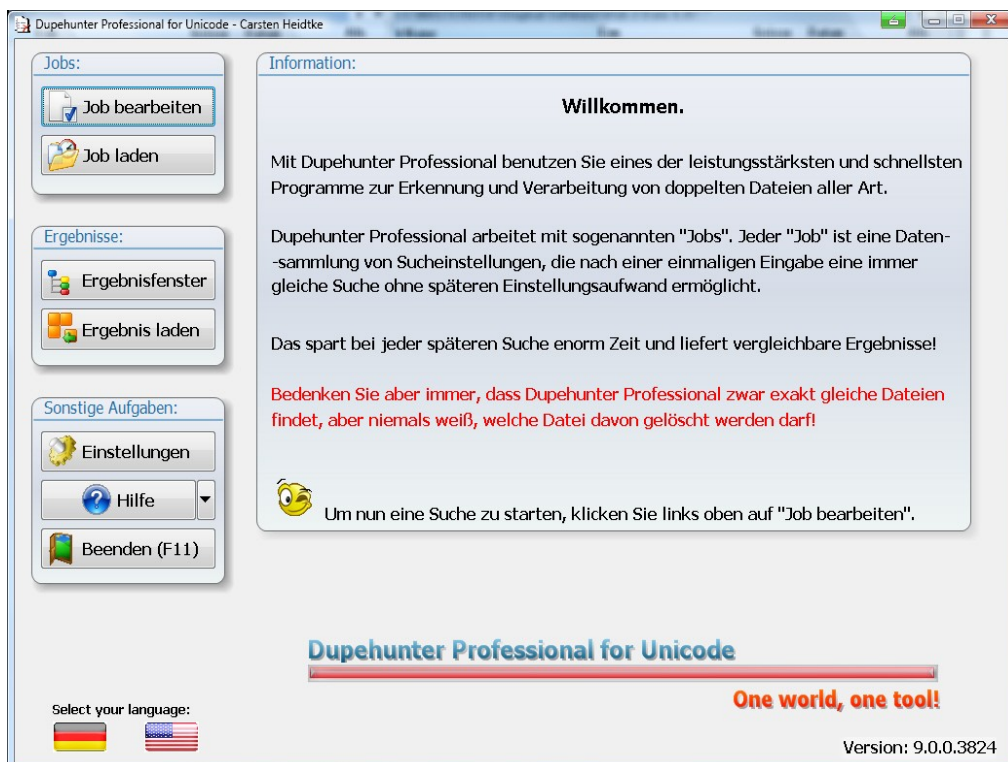


White Paper

Dupehunter Professional – XML-Unterstützung

Stand Mai 2010 – Version 9.0



Carsten Heidtke Software
Am Freibad 46
46499 Hamminkeln
Deutschland

Einführung: Was ist XML?

XML ist ein Dateiformat, welches auch mit **10 Millionen Einträgen** und mehr sehr zuverlässig und schnell arbeitet. Es ist textbasiert und kann daher mit jedem Texteditor wie etwa Notepad, als auch mit speziellen sogenannten XML-Parsern ausgelesen und bearbeitet werden. Es ist nicht gebunden an Patente Dritter oder an bestimmte Programme wie etwa Microsoft Excel. Zudem ist es an Flexibilität nicht zu überbieten.

XML in Dupehunter Professional:

Dupehunter Professional benutzt, wenn möglich, immer XML als Dateiformat. Dies vor allem, weil es Unicode-kompatibel ist, als auch die Flexibilität des Formats für diverse Anwendungsgebiete geeignet ist.

XML als Job-Datei:

Dupehunter Professional benutzt ab Version 9 XML als Format für die Job-Dateien und ersetzt damit das alte INI-Format, welches bis Version 8 benutzt wurde. Aus diesem Grund sind die alten Job-Dateien auch inkompatibel mit der neuen Version und jede Suche muss einmalig neu erstellt und als Job abgespeichert werden.

XML als Exportformat:

Neben der internen Benutzung von XML bietet Dupehunter Professional dieses Format vor allem als Exportformat an, um Ereignisse, Suchergebnisse oder Protokolle abzuspeichern. Damit bietet Dupehunter Professional individuelle Listen an, bei denen einzelne Felder gezielt abgefragt werden können und die dynamische Inhalte je nach Wunsch enthalten können. Die Spezialisierungen im Einzelnen:

Prioritätsvergaben:

Gerade in großen Firmen oder Behörden sammeln sich Unmengen von Dateien an. Aber bei mehreren tausend Dateien, die doppelt sind, verliert man den Überblick und vor allem die Kontrolle, ob im Suchergebnis wichtige Dateien, etwas Systembestandteile, erhalten sind oder nicht.

Daher bietet Dupehunter Professional die Möglichkeit, bestimmte Dateiendungen mit einer Nummer gemäß Ihrer Wichtigkeit zu definieren. Dabei können Sie selber definieren, welche Dateiendung Ihnen wichtiger ist als andere. Die Priorität, die Sie vergeben können, kann zwischen 0 und 100 liegen. So können zum Beispiel ausführbare EXE-Dateien als .EXE die Priorität 100 erhalten, während temporäre Dateien wie .TMP zum Beispiel die Priorität 0 erhalten. Über einen geeigneten Parser können dann

sicherheitsrelevante Dateien anhand der höheren Priorität ermittelt werden. Das Parsen wird auch schneller ausgeführt, wenn man nur nach dem Wert 100 scannen muss, um direkt mehrere Dateitypen, etwa .DLL, .EXE, .COM, zu erkennen.

Wichtig ist, die Dateierweiterung immer mit dem Punkt anzugeben, also .bmp und nicht bmp.

Da eine Prioritätsanalyse beim Exportieren Zeit und auch Dateigröße kostet, können Sie diese ganze Kategorie über die Checkbox „**Priorität protokollieren**“ ein- oder ausschalten.

Export von Besitzernamen:

Ab Version 9 unterstützt Dupehunter Professional auch das Exportieren von Besitzernamen der jeweiligen Dateien. Sinnvoll wird dies nur im geschäftlichen Bereich oder bei Ermittlungsarbeiten sein. Das Feld **OWNER** wird dann dynamisch während des Export gefüllt, was natürlich größere Exportdateien mit sich bringt.

Export von Seriennummern:

Ab Version 9 unterstützt Dupehunter Professional zudem das Exportieren der Seriennummern von Festplatten. Damit werden für Ermittlungsarbeiten die Festplatten genau dokumentiert und dienen als Beweise.

Hilfsprogramme und Betrachter:

Eine Rohdatenansicht von XML-Dateien ist nicht jedermanns Sache. Man wünscht sich da schon leserlichere Ausgaben. Wir arbeiten an einem Betrachter, der in der Zukunft diese Rohdaten visuell ansprechend aufbereitet. Bis dahin verweisen wir auf geeignete Hilfsprogramme wie etwa Altova XMLSpy oder andere, wie es sie bereits in vielen großen Firmen gibt. Damit lassen sich alle möglichen verschiedenen Ansichten generieren. Selbst ein normaler Internet Browser wie etwa der Internet Explorer oder Firefox können diese Dateien anzeigen.

Weitere Fragen:

Sie können uns jederzeit eine Anfrage an support@dupehunter.com schicken.