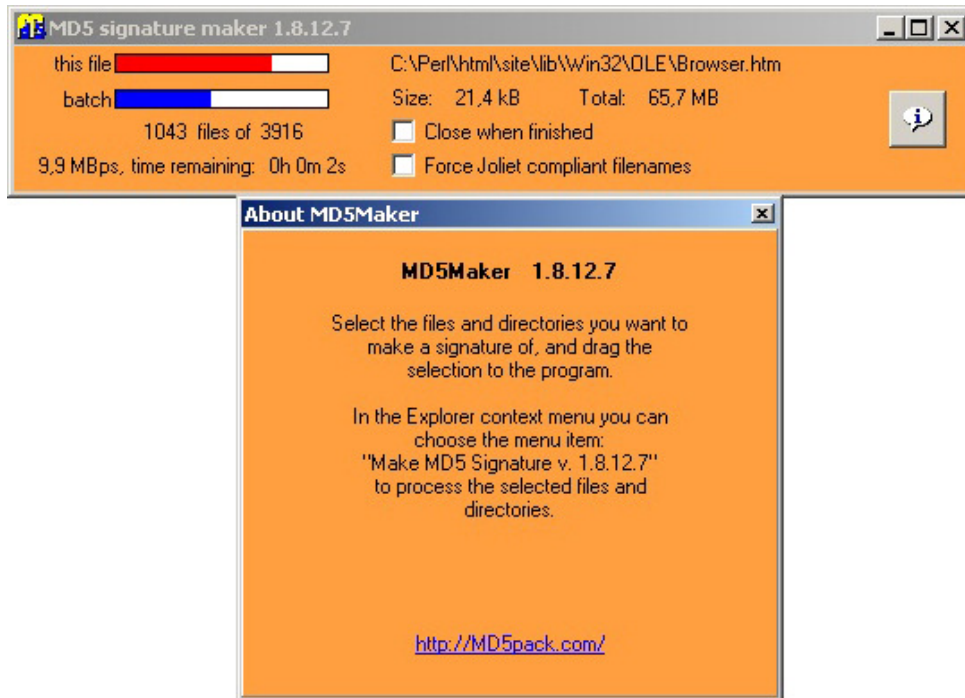


MD5Maker



MD5Maker maakt zogenaamde signatuurbestanden (of 'hashes').

Na het kopiëren van bestanden - van internet of van één type medium naar een ander type - is het vaak prettig er zeker van te kunnen zijn dat de kopie identiek is aan het origineel.

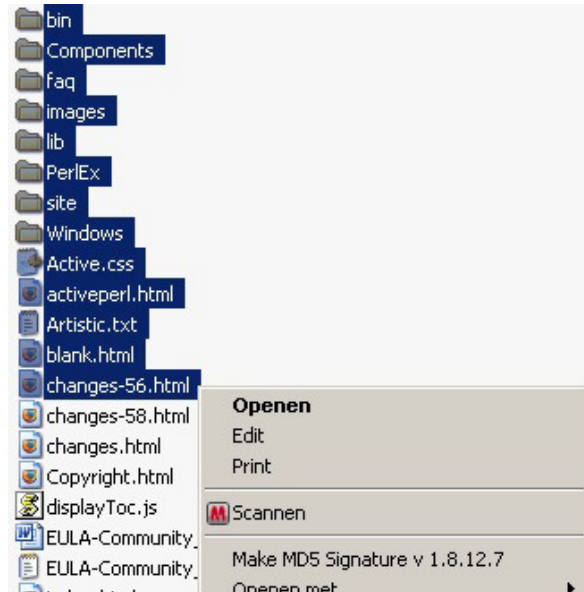
Dit wordt gedaan door de signatuur van de originele bestanden te vergelijken met die van de gekopieerde bestanden. Het md5 signatuurbestand moet worden opgeslagen in de originele map en naderhand worden gekopieerd naar dezelfde map in de kopie. Dat gaat het eenvoudigst door een md5-bestand te maken vóór het kopiëren. Voor read-only media dit is de beste manier, omdat er later geen md5-bestand op kan worden opgeslagen. ¹⁾

Vaak staat er bij een download-bestand op internet ook een md5-signatuur. Dat kan na ophalen dienen om de download te controleren.

=====

GEBRUIK

Het programma start door in de 'verkenner' met de rechter muistoets op een selectie van bestanden en/of mappen te klikken en in het contextmenu dat verschijnt het menu-item "Makel MD5 Signature v n.n.n.n" aan te klikken ("n.n.n.n" is het versienummer van MD5Maker). Ook kan het worden gestart door 'drag and drop' van een selectie naar het geopende programma. Van alle bestanden – ook die in alle sub-mappen - worden signaturen gemaakt, de submapnamen worden, waar nodig, aan de bestandsnamen toegevoegd: het 'relatieve pad'. Het bestand met de lijst met signaturen wordt dan naar de harde schijf geschreven; het heeft de extensie .md5.



=====

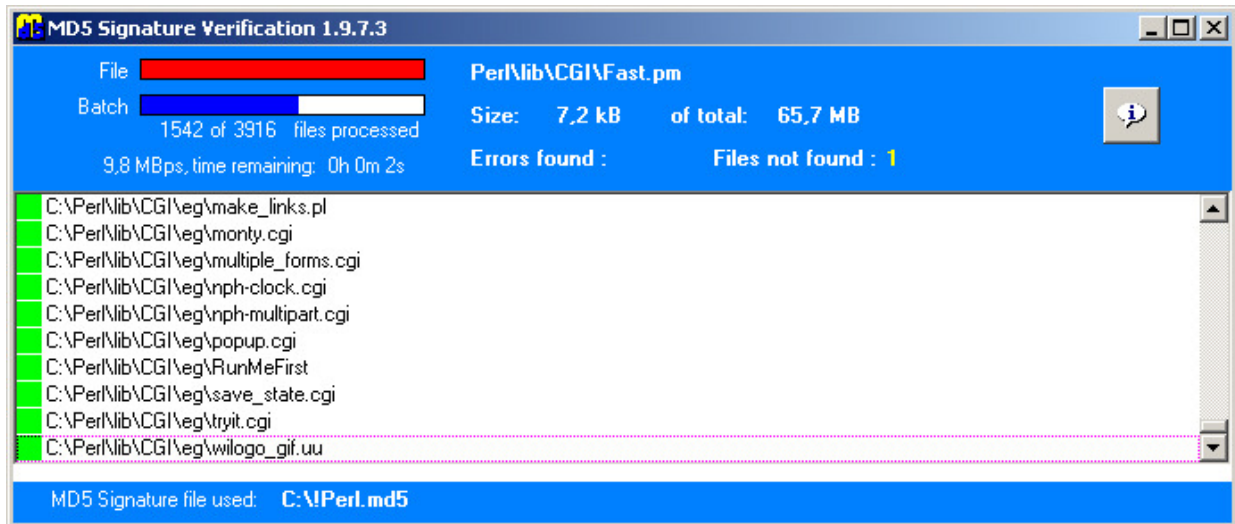
NB.

Wanneer een nieuwe versie van MD5Maker moet worden geïnstalleerd, zal eerst de oude versie automatisch worden gedeïnstalleerd. Wanneer na de installeren het MD5ext1.dll-bestand niet verdwenen is, en het ook niet met de hand gewist kan worden (omdat het nog 'geopend' is), moet de gebruiker zich eerst afmelden en daarna weer aanmelden. Dan kan het bestand alsnog met de hand worden gewist.

=====

MD5Verify

MD5Verify werkt alleen met bestanden die de extensie ".MD5" hebben. Het programma start door dubbelklikken op een MD5-bestand, of door een MD5-bestand te slepen naar het geopende programma. De controle gaat als volgt. MD5Verify berekent opnieuw de MD5 signatuur van alle bestanden waarvan de naam in het MD5-bestands voorkomt en vergelijkt de uitkomst met de signaturen in de lijst. De uitkomsten van de verificatie worden in een listbox getoond, met vóór elke bestandsnaam een gekleurd vakje. Er zijn drie mogelijke uitkomsten:



GROEN de signaturen stemmen overeen: de bestanden zijn identiek.

ROOD de signaturen verschillen: de bestanden zijn NIET identiek.

GEEL het bestand in de lijst is niet gevonden.

Ongeldige signaturen worden gezien als commentaar. Commentaarregels worden niet in de listbox getoond, maar het aantal wordt in zwarte letters bovenin getoond.

Om alleen de niet-identieke bestanden te zien, druk op de RODE filterknop; met de GELE knop worden alleen de bestanden getoond die niet werden gevonden.

Met het 'contextmenu' van het programma is het mogelijk die uitkomsten op te slaan in een tekstdocument.

Er kunnen méér dan één exemplaar van het programma tegelijk actief zijn.

=====

WAT IS EEN MD5 SIGNATUUR?

Een signatuur wordt gemaakt door de binaire inhoud van een bestand op een bekende en exact gedefinieerde manier te bewerken. Dit resulteert in een hexadecimale tekenreeks met 32 tekens (=128 bits). Het is bewezen dat het buitengewoon onwaarschijnlijk is dat twee verschillende bestanden dezelfde signatuur hebben ²⁾. Bovendien leidt een klein verschil tot een volkomen andere signatuur, zodat het eenvoudig te zien is dat ze ongelijk zijn. Het programma kent twee fasen. In fase 1 wordt een complete lijst gemaakt van alle bestanden in de selectie en de grootte van al die bestanden samen wordt bepaald. In fase 2 wordt een lijst van signaturen opgebouwd en naar bestand geschreven. Het programma kan alleen in fase 2 voortijdig worden afgebroken.

=====

DE STRUCTUUR VAN EEN MD5 SIGNATUUR-BESTAND

Zulke bestanden bevatten een of meer regels met de volgende structuur:

```
88326ff1342bde33514f7aa857ccac3c *changes-56.html
91d85a8995c8f4c0b321e89337a5c155 *bin\c2ph.html
c0772f20ad09e116c40ae74f442a6459 *bin\cpan.html
eccab9c6975996018756f0361ac7f369 *bin\dprofpp.html
```

Elke regel begint met een set van 32 hexadecimale tekens (alleen 0-9 en a-f komen voor). Grote en kleine letters zijn toegestaan. Dan volgen een spatie en een sterretje. Tenslotte volgt de bestandsnaam, waar nodig voorafgegaan door het relatieve pad als het verwerkte bestand in een subdirectory zat.

In de eerste regel van het voorbeeld bevindt het bestand 'changes-56.html' zich in de hoofdmap zelf. In de volgende regels is 'bin\' het relatieve pad, en de rest de bestandsnaam. De bestanden bevinden zich in de submap 'bin'.

Een speciale vorm van md5-signatuur komt zo nu en dan voor samen met het bestand op internet. Het bestand heet bijvoorbeeld 'foo.exe.md5' en ziet er als volgt uit:

```
fae1db8f3d3012c7b1af10beddc3cc12
```

Het is dan de signatuur van het bestand 'foo.exe'. MD5Maker kan overweg met zo'n type signatuur.

=====

1) Er is een manier om dit op te lossen. Een signatuur-bestand kan worden gemaakt van de data op een CD-R en worden opgeslagen op de harde schijf. Een 'platte' tekstverwerker laat zien dat direct na het sterretje in elke regel de stationsletter is toegevoegd:

```
539d5b568f4cb4bd1a80143a6c371e7e *G:\bin\cpan.html
```

Door in de tekstverwerker die letter te vervangen door die van het station dat de kopie bevat kan dan toch worden geverifieerd. Andersom kan natuurlijk ook!

=====

2) Het is mogelijk dat twee niet-identieke bestanden dezelfde 'hash' hebben. Een voorbeeld is te vinden op <http://stols.com/net/collision/collision!.zip>. Hierin hebben de bestanden 'abc2.bin' en 'def2.bin' op 6 plaatsen verschillende bits. Hun MD5 hashes zijn evenwel identiek.

Ref.: <http://www.reussirsurlenet.fr/v2/sections.php?op=viewarticle&artid=9>
http://www.doxpara.com/md5_someday.pdf
<http://www.codeproject.com/KB/security/HackingMd5.aspx>

=====