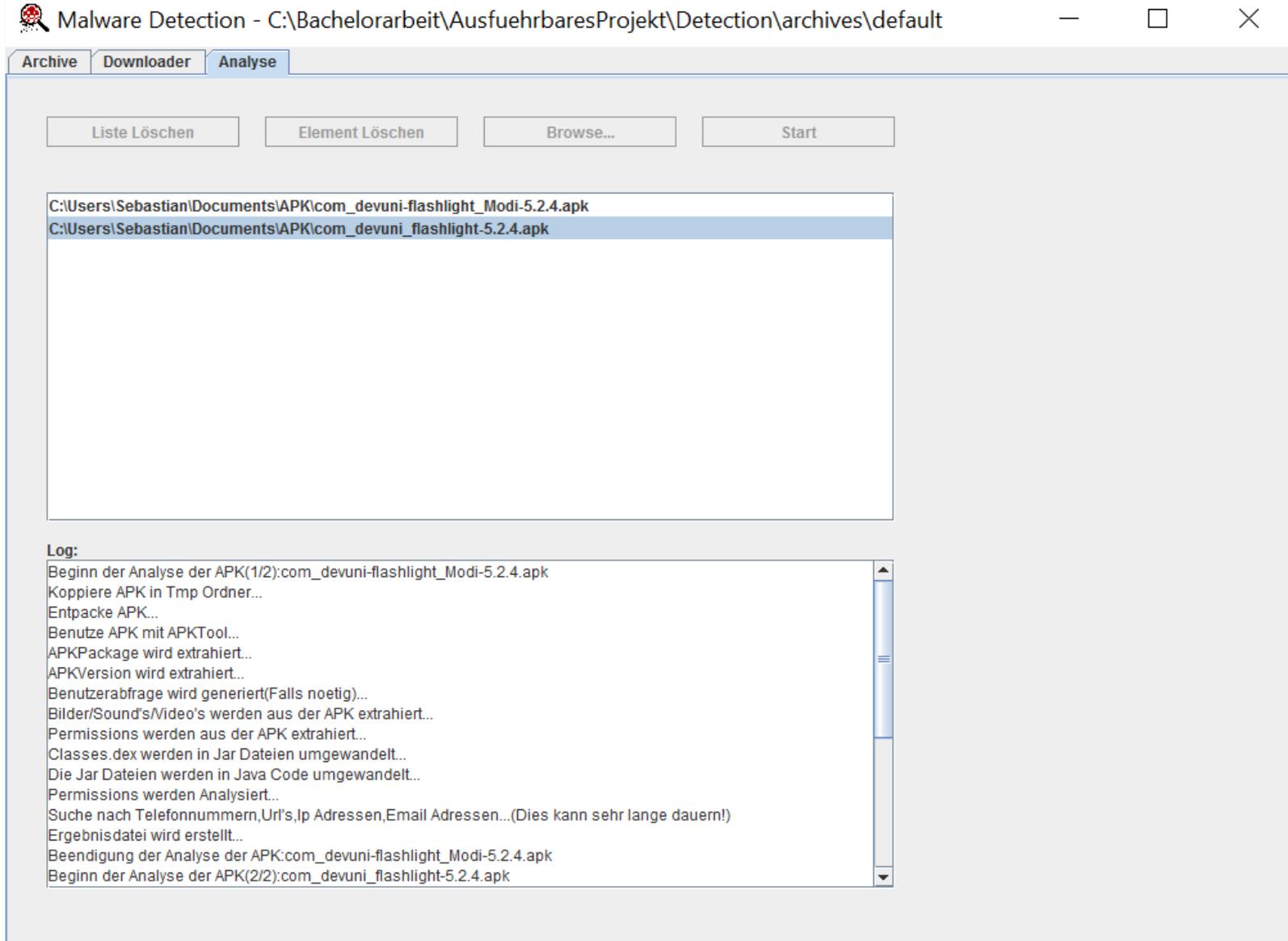
Größe	Veröffentlicht	Version	Preis	Installationen	Bewertung	Hashwert
1493012 Byte	11.02.2015	5.2.4	Kostenlos	100.000.000+	4,44	794290540dd6cebe7294e9074d6ccb346cb792d509







- 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.



The screenshot shows a window titled "Malware Detection - C:\Bachelorarbeit\AusfuehrbaresProjekt\Detection\archives\default". The window has three tabs: "Archive", "Downloader", and "Analyse". Below the tabs are four buttons: "Liste Löschen", "Element Löschen", "Browse...", and "Start". A list box contains two entries: "C:\Users\Sebastian\Documents\APK\com_devuni_flashlight_Modi-5.2.4.apk" and "C:\Users\Sebastian\Documents\APK\com_devuni_flashlight-5.2.4.apk". Below the list box is a "Log:" section with a scrollable text area containing the following text:

```
Log:  
Beginn der Analyse der APK(1/2):com_devuni_flashlight_Modi-5.2.4.apk  
Kopiere APK in Tmp Ordner...  
Entpacke APK...  
Benutze APK mit APKTool...  
APKPackage wird extrahiert...  
APKVersion wird extrahiert...  
Benutzerabfrage wird generiert(Falls noetig)...  
Bilder/Sound's/Video's werden aus der APK extrahiert...  
Permissions werden aus der APK extrahiert...  
Classes.dex werden in Jar Dateien umgewandelt...  
Die Jar Dateien werden in Java Code umgewandelt...  
Permissions werden Analysiert...  
Suche nach Telefonnummern,Uri's,Ip Adressen,Email Adressen...(Dies kann sehr lange dauern!)  
Ergebnisdatei wird erstellt...  
Beendigung der Analyse der APK:com_devuni_flashlight_Modi-5.2.4.apk  
Beginn der Analyse der APK(2/2):com_devuni_flashlight-5.2.4.apk
```

Testprotokoll



POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

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.

Testprotokoll



App Daten:

AppName	com_devuni_flashlight_Modi-5.2.4.apk	AppVersion	5.2.4
AppPackage	com.devuni.flashlight	HashWert	7294f2c1c3e7db53ad84dac39194d

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-Adressen:

/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!

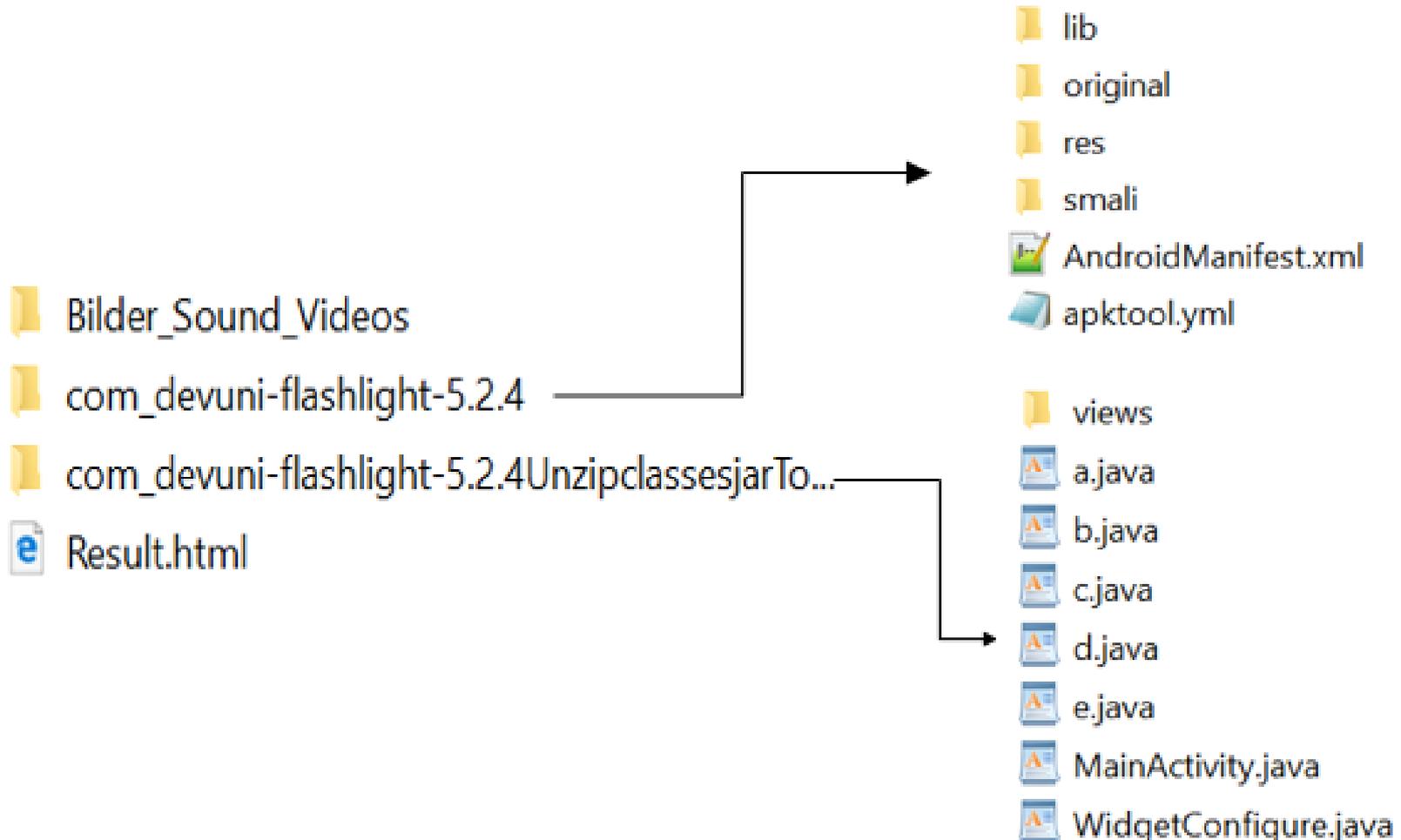
Die Datei: res\drawable\test.txt wurde in der zu Überprüfenden APK hinzugefügt!

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!



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

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

