Technische Berichte in Digitaler Forensik

Herausgegeben vom Lehrstuhl für Informatik 1 der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) in Kooperation mit dem Masterstudiengang Digitale Forensik (Hochschule Albstadt-Sigmaringen, FAU, Goethe-Universität Frankfurt am Main)

Anwendungsanalyse des Download-Managers *JDownloader* Version 2.0 Beta (Rev. 32397) - Microsoft Windows

Marius Reckers

26. Februar 2016

Technischer Bericht Nr. 3

Zusammenfassung

Sogenannte One-Click-Hoster werden heutzutage vermehrt zur illegalen Verbreitung von urheberrechtlich geschützten Inhalten genutzt und stehen in diesem Zusammenhang häufig in der Kritik von Rechtsinhabern. Aufgrund der marktführenden Stellung und der Spezialisierung im Umgang mit solchen One-Click-Hostern, wird der Download-Manager »*JDownloader*« vorzugsweise für den automatisierten Bezug von urheberrechtlich geschützten Material verwendet. Die Anwendung steht im Zuge dessen regelmäßig im Fokus digitalforensischer Untersuchungen hinsichtlich Vergehen gegen das Urheberrechtsgesetz im Internet. Die im vorliegenden Bericht beschriebenen Ergebnisse der Anwendungsanalyse sollen genutzt werden, um persistente Spuren des JDownloaders sowohl zu identifizieren als auch interpretieren zu können und anhand dessen vorangegangene Benutzerinteraktionen zu rekonstruieren.

Entstanden im Rahmen des Moduls Browser- und Anwendungsforensik des Studiengangs Digitale Forensik im Wintersemester 2015/2016 unter der Anleitung von Felix Freiling, Holger Morgenstern und Michael Gruhn.

Inhalt

Abbildungsverzeichnis **III**

Tabellenverzeichnis **IV**

Listingverzeichnis **V**

1 Einführung **1**

1.1 Projektauftrag . . . 1
1.2 Untersuchungsobjekt . . . 1
1.3 Arbeitsumgebung . . . 2
1.4 Berichtsstruktur . . . 3

2 Technische Anwendungsanalyse **4**

2.1 JDownloader - Ein Überblick . . . 4
2.2 Generelle Vorgehensweise . . . 5
2.3 Persistente Spurenmenge . . . 6
2.3.1 Installationsroutine (Adware) . . . 7
2.3.2 Verzeichnisübersicht . . . 10
2.3.3 Windows-Registrierungsdatenbank . . . 11
2.3.3.1 Programmverknüpfungen . . . 11
2.3.3.2 Dateitypverknüpfungen . . . 12
2.3.3.3 Digitale Zertifikate . . . 14
2.3.3.4 Deinstallation . . . 15
2.3.4 Deinstallationsroutine . . . 16
2.3.5 Allgemeine Konfiguration . . . 17
2.3.5.1 Allgemein . . . 18
2.3.5.2 Reconnect . . . 18
2.3.5.3 Verbindungsverwaltung . . . 19
2.3.5.4 Accountverwaltung . . . 19
2.3.5.5 Standardauthentifizierung . . . 20
2.3.5.6 Plugins . . . 21
2.3.5.7 Captchas . . . 21
2.3.5.8 Benutzeroberfläche . . . 23
2.3.5.9 Sprechblasen . . . 23
2.3.5.10 My.JDownloader . . . 24
2.3.5.11 Linkfilter . . . 24
2.3.5.12 Paketverwalter . . . 25
2.3.5.13 Archiventpacker . . . 25

2.3.5.14 Infosymbol (Passwortschutz) 26
2.3.5.15 Profieinstellungen 27
2.4 Digitale Anwendungsspuren 28
2.4.1 Versionsinformationen 28
2.4.2 Ereignisprotokollierung 28
2.4.3 Backupdateien 29
2.4.4 Download-Speicherort 30
2.4.5 Download-Verlauf 32
2.4.6 Entpackungs-Historie 35

3 Zusammenfassung **37**

A Anhang **38**
A.1 Installationsroutine der Firma InstallCore 38
A.2 Werbefreie Installationsroutine 39
A.3 Inhalt des Programmverzeichnisses 40
A.4 Windows Registrierungsdatenbank 41
A.4.1 Registry-Einträge zur Verknüpfung der Dateitypen 41
A.4.2 CA-Root Zertifikate 42
A.4.3 Registry-Informationen zur Softwaredeinstallation 43
A.5 Programmeinstellungen 46
A.5.1 Menüpunkt Allgemein 46
A.5.2 Menüpunkt Verbindung 47
A.5.3 Menüpunkt Accountverwaltung 48
A.5.4 Menüpunkt Standardauthentifizierung 49
A.5.5 Menüpunkt Plugin 50
A.5.6 Menüpunkt Captcha 51
A.5.7 Menüpunkt MyJDownloader 52
A.5.8 Menüpunkt Linkfilter 53
A.5.9 Menüpunkt Archiventpacker 53
A.5.10 Menüpunkt Paketverwalter 54
A.5.11 Menüpunkt Infosymbol 54
A.5.12 Menüpunkt Profieinstellungen 55
A.6 Deinstallationsroutine 58
A.7 Versionsinformationen 59
A.8 Protokollierungseinstellungen 62

Abbildungsverzeichnis

2.1 Hauptfenster im Download-Manager JDownloader 5
2.2 Prozessbaum während der Installationsausführung der JDownloader2Setup.exe . . . 9
2.3 JDownloader-Programmicon *i4j_extf_10_69g5ss_1kdboqw.ico* 14
2.4 Windows-Registry-Eintrag zur Deinstallation des JDownloaders 16
2.5 Passwortabfrage bei Programmstart oder Reaktivierung der Software 27
2.6 Linksammler mit hinzugefügten Downloaddateien 31
2.7 Gestarteter Download verschiedener Dateien 33

A.1 Ausführung des Installationsassistenten der Firma InstallCore mit angebotener Zusatzsoftware bei **inaktiver** Antivirus-Software 38
A.2 Ausführung des werbefreien Installationsassistenten bei **aktiver** Antivirus-Software . 39
A.3 Registry-Eintrag zum CA Root-Zertifikat „Thawte“ 42
A.4 Registry-Eintrag zum CA Root-Zertifikat „The USERTrust Network“ 43
A.5 Allgemeine Einstellungen des JDownloaders 47
A.6 Einstellungen für das Plugin der Webseite uploaded.to 50
A.7 Einstellungen für das Lösen von Captchas 51
A.8 Einstellungen zur Eingabe der Zugangsdaten des My.JDownloaders 52
A.9 Regelassistent zur Filterung von Links, Adressen und Dateien am Beispiel von Youtube 53
A.10 Regelassistent zur Filterung von Links, Adressen und Dateien am Beispiel von Youtube 54
A.11 Ausführung der Deinstallation des JDownloaders 58
A.12 Versionsinformationen des JDownloaders 59

Tabellenverzeichnis

2.2 Blockierte Internetadressen der Installationsdatei *JDownloader2Setup.exe* 8
2.4 Programmdateitypen des JDownloaders 12
2.4 Programmdateitypen des JDownloaders 13
2.5 Reconnect Einstellungen des JDownloaders 19

A.1 Genereller Inhalt des Programmverzeichnisses 40
A.1 Genereller Inhalt des Programmverzeichnisses 41
A.2 Allgemeine Einstellungen des JDownloaders 46
A.3 Konfigurationsdateien, welche den Profieinstellungen zugeordnet werden können. . . 55
A.3 Konfigurationsdateien, welche den Profieinstellungen zugeordnet werden können. . . 56
A.3 Konfigurationsdateien, welche den Profieinstellungen zugeordnet werden können. . . 57

Listingverzeichnis

2.1 Programmverknüpfungen in der Schnellstartleiste und auf dem Desktop 11
2.2 Registry-Einträge zur Hervorhebung neuer Schnellstart-Programmverknüpfungen . . 11
2.3 Installiert CA Root-Zertifikate 14
2.4 Reconnect Anmeldeinformationen 19
2.5 Erstellte Windows-Registry Einträge bei erstmaliger Konfigurationssicherung 30
2.6 Inhalt einer beispielhalften LinkCollector ExtraInfo-Datei 31
2.7 Historie zur Änderungen des Downloadpfades 32
2.8 Inhalt einer beispielhalften downloadList 00-Datei 33
2.9 Inhalt einer beispielhalften downloadList 00_0-Datei 34
2.10 Inhalt einer beispielhalften downloadList ExtraInfo-Datei 35
A.1 Registry-Einträge zur Verknüpfung der Dateitypen mit dem JDownloader 41
A.2 Gelöschte Registry-Informationen während der Softwaredeinstallation 43
A.3 Reconnect Anmeldeinformationen 47
A.4 Entschlüsselte Accountdatei 48
A.5 Entschlüsselte Accountdatei der Standardauthentifizierung 49
A.6 Entschlüsselte Konfigurationsdatei der Webseite uploaded.net 50
A.7 Captcha Einstellungen 51
A.8 Einstellungen des Captcha-Dienstes ImageTyperz 51
A.9 Einstellungen für den Zugang zu My.JDownloader 52
A.10 Einstellungen zum automatischen Entpacken von Archiven 53
A.11 Sonstige Einstellungen 54
A.12 Versionsinformationen des JDownloaders 59
A.13 Aktualisierungsverlauf des JDownloaders 60
A.14 Einstellungsmöglichkeiten bzgl. der Protokollierung 62
A.15 Inhalt einer beispielhalften LinkCollector 00-Datei 62
A.16 Inhalt einer beispielhalften LinkCollector 000-Datei 63
A.17 Protokollierte Informationen während der Extraktion des Archives OnTrHi04.part01.rar 64

1 Einführung

Die vorliegende Projektdokumentation beschreibt die Anwendungsanalyse des frei verfügbaren Download-Managers *JDownloader* (Version 2.0 Beta, Rev. 32397) auf dessen Spurenmenge für das Betriebssystem Microsoft Windows.

1.1 Projektauftrag

Die Zielsetzung der vorgenannten praktischen Arbeit besteht in der Analyse und Dokumentation der **Spurenmenge** einer ausgewählten Anwendung. Hierbei sollen insbesondere die folgenden beiden Fragestellungen beantwortet werden:

- Welche Sachverhalte kann man wo finden?
- Wie kann man die Spuren „auslesen“?

Zur Zielsetzung des Projektes gehört somit die Identifikation der von der Anwendung erstellten Spuren (Dateien) auf dem Dateisystem, welche daraufhin im Detail analysiert werden sollen. Die Dokumentation der analysierten Spurenmenge soll ferner in einer für einen Forensiker nützlichen Form erfolgen. Hierzu soll neben einer Auflistung der zentralen Dateien, welche der Anwendung zugeordnet werden können, soll der Projektbericht eine Anleitung beinhalten, wie diese Spuren analysiert werden können, sowie zusätzlich einer kurze Zusammenfassung sämtlicher Ergebnisse.

1.2 Untersuchungsobjekt

Als Untersuchungsobjekt der vorgenannten Anwendungsanalyse wurde die Software *JDownloader*[1] ausgewählt. Die Anwendung **JDownloader** (Abk. für Java Downloader) ist ein weltweit verbreiteter Download-Manager, demnach ein Programm zum komfortablen Herunterladen von Inhalten aus dem Internet (detaillierte Informationen in Kap. 2.1). Der Hersteller selbst gibt an, dass die Software mit seinen über 15 Millionen Nutzern marktführend im Bereich der Download-Manager ist[2]. Aufgrund der grundlegenden Programmierung der Anwendung mittels Java ist der JDownloader unter sämtlichen, java-unterstützenden Betriebssystemen (Windows, Linux, Mac) lauffähig. Unter Berücksichtigung des begrenzten Rahmens dieser praktischen Arbeit wird jedoch lediglich die Windows-Version untersucht.

In seiner ursprünglichen Version wurde das Programm zum automatisierten Herunterladen von Inhalten von Servern sogenannter One-Click-Hoster entwickelt. Aufgrund der technischen Infrastruktur solcher One-Click-Hoster (Ausländische Serverstandorte oder Firmensitze) werden diese vor-

[1] Herstellerwebseite: `http://jdownloader.org/download/index`, abgerufen am 27.2.2016
[2] Vgl. `http://wemakeyourappwork.com/de/`, abgerufen am 27.2.2016

zugsweise zur illegalen Verbreitung von urheberrechtlich geschützten Inhalten (Videos, Musik, Software) genutzt und stehen in diesem Zusammenhang häufig in der Kritik von Rechtsinhabern[3]. Im Zuge dessen kann implizit geschlussfolgert werden, dass auch der Download-Manager *JDownloader* verwendet wird, um explizit illegalen Inhalt von verschiedenen One-Click-Hostern zu beziehen. Insofern steht das Programm vornehmlich im Vordergrund polizeilicher Ermittlungen bzgl. Vergehen gegen das Urheberrechtsgesetz im Internet (Internetkriminalität). In diesem Rahmen wurde der Arbeitgeber des Autors - die Firma *Conturn AIG* - bereits bei einer Vielzahl von Ermittlungsverfahren konsultiert und unterstützt seit dem Jahr 2007 polizeiliche Ermittlungen im gesamten Bereich der Wirtschaftskriminalität. Aus diesem beruflichen Hintergrund und der weltweiten Verbreitung der Software im Bezug auf Urheberrechtsverletzungen im Internet, stellt sich die Anwendung des JDownloaders als interessantes Untersuchungsobjekt dar.
Mit Bezug auf den im vorherigen Kapitel 1.1 vorgestellten Projektauftrag und den Informationen zum Untersuchungsobjekt dieses Kapitels, liegt der Fokus der Programmanalyse in den folgenden drei Fragestellungen:

- Welche allgemeinen Spuren hinterlässt der Download-Manager?
- Inwieweit lassen sich vergangene Verwendungen der Software nachvollziehen?
- Kann mglw. ein bereits abgeschlossener Download im Nachhinein rekonstruiert werden?
- Können in diesem Fall detaillierte Informationen über vergangene Downloads (Download-Historie) festgestellt werden (heruntergeladene Dateien, Uhrzeit, IP-Adresse, Account, Speicherort ...)?

1.3 Arbeitsumgebung

Zur Lösung der Aufgabenstellung wurde eine virtuelle Maschine mit der Virtualisierungssoftware VirtualBox (Version 4.3.20) erstellt, auf dem das Betriebssystem Windows 7 (64-bit Version) als Arbeitsumgebung und ein gemeinsamer Ordner zum gegenseitigen Datenaustausch zwischen dem Host- und dem Gastsystem eingerichtet wurde. Abschließend wurde neben verschiedener, grundlegender Software wie einem Archivierungsprogramm (7-Zip File Manager, Version 9.20), einem Webbrowser (Mozilla Firefox), einem erweiterten Editor (Notepad++, Version 6.4.5), weiterhin das Analyseprogramm *Regshot* in der Version 1.9.0 installiert.
Regshot ist ein quelloffenes Programm zur Analyse der Windows-Registrierungsdatenbank (Windows-Registry), welches es erlaubt die Veränderungen zwischen zwei verschiedenen Zustandspunkten eines Betriebssystems zu vergleichen. Zusätzlich zu den Veränderungen in der Windows-Registry können weiterhin sämtliche Änderungen am gesamten Dateisystem oder eines bestimmten

[3] Vgl. bspw. den internationalen Skandal um den Sharehoster *Megaupload*, `https://www.fbi.gov/news/pressrel/press-releases/justice-department-charges-leaders-of-megaupload-with-widespread-online-copyright-infringement`, abgerufen am 27.2.2016

Pfades angezeigt werden. Hierzu wurde bspw. *vor* und *nach* der Installation einer Anwendung der Zustand des Betriebssystems mittels Regshot gesichert (vgl. Kap. 2.3.1). Das Programm vergleicht daraufhin die beiden gesicherten Zustände und gibt die Differenz der beiden Zustände als Ergebnis in Form einer Text- oder HTML-Datei aus. In detaillierter Formen werden die gelöschten, die veränderten und die neu erzeugten Dateien und Registry-Einträge in der Ausgabe aufgelistet.
Zur Überprüfung und Validierung der Ergebnisse, welche mittels Regshot erzeugt wurden, wurde als Referenzprogramm das System-Tool *WhatChanged* (Version 1.07) der Firma Vista Software verwendet. Durch den Vergleich der Ergebnisse beider Programme, konnte verifiziert werden, dass ermittelten Ergebnisse/Spuren von der untersuchten Anwendung stammen.
Darüber hinaus wurde der *Process Monitor* (Version 3.20) von Sysinternals eingesetzt, um während des laufenden Prozesses, gezielt Lese- und Schreibzugriffe der Software auf bestimmte Dateien und Verzeichnisse des Dateisystems nach zu vollziehen.

1.4 Berichtsstruktur

Der vorliegende Projektbericht gliedert sich in insgesamt drei einzelne Hauptkapitel, welche jeweils unterschiedliche Schwerpunkte darstellen. Hierzu gibt dieses erste Kapitel 1 eine generelle Einführung in das Thema, beschreibt den genauen Arbeitsauftrag, das Untersuchungsobjekt und die damit verbundene Zielstellung sowie die verwendete Arbeitsumgebung zur Lösung der Aufgabenstellung. Das zweite Kapitel 2 hingegen enthält eine detaillierte Beschreibung der Ergebnisse, die durch die Anwendungsanalyse erbracht werden konnte. In diesem Kapitel werden die generellen Veränderungen am Betriebs-/Dateisystem dargestellt, die durch die Installation der Anwendung entstanden sind. Weiterhin werden spezifische Merkmale sowie die zur Konfiguration verwendeten Dateien der Software beschrieben (vgl. Kap. 2.3). Aufbauend auf diesen Grundlagen werden in Kapitel 2.4 explizit die Spuren dargestellt und ausgewertet, welche durch eine aktive Benutzung der Anwendung entstehen und aus forensischer Sicht besonders relevant sind. Abschließend werden im Kapitel 3 die zentralen Ergebnisse der Arbeit zusammengefasst.

2 Technische Anwendungsanalyse

Das nachfolgende Kapitel beschreibt die technische Vorgehensweise und die daraus resultierenden Ergebnisse der Programmanalyse des Download-Managers JDownloader. Zu Anfang wird die Anwendung und deren Funktionen in kurzer Form vorgestellt und die generelle Vorgehensweise zur Akquise der Spurenmenge beschrieben. Abschließend werden die Ergebnisse der Anwendungsanalyse detailliert aufgeführt.

2.1 JDownloader - Ein Überblick

Im Rahmen der praktischen Arbeit wurde als Untersuchungsobjekt die Software *JDownloader* in der Version **2** des Herstellers *Appwork* ausgewählt (vgl. Kap. 1.2). Die Software **JDownloader** (Abk. für Java Downloader) ist ein auf der Programmiersprache Java basierender Download-Manager, demnach ein Programm zum Herunterladen von beliebigen Inhalten aus dem Internet. Das Programm bietet sämtliche Vorteile eines allgemeinen Download-Managers[4], wobei es jedoch primär zum automatisierten Herunterladen von Inhalten bei sogenannten Filehoster (auch Sharehoster oder One-Click-Hoster genannt)[5] entwickelt wurde und daher auf den Umgang mit Webseiten spezialisiert ist. Aufgrund dessen bietet die Anwendung weitaus mehr Funktionen als bei einem üblichen Download-Manager. Zu diesen Zusatzfunktionen zählt zum Beispiel der Bezug von Videos aus Videoportalen wie YouTube, Vimeo, Dailymotion oder von Online-Mediatheken wie bspw. denen der TV-Kanäle ARD, ZDF, WDR, DMAX.

Einer der bedeutendsten Vorteile, gegenüber anderen Download-Managern, ist der sog. *Linksammler* bzw. die *Click'n'Load*-Funktion des Managers. Der Linksammler durchsucht automatisch Internet-Webseiten und zeigt die gefundenen Inhalte der Webseite im Linksammler-Modul der Software an. Standardmäßig überwacht der Linksammler ebenfalls die Zwischenablage des Betriebssystems und durchsucht beim Auffinden einer oder mehrere Internetadressen ebenfalls diese Webseite nach downloadbaren Inhalten (Tiefenanalyse) und fügt diese dem Linksammler-Modul der Software hinzu. Darüber können Webseiten Betreiber bestimmte Buttons auf ihrer Webseite implementieren, mittels derer durch einen einfachen Klick auf den Button, die Click'n'Load-Funktion die entsprechenden Inhalte in die Downloadliste des JDownloaders übertragt und der Download automatisch startet. Allein durch die beiden vorgenannten Funktionen, entfällt ein - vor allem beim Download von vielen einzelnen Dateien - ein aufwändiges, manuelles Hinzufügen der zu beziehenden Inhalte. Die Software arbeitet nahezu selbstständig, weshalb sie sich in einschlägigen Kreisen explizit zum Bezug von urheberrechtlich Geschütztem Eigentum etabliert hat.

[4] Vgl. hierzu `https://de.wikipedia.org/wiki/Download-Manager`, abgerufen am 27.2.2016
[5] Vgl. hierzu `https://de.wikipedia.org/wiki/Sharehoster`, abgerufen am 27.2.2016

Die Abbildung 2.1 zeigt die generelle Benutzeroberfläche des JDownloaders. Die Anwendung besteht grundlegend aus der Menüleiste am oberen Bildschirmrand (Datei, Einstellungen, Extras, Hilfe), der darunter angeordneten Symbol-Leiste zum Start, Pausieren, Stopp und der Sortierung der Downloaddateien sowie den einzelnen Karteiregistern (Download, Linksammler, Einstellungen, My-JDownloader, Spenden).

In der nachfolgenden Abbildung 2.1 ist das Linksammler-Register ausgewählt. Durch das Kopieren verschiedener Links in die Zwischenablage, wurde diese automatisch von dem Linksammler-Modul nach herunterladbaren Inhalten durchsucht und die gefundenen Video-/Bild- und Audiodateien der verschiedenen Online-Videotheken (Youtube, ZDF, ARD) im Hauptfenster des Linksammlers angezeigt. Durch Selektion der zu entsprechenden Inhalte in der Linksammler-Auflistung, in Verbindung mit einem Klick auf den Start-/Play-Button (blaues Dreieck) in der Kopfzeile des Programms, werden die ausgewählten Inhalte heruntergeladen und der aktuelle Downloadstatus jeder einzelnen Datei im Register „Download“ angezeigt.

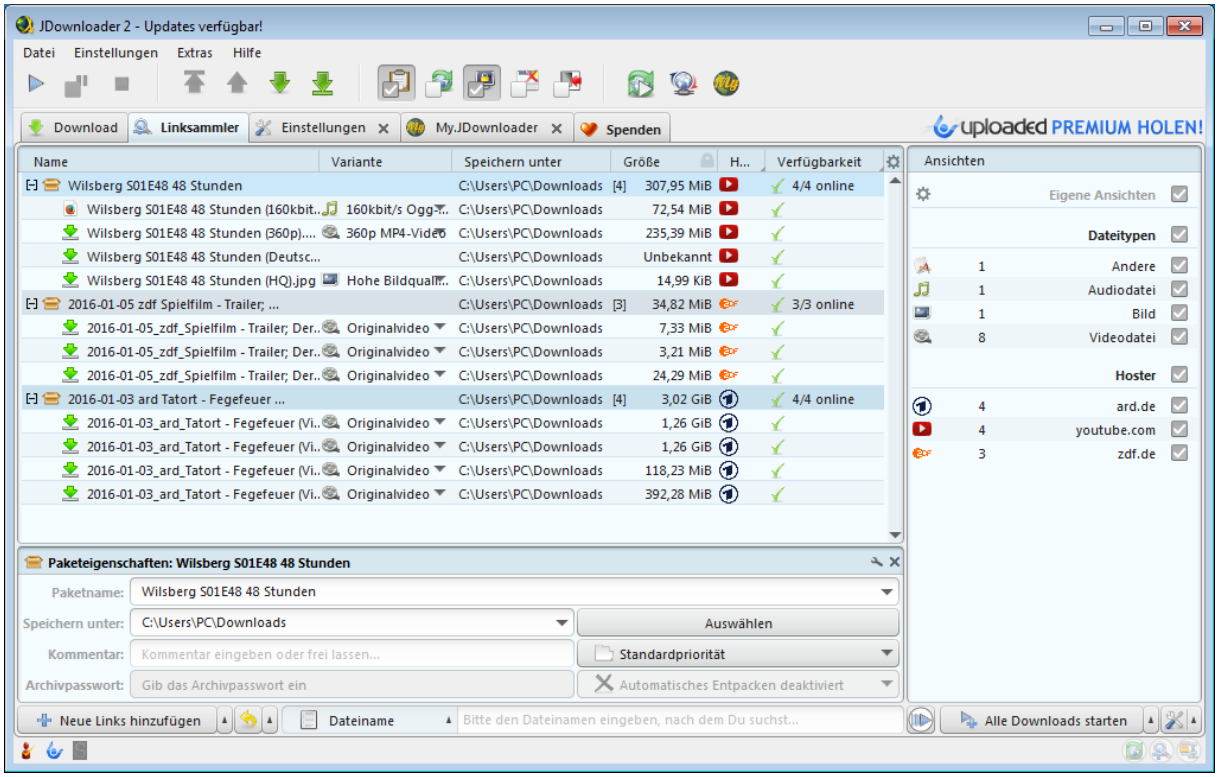


Abbildung 2.1: Hauptfenster im Download-Manager JDownloader

2.2 Generelle Vorgehensweise

Zur Akquise der Spurenmenge, welche durch die Verwendung des Download-Managers entsteht, wurde die in Kapitel 1.3 beschriebene Analyseumgebung verwendet. Unter Verwendung der in diesem Kapitel dargestellten Analyseprogramme wurde während der Anwendungsanalyse ein be-

sonderer Fokus auf die folgenden sechs Phasen gelegt, welche die markantesten Programmzustände darstellen und sich an einem allgemeinen Arbeitsablauf eines typischen Anwenders mit der Software orientieren.

Analysierte Anwendungszustände:

1. Installation
2. Programmstart
3. Start eines Downloads (Kap. 2.4)
4. Fertigstellung des Downloads (Kap. 2.4)
5. Programmende
6. Deinstallation

Die oben aufgeführten Programmphasen wurden im Laufe der Anwendungsanalyse chronologisch durchlaufen. **Vor** und direkt **nach** jeder einzelnen der sechs Phasen wurde der aktuelle Systemzustand des Betriebssystems (im Speziellen die Windows-Registry und das Dateisystem) gesichert. Auf Basis dieser Vorgehensweise kann sichergestellt werden, dass bei etwaigen Fehlern ein beliebiges Zurückkehren zu jeder einzelnen Phase möglich ist und somit die Analyse einer Phase beliebig wiederholt werden kann.
Nach der Erzeugung des Vorher-/Nacherabbildes konnte anhand der beiden vorgenannten Zustandssicherungen die Differenz und somit die Spurenmenge (im Speziellen die Windows-Registry und das Dateisystem) der jeweilige Programmphase ermittelt werden. Zur Verifikation der identifizierten Spuren wurde das vorgenannte Vorgehen nochmals mit dem System-Tool *WhatChanged* (Version 1.07) der Firma Vista Software durchgeführt und die Ergebnisse der beiden Anwendungen verglichen. In speziellen Fällen wurde weiterhin der *Process Monitor* (Version 3.20) eingesetzt, um während des laufenden Prozesses, gezielt Lese- und Schreibzugriffe auf bestimmte Dateien und Verzeichnisse des Dateisystems sowie Registry-Veränderungen, welche durch die Software hervorgerufen wurden, nachzuvollziehen.

2.3 Persistente Spurenmenge

Auf Basis des im vorherigen Kapitel beschriebenen Vorgehens wurde die persistente Spurenmenge des Download-Managers JDownloader akquiriert und analysiert. Die nachfolgenden Abschnitte beschreiben das Ergebnis dieser Analyse im Bezug auf die persistenten sowie größtenteils charakteristischen Spuren, welche während der Phasen **1**, **2**, **5**, **6** entstehen. Diejenigen Anwendungsspuren, welche bei der aktiven Verwendung in den Phasen **3** und **4** entstehen und Rückschlüsse auf die spezifischen Interaktionen des Benutzers mit der Anwendung geben, werden im nachfolgenden Kapitel 2.4 beschrieben.

2.3.1 Installationsroutine (Adware)

Zwar ist die eigentliche Anwendung des JDownloaders, aufgrund der Programmierung in Java und der damit verbundenen virtuellen Maschine, plattformunabhängig, jedoch wird die Anwendung auf der Projekt-Webseite lediglich in Form einer Installationsdatei verschiedene Betriebssysteme angeboten. Aufgrund dessen wurde, zu Anfang der Analyse, die Installationsdatei des JDownloaders von der Webseite des Projektes bezogen. Dieser wird aktuell lediglich in der (Beta)-Version 2 zum Download angeboten. Unter dem folgenden Link kann das Installations-Bundle *JDownloader2Setup.exe* heruntergeladen werden.
Zur eindeutigen Identifizierung des Untersuchungsobjektes und zur Verbesserung der Nachvollziehbarkeit der Ergebnisse, enthält die nachfolgende Tabelle 2.1 eine Auflistung der berechneten Hashwerte der Installationsdatei *JDownloader2Setup.exe*, welche unter Verwendung des MD5- und des SHA2-Algorithmus berechnet wurden.

Tabelle 2.1: Hashwerte der Installationsdatei JDownloader2Setup.exe

Algorithmus	**Hashwert**
MD5:	2e9761a4cdbe153c5bf66c0d1fb10e5e
SHA-2 [256]:	4465da52f8c9386f66913b77c70ff997cff3b2c4f3f090213af3ff53f1d9dedc

Nach einer Hintergrundrecherche im Forum der Webseite konnte festgestellt werden, dass es sich bei der Datei *JDownloader2Setup.exe* um einen Web-Installer der Plattform *InstallCore.com* handelt. Auf Grund der vom Entwicklungsteam bevorzugten Programmierung der Software, nach dem „Trial and error“-Prinzip, wird der Web-Installer verwendet, um die eigentliche Setup-Datei zur Installation des JDownloaders von einem zentralen Speicherort im Internet herunterzuladen. Der Web-Installer bezieht dabei stets den aktuellsten Stand der Software, sodass bei häufigen Änderungen an der Software, der Aufwand zum Bereitstellen der jeweils aktuellsten Version minimiert wird. Aufgrund der Tatsache, dass dieser Web-Installer jedoch von einer externen Firma angeboten und vertrieben wird, ist es daher möglich, dass nicht nur der JDownloader, sondern weitere, von der Plattform *InstallCore* ausgewählte, Software zur Installation angeboten wird. Seit der Verwendung dieses Web-Installers im Jahr 2012 häuften sich diesbezügliche Beschwerden verschiedener Benutzer, dass zusätzliche Programme installiert wurden, welche teilweise sogar unerwünschte bis schadhafte Funktionen beinhalten würden (Ad-/Mal- oder Spyware).[6]

[6] Vgl. Forum-Thread „JD inkl. Adware? Muss das sein?“, https://board.jdownloader.org/showthread.php?t=49080; http://www.chip.de/news/jDownloader-Warnung-vor-fieser-Adware-im-Installer_66546877.html; https://board.jdownloader.org/showpost.php?p=286276&postcount=346, abgerufen am 27.2.2016

Auch bei der für diese Programmanalyse durchgeführte Installation der Anwendung, innerhalb der im Kapitel 1.3 beschriebenen Arbeitsumgebung, wurden von der Antivirus-Software (ESET Endpoint Antivirus 5.0) des Host-Systems, die drei HTTP-Aufrufe der nachfolgenden Tabelle 2.2 blockiert oder als ein Download-Versuch einer unerwünschte Anwendung erkannt.[7]

Tabelle 2.2: Blockierte Internetadressen der Installationsdatei *JDownloader2Setup.exe*

Nr.	**Blockierte Internetadresse**
1.:	http://fetch.jdcdn.org/download/dl/forward?rand_13096506302283022462/2434/49/windows/32/__/0/jdownloader2
2.:	http://installer.jdownloader.org/fetch_1452026704533/wjd2oic1
3.:	http://installer.jdownloader.org/rand_13096506302283022462/2434/49/windows/32/__/0/jdownloader2

Hinter jeder der oben dargestellten Internetadressen verbirgt sich eine weitere Installationsdatei mit dem Namen *JDownloader2Setup.exe*. Ein Vergleich der Hashwerte dieser Installationsdatei mit den Werten der zu Anfang ausgeführten *JDownloader2Setup.exe* ergibt jedoch, dass es sich nicht um die gleiche Installationsdatei handelt. Eine Überprüfung der zweiten, über die Internetadressen bezogenen, Installationsdatei mit dem Antivirus-Programm *ESET Endpoint Antivirus 5.0* ergibt, dass es sich um eine potentiell gefährliche oder unerwünschte Anwendung der Typs *Win32/InstallCore.ACZ* handelt. Ein Abgleich mit der Virusdatenbank *Virustotal* ergab, dass 20 weitere Antivirus-Hersteller die Datei ebenfalls als potentiell schadhafte Anwendung des Typs *Win32/InstallCore.ACZ* einstufen.

Tabelle 2.3: Hashwerte der schadhaften Installationsdatei JDownloader2Setup.exe

Algorithmus	**Hashwert**
MD5:	7ef6b77bccaa41a50dbbf0221e344377
SHA-2 [256]:	3fb0fcafe7ba9587ca99a28ada771abb0ce77058b71e7cb49c3e273b03b80dea

Durch eine weitergehende Prüfung der Installation unter Verwendung der Analyseumgebung Cuckoo, konnte ein Prozessbaum (Abb. 2.2) erstellt werden. Hieraus ist zu erkennen, dass die Installationsdatei *JDownloader2Setup.exe* im Verzeichnis „C:\Users\PC\AppData\Local\Temp“ ausgeführt wurde und diese weitere, aus dem Internet bezogene, Dateien zur Ausführung bringt.

Neben den bereits bekannten Erkenntnissen, dass die Installationsdatei mglw. schadhafte Software aus dem Internet herunterlädt, ist insbesondere der Aufruf der systeminter-

[7] Eine gesamtheitliche Analyse der Installationsdatei, kann unter diesem Link aufgerufen werden.

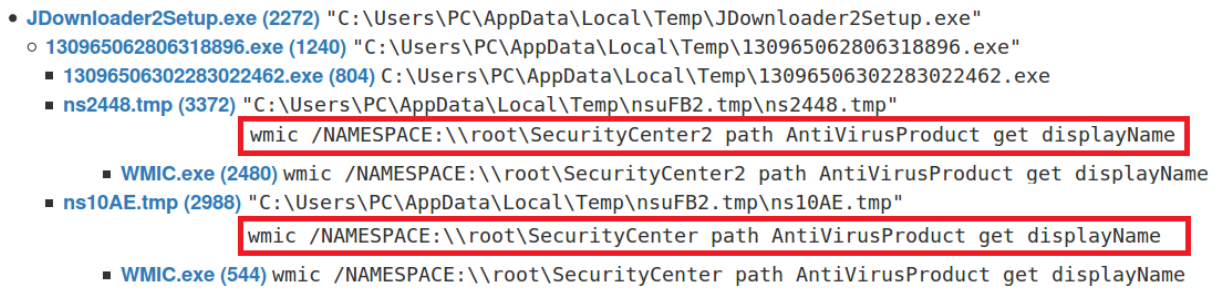


Abbildung 2.2: Prozessbaum während der Installationsausführung der JDownloader2Setup.exe

nen *WMIC.exe* interessant (vgl. Abb. 2.2, rote Umrahmung). Mittels des Programmaufrufs `wmic /NAMESPACE:\root\SecurityCenter[2] path AntivirusProduct get displayName` überprüft die Installationsdatei, ob und wenn ja, welches Antivirus-Produkt auf dem Rechner installiert ist. Durch eine zeitlich begrenzte Deaktivierung der Antivirus-Software konnte festgestellt werden, dass sich der Web-Installer bei der Ausführung auf einem Betriebssystem **mit** einem aktiven Antivirus Programm anders verhält, als wenn **kein** solches Programm aktiviert/installiert ist. Möglicherweise resultiert dies daraus, da eine aktive Antivirus-Software die entsprechende Verbindung zum Server bzw. den Download der des Installationssetups, welche eine unerwünschten Zusatzsoftware enthält, blockieren würde und insofern zur erfolgreichen Installation des JDownloaders eine **werbefreie** Installationsdatei aus einer *vertrauenswürdigen* Quelle heruntergeladen werden muss.

Die Abbildungen A.1 und A.2 des Anhangs A zeigen hierzu die unterschiedlichen Installationsroutinen, wenn diese parallel zu einem **ein**- bzw. **aus**geschaltetem Antivirus-Produkt ausgeführt werden. Bei einer aktiven Antivirus-Software wird die Installationsroutine der Abbildung A.2 ausgeführt; bei inaktiver Software, die Installationsroutine der Abbildung A.1. Insbesondere die Abbildung A.1(d) zeigt den Punkt der Installationsroutine, in der die zuvor angesprochene Installation einer unerwünschten Anwendung angeboten wird. Man beachte, diese Installationsroutine wird offensichtlich lediglich ausgeführt, wenn **kein** Antiviren-Produkt aktiv ist. Dem hingegen zeigt die Abbildung A.2 die Installationsroutine, welche ausgeführt wird, wenn ein Antivirus-Produkt **aktiv** ist.

Die Autoren eines Artikels vom 13.01.2014 des Technikportals Chip.de kommen bezüglich der Softwareinstallation zu dem Schluss, dass nach der IP-Adresse des Clients entschieden wird, ob und welche Zusatzsoftware angeboten wird. In einem weiteren Artikel wird ebenfalls darauf aufmerksam gemacht, dass das Setup unter Umständen versucht, zusätzliche Adware auf dem Rechner einzurichten. Im gleichen Zuge wird jedoch der Vorteil genannt, dass diese Version der Installation, im Gegensatz zur werbefreien Version, den Vorteil hat, dass bei Bedarf Java mitinstalliert wird.[8]

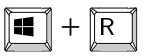
[8] Vgl. hierzu `http://www.chip.de/news/jDownloader-Warnung-vor-fieser-Adware-im-Installer_66546877.html` bzw. `http://www.chip.de/downloads/jDownloader-Adware_69618156.html`, abgerufen am 27.2.2016

Aufgrund des begrenzten Umfangs und unter Berücksichtigung der ursprünglichen Zielsetzung dieser Projektarbeit wurde an dieser Stelle auf eine detailliertere Analyse der Installationsroutine verzichtet. Abschließend kann jedoch festgehalten werden, dass der Web-Installer nicht die tatsächliche Programm des JDownloaders installiert, sondern lediglich eine entsprechende Setup-Routine zur Installation der Software aus dem Internet herunterlädt.

2.3.2 Verzeichnisübersicht

Wie in den Abbildung A.1(b) und A.2(b) zu erkennen, ist es während der Installation möglich, einen benutzerdefinierten Programmpfad, unter dem das Programm installiert werden soll, anzugeben. Standardmäßig wird der JDownloader unter dem nachfolgenden Programmpfad installiert.

Standardinstallationspfad: „C:\Users\%username%\AppData\Local\JDownloader 2.0“

Bei einer detaillierten Betrachtung der Abbildungen A.1(b) und A.2(b) fällt jedoch auf, dass die Installationsroutine der Firma InstallCore (Abb. A.1(b)) den Programmordner als „JDownloader **v**2.0“ standardmäßig benennt. Bei einer etwaigen Analyse kann dies ein Hinweis auf die Verwendung der werbebehafteten Installationsroutine sein. Jedoch sollte man diesem Merkmal nicht zu viel Bedeutung beimessen, da eine explizite, benutzerdefinierte Auswahl und Benennung des Installationspfades bei beiden Installationsroutinen möglich ist.
Durch die Tastenkombination  wird ein Fenster zur Ausführung von Programmen oder zum Öffnen von Ordnern geöffnet. Durch die Eingabe der Zeichenkette „%LOCALAPPDATA%“ gelangt man in das Verzeichnis, in dem der JDownloader standardmäßig installiert wird. Unter dieser Verzeichnisstruktur befinden sich in dem Ordner „JDownloader **v**2.0“ sämtliche Anwendungs- und Konfigurationsdateien der Anwendung. Die im Anhang A dargestellte Tabelle A.1 enthält hierzu eine Auflistung der Ordner und Dateien des Hauptverzeichnisses, die nach der Installation der Software im Hauptverzeichnis des Installationspfades vorliegen. Jeder Eintrag wurde dabei um eine kurze Beschreibung der Funktion bzw. des Inhalts ergänzt.[9]
Im Hinblick auf die in Kapitel 1.1 und 1.2 dargestellte Zielsetzung dieser Programmanalyse sind die aus forensischer Sicht wichtigsten Verzeichnisse dieses Programmverzeichnisses in der vorigen Darstellung mit einer dickeren Schrift gesondert erkenntlich gemacht. Insofern sind, wie im Folgenden noch weiter dargestellt wird, die Verzeichnisse „**cfg**“ (Kap. 2.3.5) und „**logs**“ (Kap. 2.4) von besonderer Bedeutung. Im Ordner „**cfg**“ werden sämtliche Dateien zur Konfiguration der Software hinterlegt, wohingegen der Ordner „**logs**“ verschiedene Informationen über protokollierte Ereignisse während der letzten Ausführung der Software enthält.

[9] Legende der Typendefinition: D = Directory (Verzeichnis), F = File (Datei)

2.3.3 Windows-Registrierungsdatenbank

Während der Installation des JDownloaders werden verschiedene Einträge in der Registrierungsdatenbank des Betriebssystems (Windows-Registry) angelegt. Diese konnten mit den Ergebnissen des im vorherigen Kapitel 2.2 beschriebenen Vorher-Nacher-Vergleichs identifiziert werden. Aufgrund des Vielzahl an Änderungen in der Windows-Registry werden im Folgenden lediglich die zentralen Änderungen der Registrierungsdatenbank dargestellt, welche durch bei einer Installation der Software hervorgerufen werden.

2.3.3.1 Programmverknüpfungen

Wie in den Abbildungen A.2(d) und A.1(b) des Anhangs A dargestellt, kann während der Installationsroutine vom Benutzer aktiv ausgewählt werden, ob eine Verknüpfung des Programms auf dem Desktop und/oder in der Schnellstart-Leiste des Betriebssystems angelegt werden soll. Sowohl die Desktop- als auch die Schnellstart-Verknüpfung ist standardmäßig aktiviert und wird während der Installation angelegt. Hierzu werden die jeweiligen Verknüpfungen im Format „.lnk“ unter dem Pfad „C:\Users\PC\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\JDownloader\“ für die Schnellstart-Verknüpfung, und für die Desktop-Verknüpfung, unter dem Pfad „C:\Users\PC\Desktop“ angelegt (vgl. Listing 2.2).

Listing 2.1: Programmverknüpfungen in der Schnellstartleiste und auf dem Desktop

```
1  C:\Users\PC\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\JDownloader\
       JDownloader 2 Deinstallationsprogramm.lnk
2  C:\Users\PC\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\JDownloader\
       JDownloader 2 Update & Rescue.lnk
3  C:\Users\PC\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\JDownloader\
       JDownloader 2.lnk
4  C:\Users\PC\Desktop\JDownloader 2.lnk
```

Weiterhin konnte identifiziert werden, dass die folgenden Einträge in der Windows-Registry vorgenommen wurden, um den JDownloader in der Schnellstartleiste als „neues“ Programm farblich hervorzuheben.[10]

Listing 2.2: Registry-Einträge zur Hervorhebung neuer Schnellstart-Programmverknüpfungen

```
1 HKU\S-1-5-21-539846951-2775919047-120045064-1000\Software\Microsoft\Windows\
      CurrentVersion\Explorer\StartPage\NewShortcuts\C:\Users\PC\AppData\Roaming\
      Microsoft\Windows\Start Menu\Programs\JDownloader\JDownloader 2.lnk: 0x00000001
```

[10] Weitere Informationen bzgl. des Registry-Eintrags. s. „The Start Menu's Start“ unter http://www.geoffchappell.com/notes/windows/shell/explorer/startmenu.htm, abgerufen am 27.2.2016

```
2 HKU\S-1-5-21-539846951-2775919047-120045064-1000\Software\Microsoft\Windows\
    CurrentVersion\Explorer\StartPage\NewShortcuts\C:\Users\PC\AppData\Roaming\
    Microsoft\Windows\Start Menu\Programs\JDownloader\JDownloader 2 Update & Rescue.
    lnk: 0x00000001
```

2.3.3.2 Dateitypverknüpfungen

Während bei der werbefreien Installation explizit eine benutzerdefinierte Auswahl zur Verknüpfung verschiedener Dateitypen mit der Software, manuell vorgenommen werden kann (vgl. Abb. A.2(c)), ist dies bei der Installationsroutine der Firma InstallCore **nicht** möglich, wird jedoch automatisch durchgeführt.
Zusammen mit dem JDownloader konzipierten die Entwickler der Software im Laufe der Jahre verschiedene Formate zum *verschlüsselten* Speichern von Download-Links in Containerdateien. Daraus ergibt sich der Vorteil, dass einzelne Links gebündelt in einer einzigen Datei verbreitet und daraufhin heruntergeladen werden können. Aufgrund der Tatsache, dass die Links verschlüsselt in der Containerdatei abgespeichert sind, verbindet sich der JDownloader automatisch mit einem zentralen Server, um den Schlüssel zum Entschlüsseln der Containerdatei und der darin befindlichen Links zu beziehen. Im Laufe der Jahre wurden aufgrund von Sicherheitsmängeln verschiedene Dateiformate entwickelt. Eine übersichtliche Beschreibung der einzelnen Dateiformate kann unter diesem Link eingesehen werden. In der folgenden Tabelle 2.4 sind die einzelnen Dateiformate aufgelistet, die während der Installation mit dem Download-Manager JDownloader verknüpft werden.[11]

Tabelle 2.4: Programmdateitypen des JDownloaders[12]

Nr.	Dateityp	Name	Beschreibung
1.	*.ccf	**Cryptload Link Container**	Das Cryptload Container Format wurde für das Programm Cryptload entwickelt, wurde jedoch nicht vom Cryptload Team zur Verwendung für andere Downloadmanager freigegeben. Neben den URLs kann eine CCF noch weitere Informationen wie Archivpasswörter oder Kommentare enthalten.

[11] Vgl. `https://de.wikipedia.org/wiki/JDownloader`, abgerufen am 27.2.2016

Tabelle 2.4: Programmdateitypen des JDownloaders[12]

Nr.	Dateityp	Name	Beschreibung
2.	*.rsdf	**RSD Link Container**	Das Rapidshare Downloader Format wurde für den „Rapidshare Downloader“ (RSD) entwicklet. Die Verschlüsselung basiert auf dem AES Algorithmus. Außer URLs können in einer RSDF keine weiteren Informationen abgelegt werden. Das Format wurde bereits vor längerer Zeit entschlüsselt.
3.	*.dlc	**JDownloader Link Container**	Nachdem RSDF und CCF genackt wurden, wurde der Wunsch nach einem neuen Container laut. Der JDownloader Container sollte die alte Rivalität zwischen RSDF und CCF beenden. Um dieses Ziel zu verwirklichen wird ein Client-Server Model zur Verschlüsselung und Entschlüsselung verwendet. Alle Linkinformationen werden dabei beim Benutzer verarbeitet. Der Server kümmert sich lediglich um den Schlüsselaustausch. Es werden keine relevanten Daten zum Container verschickt.
4.	*.jdc	**JDownloader Linkbackup Format**	Format zum Backup von *.dlc-Containern
5.	*.metalink	**Metalinks**	Metalink ist ein plattform- und anwendungsübergreifender offener Standard für Containerdateien mit Links und weiteren Metainformationen.[13]

Zur Verknüpfung der in Tabelle 2.4 dargestellten Dateiformate mit dem JDownloader, werden während der Installation automatisch verschiedene Einträge in der Windows-Registry vorgenommen. Wie der Auflistung A.1 des Anhangs A zu entnehmen ist, werden unter dem Pfad „HKEY_LOCAL_MASCHINE\SOFTWARE\Classes\“ die Klassen zu den Dateitypen *.dlc, .jdc, .ccf, .rsdf* sowie *.metalink* eingetragen und jeweils der Wert „JDownloader2 [1 - 4]“ hinterlegt (vgl. Listing A.1, Z. 1 - 5). Weiterhin werden unter dem Pfad „HKEY_LOCAL_MASCHINE\SOFTWARE\Classes\“ die Schlüssel

JDownloader2 : „JDownload Link Container“

JDownloader2 1: „JDownloader Linkbackup Format“

[13] Für weitere Informationen s. `https://de.wikipedia.org/wiki/Metalink`, abgerufen am 27.2.2016

JDownloader2 2: „Cryptload Link Container“

JDownloader2 3: „RSD Link Container“

JDownloader2 4: „Metalinks“

angelegt (vgl. Listing A.1, Z. 7, 11, 15, 19, 23). Jeder dieser Schlüssel enthält wiederum jeweils einen Schlüssel zur Angabe des Datei-Icons („DefaultIcon“, vgl. Listing A.1, Z. 8, 12, 16, 20, 24) und zur Angabe des Programms („shell\open\command“, vgl. Listing A.1, Z. 9, 13, 17, 21, 25), mit dem das entsprechende Format geöffnet werden soll. Die nachfolgende Abbildung 2.3 zeigt das Programmicon „*i4j_extf_10_69g5ss_1kdboqw.ico*“, welches für jeden Dateityp gewählt wurde und während der Installation der Software im Programmverzeichnis unter Ordner „*.install4j*“ abgespeichert wird.

Abbildung 2.3: JDownloader-Programmicon *i4j_extf_10_69g5ss_1kdboqw.ico*

Nachdem die Dateitypen als Klassen angelegt, das Dateiicon spezifiziert und die auszuführende Anwendung ausgewählt wurde, werden die einzelnen Dateitypen im Windows Explorer registriert (vgl. Listing A.1, Z. 27 - 31).[14]

2.3.3.3 Digitale Zertifikate

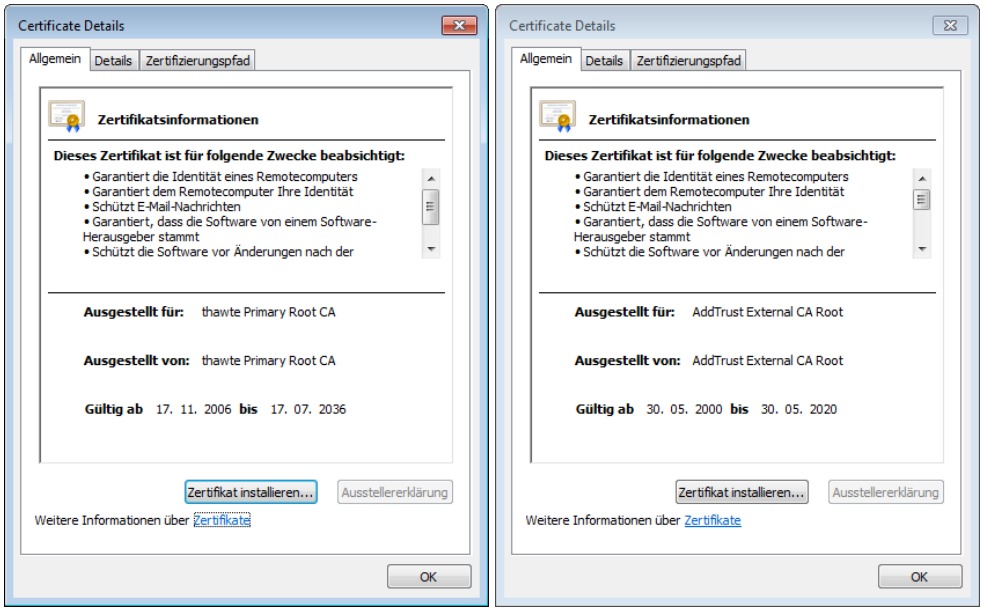
Anhand der Ergebnisse des Vorher-/Nacher-Vergleichs, welcher unter Verwendung der Analysesoftware RegShot durchgeführt wurde (vgl. Kap. 2.3.3), konnte weiterhin festgestellt werden, dass während der Installation zwei CA Root-Zertifikate auf dem System installiert und somit in der Windows-Registry importiert wurden. Diese Zertifikate wurden unter den Pfaden des nachfolgenden Listings 2.3 angelegt und enthalten jeweils einen Binärwert mit dem Namen „Blob“ (vgl. Abb. A.3 u. A.4).

Listing 2.3: Installiert CA Root-Zertifikate

```
1 HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\91
      C6D6EE3E8AC86384E548C299295C756C817B81
2 HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\
      E12DFB4B41D7D9C32B30514BAC1D81D8385E2D46
```

[14] Weitere Informationen bzgl. der Dateizuordnung von neuen Dateitypen s. `http://www.wintotal.de/tipparchiv/?id=1622`, abgerufen am 27.2.2016

Durch die Analyse der jeweiligen Registry-Einträge konnte festgestellt werden, dass es sich hierbei um die Zertifikate `Thawte` sowie `The USERTrust Network` handelt. Mithilfe des systeminternen Windows-Tools **certutil** in Verbindung mit den Parameters **-viewstore authroot** können Details zu den auf dem Betriebssystem installierten Root-Zertifikate eingesehen werden.



(a) Thawte CA Root-Zertifikat (b) Trust CA Root-Zertifikat

Vermutlich werden diese digitalen Zertifikate genutzt, um die Authentizität und Integrität des zentralen JDownload-Servers während des Schlüsselaustauschs zu gewährleisten, der zur Entschlüsslung der in Kapitel 2.3.3.2 beschriebenen Link Container benötigt wird. Diese Vermutung konnte bisher jedoch noch nicht validiert werden.

2.3.3.4 Deinstallation

Während der Installation des JDownloaders werden verschiedene Einträge für eine mögliche Deinstallation der Software in der Registry vorgenommen (vgl. Listing A.1, Z. 97 - 104). Die nachfolgende Abbildung zeigt die einzelnen Inhalte des Windows-Registry Pfades „HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\jdownloader2“. Neben den Informationen zum *Programmnamen*, der *Programmversion* und des *Herausgebers* werden das *Installationsverzeichnis* und der *Pfad zur Deinstallationsroutine* angegeben. Ein Versuch zeigte, dass die systeminterne Funktion zur Deinstallation von Programmen auf diese Informationen zugreift. In dem Versuch wurde der Pfad zur Deinstallationsroutine (Eintrag „**UnistallString**“) auf eine nicht existente Datei geändert. Daraufhin zeigte die betriebssysteminterne Software-Deinstallationsfunktion, dass ein Fehler auftrat und das Programm nicht deinstalliert werden könnte. Weiterhin werden ver-

änderte Angaben zum Hersteller (Publisher) angezeigt, wenn diese ebenfalls in der Registry geändert wurden. Die systeminterne Funktion zur Deinstallation von Programmen unter Windows kann wie folgt gestartet werden: `Start` → `Systemsteuerung` → `Programme und Funktionen` → `Programm deinstallieren` → `JDownloader 2`.

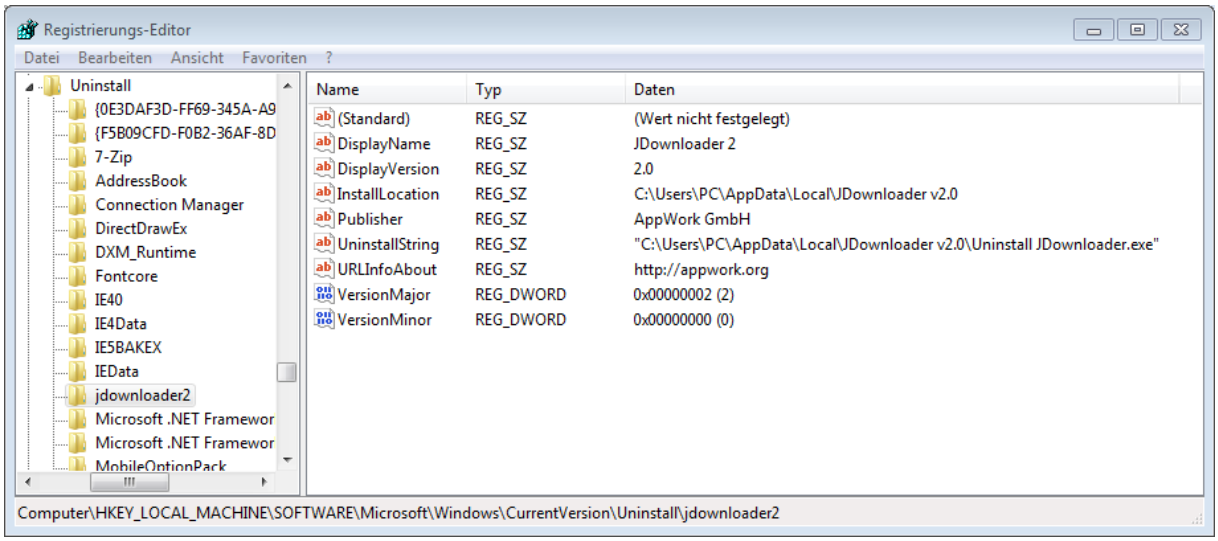


Abbildung 2.4: Windows-Registry-Eintrag zur Deinstallation des JDownloaders

2.3.4 Deinstallationsroutine

Wie bereits in Kapitel 2.3.3.4 dargestellt, wird während der Installation in der Windows-Registry der Schlüssel "UnistallString" angelegt, dessen Wert auf die Deinstallationsroutine des JDownloaders verweist (vgl. Abb. 2.4). Diese ist standardmäßig im Programmhauptverzeichnis "C:\PC\AppData\Local\JDownloader v2.0\" enthalten und trägt den Namen "Unistall JDownloader.exe". Die Abbildung A.11 des Anhangs A zeigt hierzu den Verlauf der Deinstallationsroutine. Während der Deinstallation wird der Anwender im zweiten Schritt gefragt, ob er die aktuellen Einstellungen und bestehende Linklisten der Software erhalten möchte (vgl. Abb. A.11(b)). Falls die Frage dieses Anwenderdialogs mit „Ja“ beantwortet wird, bleibt das gesamte "\cfg"-Konfigurationsverzeichnis erhalten und wird trotz Deinstallation der Software nicht gelöscht, sodass sämtliche Konfigurationseinstellungen (vgl. Kap. 2.3.5 sowie explizit Tab. A.3) der Software erhalten bleiben.
Wird die Frage jedoch mit „Nein“ beantwortet, wird auch der Inhalt des "\cfg"-Ordners und somit die Konfigurationseinstellungen bereinigt. **Bereits abgeschlossene Downloads** bzw. vollständig heruntergeladene Dateien werden jedoch nicht automatisch gelöscht, auch wenn diese zum Zeitpunkt der Deinstallation noch in der Downloadliste der Software vorhanden sind!
Im vorliegenden Fall kam jedoch, auch bei mehrmaliger Ausführung der Deinstallationsroutine auf verschiedenen Arbeitsumgebungen, die in der Abbildung A.11(c) dargestellte Fehlermeldung auf.

Unabhängig der im zweiten Schritt der Deinstallation getätigten Entscheidung (vgl. Abb. A.11(b)), versucht die Deinstallationsroutine sämtliche Protokollinformationen der Software während der Deinstallation zu bereinigen. Bei den zu dieser Dokumentation durchgeführten Deinstallationsversuchen, trat hierbei stets der in Abbildung A.11(c) dargestellte Fehler auf. Unabhängig der zuvor getätigten Entscheidung bleiben somit, zumindest in der aktuellen Version der Software, zum einen die aktuelle Konfigurationsdatei zur Protokollierung „\cfg\org.appwork.utils.logging2.LogConfig.json“ (vgl. Tab. A.3, Nr. 16) sowie die aktuelle Protokolldatei der letzten Sitzung „\logs\<Datum in s/ms>_<aktuelles Datum + Uhrzeit & Zeitzone>\Log.L.log.0“ (vgl. Kap. 2.4.2) erhalten, da diese von der Deinstallationsroutine nicht gelöscht werden konnten.
Während der Deinstallation der Software werden lediglich die Einträge der Auflistung A.2 des Anhangs A aus der Windows-Registry entfernt. Sämtliche weiteren Einträge, die während der Installation der Software durchgeführt wurden (vgl. Kap. 2.3.3), werden nicht entfernt und lassen sich somit auch nach einer Deinstallation in der Registrierungsdatenbank auffinden, sodass anhand der verbleibenden Registry-Einträge (vgl. Kap. 2.3.3.3, wie installierten Zertifikaten und alten Pfadartefakten) auf eine ehemalige Installation der Software geschlossen werden kann.

2.3.5 Allgemeine Konfiguration

Wie bereits in der Verzeichnisübersicht des Kapitels 2.3.2 bzw. der Tabelle A.1 dargestellt, enthält der Ordner „cfg“ des Programmverzeichnisses eine Vielzahl an Konfigurationsdateien mit denen sämtliche Einstellungen der Software vorgenommen werden können. Die jeweiligen Einstellungsparameter liegen dabei in unterschiedlichen Dateien des Typ „.json“ (JavaScript Object Notation) vor. Innerhalb der Anwendung sind die Einstellungen über den gleichnamigen Punkt in der Menüleiste einsehbar. Nach der Auswahl des Menüpunktes wird ein entsprechendes Kontextmenü im Hauptfenster der Anwendung angezeigt, welches wiederum verschiedene Menüunterpunkte beinhaltet. Im Nachfolgenden werden sämtliche dieser Menüunterpunkte dargelegt.
Die einzelnen Ergebnisse der nachfolgenden Kapitel konnten durch den bereits im vorherigen Kapitel 2.2 beschriebenen Vorher-Nacher-Vergleich identifiziert werden. Für diesen Vergleich wurde weiterhin das die Analysesoftware *Regshot* verwendet und jeweils **vor** sowie **nach** einer Änderung an den Einstellungen in der Benutzeroberfläche, der Systemzustand gesichert, darauffolgend verglichen und die Differenzmenge analysiert. Zur Validierung der dadurch erlangten Ergebnisse wurde *WhatChanged* als Referenztool verwendet (s. Kap. 1.3). Weiterhin wurden verschiedene Einstellungen direkt in den jeweiligen Konfigurationsdateien vorgenommen und die Reaktion, d.h. die jeweilige Änderung in der Benutzeroberfläche beobachtet, wodurch die nachfolgenden Ergebnisse abschließend verifiziert werden konnten.

2.3.5.1 Allgemein

In der Abbildung A.5 des Anhangs A ist der Menüpunkt „Allgemein“ in den Einstellungen des JDownloaders dargestellt. Sämtliche Einstellungsmöglichkeiten dieses Menüs werden in der folgenden Datei des Konfigurationsordners "cfg" gespeichert.

Allgemeine Einstellungen: „org.jdownloader.settings.GeneralSettings.json“

Die Tabelle A.2 des Anhangs A enthält eine Auflistung mit verschiedenen Variablen aus der Einstellungsdatei "GeneralSettings.json" und deren Bedeutung. Durch eine Veränderung dieser Werte konnte festgestellt werden, dass sich die in Abbildung A.5 dargestellten Einstellungen der Benutzeroberfläche ebenso veränderten. Unter Verwendung dieser Vorgehensweise konnten die Einstellungsvariablen ihrer Bedeutung zugeordnet werden. Es ist jedoch ein Neustart der Anwendung nötig, damit die Änderungen wirksam werden.

2.3.5.2 Reconnect

Falls ein Anwender des JDownloaders kein kostenpflichtiges Premium-Konto bei einem Filehoster besitzt, hat dieser die Möglichkeit den kostenfreien, jedoch langsamen Freedownload zu nutzen. Hierbei werden jedoch Zeitsperren gesetzt, sodass üblicher Weise ein User pro Stunde maximal eine Datei herunterladen darf. Da der Freedownload ohne ein Benutzerkonto beim entsprechenden Anbieter möglich ist, wird der jeweilige Nutzer bei dieser Methode über seine IP-Adresse identifiziert. Zur Umgehung der Zeitsperren ist es lediglich notwendig, eine neue IP-Adresse zu beziehen. Dies ist meist durch einen Neustart des Routers möglich. An dieser Stelle setzt das Plugin "Reconnect" an. Bei einem Download von vielen einzelnen Dateien, ist ein manueller Routerneustart sehr aufwendig. Das Plugins Reconnect automatisiert diesen Routerneustart anhand von vorgefertigen Skripts. Es muss lediglich IP-Adresse des Routers und die Anmeldedaten (Benutzername & -kennwort) eingegeben werden. Diesbezüglich konnte durch Eingabe von Informationen und einem darauffolgenden Abgleich des Dateisystems festgestellt werden, dass die Anmeldedaten (vgl. Listing 2.4) und die generellen Reconnect Einstellungen (vgl. Tabelle 2.5) unverschlüsselt in den folgenden Dateien des Konfigurationsordners "cfg" abgespeichert sind.

Reconnect-Einstellungen: „jd.controlling.reconnect.ReconnectConfig.json“

Anmeldedaten: „jd.controlling.reconnect.pluginsinc.liveheader.LiveHeaderReconnectSettings“

Tabelle 2.5: Reconnect Einstellungen des JDownloaders

Nr.	Einstellungsvariable	Beschreibung
1.	reconnectallowedtointerrupt-resumabledownloads	[Checkbox]: Reconnects können fortsetzbare Downloads unterbrechen.
2.	successcounter	-
3.	autoreconnectenabled	[Checkbox]: Automatischer Reconnect
4.	activepluginid	-
5.	downloadcontrollerprefers-reconnectenabled	[Checkbox]: Downloads nicht starten, wenn andere auf einen Reconnect warten.

Listing 2.4: Reconnect Anmeldeinformationen

```
1 jd.controlling.reconnect.pluginsinc.liveheader.LiveHeaderReconnectSettings
2 {
3   "routerip" : "192.168.178.1",
4   "password" : "admin",
5   "alreadysendtocollectserver3" : false,
6   "script" : null,
7   "username" : "Admin"
8 }
```

2.3.5.3 Verbindungsverwaltung

Falls zur Internetverbindung ein Proxy benötigt wird, kann dieser im dritten Menüpunkt der Einstellungen vom vorgenommen werden. Zur Vermeidung von IP-Wartezeiten (vgl. Kap. 2.3.5.2), können in den Einstellungen mehrere Proxy-Server eingetragen werden. Die im Benutzermenü angezeigte Liste mit den verschiedenen Einstellungen zu jedem einzelnen Proxy-Server ist in der nachfolgenden Datei des Konfigurationsordners "cfg" gespeichert. Sowohl die IP-Adresse als auch *Benutzername* sowie *-passwort* werden in dieser Datei im **Klartext** abgelegt (vgl. Listing A.3 des Anhangs A).

Proxy-Einstellungen: „org.jdownloader.settings.InternetConnectionSettings.customproxylist.json“

2.3.5.4 Accountverwaltung

Das Kernstück des JDownloaders und die somit wohl wichtigste Einstellung der gesamten Anwendung ist die Accountverwaltung. In diesem Menüpunkt werden die Informationen zur Anmeldung bei den entsprechenden Sharehostern hinterlegt. Sämtliche Informationen sind hierbei in der folgenden Datei im Konfigurationsordner "cfg" **verschlüsselt** abgespeichert.

Accountinformationen: „org.jdownloader.settings.AccountSettings.accounts.ejs“

Aufgrund der Verschlüsselung der Anmeldeinformationen sind diese **nicht** im Klartext einsehbar. Eine Recherche im Internet und eine Analyse der verschlüsselten Datei ergab, dass der JDownloader die Anmeldeinformationen unter Verwendung des **Advanced Encryption Standard**-Verfahren (AES) in Kombination mit einer Schlüssellänge von **128bit** verschlüsselt. Aller Voraussicht aufgrund des freigegebenen Quellcodes des JDownloaders, welcher unter der GNU General Public License vertrieben wird, ist der Schlüssel bereits bekannt. Daher können im Internet verschiedene Tools zum Entschlüsseln der Accountdatei bezogen werden.
Mithilfe eines solchen Programms, des jDecrypt in der Version 1.9, konnte die vorliegende Accountdatei entschlüsselt werden, nachdem zuvor ein beispielhafter Free-Account des Sharehosters Uploaded.net angelegt wurde. Der Schlüssel zum Konvertieren des verschlüsselten Dateiinhalts in einen Klartext lautet:

{ 1, 6, 4, 5, 2, 7, 4, 3, 12, 61, 14, 75, -2, -7, -44, 33 }.

Sämtliche (Premium-/Free-)Account zum Herunterladen können durch eine Checkbox in diesem Menüpunkt aktiviert und deaktiviert werden. Die Einstellung hierfür wird jedoch in der Datei zur Speicherung der allgemeinen Einstellungen vorgenommen (vgl. Kap. 2.3.5.1 bzw. Tab. A.2 des Anhangs A, Eintrag „useavailableaccounts“).

2.3.5.5 Standardauthentifizierung

Zum Download von HTTP- oder FTP-Servern wird kein eigenes JDownloader Plugin benötigt. Sollte der Zugang jedoch geschützt sein, müssen die Anmeldeinformationen für den jeweiligen HTTP-/FTP-Zugang unter diesem Menüpunkt separat eingetragen werden. Wie bereits im vorherigen Kapitel 2.3.5.4 werden auch die Informationen der Standardauthentifizierung mittels eines 128bit-langen Passworts und dem AES-Verfahren verschlüsselt. Unter Verwendung des bereits im vorherigen Kapitel vorgestellten Analysewerkzeugs jDecrypt kann diese Datei jedoch entschlüsselt werden. Der Schlüssel zum Konvertieren des verschlüsselten Dateiinhalts in einen Klartext lautet hierbei:

{ 2, 4, 4, 5, 2, 7, 4, 3, 12, 61, 14, 75, -2, -7, -44, 33 }.

Die Accountinformationen der Standardauthentifizierung sind im Konfigurationsordner "cfg" als verschlüsselter Inhalt in der folgenden Datei abgelegt. Nachdem die Accountinformationen durch das Programm jDecrypt entschlüsselt wurden, sind die Klartextinformationen in einer Datei im Ordner des Entschlüsselungstools einsehbar. Die Auflistung A.5 des Anhangs A zeigt den Inhalt einer Beispieldatei in der insbesondere der *Benutzernamen* sowie das *Kennwort* im **Klartext** enthalten sind.

Standardauthentifizierung: „jd.controlling.authentication.AuthenticationControllerSettings.list.ejs“

2.3.5.6 Plugins

Der JDownloader benutzt "Plugins" um, nach eigenen Angaben, einen automatisierten Download für 3300 Webseiten zur Verfügung zu stellen. Im Menüpunkt "Plugins" können einige dieser Webseite-Erweiterungen benutzerspezifisch angepasst werden. Beispielsweise können bei dem Youtube-Plugin die verschiedenen Medien-Typen ausgewählt werden, die von der Webseite bezogen werden sollen. Weiterhin kann bei dieser Erweiterung ein Proxy definiert werden, der nur bei der Kommunikation mit Youtube.com verwendet wird. Jedes Plugin hat gänzlich eigene Einstellungen. Eine umfängliche Analyse der einzelnen Plugins und der damit verbundenen, unter Umständen sehr verschiedenen Einstellungen, ist in Anbetracht des begrenzten Rahmens dieser Arbeit nicht vorgesehen und wurde daher nicht berücksichtigt.
Es wird jedoch vermutet, dass die standardmäßigen Einstellungen jeder Webseite in der jeweiligen Java-Klasse hinterlegt sind. Dies begründet sich in der Tatsache, dass bis dato keine expliziten Dateien identifiziert werden konnten, welche die standardmäßigen Einstellungen einer Webseite enthalten. Wenn jedoch über die Benutzeroberfläche (im Menüpunkt "Plugins" der Einstellungen), Änderungen an den standardmäßigen Einstellungen einer Webseite vorgenommen wurden, werden diese entweder in verschiedenen Dateien im Plugins-Ordner des Anwendungsverzeichnisses

(C:\Users\PC\AppData\Local\JDownloader v2.0\cfg\plugins)

oder in der jeweiligen **subconfig-Datei**, welche direkt im Programmverzeichnis abgespeichert (bspw. "cfg\subconf_uploaded.to.ejs"). Diese ist jedoch verschlüsselt und muss ebenfalls mit dem zuvor bereits mehrmals erwähnten Entschlüsselungsprogramm jDecrypt in einen Klartext konvertiert werden. Der hierzu verwendete Schlüssel lautet wie folgt:

{ 1, 2, 17, 1, 1, 84, 1, 1, 1, 1, 18, 1, 1, 1, 34, 1 }.

Die Auflistung A.6 des Anhangs A zeigt hierzu einen beispielhaften Inhalt des zuvor in der Benutzeroberfläche veränderten Plugins der Webseite uploaded.net. Hierbei wurden sämtliche Auswahlmöglichkeiten des Plugins deaktiviert. Im JDownloader unter dem Einstellungen im Menüpunkt "Plugins" kann das Plugin "uploaded.to" ausgewählt und die nachfolgenden Einstellungen verifiziert werden. In der Abbildung A.6 des Anhangs A sind diese beispielhaft für das Plugin "uploaded.to" abgebildet.

2.3.5.7 Captchas

Aus Sicherheitsgründen verwenden Sharehoster sogenannte "Captchas", um festzustellen, ob ein Mensch oder eine Maschine (Roboter, kurz [Bot]) der Besucher einer entsprechenden Web-Seite/-Adresse ist. Üblicher Weise besteht ein Captcha aus einem kleinen Bild, auf dem eine Zeichenkette abgebildet ist. Im Bezug auf den Download von Dateien versuchen die Sharehoster mittels Chaptchas

zu verhindern, dass eine Maschine/ein Bot automatisiert eine Vielzahl von Dateien herunterladen kann. Aufgrund der primären Auslegung des JDownloaders auf den Download bei Sharehostern, verfügt JDownloader über spezielle Skripte, die automatisch aufkommende Captchas abtasten und versuchen die korrekten Abfragen zu beantworten. Falls die Captcha-Erkennung fehlt schlägt, fordert der JDownloader den Benutzer auf, das Captcha manuell einzugeben.[15]
Die generellen Einstellungen bzgl. des "Captcha"-Moduls werden in der folgenden Datei des Konfigurationsordners "cfg" gespeichert. Die ebenfalls Auflistung A.7 des Anhangs A zeigt die allgemeinen Einstellungsparameter bzgl. des Captcha-Moduls.

Captcha-Einstellungen: „jd.controlling.captcha.CaptchaSettings.json“

Weiterhin gibt es verschiedene Dienste, die ein vollautomatisiertes Lösen von Captchas ermöglichen. Standardmäßig sind bereits verschiedene Dienste zum Lösen von Captchas im JDownloader hinterlegt. Im Menüpunkt "Captchas" können zu jedem Dienst verschiedene Einstellungen vorgenommen werden (vgl. Abb. A.7 des Anhangs A). Das Hauptaufgabe des Captcha-Lösens bei einem standardmäßig konfigurierten JDownloader übernimmt der Dienst "JAntiCaptcha" (Abk. JAC). Die Einstellungen dieses Dienstes sind in den folgenden Dateien hinterlegt.

JAC-Config (1): „org.jdownloader.captcha.v2.solver.jac.JACSolverConfig.json“

JAC-Config (2): „org.jdownloader.captcha.v2.solver.jac.JACSolverConfig.jacthreshold.json“

JAC-Config (3): „org.jdownloader.captcha.v2.solver.jac.JACSolverConfig.whitelistentries.json“

JAC-Config (4): „org.jdownloader.captcha.v2.solver.jac.JACSolverConfig.blacklistentries.json“

JAC-Config (5): „org.jdownloader.captcha.v2.solver.jac.JACSolverConfig.waitformap.json“

Zu jedem der in Abbildung A.7 abgebildeten Dienste, werden die Einstellungen unter den vorgenannten Dateien abgespeichert. Die Struktur zur Ablage der Einstellungsinformationen stellt sich für die jeweiligen Dienste wie folgt dar. **Captcha Dateinamensstruktur:**

„org.jdownloader.captcha.v2.solver.<Dienstname>.<Konfigurationsname>.json“

Teilweise sind diese Dienste jedoch kostenpflichtig. Als Beispiele seien hier zu nennen: deathbycaptcha, imagetyperz, cheapcaptcha oder EndCaptcha. Besitzt der Benutzer ein kostenpflichtiges Konto bei einem der vorgenannten Dienste, können die Anmeldeinformationen über das Einstellungsmenü

[15] Vgl. hierzu Catpcha-FAQ `https://board.jdownloader.org/showthread.php?t=42165` sowie `https://de.wikipedia.org/wiki/Captcha`, `http://www.giga.de/downloads/jdownloader/tipps/jdownloader-captcha-so-lauft-die-automatische-erkennung/`, abgerufen am 27.2.2016

des jeweiligen Dienstes eingegeben werden (vgl. Abb. A.7). In diesem Falle werden die *Anmeldeinformationen* als **Klartext** in einer Konfigurationsdatei abgespeichert. Der Dateiname dieser Konfigurationsdatei entspricht der folgenden Struktur:

„org.jdownloader.captcha.v2.solver.<Dienstname>.<Dienstname>ConfigInterface.json“

In der Auflistung A.8 des Anhangs A ist der Inhalt einer solchen Konfigurationsdatei abgebildet. Neben allgemeinen Diensteinstellungen ist ebenfalls der *Benutzername* und das *Passwort* im **Klartext** zu erkennen.

2.3.5.8 Benutzeroberfläche

Im Menüpunkt „Benutzeroberfläche“ kann das Aussehen des JDownloaders verändert werden. So kann in diesem Einstellungsmenü die Sprache der Anwendung, die Anzeigeinformationen im Hauptfenster "Download" und die einzelnen Kontextmenüs individuell angepasst werden. Die generellen Einstellungen, die in diesem Menüpunkt vorgenommen werden können, werden in der folgenden Dateien des Konfigurationsordners "cfg" gespeichert.

GUI-Einstellungen: „org.jdownloader.settings.GraphicalUserInterfaceSettings.json“

In dieser Datei werden die allgemeine Einstellungen bzgl. der Benutzeroberfläche des JDownloaders gespeichert. Beispielsweise wird in dieser Datei der Überwachungsstatus der Zwischenablage, welcher mit dem Button  in der Symbolleiste de- sowie aktiviert wird (vgl. Abb. 2.1), in die Variable "clipboardmonitored" gespeichert[16]. Die Sprache der Anwendung, welche ebenfalls in diesem Menüpunkt geändert werden kann, wird hingegen in der folgenden Datei gespeichert. Durch die Eingabe des jeweiligen Kürzels der Sprache, bspw. "de" für Deutsch, "en" für Englisch, kann die Sprache der Anwendung verändert werden.

Sprach-Einstellungen: „language.json“

2.3.5.9 Sprechblasen

Im Menüppunkt „Sprechblasen“ kann können Einstellungen bzgl. der Anzeige von Popup-Nachrichten vorgenommen werden. Standardmäßig ist beispielsweise das Aufkommen einer Sprechblase aktiviert, wenn ein neuer Link der Zwischenablage hinzugefügt und daraufhin vom Linkgrabber-Modul nach herunterladbaren Inhalten durchsucht wird. Die Einstellungen bzgl. der Anzeigebenachrichtigungen in Form einer Sprechblase werden in der folgenden Datei abgespeichert.[16]

Sprechblasen-Einstellungen: „org.jdownloader.gui.notify.gui.BubbleNotifyConfig.json“

[16] Aufgrund der Vielzahl an Einstellungsmöglichkeiten dieser Datei und der geringen Relevanz des Menüpunktes hinsichtlich einer forensischen Untersuchung wird auf die Darstellung des Inhalts dieser Dateien verzichtet.

2.3.5.10 My.JDownloader

Mithilfe der Zusatzsoftware "My JDownloader" ist es möglich, seinen lokal installierten JDownloader und die damit verbundenen Downloads dezentral über das Internet zu steuern. Hierzu kann man einen kostenloses Benutzerkonto auf der Webseite des Projektes erstellen. Diese Zugangsdaten werden im Einstellungsmenü "My.JDownloader" hinterlegt, woraufhin der Zugriff auf sämtliche Funktionen des JDownloaders (Downloads hinzufügen/entfernen, Geschwindigkeiten regulierten und allgemeine Einstellungen vornehmen) über die Webseite/Web-App des Projektes möglich ist. Des Weiteren ist "My JDownloader" ebenfalls über entsprechende Apps für die mobilen Betriebssysteme IOS, Android und Windows Phone verfügbar, sodass der JDownloader ebenfalls über das Smartphone gesteuert werden kann.
Die Zugangsdaten zum Verbinden des lokalen JDownloaders mit der Webplattform "My JDownloader" werden über den Menüpunkt "My.JDownloader" in den Einstellungen der Software vorgenommen. Die Abbildung A.8 des Anhangs A zeigt hierzu eine erfolgreiche Verbindung des JDownloaders mit My.JDownloader, nachdem gültige Anmeldeinformationen eingegeben und diese durch Auswahl des Buttons "Verbinden" vom Server bestätigt wurden. Die Anmeldeinformationen zur Benutzung des My.JDownloaders werden in der nachfolgenden Datei des Konfigurationsverzeichnisses "cfg" abgespeichert. Die Auflistung A.9 des Anhangs A zeigt den Inhalt dieser Datei, in der unter Anderem die *Anmeldeinformationen* für den Zugang zum My.JDownloader (vgl. Abb. A.8) im **Klartext** abgespeichert werden.

My.JDownloader-Einstellungen:

„org.jdownloader.api.myjdownloader.MyJDownloaderSettings.json“

2.3.5.11 Linkfilter

Der "Linkfilter" kann genutzt werden, um ausgewählte Links, Adressen und Dateien mit bestimmten Eigenschaften zu filtern, gruppieren oder zu ignorieren. Dieser Objekte werden daraufhin einer schwarzen Liste hinzugefügt und von der Anwendung ignoriert, sodass beispielsweise das automatische Sammeln bestimmter Links verhindert wird. Hierzu wird der Regelassistent der Abbildung A.9 des Anhangs A verwendet.
Mit dem oben dargestellten Regelassistent kann eine beliebige Anzahl an Links, Adressen und Dateien erstellt werden, die von der Anwendung ignoriert werden sollen. Diese Liste mit sämtlichen Filterregeln wird in der folgenden Datei des Konfigurationsordners "cfg" abgespeichert.

Linkfilter-Einstellungen: „org.jdownloader.controlling.filter.LinkFilterSettings.filterlist.json“

2.3.5.12 Paketverwalter

Mithilfe des Moduls "Paketverwaltung" werden bestimmte Download-Einstellungen (Speicherort, Priorität, Automatisierter Download, Verwendung bestimmter Plugins...) anhand von zuvor fest definierten Bedingungen auf neu hinzugefügte Pakete angewandt. Die Abbildung A.10 des Anhangs A zeigt hierzu den Regelassistent, welcher unter den Einstellungen im Menüpunkt "Paketverwalter" abrufbar ist. Mithilfe des Regelassistenten kann die Verwaltung von neu hinzugefügten Paketen automatisiert werden. Die Paketregel der Abbildung A.10 des Anhangs A speichert beispielsweise sämtliche neu hinzugefügten Dateien mit der Zeichenkette „M16_FilmDatei“ im Dateinamen unter dem Pfad „C:\PC\Download\Filme“ und setzt für diese Pakete die höchste Priorität. Anhand der Priorität eines Paketes wird ausgewählt, mit welches Paket nach der Fertigstellung des aktuellen Downloads als nächstes heruntergeladen werden soll.
Mit dem Regelassistent der Abbildung A.10 kann eine beliebige Anzahl an Paketverwaltungsregeln erstellt werden. Diese Liste mit sämtlichen Verwaltungsregeln wird in der folgenden Datei des Konfigurationsordners "cfg" abgespeichert.

Paketverwaltungs-Einstellungen:

„org.jdownloader.controlling.packagizer.PackagizerSettings.rulelist.json“

2.3.5.13 Archiventpacker

Eines der wichtigsten Plugins für solche Anwender der Software, die massenhaft Dateien von Sharehostern beziehen, ist der "Archiventpacker". Aufgrund der Begrenzung der maximalen Dateigröße bei den meisten One-Click-Hostern (Share-Online.biz 300Mb, Uploaded.net 500Mb)[17], werden große Datenmengen (bspw. Videodateien) auf einzelne, kleinere Archive mit geringerer Dateigröße aufgeteilt. Ohne ein entsprechendes Modul, müsste der Anwender nach erfolgreichem Abschluss des Downloads jedes einzelne Archiv manuell entpacken. Das Plugin "Archiventpacker" übernimmt standardmäßig diese Arbeit und startet automatisch den Entpackungsvorgang nach erfolgreichem Abschluss des Downloads. Selbst wenn das Archiv mit einem Passwort geschützt ist, versucht der Archiventpacker, anhand einer internen Passwortliste, das richtige Passwort zu erraten. Weiterhin kann beispielsweise ein explizites Verzeichnis angegeben werden, in das der Archiventpacker die Daten nach erfolgreicher Dekomprimierung verschieben soll.
Die allgemeinen Einstellungen des Archiventpackers werden in der folgenden Datei des Konfigurationsordners "cfg" abgespeichert. Hierzu enthält die Auflistung A.10 des Anhangs A eine Aufstellung mit sämtlichen Einstellungsmöglichkeiten, die unter dem Menüpunkt "Archiventpacker" in den Einstellungen verändert werden können.

[17] Vgl. hierzu `http://filehoster.info/filehoster`, abgerufen am 27.2.2016

Archiventpacker-Einstellungen:

„org.jdownloader.extensions.extraction.ExtractionExtension.json“

Die zu Anfang erwähnte Liste mit sämtlichen Passwörtern, die der Archiventpacker nacheinander ausprobiert, falls ein Archiv mit einem Kennwort geschützt ist, wird jedoch separat in der folgenden Datei abgelegt.

Archiventpacker-Passwortliste:

„org.jdownloader.extensions.extraction.ExtractionExtension.passwordlist.json“

Unter Verwendung von regulären Ausdrücken können sämtliche Dateien, die explizit nicht entpackt werden sollen, im oben dargestellten Menüpunkt der Einstellungen definiert werden. Diese regulären Ausdrücke werden nochmals in einer unabhängigen Datei unter dem nachstehenden Pfad gespeichert.

Archiventpacker-Ausnahmen:

„org.jdownloader.extensions.extraction.ExtractionExtension.blacklistpatterns.json“

2.3.5.14 Infosymbol (Passwortschutz)

Im Menüpunkt "Infosymbol" der Einstellungen kann die standardmäßig aktivierte Minimierung des JDownloaders in den Infobereich/Taskleiste deaktiviert werden. Weiterhin können die Aktionen ausgewählt werden, welche ausgeführt werden, wenn der Benutzer versucht den JDownloader zu minimieren oder zu schließen. Diese und weitere Einstellungen werden in der folgenden Datei des Konfigurationsordners "cfg" abgespeichert. Hierzu enthält die nachfolgende Auflistung A.11 des Anhangs A eine Aufstellung mit sämtlichen Einstellungsmöglichkeiten, die unter dem Menüpunkt "Infosymbol" in den Einstellungen verändert werden können.

Infosymbol-Einstellungen: „org.jdownloader.gui.jdtrayicon.TrayExtension.json“

Aus forensischer Sicht ist jedoch eine andere Einstellungsmöglichkeit von weitaus größerer Bedeutung. Denn zusätzlich zu den vorgenannten Einstellungen kann in diesem Menüpunkt ein Passwort zum Schutz gegen den unbefugten Zugriff auf den JDownloader definiert werden, welches bei Programmstart und bei der Maximierung der Anwendung aus der Taskleiste abgefragt wird. Die nachfolgende Abbildung 2.5 zeigt hierzu das Fenster zur Abfrage des zuvor in den Einstellungen definierten Passwortes.
Unter Verwendung der zu Anfang dargestellten Vorgehensweise des Vorher-Nacher-Vergleichs (vgl. 2.3.5, konnte diesbezüglich festgestellt werden, dass das Passwort nicht in der oben genannten Datei, welche zur Speicherung der Einstellungen des Menüpunktes "Infosymbol" verwendet wird, hinterlegt

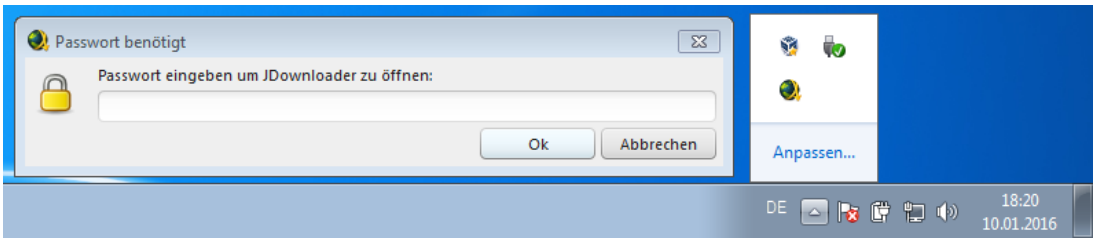


Abbildung 2.5: Passwortabfrage bei Programmstart oder Reaktivierung der Software

ist (vgl. Listing A.11). Dieses *Passwort* wird obskurer Weise mit den Einstellungen der Benutzeroberfläche zusammen im **Klartext** in der nachfolgenden Datei abgelegt (vgl. Kap. 2.3.5.8). Insofern ist das jeweilige Passwort zu eigentlichen Schutz der Anwendung vor unautorisierter Nutzung in der folgenden Datei hinter der Variable "password" einsehbar.

Passwort-Einstellungen: „org.jdownloader.settings.GraphicalUserInterfaceSettings.json“

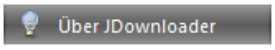
2.3.5.15 Profieinstellungen

Im Menüpunkt "Profeinstellungen" können erfahrene Anwender spezifische Einstellungen der Software auf direktem Wege vornehmen. Vor diesem Hintergrund enthält das Einstellungsmenü keine benutzerfreundlichen Auswahlfelder, sondern lediglich eine Auflistung mit softwareinternen Variablen und deren Standardwerten. Die aufgelisteten Variablen überschneiden sich teilweise mit den jeweiligen Einstellungen, die in den vorherigen Kapiteln vorgestellt wurden. Der Unterschied liegt darin, dass in diesem Menü den programminternen Variablen unmittelbar Werte zugewiesen werden können. Eine Überprüfung der Werte auf Gültigkeit findet nicht statt, sodass der Anwender dazu aufgefordert wird, sehr vorsichtig und gewissenhaft bei Veränderungen der Werte vorzugehen.
Wie bereits erwähnt, überschneiden sich die Variablen teilweise mit den Einstellungen der vorherigen Kapitel, welche durch die Benutzeroberfläche vorgenommen werden konnten. Aufgrund der Vielzahl an Einstellungsmöglichkeiten in diesem Profimenü, wurden anhand des Variablennamens (Schlüssel) und der dazugehörigen Beschreibung die jeweiligen Einstellungsmöglichkeiten verschiedenen Kategorien und den zugrundeliegenden Konfigurationsdateien, in denen die Einstellungswerte gespeichert werden, zugeordnet. Die Tabelle A.3 des Anhangs A zeigt diese Kategorien und führt weiterhin die zugrundeliegende Konfigurationsdatei auf.

2.4 Digitale Anwendungsspuren

Das vorherige Kapitel 2 beschreibt die Ergebnisse der technischen Anwendungsuntersuchung des JDownloaders und somit die jeweiligen Dateien, welche zur persistenten Speicherung der Programmeinstellungen verwendet werden. Auf der Grundlage dieser Ergebnisse werden im Folgenden explizit diejenigen digitalen Spuren vorgestellt, welche bei einer allgemein typischen Verwendung der Software entstehen (vgl. Kap. 2.2, Phase 3 & 4) und daher zur Rekonstruktion der vergangener Benutzerinteraktionen mit der Software von elementarer Bedeutung sind.
An dieser Stelle sei darauf hingewiesen, dass in keinem Fall die Anwendung gestartet oder etwaige Änderungen vorgenommen werden sollten, da somit wichtige, teilweise protokollierte, Ereignisse mit Informationen über die vergangene Verwendung der Software überschrieben oder gelöscht werden können. Von der Anwendung sollte daher zu Anfang eine Arbeitskopie erzeugt werden, auf Basis derer eine statische Untersuchung der Software durchgeführt werden kann.

2.4.1 Versionsinformationen

Die Versionsinformationen zur aktuell verwendeten Version des JDownloaders kann in der Symbolleiste der Benutzeroberfläche über den Menüpunkt `Hilfe` → 

eingesehen werden. Die Darstellung A.12 des Anhangs A zeigt hierzu die angezeigten Versionsinformationen.
Wie in der Einführung dieses Kapitels geraten, sollte jedoch bei einer forensischen Untersuchung die Software nicht ausgeführt werden. Stattdessen können die Versionsinformationen in der Datei „build.json“ des Hauptverzeichnisses eingesehen werden. Die Auflistung A.12 des Anhangs A zeigt hierzu die in dieser Datei enthaltenen Informationen, welche mit über die grafische Oberfläche der Abbildung A.12 dargestellt werden.
Über den Button  in der Symbolleiste der Software kann der Aktualisierungsprozess gestartet und neue Versionen der Software installiert werden. Bei jeder Versionsaktualisierung werden nicht nur die alten Dateien der Software mit den neuen Dateien überschrieben, sondern zudem ein Aktualisierungsprotokoll erzeugt. Durch die genaue Protokollierung jeder Aktualisierung ist der gesamte Versionsverlauf anhand der Protokolle der nachfolgenden Struktur einzusehen. Das nachfolgende Listing A.13 des Anhangs zeigt beispielsweise die Aktualisierung der Software von der Revision 7150 auf die Revision 7165.

Versionsverlauf: „\logs\updatehistory\<oldVersion>_to_<newVersion>.log“

2.4.2 Ereignisprotokollierung

Die Tabelle A.1 des Anhangs A zeigt sämtliche Dateien und Verzeichnisse des Hauptverzeichnisses, unter dem der JDownloader installiert wurde. In der Zeile 9 der vorgenannten Tabel-

le ist der Ordner „\logs\“ dargestellt. In diesem Ordner werden während der Verwendung des JDownloaders eine Vielzahl an Ereignissen (Status-/Fehlermeldungen) protokolliert. Hierzu wird bei jedem Programmstart ein neues Verzeichnis unter Verwendung der Struktur „<Datum in ms>_<Datumsangabe, Uhrzeit Zeitzone>“ erzeugt (bspw. „1450968837647_Thu, Dec 24, 2015 15.53 +0100“), in dem **jedes einzelne** Modul der Software seine durchgeführten Aktionen protokolliert. Beispielsweise wird vom „hoster“-Plugin die **Uhrzeit** und die **IP-Adresse** des Clients für den letzten Verbindungsversuch mit jedem Hoster protokolliert (vgl. „\cfg\<hoster, bspw. uploaded.to>_jd.plugins.hoster.Uploadedto.log.0“).
Diese Verzeichnisse stellen den Ausgangspunkt einer forensischen Analyse dar, da die darin enthaltenen Informationen detaillierte Angaben zur Benutzung der Software enthalten und anhand dieser Spuren vergangenen Sitzungen nahezu vollständig rekonstruiert werden können. Ursprünglicher Weise sind diese Protokolle für den Anwendersupport gedacht. Über den Menüpunkt `Help` → `Create Log` werden die Protokolle der aktuellen oder einer vergangenen Benutzung der Software an einen Server des Herstellers gesendet und dem Benutzersupport gemeldet.
Standardmäßig werden jedoch lediglich die Protokolle der letzten beiden Tage gespeichert. Bei jedem Programmstart werden die Datumsangaben der Protokolle überprüft und ggf. veraltete Protokolle (älter als zwei Tage) **gelöscht**. Die maximale Anzahl der Tage zur Vorhaltung der Protokolle wird in der Konfigurationsdatei „org.appwork.utils.logging2.LogConfig.json“ des Ordners „\cfg\“, in der Variable „cleanuplogsolderthanxdays“, gespeichert (vgl. Listing A.14 des Anhangs A).

2.4.3 Backupdateien

Ein weiteres wichtiges Untersuchungsobjekt im Bezug auf die Analyse und Rekonstruktion vergangener Verwendungen des JDownloaders sind Sicherungskopien der Softwareeinstellungen. Hierzu sollte bei jeder Analyse überprüft werden, ob sich auf dem Dateisystem des Untersuchungsobjektes eine Backup-Datei auffinden lässt. Diese Sicherungskopien werden im Dateiformat „.jd2backup“ abgespeichert. Eine Sicherung der aktuellen Einstellungen kann über den Menüpunkt `Datei` → `Sicherung` → `Speicherort wählen` → `*.jd2backup` erstellt werden. Da sämtliche Einstellungen in einer einzigen Backup-Datei komprimiert abgelegt werden, muss zur Wiederherstellung der Einstellungen, die Datei in den JDownloader innerhalb einer separaten Analyseumgebung importiert werden. Lediglich bei der erstmaligen Erstellung einer Sicherungskopie der Einstellungen werden in der Windows-Registry die folgenden Einträge der Auflistung 2.5 vorgenommen. Sollten insofern auf dem Untersuchungsobjekt diese Einträge vorhanden sein, kann davon ausgegangen werden, dass mindestens eine Sicherung der Einstellungen vom Benutzer durchgeführt wurde. Sind diese Einträge nicht vorhanden, kann dementsprechend davon ausgegangen werden, dass vom Benutzer keine Sicherungskopien erstellt wurden.

Listing 2.5: Erstellte Windows-Registry Einträge bei erstmaliger Konfigurationssicherung

```
1 HKU\S-1-5-21-539846951-2775919047-120045064-1000\Software\Microsoft\Windows\
      CurrentVersion\Explorer\FileExts\.jd2backup
2 HKU\S-1-5-21-539846951-2775919047-120045064-1000\Software\Microsoft\Windows\
      CurrentVersion\Explorer\FileExts\.jd2backup\OpenWithList
```

2.4.4 Download-Speicherort

Wie bereits in Kapitel 2.1 beschrieben beinhaltet der JDownloader ein „Linksgrabber/-sammler“-Modul, welches standardmäßig die Zwischenablage des Betriebssystems überwacht und automatisch aufgefundene HTTP-Adressen nach herunterladbaren Inhalten durchsucht und gefundene Inhalte im JDownloader anzeigt. Sobald über diese Funktion - alternativ über den Button `Neue Links hinzufügen` - herunterladbare Inhalte dem Linksammler hinzugefügt werden, erstellt JDownloader ein Archiv mit den Informationen zu diesen Dateien im Konfigurationsordner „cfg“. Hierbei werden jedoch standardmäßig lediglich die letzten fünf hinzugefügten Links abgespeichert, die dem Linksammler hinzugefügt wurden. Diese Eigenschaft wird in der Konfigurationsdatei der allgemeinen Einstellungen („org.jdownloader.settings.GeneralSettings.json“, vgl. Kap. 2.3.5.1, Tab. A.2, Z. 14) mit der Variable „keepxoldlists“ definiert. Wird dem Linksammler nun ein herunterladbarer Inhalt angezeigt, erstellt der JDownloader automatisch ein Archiv im „cfg“-Verzeichnis unter der Namensstruktur „linkcollector<fortlaufendeNr>.zip“. Die Nummer im Dateinamen zeigt dabei an, wie viele Links bereits dem Linksammler hinzugefügt wurden.
Die nachfolgende Abbildung 2.6 zeigt mehrere beispielhafte Downloaddateien, die durch ein Kopieren der jeweiligen Downloadadressen in die Zwischenablage, automatisch vom JDownloader der Linksammler-Liste hinzugefügt wurden. Parallel hierzu wurde von JDownloader eine Archivdatei mit dem Namen „linkcollector1337.zip‘ erstellt.
Bereits anhand der fortlaufenden Nummer 1337 der vorgenannten Archiv-Datei „linkcollector1337.zip“ kann bei einer forensischen Untersuchung erkannt werden, dass bereit zuvor insgesamt 1336 weitere Male verschiedene Dateien dem JDownloader hinzugefügt wurden. Das Archiv enthält insgesamt 12 Textdateien ohne Angabe eines Dateityps (00, 00_0 - 00_9, extraInfo). Jedes Archiv ist hierbei unter derselben Struktur gleich aufgebaut. Die Datei „00“ enthält hierbei Informationen über das generelle Paket, welches heruntergeladen werden soll. In der Auflistung A.15 des Anhangs A ist der Inhalt einer „00“-Datei aufgeführt.
Weiterhin enthält das Archiv „linkcollector1337.zip“ zu jeder einzelnen Datei, die dem Linksammler hinzugefügt wurde (OnTrHi01.part01.rar - OnTrHi01.part10.rar, vgl. Abb. 2.6), eine Datei, die spezifische Informationen zum Bezug der Datei von einer bestimmten Quelle enthält. Diesbezüglich zeigt die Auflistung A.16 des Anhangs den beispielhaften Inhalt einer solchen Datei. Wesentlicher

Bestandteil dieser Datei sind der **Dateiname**, **Bezugsquelle/Downloadlink**, **Dateigröße** und weitere Informationen zur eindeutigen Identifizierung der Datei gegenüber der Bezugsquelle.

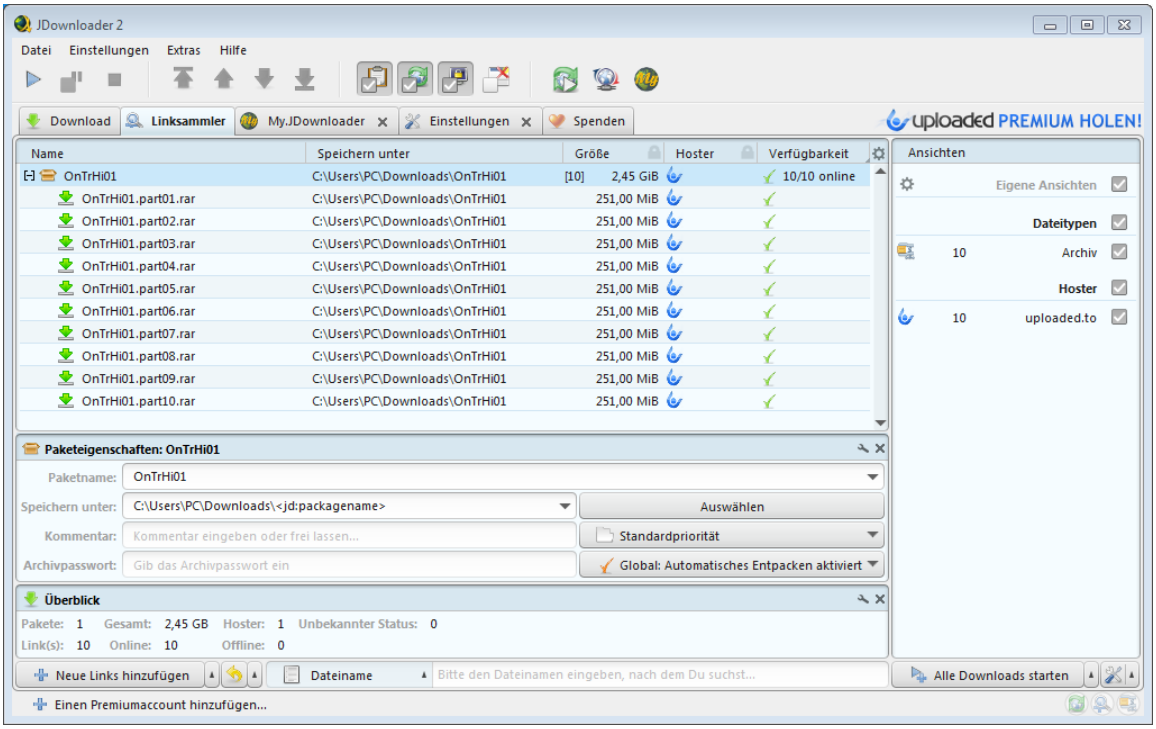


Abbildung 2.6: Linksammler mit hinzugefügten Downloaddateien

Abschließend enthält das Archiv jedoch zusätzlich zu den vorgenannten Informationen eine Datei mit der **Pfadangabe**, unter dem der Download auf dem Client gespeichert werden soll sowie einen Zeitstempel in Sekunden, der angibt, zu welchem Zeitpunkt die Dateien dem Linksammler hinzugefügt wurden. Die nachfolgende Auflistung 2.6 zeigt den Inhalt der „ExtraInfo“-Datei, welche bezüglich des Paketes in der Linksammler-Ansicht erstellt wurde, das in der Abbildung 2.6 dargestellt wird.

Listing 2.6: Inhalt einer beispielhalften LinkCollector ExtraInfo-Datei

```
1 \cfg\linkcollector1337.zip\extraInfo
2 {
3   "rootPath" : "C:\\Users\\PC\\AppData\\Local\\JDownloader v2.0",
4   "timeStamp" : 1362761650
5 }
```

Unabhängig der vorgenannten Informationen wird bei jeder Änderung des Speicherortes, der **Ort** sowie der **Zeitpunkt** der Änderung in einer Downloadpfad-Historie abgespeichert. Diese Daten bzgl. der Historie sind in der Verlaufsdatei „org.jdownloader.gui.views.linkgrabber.addlinksdialog.-LinkgrabberSettings.downloaddestinationhistory.json‘ im Konfigurationsordner „\cfg\“ abgespeichert. Die nachfolgende Auflistung 2.7 enthält den beispielhaften Inhalt einer solchen Datei. Anhand

dieser Datei sind die jeweiligen Downloadpfade, die der JDownloader als Speicherort für die heruntergeladenen Dateien benutzte, sehr gut nachzuverfolgen. Beispielsweise lässt sich anhand des Inhalts der Auflistung 2.7 feststellen, dass als Speicherort der Downloads mehrmals Laufwerksbuchstaben „F:“ und „G:“ benutzt wurden. Weitere allgemeine forensische Analysen des Betriebssystem könnten hierzu detaillierte Informationen liefern, ob es sich möglicherweise hierbei um externe Speichermedien handelte.

Listing 2.7: Historie zur Änderungen des Downloadpfades

```
1  org.jdownloader.gui.views.linkgrabber.addlinksdialog.LinkgrabberSettings.
       downloaddestinationhistory.json
2  [ {
3    "name" : "C:\\Users\\PC\\Desktop\\Test",
4    "time" : 1448922278792
5    }, {
6    "name" : "F:\\Download",
7    "time" : 1446761876342
8    }, {
9    "name" : "C:\\Users\\PC\\downloads",
10   "time" : 1423085356417
11   }, {
12   "name" : "G:\\DL",
13   "time" : 1394732369600
14   }, {
15   "name" : "F:\\DL",
16   "time" : 1393014433081
17 } ]
```

2.4.5 Download-Verlauf

Sobald der Download eines Paketes im JDownloader gestartet wird, wird dieses Paket von der Ansicht des „Linksammler“-Moduls in die „Download‘-Ansicht/-Register verschoben und der Download des ausgewählten Paketes beginnt. Im Zuge dessen wird ebenfalls, wie bereits in Kapitel 2.4.4 beschrieben, automatisch ein Archiv mit den Informationen zu den Dateien erstellt, die aktuell heruntergeladen werden. Die bereits im vorgenannten Kapitel erwähnte Programmvariable „keepxoldlists“ der Konfigurationsdatei „org.jdownloader.settings.GeneralSettings.json“ definiert hierbei die maximale Anzahl an vorgehaltenen Downloadlisten. Der Wert dieser Variable ist standardmäßig auf 5 gesetzt (vgl. Kap. 2.4.4). Ab dem 6ten Download wird daher die jeweils älteste Download-Liste gelöscht, um eine neue Liste für den aktuellen Download erzeugen zu können. Diese Archivdateien werden jeweils im „cfg“-Verzeichnis unter der Namensstruktur „downloadList<fortlaufendeNr>.zip“ erstellt.

Die fortlaufende Nummer im Dateinamen gibt, wie bereits zuvor bei den erstellten Archiven zu den Link-Listen, die Anzahl der bereits durchgeführten Downloads an.

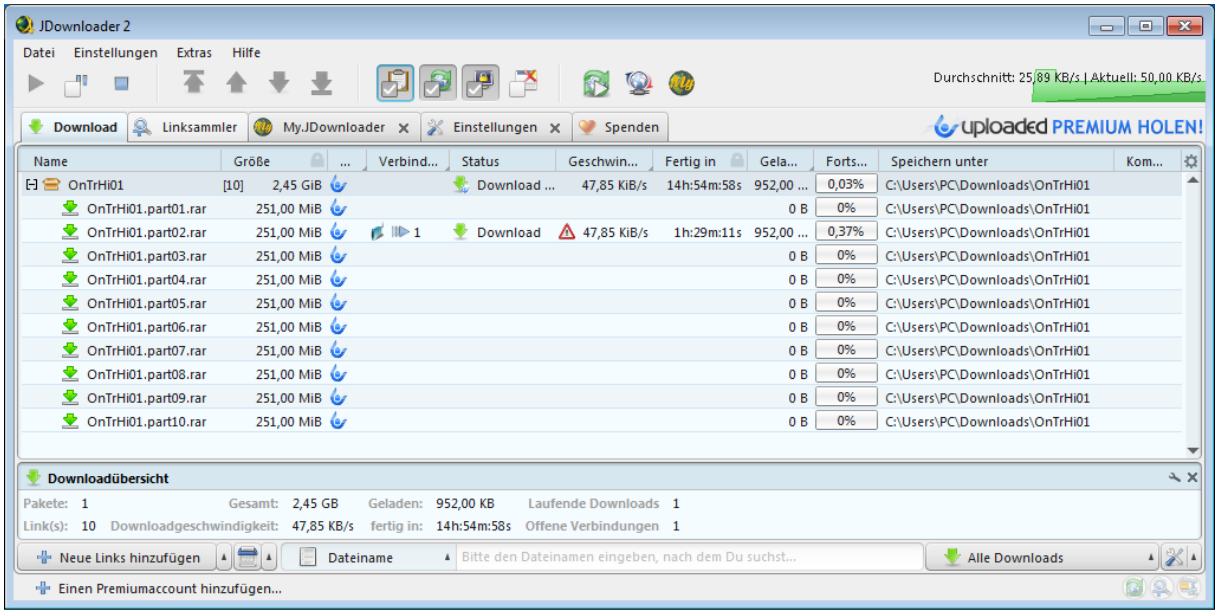


Abbildung 2.7: Gestarteter Download verschiedener Dateien

Die oben dargestellte Abbildung 2.7 zeigt den Start der zuvor im vorherigen Kapitel 2.4.4 dem Linksammler hinzugefügten Downloads. Parallel zu diesem Download wurde vom JDownloader eine Archivdatei mit dem Namen „downloadList1337.zip“ erstellt. Das Archiv enthalten ebenfalls 12 verschiedene Textdateien ohne Angabe eines Dateityps (00, 00_0 - 00_9, extraInfo). Wie bereits im vorherigen Kapitel enthält die Datei „00“ generelle Informationen über das Paket, welches aktuell heruntergeladen wird. Die nachfolgende Auflistung zeigt den Inhalt der „00“-Datei des zuvor gestarteten Downloads der Abbildung 2.7.

Listing 2.8: Inhalt einer beispielhalften downloadList 00-Datei

```
1  \cfg\downloadList1337.zip\00
2  {
3    "links" : [ ],
4    "name" : "OnTrHi01",
5    "properties" : {
6    "EXPANDED" : true
7    },
8    "uid" : 1452536813263,
9    "created" : 1452531251110,
10   "downloadFolder" : "C:\\Users\\PC\\Downloads\\OnTrHi01"
11 }
```

Weiterhin enthält das Archiv „downloadList1337.zip“ zu jeder einzelnen Datei, die in der Abbildung 2.7 dargestellt wird (OnTrHi01.part01.rar - OnTrHi01.part10.rar), eine Textdatei innerhalb des vorgenannten Archives, die spezielle Informationen zum Download dieser Datei enthält. Hierzu zeigt die nachfolgende Auflistung 2.9 den beispielhaften Inhalt der „00_0“-Datei des vorgenannten Archivs, welche detaillierte Informationen über den Bezug der Datei „OnTrHi01.part01.rar“ beinhaltet.

Listing 2.9: Inhalt einer beispielhalften downloadList 00_0-Datei

```
1  \cfg\downloadList1337.zip\00\_0
2  {
3    "name" : "OnTrHi01.part01.rar",
4    "url" : "http://uploaded.net/file/mgkt722z",
5    "properties" : {
6      "FINAL_FILENAME" : "OnTrHi01.part01.rar",
7      "URL_CONTENT" : "http://ul.to/mgkt722z",
8      "SHA1" : "4e12583812fe3994db899c51a9b663ab22ed6cea",
9      "LINKDUPEID" : "uploaded.to://mgkt722z",
10     "ARCHIVE_ID" : "19887b5d0a705491bab5cd364899cd7685916fdf4b241ea68ac36059339bb2e2
           ",
11     "VERIFIEDFILESIZE" : 263192616
12   },
13   "size" : 263192616,
14   "host" : "uploaded.to",
15   "enabled" : true,
16   "uid" : 1452531251112,
17   "created" : 1452531250437,
18   "propertiesString" : null,
19   "availablestatus" : "TRUE",
20   "urlProtection" : "UNSET",
21   "linkStatus" : null,
22   "current" : 0,
23   "chunkProgress" : null,
24   "finalLinkState" : null
25 }
```

Abschließend enthält das Archiv, zusätzlich zu den vorgenannten Dateien (00, 00_0 - 00_9) eine weitere Datei mit dem Namen „extraInfo“, welche Informationen bzgl. des Speicherortes der heruntergeladenen Dateien und dem Zeitpunkt, an dem der Download gestartet wurde, beinhaltet. Die nachfolgende Auflistung 2.10 zeigt hierzu den Inhalt der „ExtraInfo“-Datei, welche für das heruntergeladene Paket im Download-Ansicht erstellt wurde, das in der Abbildung 2.7 dargestellt wird.

Listing 2.10: Inhalt einer beispielhalften downloadList ExtraInfo-Datei

```
1 \cfg\linkcollector1337.zip\extraInfo
2 {
3   "rootPath" : "C:\\Users\\PC\\AppData\\Local\\JDownloader v2.0",
4   "timeStamp" : 1362761650
5 }
```

2.4.6 Entpackungs-Historie

Das Kapitel 2.3.5.13 beschreibt das Modul des „Archiventpackers“, welcher automatisch komprimierte Archivdateien entpackten kann. Bezogen auf den illegalen Bezug von urheberrechtlich geschütztem Material, kann dieses Modul bei einer forensischen Untersuchung möglicherweise die zuverlässigsten Informationen liefern, wenn es um die Frage geht, ob von einem System mit dem JDownloader entsprechend geschütztes Material bezogen wurde.
Wie bereits im Kapitel 2.3.5.13 beschrieben, müssen große Dateien aufgrund einer maximalen Beschränkung der Dateigröße bei fast sämtlichen Filehostern auf kleinere Archive mit geringerer Dateigröße aufgeteilt werden. Dadurch geht oftmals der Bezug verloren, um welche gesamtheitliche Datei es sich überhaupt handelt. Wird beispielsweise ein neuer Kinofilm in mehrere Archive aufgeteilt, welche darauffolgend bei einem Filehoster hochgeladen werden, ist es dem Anbieter (Filehoster) und Anderen, nur sehr schwer möglich, den eigentlichen Bezug der einzelnen Archive zum zugrundeliegenden Kinofilm herzustellen. Dies macht das den Download von illegalem Material explizit von Sharehostern bei Raubkopierern so beliebt. Das Verfahren machen sich somit Raubkopierer zu Nutze, um eine Vielzahl an unter Schutz stehendem Material im Internet **unerkannt** zu verbreiten. Liegt einem Forensiker ein Untersuchungsobjekt eines Raubkopierers vor, ist es an ihm, den Bezug zwischen den heruntergeladenen Dateien und dem zugrundeliegendem, mglw. urheberrechtlich geschütztem Material wiederherzustellen. Wurde zum Bezug der Dateien der JDownloader verwendet, sollte dem Modul „Archiventpacker“ besondere Aufmerksamkeit gewidmet werden.
Sofern im Programmverzeichnis „\logs“ noch Informationen über vorherige Sitzungen vorhanden sind, sollten die vom Archivenpacker-Modul erstellten Protokolldateien untersucht werden. Diese sind unter im vorgenannten Ordner unter dem Verzeichnis der jeweilig Sitzung (vgl. Kap. 2.4.2) enthalten und protokollieren die Uhrzeit und die Datei beim Entpacken eines jeden verschiedener Archives. Falls das jeweilige Archiv mit einem Passwort geschützt ist, wird ebenfalls protokolliert, welche Passwörter zum Entpacken des Archives ausprobiert wurden und der damit einhergehende Entpackungsvorgang, unter Verwendung des entsprechenden Passwortes, erfolgreich war oder abgebrochen wurde. Hierzu sind insbesondere die folgenden Dateien unter dem beispielhaften Pfad

„C:\Users\PC\AppData\Local\JDownloader v2.0\logs\1449661833932_Wed, Dec 9, 2015 12.50 CET\“ von Bedeutung.

Archiventpacker-Protokollinformationen:

(1.) „ExtractionExtension.log.0“
(2.) „org.jdownloader.extensions.extraction.ArchiveController.log.0“
(3.) „org.jdownloader.extensions.extraction.ExtractionController.log.0“

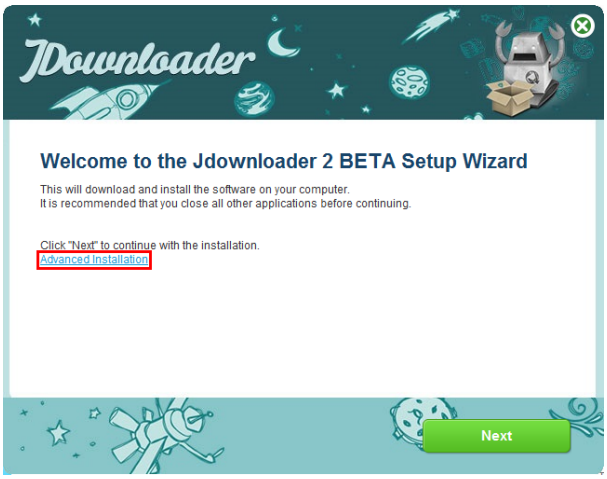
Weiterhin wird unter dem Verzeichnis „\logs\extracting\“ jeder einzelne Entpackungsvorgang protokolliert. Im Gegensatz zum vorgenannten Protokoll enthält das Verzeichnis „\logs\extracting\“ eine Protokolldatei zu jedem durchgeführten Extraktionsvorgang. Unter Angabe eines Zeitstempels in Sekunden (bspw. 1449539260352 für den 12/08/2015 02:47:40 Uhr) werden in den einzelnen Protokollen zum Entpackungsvorgang, sämtliche Detailinformationen über die Extraktion des jeweiligen Archives festgehalten. Hierzu zählen beispielsweise sämtliche verbundene **(Teil-)Archive**, der finale **Extraktionspfad**, ggf. das **verwendete Passwort** zum Entschlüsseln des Archives und der extrahierte **Klartextname der Dateien**, die im jeweiligen Archiv enthalten sind.
In der Auflistung A.17 des Anhangs A ist der Inhalt des Protokolls dargestellt, welches während des Extraktionsvorgangs des Archivs „OnTrHi04.part01.rar“ erzeugt wurde (vgl. Abb. 2.6 und 2.7). Anhand dieses Protokolls kann beispielsweise der Bezug zwischen den Dateien „OnTrHi04.part01.rar“ - „OnTrHi04.part10.rar“ und der extrahierten, mglw. urheberrechtlich geschützten Datei „tvs-one-tree-hill-ded-dl-ithd-x264-401.mkv“ hergestellt werden, welche auf dem Laufwerk „C:“ unter dem Pfad „\Users\PC\Desktop\Downloads\OnTrHi01\One.Tree.Hill.S04.German.Dubbed.DL.iTunesHD.x264-TVS\One.Tree.Hill.S04E01.Das.grosse.Erwachen.German.Dubbed.DL.iTunesHD.x264-TVS“ abgespeichert wurde.

3 Zusammenfassung

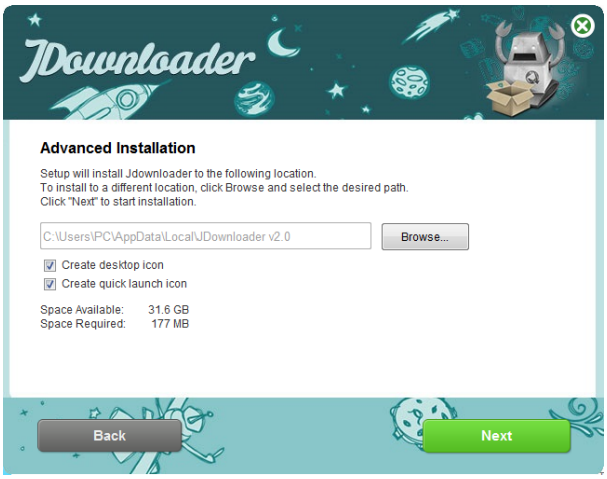
Die vorliegenden Dokumentation der Anwendungsanalyse des JDownloaders zeigt, dass während der Benutzung der Software eine Vielzahl von Spuren auf dem Dateisystem des Betriebssystems entstehen, von denen der jeweilige Anwender im Allgemeinen keine Kenntnis hat. So wird aufgezeigt, dass sämtliche Einstellungen, die im Download-Manager über die Benutzeroberfläche vorgenommen werden können, in einzelnen Dateien im Installationsverzeichnis der Software abgespeichert werden (vgl. Kap. 2.3.5). Doch nicht nur bei der Änderung der Softwareeinstellungen hinterlässt der JDownloader digitale Spuren auf dem Betriebssystem. Bereits bei einer klassischen Verwendung des Download-Managers - vom Programmstart, dem Bezug von Dateien aus dem Internet, bis zur Beendigung der Software - werden zahlreiche Informationen bzgl. der vom Benutzer getätigten Interaktionen von verschiedensten Programmmodulen festgehalten (vgl. Kap. 2.4).
Vordergründig wird in diesem Bericht auf verschiedene Protokolldateien verwiesen, welche bereits zu jedem Programmstart angelegt werden und sämtliche Interaktion mit der Software festhalten. Primär dazu entwickelt, die Benutzerfreundlichkeit und den Anwendersupport zu vereinfachen, sind die Log-Dateien für einen Forensiker ein wahrer „Goldschatz“ im Bezug auf die Nachvollziehbarkeit und den Versuch der Rekonstruktion vergangener Interaktionen des Benutzers mit der Software. Insofern konnten die zu Anfang gestellten, allgemeinen Fragestellungen des Kapitels 1.1 sowie die spezifischen Fragestellungen des Kapitels 1.2 positiv beantwortet werden. Hierzu wurde im Kapitel 2.3.5 dargelegt, welche expliziten Dateien Informationen über bereits vergangene Verwendungen der Software beinhalten. Anhand dieses Basiswissens konnten daraufhin im Kapitel 2.4 spezifische Fragestellungen aus der Sicht eines Forensikers beantwortet werden. Im Vordergrund steht hierbei die Tatsache, dass grundlegend verifiziert werden konnte, dass selbst bereits abgeschlossene Downloads im Nachhinein noch rekonstruierbar sind. Dabei konnte nicht nur die Tatsache eines Downloads an sich bewiesen werden, sondern zudem detaillierte Informationen über die **heruntergeladenen Dateien** inkl. eindeutiger **Hash-Werte**, spezifischen **Zeit- und Datumsangaben**, **Quellesystem/Bezugsadressen**, verwendete **Passwörter** (bzgl. verwendeter Proxy-/Internetverbindungen, verschlüsselter Archive oder gegen einen unbefugten Zugriff auf die Software), **Speicherorte** der geladenen Daten sowie die **verschlüsselten Zugangsdaten** zu teilweise, kostenpflichtigen Filehostern im Internet rekonstruiert werden.
Ein Forensiker kann somit bei einer der in Kapitel 1.2 dargestellten oder ähnlichen Fragestellungen, auf der Grundlage dieser Projektdokumentation, detaillierte Aussagen bezüglich einer vergangenen Verwendung des JDownloaders machen. Die bei solchen Konstellationen im Mittelpunkt stehende Fragestellung, ob von einem Computersystem urheberrechtlich geschütztes Material mittels des JDownloaders bezogen wurde, kann somit eingehend untersucht und beantwortet werden.

A Anhang

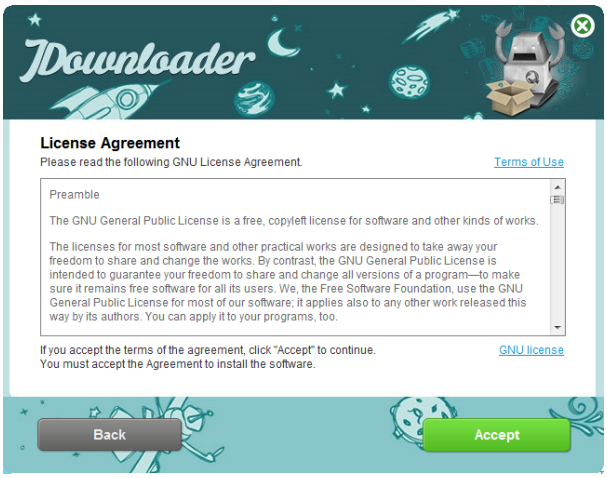
A.1 Installationsroutine der Firma InstallCore



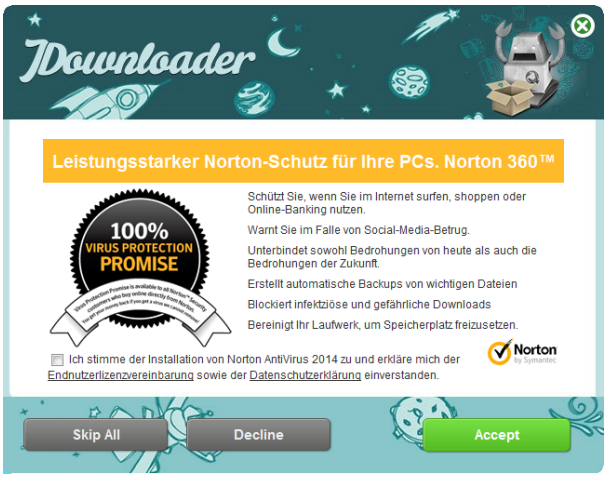
(a) Adware-Installationsclient



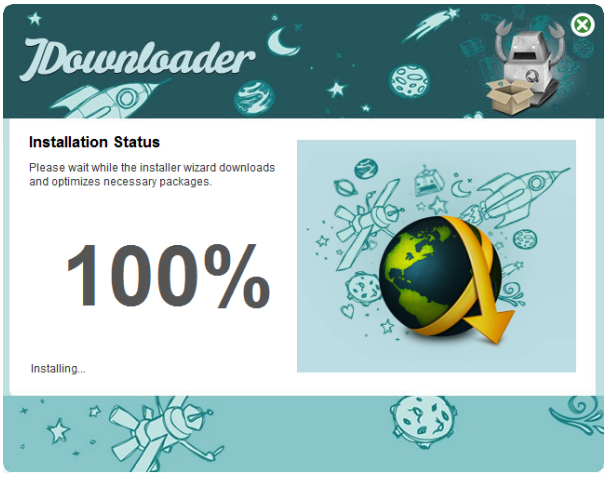
(b) Auswahl des Installationspfades



(c) Lizenzbestimmungen



(d) Zusatzsoftware des externen Anbieters InstallCore

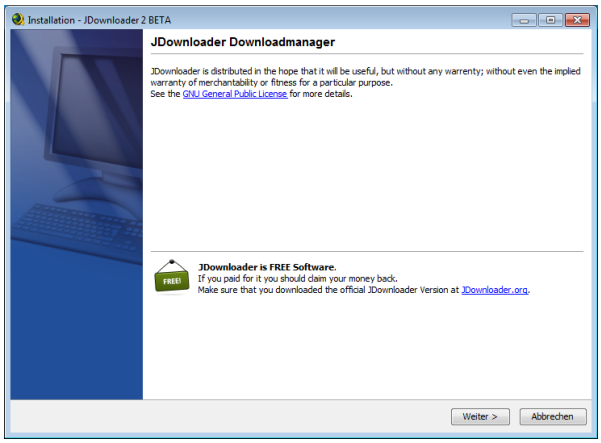


(e) Fertigstellung der Installation

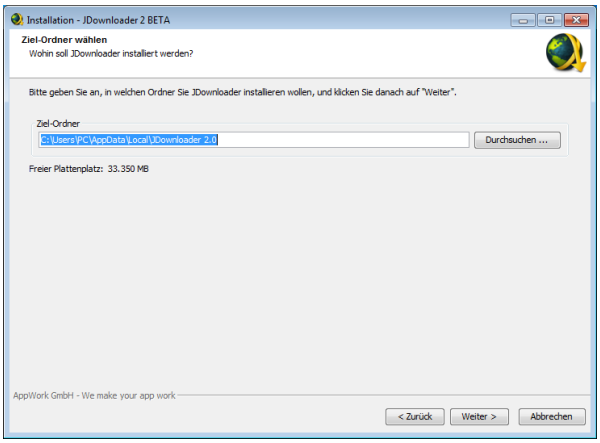
(f) Anzeige der JD-Webseite nach Fertigstellung

Abbildung A.1: Ausführung des Installationsassistenten der Firma InstallCore mit angebotener Zusatzsoftware bei **inaktiver** Antivirus-Software

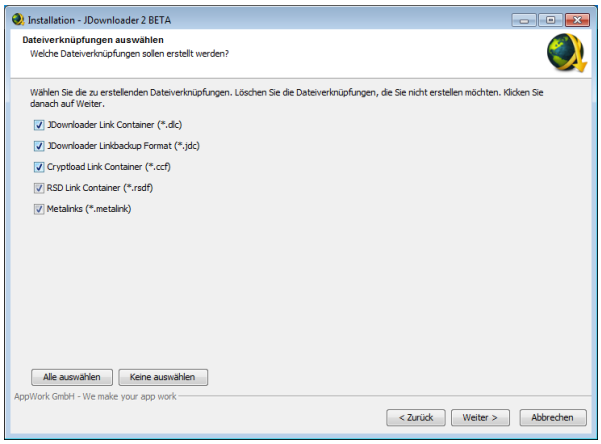
A.2 Werbefreie Installationsroutine



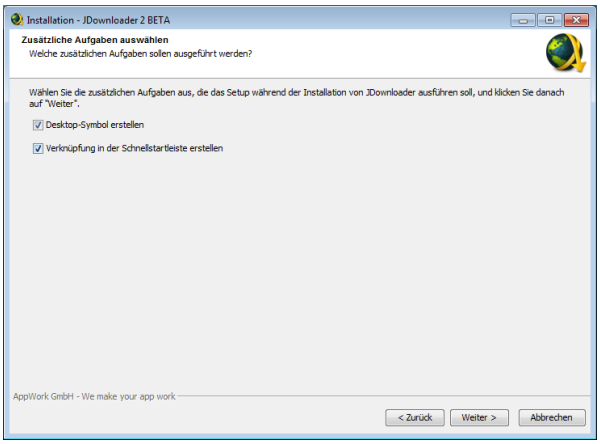
(a) Werbefreier Installationsassistent



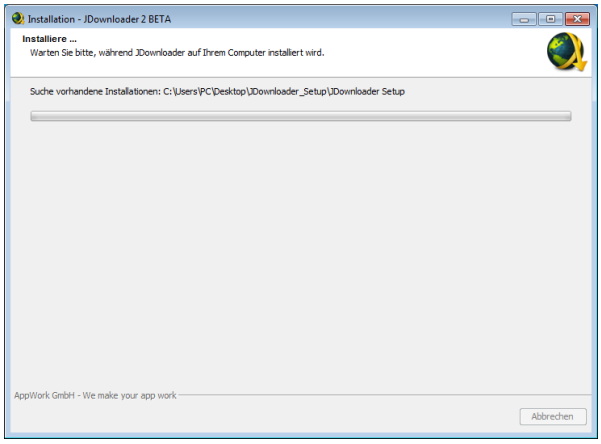
(b) Auswahl des Installationspfades



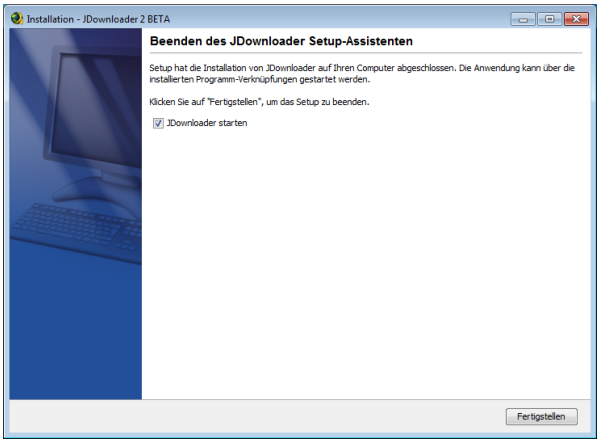
(c) Dateitypverknüpfungen der Software



(d) Auswahl der Programmverknüpfungen



(e) Installationsvorgang



(f) Fertigstellung der Installation

Abbildung A.2: Ausführung des werbefreien Installationsassistenten bei **aktiver** Antivirus-Software

A.3 Inhalt des Programmverzeichnisses

Tabelle A.1: Genereller Inhalt des Programmverzeichnisses

Nr.	Name	Typ	Beschreibung
1.	\.install4j\	D	Assistent zur Erstellung von Programmsetups einer selbstentwickelten Java-Software für die gängigen Plattformen.[18].
2.	**\cfg**	**D**	**Konfigurationseinstellungen**
3.	\extensions\	D	Erweiterungsmodule (Addons)
4.	\java\	D	Leeres Verzeichnis
5.	\jd\	D	Java-Programmklassen (Hoster/Decrypter)
6.	\jre\	D	Portable Java Plattform
7.	\libs\	D	Eingebundene Java-Bibliotheken
8.	\licenses\	D	Lizenzen verwendeter Programmbibliotheken und -ressourcen von Drittanbietern.
9.	**\logs**	**D**	**Anwendungs-/Ereignisprotokoll**
10.	\themes\	D	Programmdesign
11.	\tmp\	D	Temporäres Verzeichnis zur Zwischenspeicherung von Programmdaten.
12.	\tools\	D	Eingebundene, externe Programme
13.	\translations\	D	Übersetzungen in andere Sprachen
14.	\update\	D	Aktualisierungsinformationen
15.	\build.json	F	Programmerstellungs- und Versionsinformationen [19]
16.	\Core.jar	F	Jar-Archiv mit verschiedenen Java-Klassen bzgl. der Kernfunktionalitäten
17.	\JDownloader.jar	F	Jar-Archiv mit verschiedenen Java-Klassen bzgl. des Layouts
18.	\JDownloader2.exe	F	Programmstart

[18] Unter Verwendung der Software install4j können Installationsroutinen für Java-Programme für die gängigen geläufigen Betriebssystemplattformen (Windows, Mac OS X, Linux, Unix) erstellt und somit ein spezifisches Java-Programm auf verschiedenen Plattformen ausführbar gemacht werden. Für weitere Informationen siehe Herstellerseite

[19] Unabhängige Objektstruktur mit Informationen zur Erstellung der Software. "JSON", JavaScript Object Notation. Informationen zur Spezifikation eines spezifischen Objektes.

Tabelle A.1: Genereller Inhalt des Programmverzeichnisses

Nr.	Name	Typ	Beschreibung
19.	\JDownloader2.vmoptions	F	Java-Parameter zur Programmausführung (Speicherauslastung/3D-Darstellung)
20.	\JDownloader2Update.exe	F	Aktualisierung der Software
21.	\JDownloader2Update.vmoptions	F	Java-Parameter zur Aktualisierungsausführung (Speicherauslastung/3D-Darstellung)
22.	\license.txt	F	Lizenzinformationen der Software
23.	\license_german.txt	F	Lizenzinformationen (Deutsch)
24.	\output.log	F	Ausgabeprotokoll (JarHandlerWorkaroundOracle)
25.	\UpdateOoutput.log	F	Ausgabeprotokoll (JarHandlerWorkaroundOracle)
26.	\Unistall JDownloader.exe	F	Deinstallationsroutine

A.4 Windows Registrierungsdatenbank

A.4.1 Registry-Einträge zur Verknüpfung der Dateitypen

Listing A.1: Registry-Einträge zur Verknüpfung der Dateitypen mit dem JDownloader

```
1  HKLM\SOFTWARE\Classes\.dlc\: "JDownloader2"
2  HKLM\SOFTWARE\Classes\.jdc\: "JDownloader2 1"
3  HKLM\SOFTWARE\Classes\.ccf\: "JDownloader2 2"
4  HKLM\SOFTWARE\Classes\.rsdf\: "JDownloader2 3"
5  HKLM\SOFTWARE\Classes\.metalink\: "JDownloader2 4"
6
7  HKLM\SOFTWARE\Classes\JDownloader2\: "JDownloader Link Container"
8  HKLM\SOFTWARE\Classes\JDownloader2\DefaultIcon\: "C:\Users\PC\AppData\Local\
       JDownloader v2.0\.install4j\i4j_extf_10_69g5ss_1kdboqw.ico"
9  HKLM\SOFTWARE\Classes\JDownloader2\shell\open\command\: ""C:\Users\PC\AppData\Local\
       JDownloader v2.0\JDownloader2.exe" "%1""
10
11 HKLM\SOFTWARE\Classes\JDownloader2 1\: "JDownloader Linkbackup Format"
12 HKLM\SOFTWARE\Classes\JDownloader2 1\DefaultIcon\: "C:\Users\PC\AppData\Local\
       JDownloader v2.0\.install4j\i4j_extf_10_69g5ss_1kdboqw.ico"
13 HKLM\SOFTWARE\Classes\JDownloader2 1\shell\open\command\: ""C:\Users\PC\AppData\
       Local\JDownloader v2.0\JDownloader2.exe" "%1""
14
15 HKLM\SOFTWARE\Classes\JDownloader2 2\: "Cryptload Link Container"
```

```
16 HKLM\SOFTWARE\Classes\JDownloader2 2\DefaultIcon\: "C:\Users\PC\AppData\Local\
       JDownloader v2.0\.install4j\i4j_extf_10_69g5ss_1kdboqw.ico"
17 HKLM\SOFTWARE\Classes\JDownloader2 2\shell\open\command\: ""C:\Users\PC\AppData\
       Local\JDownloader v2.0\JDownloader2.exe" "%1""
18
19 HKLM\SOFTWARE\Classes\JDownloader2 3\: "RSD Link Container"
20 HKLM\SOFTWARE\Classes\JDownloader2 3\DefaultIcon\: "C:\Users\PC\AppData\Local\
       JDownloader v2.0\.install4j\i4j_extf_10_69g5ss_1kdboqw.ico"
21 HKLM\SOFTWARE\Classes\JDownloader2 3\shell\open\command\: ""C:\Users\PC\AppData\
       Local\JDownloader v2.0\JDownloader2.exe" "%1""
22
23 HKLM\SOFTWARE\Classes\JDownloader2 4\: "Metalinks"
24 HKLM\SOFTWARE\Classes\JDownloader2 4\DefaultIcon\: "C:\Users\PC\AppData\Local\
       JDownloader v2.0\.install4j\i4j_extf_10_69g5ss_1kdboqw.ico"
25 HKLM\SOFTWARE\Classes\JDownloader2 4\shell\open\command\: ""C:\Users\PC\AppData\
       Local\JDownloader v2.0\JDownloader2.exe" "%1""
26
27 HKU\S-1-5-21-539846951-2775919047-120045064-1000\Software\Microsoft\Windows\
       CurrentVersion\Explorer\FileExts\.dlc\Progid: "JDownloader2"
28 HKU\S-1-5-21-539846951-2775919047-120045064-1000\Software\Microsoft\Windows\
       CurrentVersion\Explorer\FileExts\.jdc\Progid: "JDownloader2 1"
29 HKU\S-1-5-21-539846951-2775919047-120045064-1000\Software\Microsoft\Windows\
       CurrentVersion\Explorer\FileExts\.ccf\Progid: "JDownloader2 2"
30 HKU\S-1-5-21-539846951-2775919047-120045064-1000\Software\Microsoft\Windows\
       CurrentVersion\Explorer\FileExts\.rsdf\Progid: "JDownloader2 3"
31 HKU\S-1-5-21-539846951-2775919047-120045064-1000\Software\Microsoft\Windows\
       CurrentVersion\Explorer\FileExts\.metalink\Progid: "JDownloader2 4"
```

A.4.2 CA-Root Zertifikate

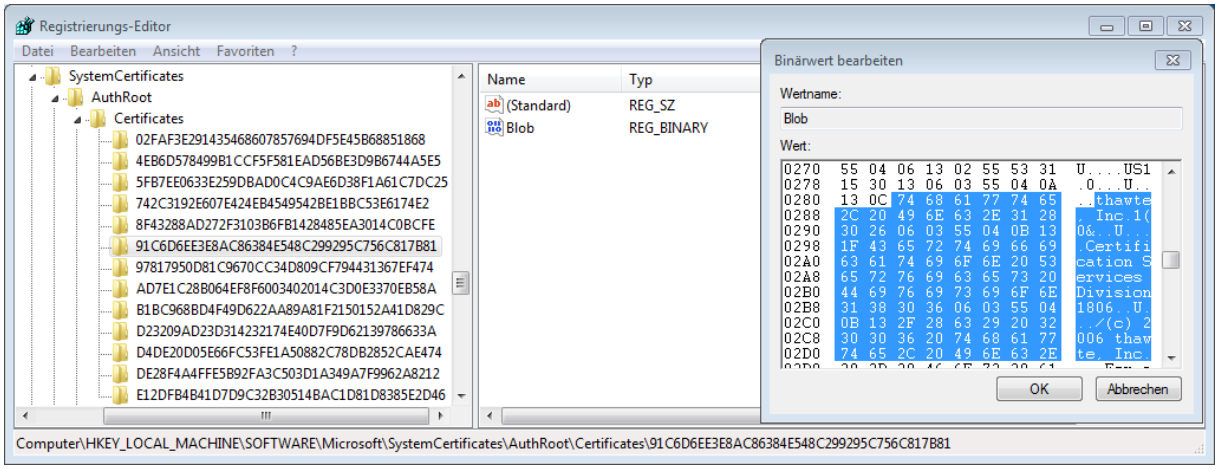


Abbildung A.3: Registry-Eintrag zum CA Root-Zertifikat „Thawte“

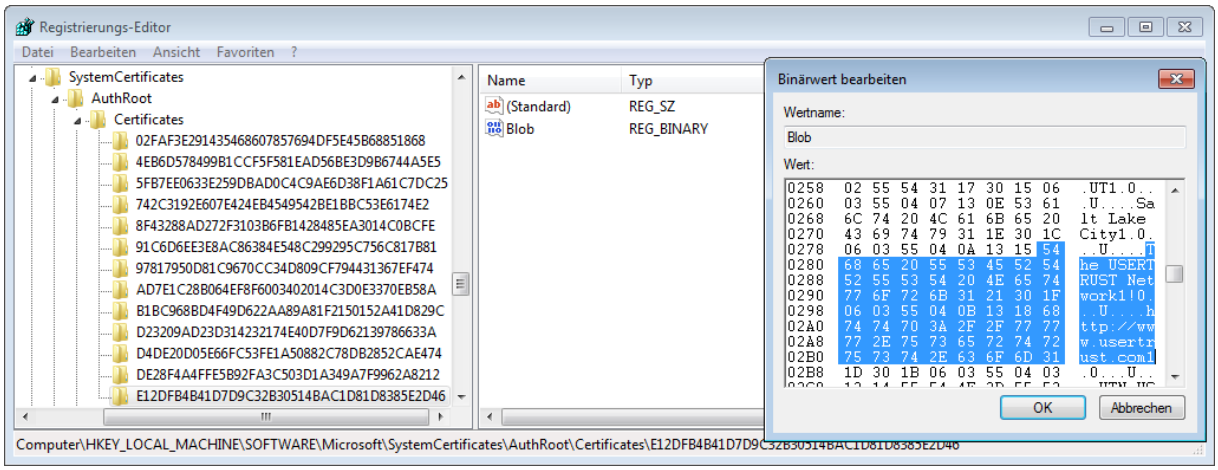


Abbildung A.4: Registry-Eintrag zum CA Root-Zertifikat „The USERTrust Network“

A.4.3 Registry-Informationen zur Softwaredeinstallation

Listing A.2: Gelöschte Registry-Informationen während der Softwaredeinstallation

```
1  Regshot 1.9.0 x64 ANSI
2  Datetime: 2016/1/8 14:19:20 , 2016/1/9 01:26:45
3  Computer: PC-PC , PC-PC
4  Username: PC , PC
5
6  ----------------------------------------
7  Keys deleted: 26
8  ----------------------------------------
9  HKLM\SOFTWARE\Classes\JDownloader2
10 HKLM\SOFTWARE\Classes\JDownloader2\DefaultIcon
11 HKLM\SOFTWARE\Classes\JDownloader2\shell
12 HKLM\SOFTWARE\Classes\JDownloader2\shell\open
13 HKLM\SOFTWARE\Classes\JDownloader2\shell\open\command
14 HKLM\SOFTWARE\Classes\JDownloader2 1
15 HKLM\SOFTWARE\Classes\JDownloader2 1\DefaultIcon
16 HKLM\SOFTWARE\Classes\JDownloader2 1\shell
17 HKLM\SOFTWARE\Classes\JDownloader2 1\shell\open
18 HKLM\SOFTWARE\Classes\JDownloader2 1\shell\open\command
19 HKLM\SOFTWARE\Classes\JDownloader2 2
20 HKLM\SOFTWARE\Classes\JDownloader2 2\DefaultIcon
21 HKLM\SOFTWARE\Classes\JDownloader2 2\shell
22 HKLM\SOFTWARE\Classes\JDownloader2 2\shell\open
23 HKLM\SOFTWARE\Classes\JDownloader2 2\shell\open\command
24 HKLM\SOFTWARE\Classes\JDownloader2 3
25 HKLM\SOFTWARE\Classes\JDownloader2 3\DefaultIcon
```

```
26 HKLM\SOFTWARE\Classes\JDownloader2 3\shell
27 HKLM\SOFTWARE\Classes\JDownloader2 3\shell\open
28 HKLM\SOFTWARE\Classes\JDownloader2 3\shell\open\command
29 HKLM\SOFTWARE\Classes\JDownloader2 4
30 HKLM\SOFTWARE\Classes\JDownloader2 4\DefaultIcon
31 HKLM\SOFTWARE\Classes\JDownloader2 4\shell
32 HKLM\SOFTWARE\Classes\JDownloader2 4\shell\open
33 HKLM\SOFTWARE\Classes\JDownloader2 4\shell\open\command
34 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\jdownloader2
35
36 ----------------------------------------
37 Values deleted: 35
38 ----------------------------------------
39 HKLM\SOFTWARE\Classes\JDownloader2\: "JDownloader Link Container"
40 HKLM\SOFTWARE\Classes\JDownloader2\DefaultIcon\: "C:\Users\PC\AppData\Local\
       JDownloader v2.0\.install4j\i4j_extf_10_69g5ss_1kdboqw.ico"
41 HKLM\SOFTWARE\Classes\JDownloader2\shell\open\command\: ""C:\Users\PC\AppData\Local\
       JDownloader v2.0\JDownloader2.exe" "%1""
42 HKLM\SOFTWARE\Classes\JDownloader2 1\: "JDownloader Linkbackup Format"
43 HKLM\SOFTWARE\Classes\JDownloader2 1\DefaultIcon\: "C:\Users\PC\AppData\Local\
       JDownloader v2.0\.install4j\i4j_extf_10_69g5ss_1kdboqw.ico"
44 HKLM\SOFTWARE\Classes\JDownloader2 1\shell\open\command\: ""C:\Users\PC\AppData\
       Local\JDownloader v2.0\JDownloader2.exe" "%1""
45 HKLM\SOFTWARE\Classes\JDownloader2 2\: "Cryptload Link Container"
46 HKLM\SOFTWARE\Classes\JDownloader2 2\DefaultIcon\: "C:\Users\PC\AppData\Local\
       JDownloader v2.0\.install4j\i4j_extf_10_69g5ss_1kdboqw.ico"
47 HKLM\SOFTWARE\Classes\JDownloader2 2\shell\open\command\: ""C:\Users\PC\AppData\
       Local\JDownloader v2.0\JDownloader2.exe" "%1""
48 HKLM\SOFTWARE\Classes\JDownloader2 3\: "RSD Link Container"
49 HKLM\SOFTWARE\Classes\JDownloader2 3\DefaultIcon\: "C:\Users\PC\AppData\Local\
       JDownloader v2.0\.install4j\i4j_extf_10_69g5ss_1kdboqw.ico"
50 HKLM\SOFTWARE\Classes\JDownloader2 3\shell\open\command\: ""C:\Users\PC\AppData\
       Local\JDownloader v2.0\JDownloader2.exe" "%1""
51 HKLM\SOFTWARE\Classes\JDownloader2 4\: "Metalinks"
52 HKLM\SOFTWARE\Classes\JDownloader2 4\DefaultIcon\: "C:\Users\PC\AppData\Local\
       JDownloader v2.0\.install4j\i4j_extf_10_69g5ss_1kdboqw.ico"
53 HKLM\SOFTWARE\Classes\JDownloader2 4\shell\open\command\: ""C:\Users\PC\AppData\
       Local\JDownloader v2.0\JDownloader2.exe" "%1""
54 HKLM\SOFTWARE\ej-technologies\install4j\installations\allinstdirsjdownloader2: "C:\
       Users\PC\AppData\Local\JDownloader v2.0"
55 HKLM\SOFTWARE\ej-technologies\install4j\installations\instdirjdownloader2: "C:\Users
       \PC\AppData\Local\JDownloader v2.0"
```

```
56 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\jdownloader2\DisplayName: "
       JDownloader 2"
57 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\jdownloader2\
       UninstallString: ""C:\Users\PC\AppData\Local\JDownloader v2.0\Uninstall
       JDownloader.exe""
58 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\jdownloader2\Publisher: "
       AppWork GmbH"
59 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\jdownloader2\URLInfoAbout:
       "http://appwork.org"
60 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\jdownloader2\
       InstallLocation: "C:\Users\PC\AppData\Local\JDownloader v2.0"
61 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\jdownloader2\DisplayVersion
       : "2.0"
62 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\jdownloader2\VersionMajor:
       0x00000002
63 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\jdownloader2\VersionMinor:
       0x00000000
64
65 HKU\S-1-5-21-539846951-2775919047-120045064-1000\Environment\JD2_HOME: "C:\Users\PC\
       AppData\Local\JDownloader v2.0"
66 HKU\S-1-5-21-539846951-2775919047-120045064-1000\Software\ej-technologies\install4j\
       installations\allinstdirsjdownloader2: "C:\Users\PC\AppData\Local\JDownloader v2"
67 HKU\S-1-5-21-539846951-2775919047-120045064-1000\Software\ej-technologies\install4j\
       installations\instdirjdownloader2: "C:\Users\PC\AppData\Local\JDownloader v2.0"
68 HKU\S-1-5-21-539846951-2775919047-120045064-1000\Software\Microsoft\Windows\
       CurrentVersion\Explorer\FileExts\.ccf\Progid: "JDownloader2 2"
69 HKU\S-1-5-21-539846951-2775919047-120045064-1000\Software\Microsoft\Windows\
       CurrentVersion\Explorer\FileExts\.dlc\Progid: "JDownloader2"
70 HKU\S-1-5-21-539846951-2775919047-120045064-1000\Software\Microsoft\Windows\
       CurrentVersion\Explorer\FileExts\.jdc\Progid: "JDownloader2 1"
71 HKU\S-1-5-21-539846951-2775919047-120045064-1000\Software\Microsoft\Windows\
       CurrentVersion\Explorer\FileExts\.metalink\Progid: "JDownloader2 4"
72 HKU\S-1-5-21-539846951-2775919047-120045064-1000\Software\Microsoft\Windows\
       CurrentVersion\Explorer\FileExts\.rsdf\Progid: "JDownloader2 3"
```

A.5 Programmeinstellungen

A.5.1 Menüpunkt Allgemein

Tabelle A.2: Allgemeine Einstellungen des JDownloaders

Nr.	Einstellungsvariable	Beschreibung
1.	defaultdownloadfolder	Standardmäßiger Speicherort
2.	maxsimultanedownloads	Max. gleichzeitige Downloads
4.	maxdownloadsperhostenabled	[Checkbox]: Max. Downloads pro Hoster
3.	maxsimultanedownloadsperhost	Max. gleichzeitige Downloads pro Hoster
5.	maxchunksperfile	Max. Verbindungen pro Download
6.	cleanupafterdownloadaction	Entferne fertigstellte Downloads
7.	iffileexistsaction	Aktion, wenn die Datei bereits vorhanden.
8.	autostartdownloadoption	Downloads automatisch starten
9.	showcountdownonautostartdownloads	[Checkbox]: Countdown zeigen
10.	autostartcountdownseconds	Countdown zeigen (Sekunden)
11.	hashcheckenabled	[Checkbox]: SFC/CRC wenn möglich durchführen
12.	hashretryenabled	[Checkbox]: Restart Download when SFC/CRC check fails
13.	autoopencontainerafterdownload	[Checkbox]: geladene Link Container autom. öffnen
14.	keepxoldlists	Max. Anzahl vorzuhaltener Download-/Linklisten
15.	pausespeed	Downloadgeschwindigkeit, wenn die Downloads pausiert wurden.
16.	downloadspeedlimitenabled	Geschwindigkeitsbegrenzung aktivieren
17.	downloadspeedlimit	Geschwindigkeitsbegrenzung in B/s
18.	useavailableaccounts	Nutzung von Premiumaccounts (de)-aktivieren (Button in der Symbolleiste)

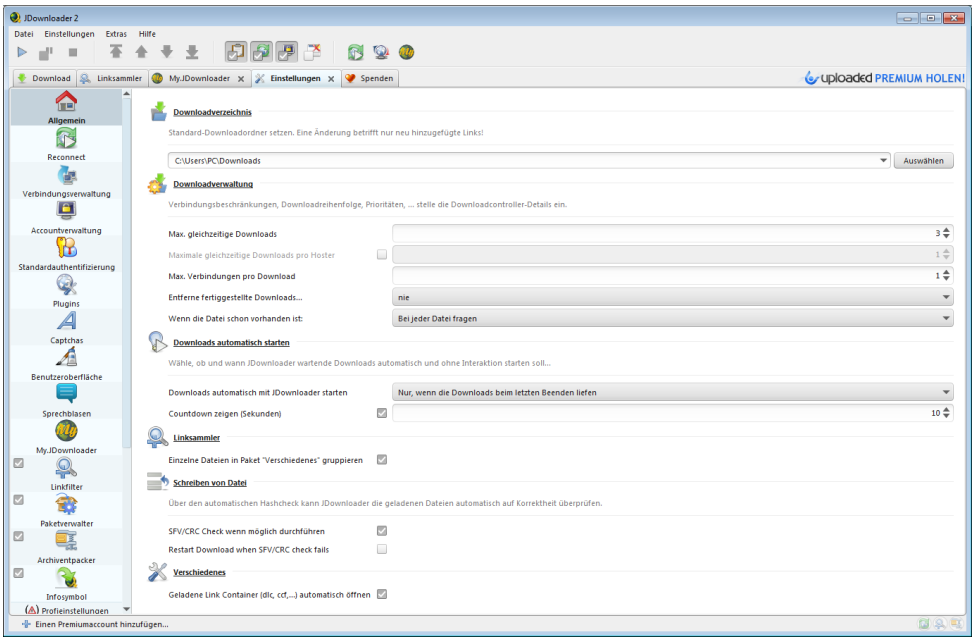


Abbildung A.5: Allgemeine Einstellungen des JDownloaders

A.5.2 Menüpunkt Verbindung

Listing A.3: Reconnect Anmeldeinformationen

```
org.jdownloader.settings.InternetConnectionSettings.customproxylist.json
[
  {
    "proxy" : {
    "username" : null,
    "password" : null,
    "port" : 80,
    "address" : null,
    "type" : "NONE",
    "preferNativeImplementation" : false,
    "connectMethodPrefered" : false
    },
    "rangeRequestsSupported" : true,
    "filter" : null,
    "pac" : false,
    "reconnectSupported" : true,
    "enabled" : true
  }, {
    "proxy" : {
    "username" : "ProxyBenutzer",
    "password" : "ProxyPasswort",
```

```
22      "port" : 8080,
23      "address" : "192.168.178.1",
24      "type" : "HTTP",
25      "preferNativeImplementation" : false,
26      "connectMethodPrefered" : false
27      },
28      "rangeRequestsSupported" : true,
29      "filter" : null,
30      "pac" : false,
31      "reconnectSupported" : false,
32      "enabled" : true
33    }
34  ]
```

A.5.3 Menüpunkt Accountverwaltung

Listing A.4: Entschlüsselte Accountdatei

```
1  C:\Users\pc\Desktop\jDecrypt\binary>jdecrypt.exe org.jdownloader.settings.
       AccountSettings.accounts.ejs
2
3  {
4    "uploaded.to" : [ {
5    "properties" : {
6    "IS_MULTI_HOSTER_ACCOUNT" : false,
7    "ACCOUNT_TYPE" : "FREE",
8    "added" : 1451498912025,
9    "lastKnownAccountType" : "FREE",
10   "LATEST_VALID_TIMESTAMP" : 1451498911132,
11   "tokenType" : "free",
12   "free" : true,
13   "token" : "4MJ5RYVvcrEQKa9GS7MJ"
14   },
15   "hoster" : "uploaded.to",
16   "maxSimultanDownloads" : 1,
17   "password" : "TestM16Test!",
18   "infoProperties" : {
19   },
20   "createTime" : 0,
21   "trafficLeft" : 0,
22   "trafficMax" : 0,
23   "validUntil" : -1,
24   "active" : false,
```

```
25    "enabled" : true,
26    "trafficUnlimited" : true,
27    "specialtraffic" : false,
28    "user" : "13267519",
29    "concurrentUsePossible" : true,
30    "id" : 1451498907431,
31    "errorType" : null,
32    "errorString" : null,
33    "statusString" : "Free account"
34    } ]
35  }
```

A.5.4 Menüpunkt Standardauthentifizierung

Listing A.5: Entschlüsselte Accountdatei der Standardauthentifizierung

```
1  C:\Users\PC\Desktop\JDDecryptor\jDecrypt-master\binary>jdecrypt.exe -keyid 2 jd.
       controlling.authentication.AuthenticationControllerSettings.list.ejs
2  [ {
3    "created" : 1452403103909,
4    "lastValidated" : -1,
5    "enabled" : true,
6    "username" : "Admin",
7    "password" : "AdminWeb",
8    "type" : "FTP",
9    "hostmask" : "web.de"
10 }, {
11   "created" : 1452403487049,
12   "lastValidated" : -1,
13   "enabled" : true,
14   "username" : "Admin",
15   "password" : "AdminGmx",
16   "type" : "HTTP",
17   "hostmask" : "gmx.de"
18 } ]
```

A.5.5 Menüpunkt Plugin

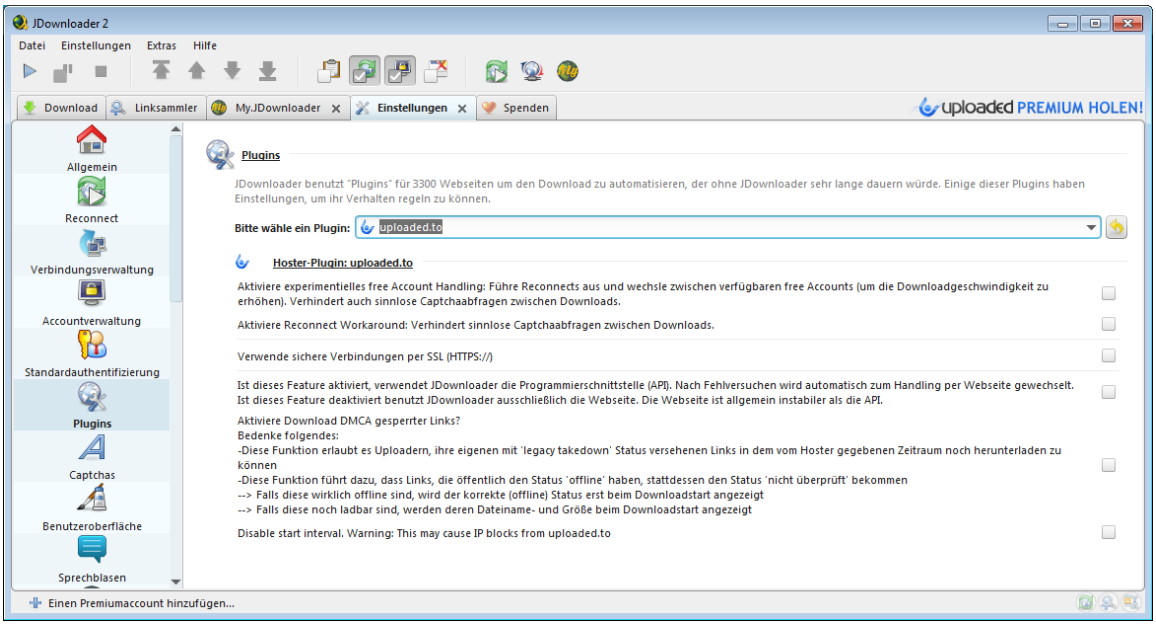


Abbildung A.6: Einstellungen für das Plugin der Webseite uploaded.to

Listing A.6: Entschlüsselte Konfigurationsdatei der Webseite uploaded.net

```
1 C:\Users\PC\Desktop\JDDecryptor\jDecrypt-master\binary>jdecrypt.exe -keyid 5
      subconf_uploaded.to.ejs
2 {
3   "DOWNLOAD_ABUSED" : false,
4   "DISABLE_START_INTERVAL" : false,
5   "ACTIVATEACCOUNTERRORHANDLING" : false,
6   "EXPERIMENTALHANDLING" : false,
7   "SSL_CONNECTION" : false,
8   "PREFER_PREMIUM_DOWNLOAD_API_V2" : false
9 }
```

A.5.6 Menüpunkt Captcha

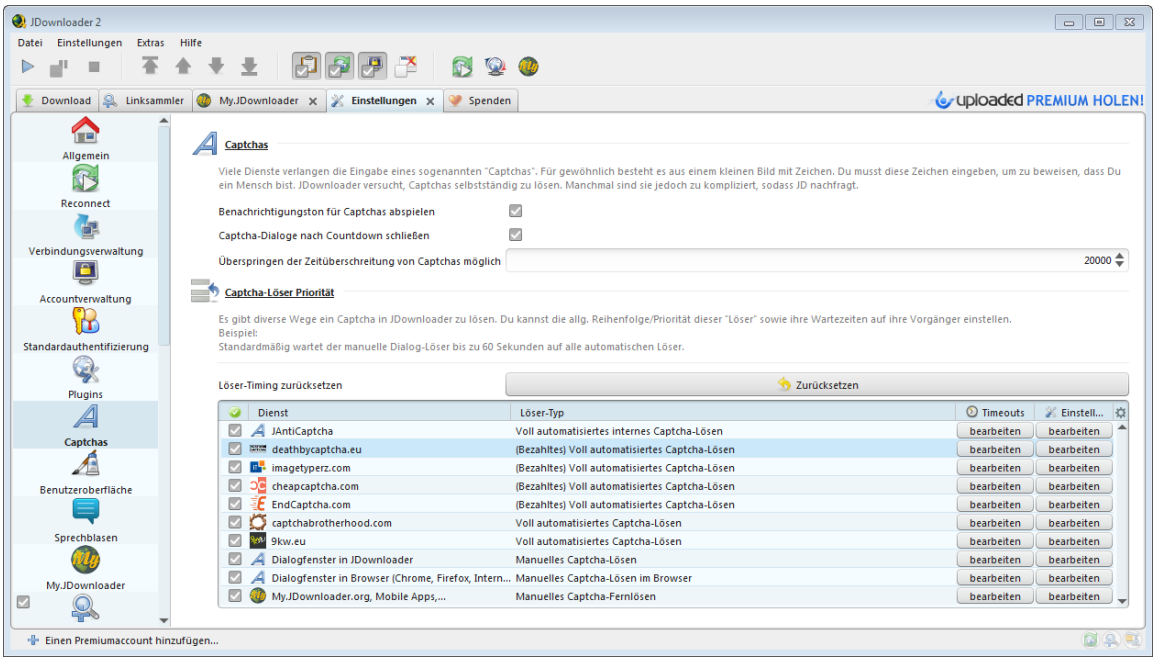


Abbildung A.7: Einstellungen für das Lösen von Captchas

Listing A.7: Captcha Einstellungen

```
1 jd.controlling.captcha.CaptchaSettings.json
2 {
3   "dialogcountdownfordownloadsenabled" : true,
4   "captchamode" : "NORMAL",
5   "captchaexchangechancetoskipbubbletimeout" : 10000,
6   "remotecaptchabubbleenabled" : true
7 }
```

Listing A.8: Einstellungen des Captcha-Dienstes ImageTyperz

```
1 org.jdownloader.captcha.v2.solver.imagetyperz.ImageTyperzConfigInterface.json
2 {
3   "blackwhitelistingenabled" : true,
4   "password" : "TestPasswort",
5   "feedbacksendingenabled" : false,
6   "enabled" : true,
7   "threadpoolsize" : 5,
8   "username" : "M16TestName"
9 }
```

A.5.7 Menüpunkt MyJDownloader

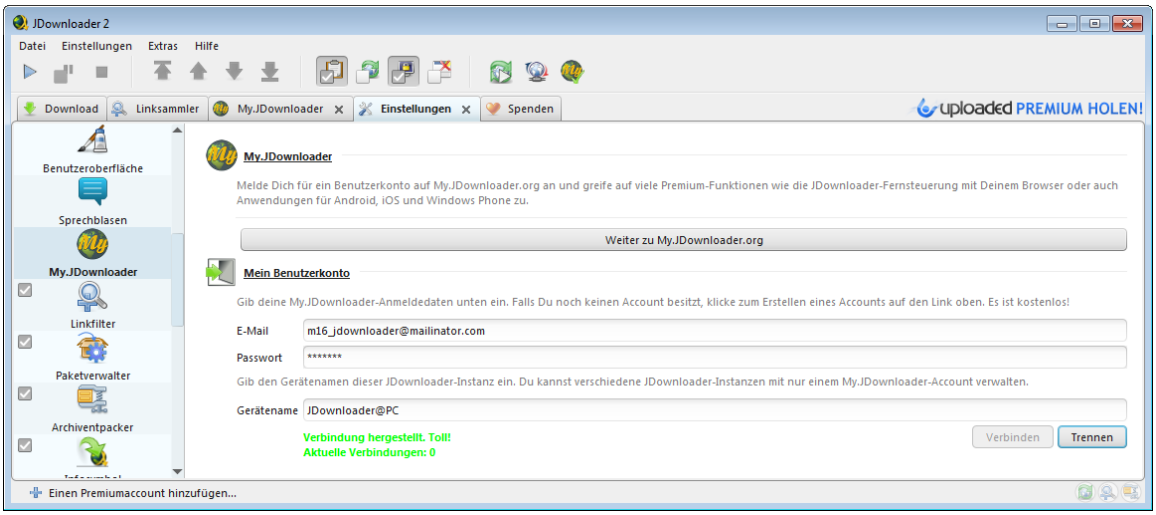


Abbildung A.8: Einstellungen zur Eingabe der Zugangsdaten des My.JDownloaders

Listing A.9: Einstellungen für den Zugang zu My.JDownloader

```
1  org.jdownloader.api.myjdownloader.MyJDownloaderSettings.json
2  {
3    "uniquedeviceidsaltv2" : "85033
         f0b90d848a0116eb3fc8d98994e3c72cfa97a04c42792f678ef3ffd20e9",
4    "autoconnectenabledv2" : true,
5    "debugenabled" : false,
6    "uniquedeviceid" : null,
7    "lastlocalport" : 49870,
8    "connectip" : "api.jdownloader.org",
9    "latesterror" : "NONE",
10   "password" : "Marius312!",
11   "clientconnectport" : 80,
12   "directconnectmode" : "LAN",
13   "devicename" : "JDownloader_M16@PC",
14   "uniquedeviceidv2" : "af4704bd4490c7c73edc169cebdb73e1",
15   "email" : "m16_jdownloader@mailinator.com"
16 }
```

A.5.8 Menüpunkt Linkfilter

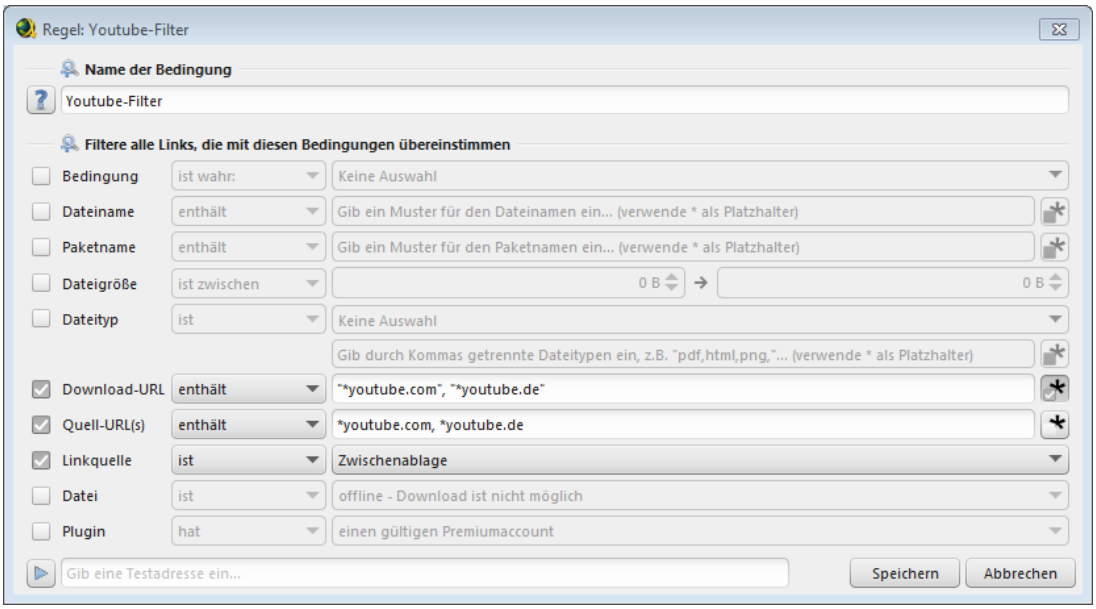


Abbildung A.9: Regelassistent zur Filterung von Links, Adressen und Dateien am Beispiel von Youtube

A.5.9 Menüpunkt Archiventpacker

Listing A.10: Einstellungen zum automatischen Entpacken von Archiven

```
org.jdownloader.extensions.extraction.ExtractionExtension.json
{
  "deletearchivefilesafterextractionaction" : "NO_DELETE",
  "iffileexistsaction" : "SKIP_FILE",
  "customextractionpathenabled" : false,
  "bubbleenabledifarchiveextractionisinprogress" : true,
  "subpath" : "%PACKAGENAME%",
  "subpathminfolderstreshhold" : 0,
  "deletearchivedownloadlinksafterextraction" : false,
  "customextractionpath" : "C:\\Users\\PC\\Downloads\\extracted",
  "enabled" : true,
  "subpathenabled" : false,
  "subpathminfilesorfolderstreshhold" : 2,
  "subpathminfilestreshhold" : 0,
  "useoriginalfiledate" : true,
  "freshinstall" : false,
  "oldpwlistimported" : true,
  "writeextractionlogenabled" : true
}
```

A.5.10 Menüpunkt Paketverwalter

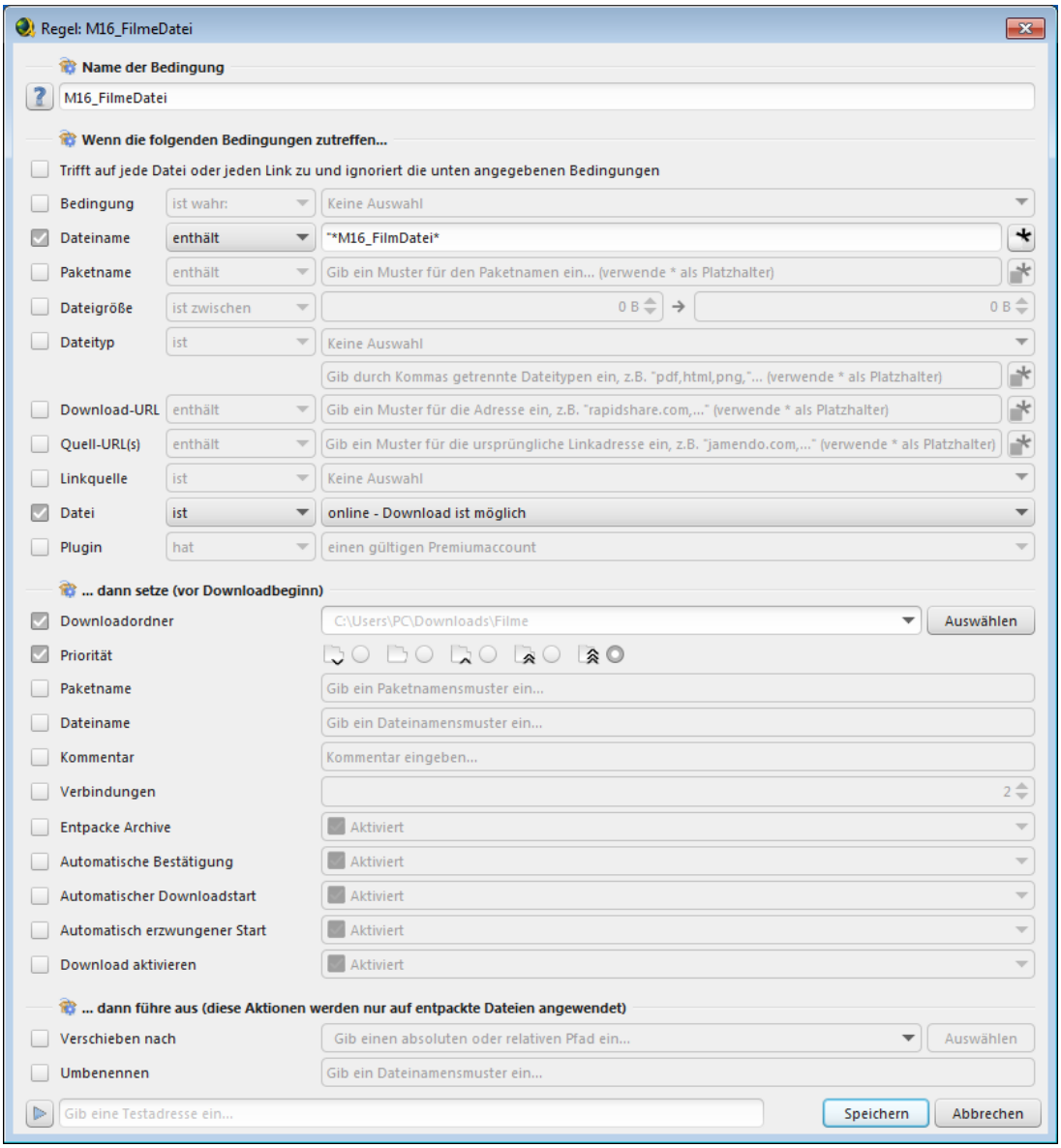


Abbildung A.10: Regelassistent zur Filterung von Links, Adressen und Dateien am Beispiel von Youtube

A.5.11 Menüpunkt Infosymbol

Listing A.11: Sonstige Einstellungen

```
1 org.jdownloader.gui.jdtrayicon.TrayExtension.json
2 {
3   "freshinstall" : false,
4   "onminimizeaction" : "TO_TASKBAR",
5   "tooltipenabled" : true,
```

```
6    "oncloseaction" : "ASK",
7    "tooglewindowstatuswithsingleclickenabled" : false,
8    "greyiconenabled" : false,
9    "gnometrayicontransparentenabled" : true,
10   "enabled" : true,
11   "startminimizedenabled" : false,
12   "trayonlyvisibleifwindowishiddenenabled" : false
13 }
```

A.5.12 Menüpunkt Profieinstellungen

Tabelle A.3: Konfigurationsdateien, welche den Profieinstellungen zugeordnet werden können.

Nr.	Kategorie	Konfigurationsdatei
1.	Youtube	plugins\.plugins.hoster.YoutubeDashV2$YoutubeConfig-.json
2.	UPUPReconnect[20]	jd.controlling.reconnect.pluginsinc.upnp.-UPUPReconnectSettings.json
3.	UpdateSettings	org.jdownloader.updatev2.UpdateSettings.json
4.	Tray	org.jdownloader.gui.jdtrayicon.TrayExtension.json
5.	SyntheticaSettings	org.appwork.swing.synthetica.SyntheticaSettings.json
6.	StatsManagerV2	org.jdownloader.jdserv.stats.StatsManagerConfigV2.json
7.	SoundSettings	org.jdownloader.settings.SoundSettings.json
8.	SilentModeSettings	org.jdownloader.settings.SilentModeSettings.json
9.	Shutdown	org.jdownloader.extensions.shutdown.-ShutdownExtension.json
10.	ShortcutSettings	org.jdownloader.gui.shortcuts.ShortcutSettings.json
11.	RtmpdumpSettings	org.jdownloader.settings.RtmpdumpSettings.json
12.	RemoteAPI	org.jdownloader.api.RemoteAPIConfig.json
13.	Reconnect	jd.controlling.reconnect.ReconnectConfig.json
14.	PackagizerSettings	org.jdownloader.controlling.packagizer.-PackagizerSettings.rulelist.json

[20] Universal Plug and Play, s. `http://jdownloader.org/de/knowledge/wiki/reconnect/upnp-reconnect`, abgerufen am 27.2.2016

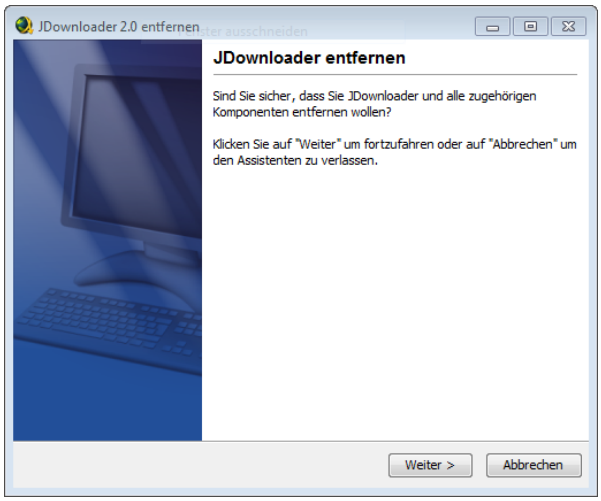
Tabelle A.3: Konfigurationsdateien, welche den Profieinstellungen zugeordnet werden können.

Nr.	Kategorie	Konfigurationsdatei
15.	MyJDownloaderSettings	org.jdownloader.api.myjdownloader.- MyJDownloaderSettings.json org.jdownloader.api.myjdownloader.- MyJDownloaderSettings.deviceconnectports.json
16.	Log	org.appwork.utils.logging2.LogConfig.json
17.	LiveHeaderReconnectSettings	jd.controlling.reconnect.pluginsinc.liveheader.- LiveHeaderReconnectSettings.json
18.	LinkgrabberSettings	org.jdownloader.gui.views.linkgrabber.addlinksdialog.- LinkgrabberSettings.json
19.	LinkFilterSettings	org.jdownloader.controlling.filter.LinkFilterSettings.json org.jdownloader.controlling.filter.LinkFilterSettings.- filterlist.json
20.	LinkCrawler	jd.controlling.linkcrawler.LinkCrawlerConfig.json jd.controlling.linkcrawler.LinkCrawlerConfig.- linkcrawlerrules.json
21.	LinkCollector	jd.controlling.linkcollector.LinkCollectorConfig.json
22.	LinkChecker	jd.controlling.linkchecker.LinkCheckerConfig.json
23.	LAFSettings	laf\JDDefaultLookAndFeel.json laf\JDDefaultLookAndFeel.popupborderinsets.json
24.	JACSolver	org.jdownloader.captcha.v2.solver.jac.- JACSolverConfig.json
25.	InternetConnectionSettings	org.jdownloader.settings.InternetConnectionSettings.json org.jdownloader.settings.InternetConnectionSettings.- customproxylist.json
26.	ImageTyperzInterface	org.jdownloader.captcha.v2.solver.imagetyperz.- ImageTyperzConfigInterface.json
27.	GraphicalUserInterfaceSettings	org.jdownloader.settings.Graphical- UserInterfaceSettings.json
28.	GeneralSettings	org.jdownloader.settings.GeneralSettings.json

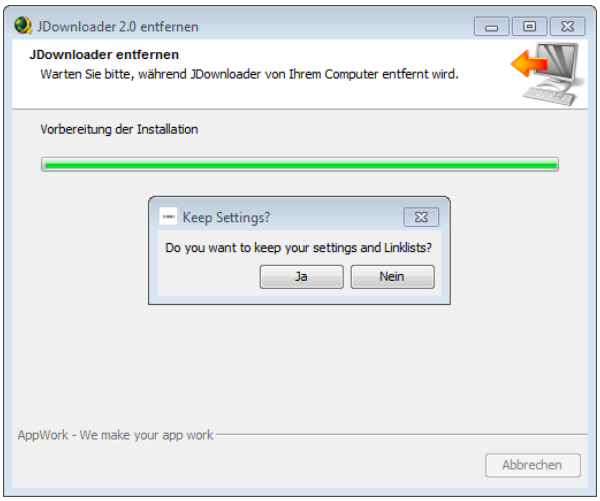
Tabelle A.3: Konfigurationsdateien, welche den Profieinstellungen zugeordnet werden können.

Nr.	Kategorie	Konfigurationsdatei
29.	FFmpedSetup	org.jdownloader.controlling.ffmpeg.FFmpegSetup.-demux2aaccommand.json org.jdownloader.controlling.ffmpeg.FFmpegSetup.-muxtowebmcommand.json
30.	Extraction	org.jdownloader.extensions.extraction.-ExtractionExtension.json
31.	EndCaptchaInterface	org.jdownloader.captcha.v2.solver.endcaptcha.-EndCaptchaConfigInterface.json
32.	DialogCaptchaSolver	org.jdownloader.captcha.v2.solver.gui.-DialogCaptchaSolverConfig.json
33.	DeathByCaptchaSettings	org.jdownloader.captcha.v2.solver.dbc.-DeathByCaptchaSettings.json
34.	CheapCaptchaInterface	org.jdownloader.captcha.v2.solver.cheapcaptcha.-CheapCaptchaConfigInterface.json
35.	CaptchaSettings	jd.controlling.captcha.CaptchaSettings.json
36.	CaptchaMyJDownloader-RemoteSolverSettings	org.jdownloader.api.captcha.-CaptchaMyJDownloaderRemoteSolverSettings.json
37.	CaptchaBrotherHoodSettings	org.jdownloader.captcha.v2.solver.captchabrotherhood.-CaptchaBrotherHoodSettings.json
38.	Captcha9kwSettings	org.jdownloader.captcha.v2.solver.solver9kw.-Captcha9kwSettings.json
39.	BubbleNotify	org.jdownloader.gui.notify.gui.BubbleNotifyConfig.json
40.	BrowserCaptchaSolver	org.jdownloader.captcha.v2.solver.browser.-BrowserCaptchaSolverConfig.json
41.	AntiStandby	org.jdownloader.extensions.antistandby.-AntiStandbyExtension.json
42.	AccountSettings	org.jdownloader.settings.AccountSettings.json

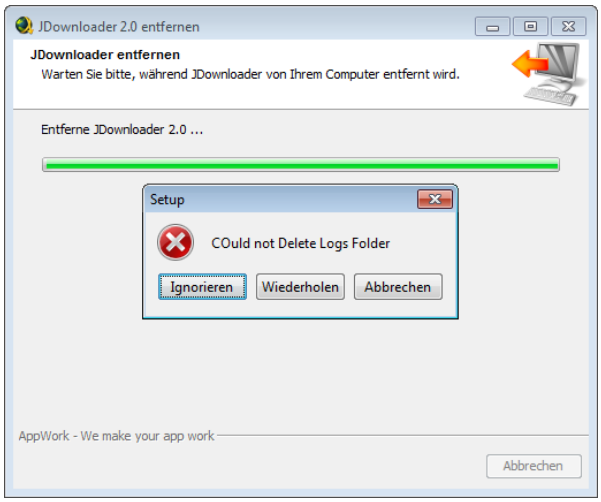
A.6 Deinstallationsroutine



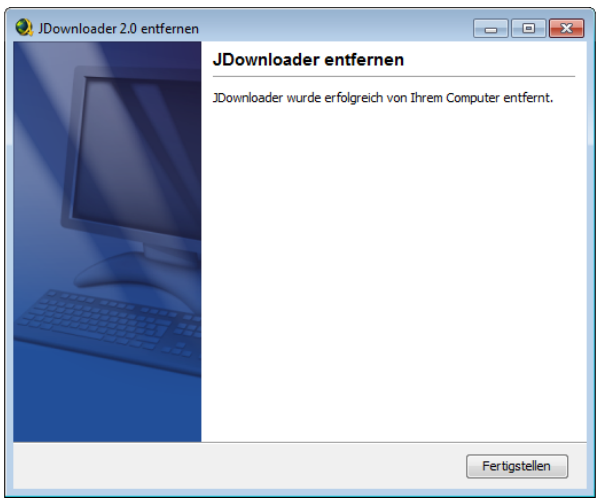
(a) Deinstallationsvorgang (1)



(b) Deinstallationsvorgang (2)



(c) Deinstallationsvorgang (3)



(d) Deinstallationsvorgang (4)

Abbildung A.11: Ausführung der Deinstallation des JDownloaders

A.7 Versionsinformationen

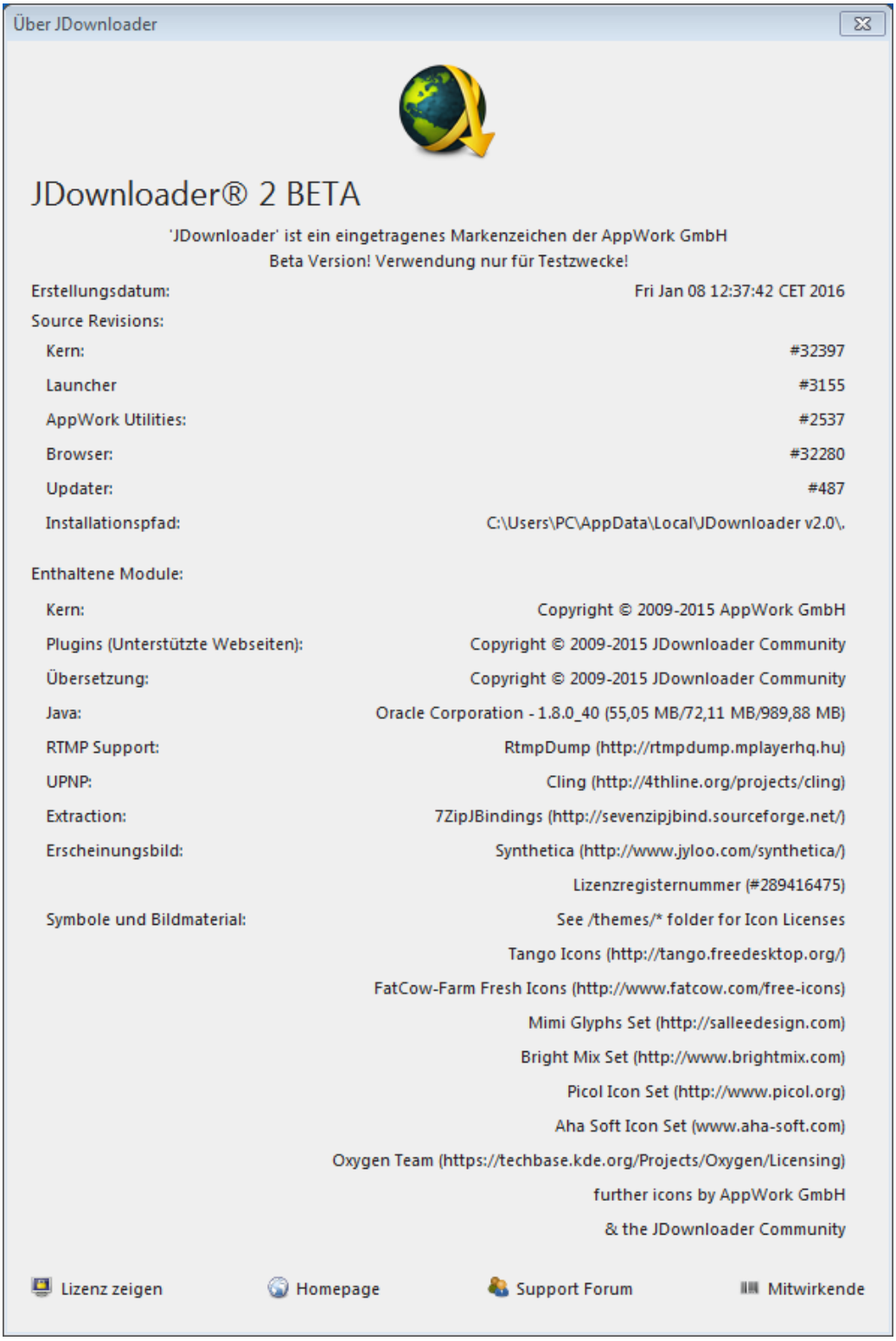


Abbildung A.12: Versionsinformationen des JDownloaders

Listing A.12: Versionsinformationen des JDownloaders

```
"C:\Users\PC\AppData\Local\JDownloader v2.0\build.json"
{
  "JDownloaderRevision":32397
  ,"JDownloaderServerOptionsRevision":3109
  ,"MyJDownloaderClientRevision":32297
  ,"JDClosedRevision":234
  ,"JDownloaderUpdaterRevision":3155
  ,"buildDate":"Fri Jan 08 12:37:42 CET 2016"
  ,"buildTimestamp":1452253062132
  ,"AppWorkUtilsRevision":2537
  ,"UpdateClientV2Revision":487
  ,"JDBrowserRevision":32280
}
```

Listing A.13: Aktualisierungsverlauf des JDownloaders

```
"C:\Users\PC\AppData\Local\JDownloader v2.0\logs\updatehistory\7150_to_7165.log"
Mon Jan 11 16:51:28 CET 2016
Package: package_1452525446888.awf
Install
Write Revision: 7164
----------------Plugins----------------
jd/plugins/decrypter/CpvLinkCom.class.removed
jd/plugins/decrypter/Ftp$1.class
jd/plugins/decrypter/Ftp.class
jd/plugins/decrypter/GenericAutoContainer.class
jd/plugins/decrypter/ImageHosterDecrypter.class
jd/plugins/decrypter/ImgurCom.class
jd/plugins/decrypter/LiensProtectorCom.class.removed
jd/plugins/decrypter/LolaBitsEsDecrypter.class
jd/plugins/decrypter/MpLemonNet.class.removed
jd/plugins/decrypter/PinterestComDecrypter.class
jd/plugins/decrypter/PornHubCom.class
jd/plugins/decrypter/SloozieCom.class.removed
jd/plugins/decrypter/XFileShareProFolder.class
jd/plugins/hoster/DateiTo.class
jd/plugins/hoster/FileBulkCom.class.removed
jd/plugins/hoster/Ftp.class
jd/plugins/hoster/MangaTradersOrg.class
jd/plugins/hoster/OffCloudCom$1.class
jd/plugins/hoster/OffCloudCom$2.class
jd/plugins/hoster/OffCloudCom$PanelGenerator.class
```

```
27 jd/plugins/hoster/OffCloudCom.class
28 jd/plugins/hoster/Offline.class
29 jd/plugins/hoster/OneEightZeroUploadCom$1.class.removed
30 jd/plugins/hoster/OneEightZeroUploadCom$2.class.removed
31 jd/plugins/hoster/OneEightZeroUploadCom.class.removed
32 jd/plugins/hoster/PinterestCom.class
33 jd/plugins/hoster/RapideoPl.class
34 jd/plugins/hoster/SloozieCom.class.removed
35 jd/plugins/hoster/SnelNLUsenet.class
36 jd/plugins/hoster/Speedy_ShareCom.class.removed
37 jd/plugins/hoster/StageFlvCom.class.removed
38 jd/plugins/hoster/ZeveraCom.class
39 ----------Extensions----------
40 ----------Direct Files----------
41 build.json
42 translations/jd/captcha/translate/CaptchaTranslation.zh_CN.lng
43 translations/jd/controlling/reconnect/pluginsinc/liveheader/translate/
       LiveheaderTranslation.zh_CN.lng
44 translations/org/jdownloader/extensions/extraction/translate/ExtractionTranslation.
       zh_CN.lng
45 translations/org/jdownloader/gui/jdtrayicon/translate/TrayiconTranslation.zh_CN.lng
46 translations/org/jdownloader/gui/translate/GuiTranslation.tr.lng
47 translations/org/jdownloader/gui/translate/GuiTranslation.zh_CN.lng
48 translations/org/jdownloader/translate/JdownloaderTranslation.zh_CN.lng
49 translations/org/jdownloader/updatev2/UpdaterTranslation.zh_CN.lng
50 ----------Core Files----------
51 Core.jar
52 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$10.class
53 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$11.class
54 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$12.class
55 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$13.class
56 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$14.class
57 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$15.class
58 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$16.class
59 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$17.class
60 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$18.class
61 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$19.class
62 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$20$1.class
63 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$20.class
64 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$21$1.class
65 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$21.class
66 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$22.class
67 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$23.class
```

```
68 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$24.class
69 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$25.class
70 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$5.class
71 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$6.class
72 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$7.class
73 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$8.class
74 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler$9.class
75 JD: Core.jar/jd/controlling/linkcrawler/LinkCrawler.class
76 JD: Core.jar/jd/parser/html/HTMLParser.class
77 JD: Core.jar/org/jdownloader/captcha/v2/challenge/recaptcha/v2/recaptcha.html
78 JD: Core.jar/org/jdownloader/captcha/v2/solver/browser/html/browserCaptcha.js
79 Package: package_1452527252357.awf
80 Install
81 Write Revision: 7165
82 ----------------Plugins----------------
83 jd/plugins/decrypter/Srnnks$DecryptRunnable.class
84 jd/plugins/decrypter/Srnnks.class
85 ----------------Extensions----------------
86 ----------------Direct Files----------------
87 build.json
88 ----------------Core Files----------------
```

A.8 Protokollierungseinstellungen

Listing A.14: Einstellungsmöglichkeiten bzgl. der Protokollierung

```
1 org.appwork.utils.logging2.LogConfig.json
2 {
3   "maxlogfilesize" : 2147483647,
4   "debugmodeenabled" : true,
5   "cleanuplogsolderthanxdays" : 2,
6   "maxlogfiles" : 5,
7   "logflushtimeout" : 60
8 }
```

A.9 LinkCollector-Informationen

Listing A.15: Inhalt einer beispielhalften LinkCollector 00-Datei

```
1 \cfg\linkcollector1337.zip\00
2 {
3   "type" : "NORMAL",
```

```
4    "packageID" : "null|_|ontrhi01|_|<jd:packagename>",
5    "links" : [ ],
6    "name" : "OnTrHi01",
7    "priority" : "DEFAULT",
8    "comment" : "",
9    "expanded" : true,
10   "uid" : 1452531251110,
11   "created" : 1452531251110,
12   "sorterId" : "ASC.jd.controlling.linkcrawler.CrawledPackage",
13   "downloadFolder" : "<jd:packagename>"
14 }
```

Listing A.16: Inhalt einer beispielhalften LinkCollector 000-Datei

```
1  \cfg\linkcollector1337.zip\00_0
2  {
3    "id" : null,
4    "name" : null,
5    "enabled" : true,
6    "uid" : 1452531251112,
7    "created" : 1362761638,
8    "downloadLink" : {
9    "name" : "OnTrHi01.part01.rar",
10   "url" : "http://uploaded.net/file/mgkt722z",
11   "properties" : {
12   "FINAL_FILENAME" : "OnTrHi01.part01.rar",
13   "URL_CONTENT" : "http://ul.to/mgkt722z",
14   "SHA1" : "4e12583812fe3994db899c51a9b663ab22ed6cea",
15   "LINKDUPEID" : "uploaded.to://mgkt722z",
16   "ARCHIVE_ID" : "19887b5d0a705491bab5cd364899cd7685916fdf4b241ea68ac36059339bb2e2",
17   "VERIFIEDFILESIZE" : 263192616
18   },
19   "size" : 263192616,
20   "host" : "uploaded.to",
21   "enabled" : true,
22   "uid" : 1452531251112,
23   "created" : 1362761760,
24   "propertiesString" : null,
25   "availablestatus" : "TRUE",
26   "urlProtection" : "UNSET",
27   "linkStatus" : null,
28   "current" : 0,
29   "chunkProgress" : null,
30   "finalLinkState" : null
```

```
31    },
32    "originDetails" : {
33    "id" : "CLIPBOARD",
34    "details" : null
35    },
36    "archiveInfo" : null,
37    "sourceUrls" : [ "http://ul.to/mgkt722z" ]
38  }
```

A.10 Entpackungs-Informationen

Listing A.17: Protokollierte Informationen während der Extraktion des Archives OnTrHi04.part01.rar

```
1  1449672428830 - Archive Name: OnTrHi04
2  1449672428830 - Archive Path: C:\Users\PC\Desktop\OnTrHi01\OnTrHi04.part01.rar
3  1449672428862 - Date: Wed Dec 09 15:47:08 CET 2015
4  1449672428862 - Start Extracting
5  1449672428863 - Extension Setup:
6  {
7    "useoriginalfiledate" : true,
8    "passwordlist" : [ "Test", "SP", "fg", "markant", "Angel", "Password", "0815", "
         Password1", "Password2", "Password3" ],
9    "guienabled" : false,
10   "deleteinfofilesafterextraction" : false,
11   "maxcheckedfilesizeduringoptimizedpasswordfindinginbytes" : 1024000,
12   "customextractionpathenabled" : false,
13   "latestiffileexistsaction" : "OVERWRITE_FILE",
14   "askforpassworddialogtimeoutinms" : 600000,
15   "blacklistpatterns" : [ "" ],
16   "subpathminfilesorfolderstreshhold" : 2,
17   "enabled" : true,
18   "cpupriority" : "HIGH",
19   "askforunknownpasswordsenabled" : true,
20   "deepextractionblacklistpatterns" : [ "##Lines with XX are comments", "##Skip
         deep extraction of archives that contain exe files", ".\\.exe" ],
21   "subpath" : "%PACKAGENAME%",
22   "deletearchivefilesafterextractionaction" : "NULL",
23   "restorefilepermissions" : true,
24   "iffileexistsaction" : "SKIP_FILE",
25   "passwordfindoptimizationenabled" : true,
26   "oldpwlistimported" : true,
27   "customextractionpath" : "C:\\Users\\PC\\extracted",
28   "deletearchivedownloadlinksafterextraction" : true,
```

```
29   "deepextractionenabled" : true,
30   "subpathminfilestreshhold" : 0,
31   "writeextractionlogenabled" : true,
32   "subpathenabled" : false,
33   "bubblecontentcurrentfilevisible" : true
34 }
35 1449672428863 - Archive Setup:
36 {
37   "autoExtract" : "UNSET",
38   "extractionInfo" : null,
39   "extractPath" : null,
40   "finalPassword" : null,
41   "ifFileExistsAction" : null,
42   "passwords" : [ ],
43   "removeDownloadLinksAfterExtraction" : "UNSET",
44   "removeFilesAfterExtraction" : "UNSET"
45 }
46 1449672428863 -  (Part)File: C:\Users\PC\Desktop\OnTrHi01\OnTrHi04.part01.rar
47 1449672428863 -  (Part)File: C:\Users\PC\Desktop\OnTrHi01\OnTrHi04.part02.rar
48 1449672428863 -  (Part)File: C:\Users\PC\Desktop\OnTrHi01\OnTrHi04.part03.rar
49 1449672428863 -  (Part)File: C:\Users\PC\Desktop\OnTrHi01\OnTrHi04.part04.rar
50 1449672428863 -  (Part)File: C:\Users\PC\Desktop\OnTrHi01\OnTrHi04.part05.rar
51 1449672428863 -  (Part)File: C:\Users\PC\Desktop\OnTrHi01\OnTrHi04.part06.rar
52 1449672428863 -  (Part)File: C:\Users\PC\Desktop\OnTrHi01\OnTrHi04.part07.rar
53 1449672428863 -  (Part)File: C:\Users\PC\Desktop\OnTrHi01\OnTrHi04.part08.rar
54 1449672428863 -  (Part)File: C:\Users\PC\Desktop\OnTrHi01\OnTrHi04.part09.rar
55 1449672428863 -  (Part)File: C:\Users\PC\Desktop\OnTrHi01\OnTrHi04.part10.rar
56 1449672428865 - Prepare
57 1449672435642 - Extract To: C:\\Users\\PC\\Desktop\\OnTrHi01\\
58 1449672435643 - Use Password: null|PW Protected:false:false
59 1449672435643 - Start Extracting org.jdownloader.extensions.extraction.multi.
       Multi@3e72e6a9
60 1449675079763 - Extractor Returned
61 1449675079767 - ExitCode: 0
62 1449675079772 - Info:
63 {
64   "extractToFolder" : "C:\\Users\\PC\\Desktop\\OnTrHi01\\",
65   "files" : [ "C:\\Users\\PC\\Desktop\\OnTrHi01\\One.Tree.Hill.S04E01.Das.grosse.
         Erwachen.German.Dubbed.DL.iTunesHD.x264-TVS\\tvs-one-tree-hill-ded-dl-ithd-
         x264-401.mkv",
66 }
67 1449675079776 - Successful
```