

## Berekening van de hash-code van een bestand of CD

### Inhoudsopgave

1. Inleiding	2
2. Te gebruiken commando bij verschillende besturingsomgevingen	2
3. Download en installatie Cygwin	3
4. Bereken hash-code met Cygwin voor CD of bestand	11

## 1. Inleiding

De authenticatie van de OSV software vindt plaats door het vaststellen van de hash-code van het gedownloade bestand of de ontvangen CD. Afhankelijk van het besturingssysteem waarop men de software installeert is de werkwijze iets verschillend.

## 2. Te gebruiken commando bij verschillende besturingsomgevingen

### Linux omgeving:

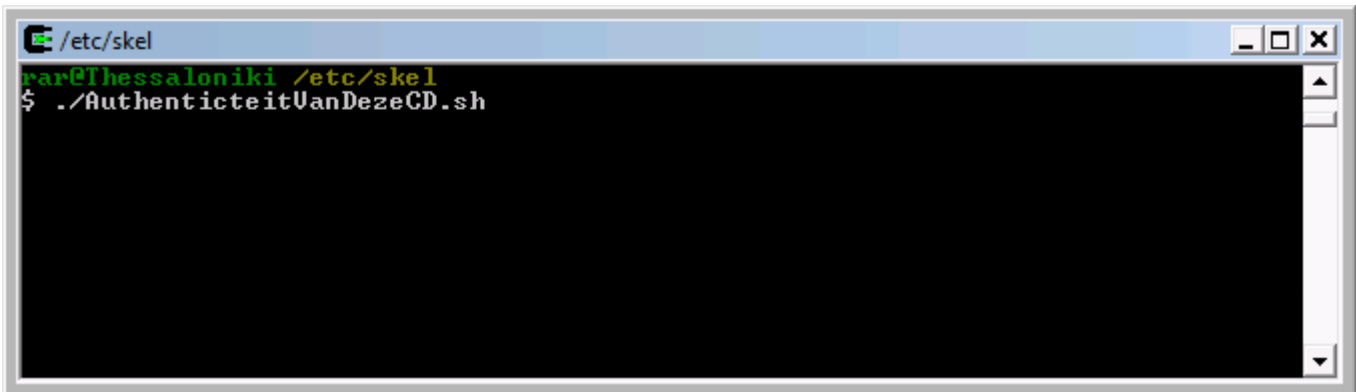
Voor een *bestand* geldt het volgende commando:

```
openssl dgst -sha1 bestandsnaam
```

Voor een *cd* is het commando dat ingegeven dient te worden uitgebreider, zie hfdst. 4. Het uitgebreide commando kan echter snel ingegeven worden door in een terminal venster een shell-script aan te roepen. De naam van het Shell script is 'AuthenticiteitVanDezeCD.sh'.

**Let op:** Als u van dit shell script gebruik wilt maken, moet er om het commando uit te kunnen voeren, een punt ( . ) en een slash ( / ) voorgezet worden. U dient overigens wel het recht te hebben om programma's uit te kunnen voeren! Het commando ziet er als volgt uit:

```
./AuthenticiteitVanDezeCD.sh
```



Figuur 2.1 Uitvoeren shell script

### Apple omgeving:

Bij een Apple omgeving is de procedure hetzelfde. Men opent een terminal venster en voert het script uit zoals onder de beschrijving voor de Linux omgeving is aangegeven.

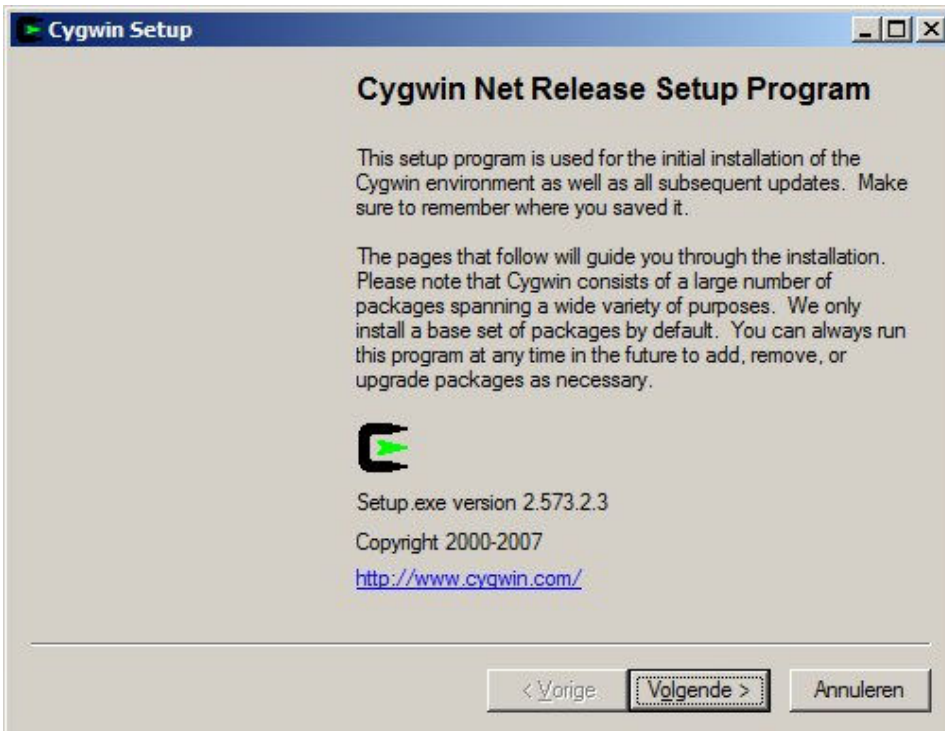
### Windows omgeving:

Windows is niet net als Linux en Apple in staat om de hiervoor aangegeven procedure te volgen. Echter met het programma Cygwin dat u op een willekeurige Windows PC installeert, creëert u een soort Linux- omgeving op de PC. Na installatie van dit programma kunt u allerlei Linux commando's uitvoeren op uw PC waaronder het vaststellen de hash-code van een bestand of CD. Dit programma kan men vinden op <http://cygwin.com/>. Hieronder is de procedure beschreven hoe men Cygwin download, daarna installeert op het 'gesloten' system waarop de OSV-software draait en vervolgens de hash-code bepaalt over het gedownloade ZIP-bestand of de ontvangen CD.

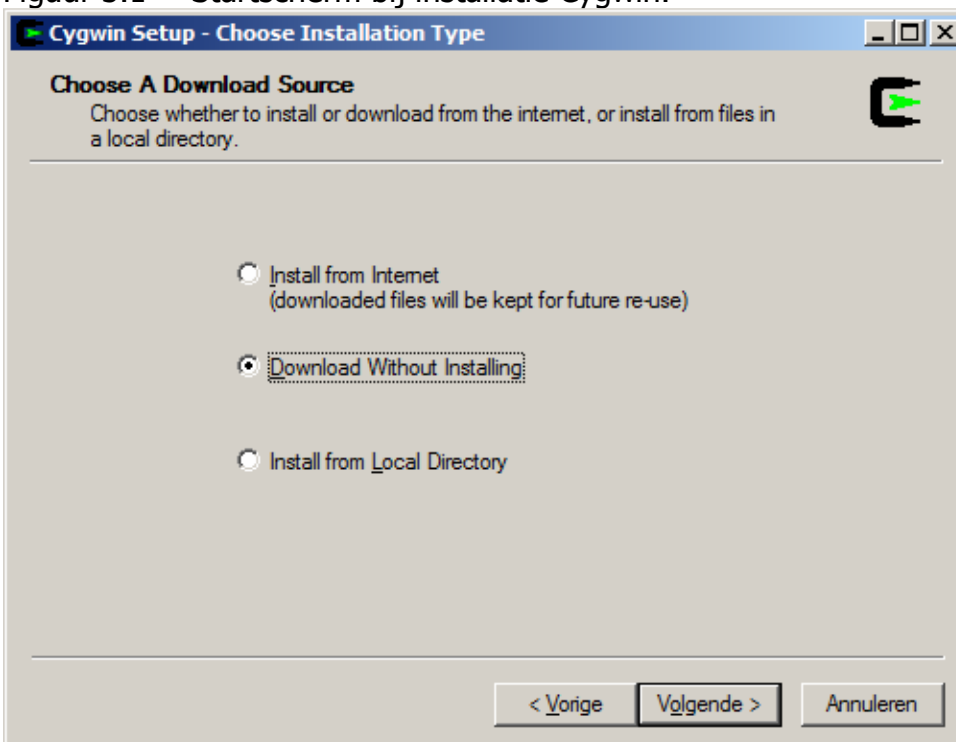
Ter volledigheid: Het downloaden van Cygwin moet plaatsvinden op een PC met internet verbinding. Het setup-bestand dat gedownload is wordt via CD of USB-stick naar de beschermde omgeving overgebracht en daar geïnstalleerd.

### 3. Download en installatie Cygwin

Om Cygwin te installeren zal een setup-bestand gedownload moeten worden via de url: <http://cygwin.com/setup.exe>. Het opstartscherm staat in figuur 3.1. Hier klikt u op [Volgende](#). Deze handleiding beschrijft hoe u het programma download en installeert. Het downloaden van Cygwin moet plaatsvinden op een PC met internet verbinding. Het setup-bestand dat gedownload is, wordt, via CD of USB-stick naar de 'beschermde' omgeving overgebracht en daar geïnstalleerd.

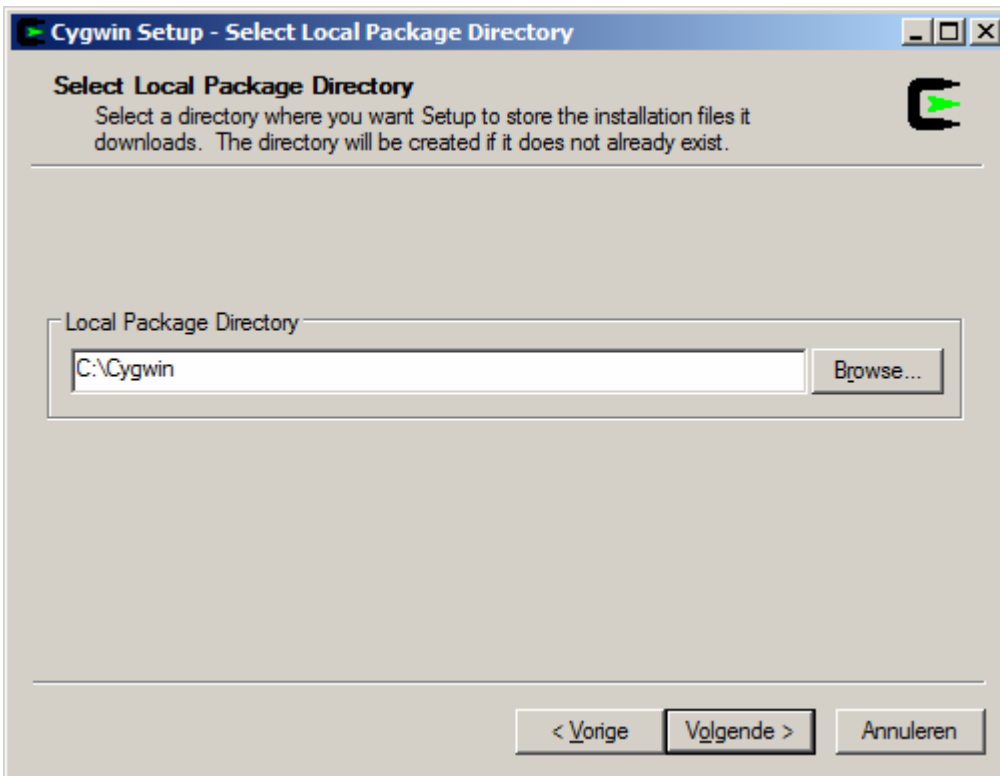


Figuur 3.1 Startscherm bij installatie Cygwin.



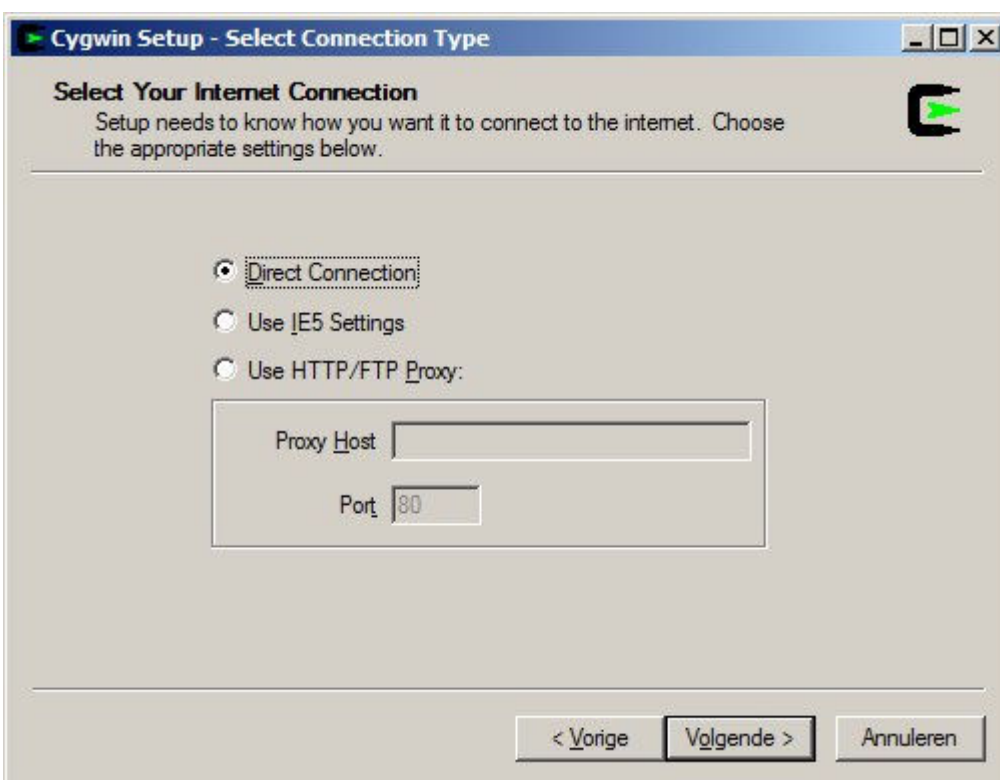
Figuur 3.2 Keuze installatiebron en -wijze.

Nu kunt u kiezen of u installeert van internet, bestanden wilt downloaden zonder te installeren of wilt installeren vanaf een lokale directory. Kies hier voor de [Download Without Installing](#) en klik op [Volgende](#).



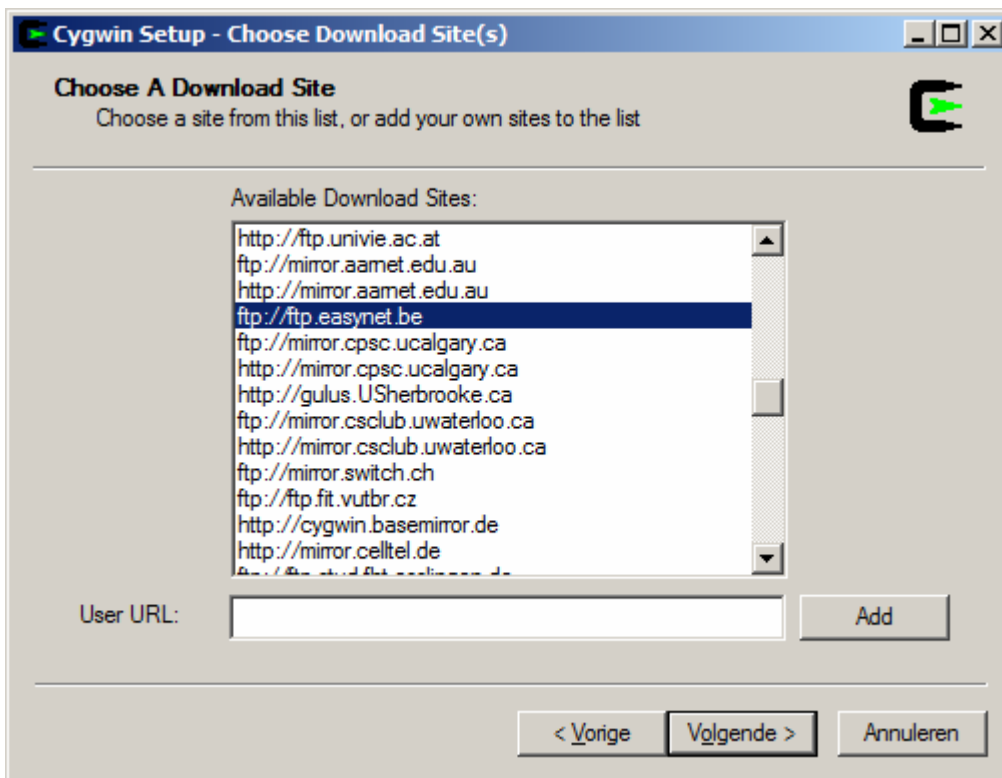
Figuur 3.3 Locatie keuze waar packages bewaard moeten worden.

Hier kunt u aangeven waar Cygwin geïnstalleerd moet worden. Het is aan te bevelen dat u de directory kiest waar ook de Cygwin setup.exe zich bevindt. Klik op [Volgende](#).



Figuur 3.4 Hoe is de verbinding met internet

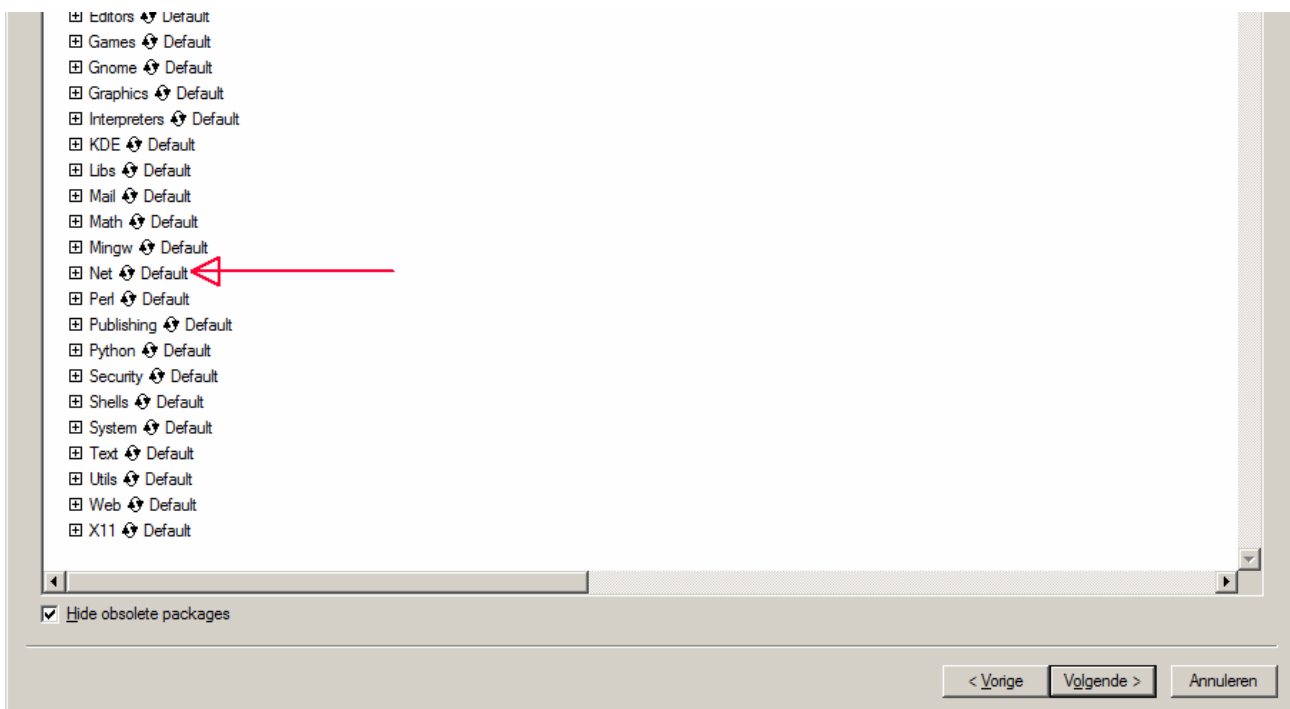
Daarna wordt gevraagd hoe de computer waarop u Cygwin installeert, verbonden is met internet, zie ook figuur 3.4. Deze instelling kunt u eventueel navragen bij uw netwerkbeheerder. Klik op [Volgende](#).



Figuur 3.5 Selectie website waarvan het programma gedownload wordt.

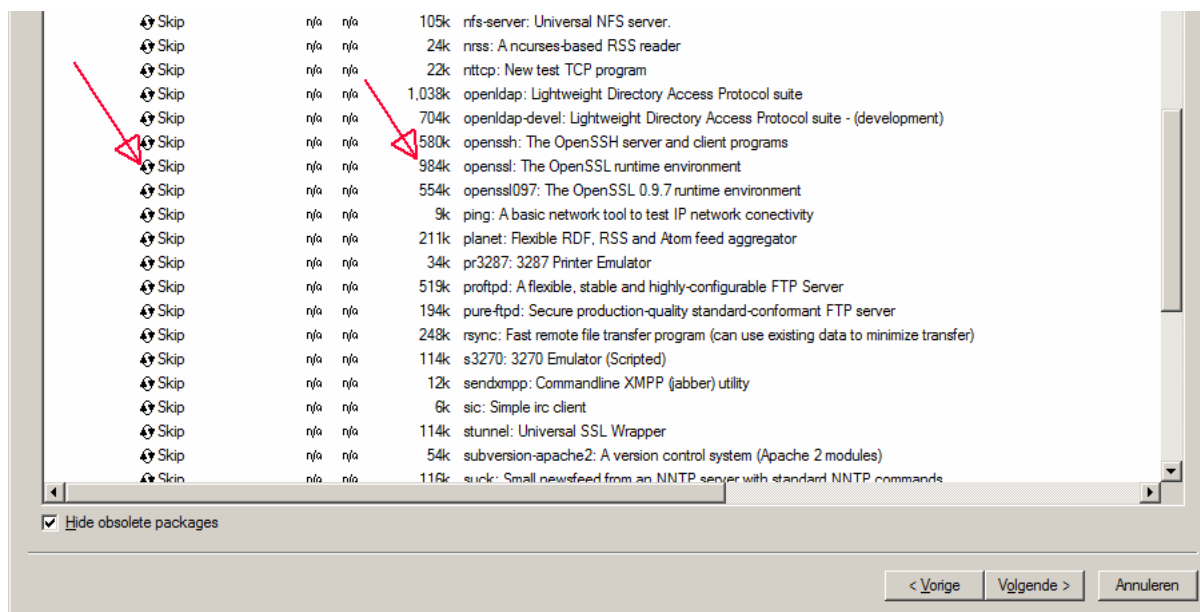
Vervolgens moet u aangeven van welke website u de software wilt downloaden, zie figuur 3.5. Als tijdens de download van Cygwin blijkt dat uw verbinding erg traag is kunt u de setup afbreken, opnieuw opstarten en een andere website kiezen. Klik op [Volgende](#).

Daarna maakt u de keuze om een speciaal onderdeel, een 'package' te installeren. In de figuren 3.6, 3.7 en 3.8 is aangegeven hoe dit in zijn werk gaat.

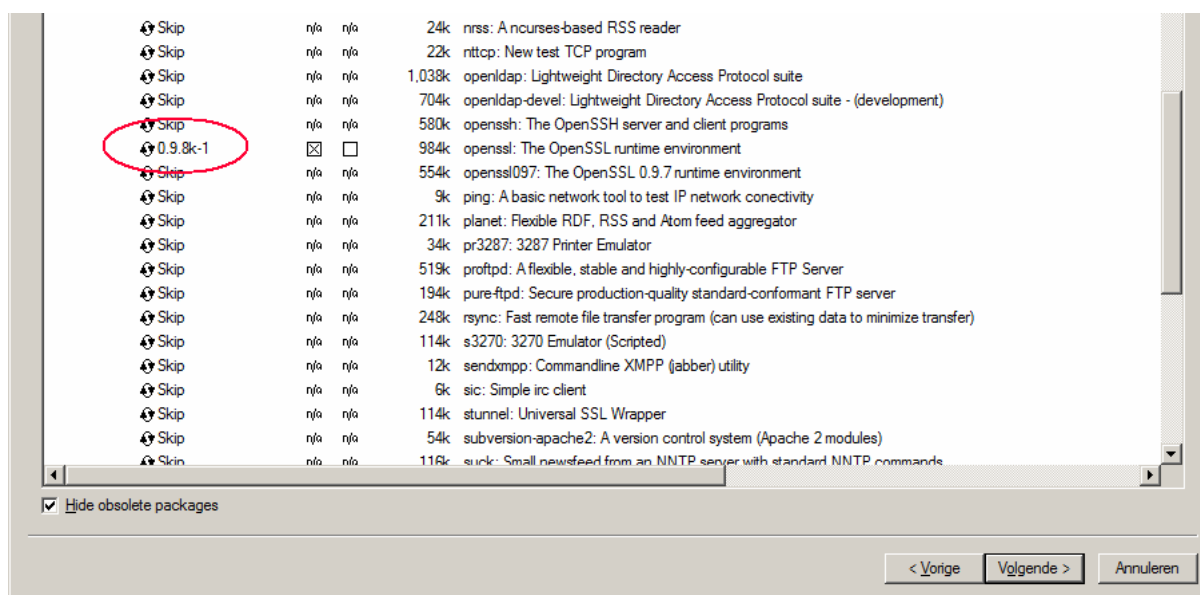


Figuur 3.6 Selectie installatie van het package 'Net'

Klik op het **+ teken** voor Net, zie figuur 3.6. Er opent zich nu een submenu met daarin allerlei onderdelen, zie figuur 3.7. Alleen het onderdeel OpenSSL dient geselecteerd te worden. Klik nu op **Skip** bij de package OpenSSL om dit onderdeel toe te voegen aan de te installeren onderdelen.

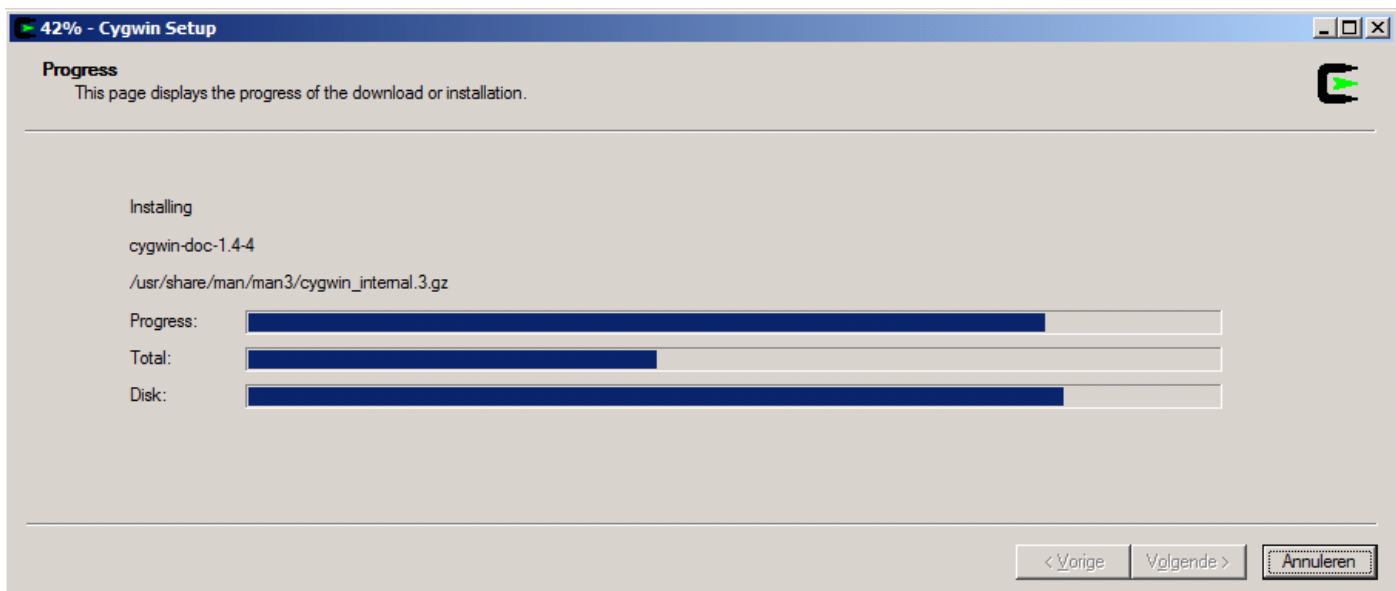


Figuur 3.7 Selectie OpenSSL runtime environment

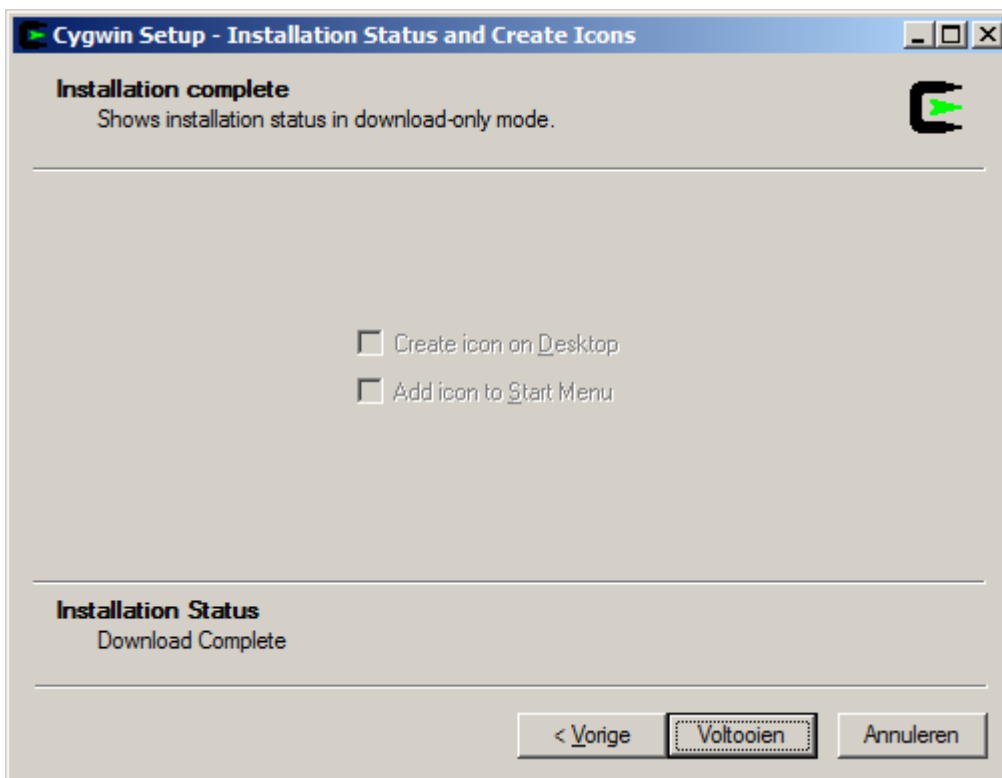


Figuur 3.8 Controleer dat de versie 0.9.8k-1 ingevuld is.

Klik na selectie van OpenSSL, zie figuur 3.8, op **Volgende**. Nu wordt de software gedownload, zie ook figuur 3.9. Klik nu op **Volgende**.

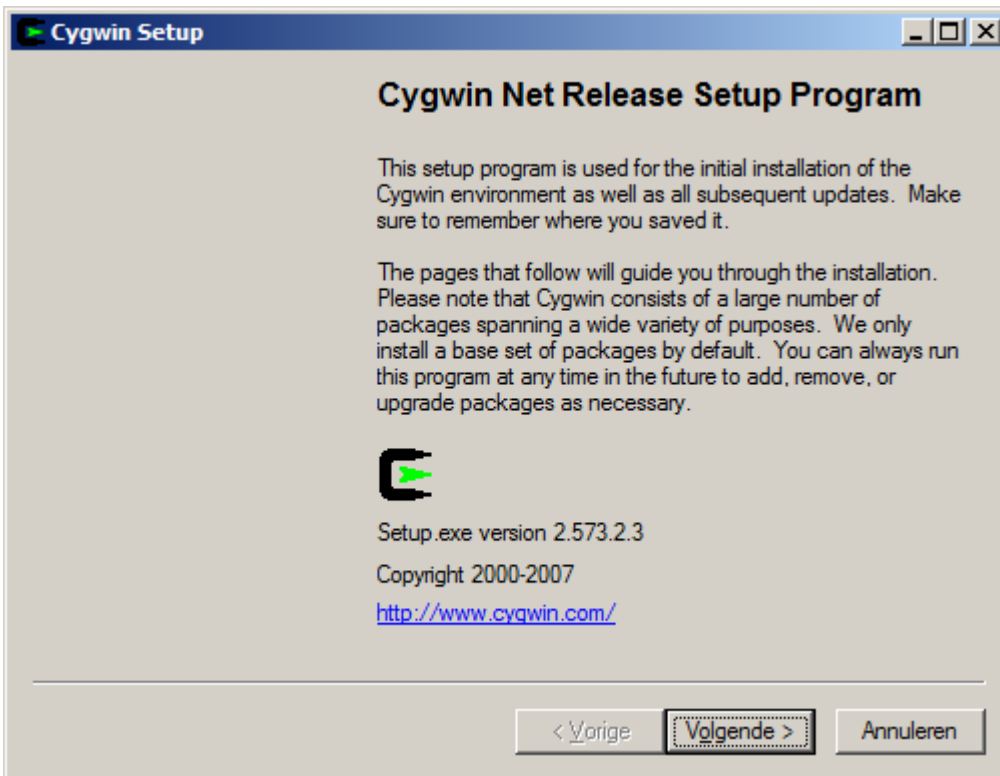


Figuur 3.9 Voortgangsscherm tijdens download Cygwin

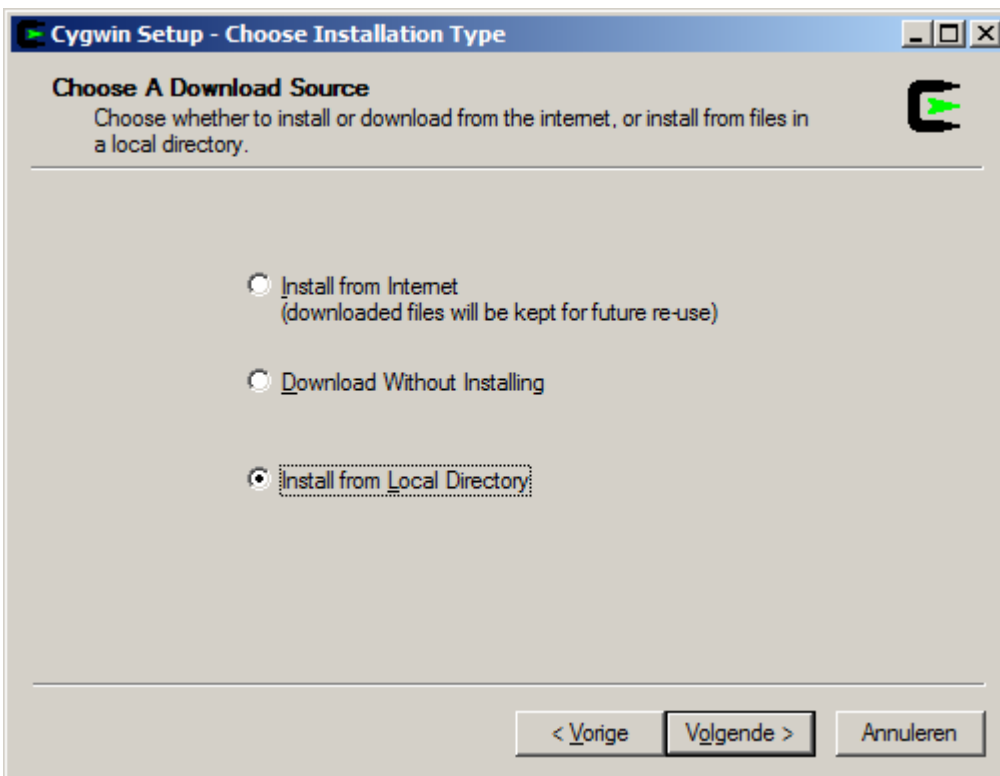


Figuur 3.10 Klik op [Voltooien](#).

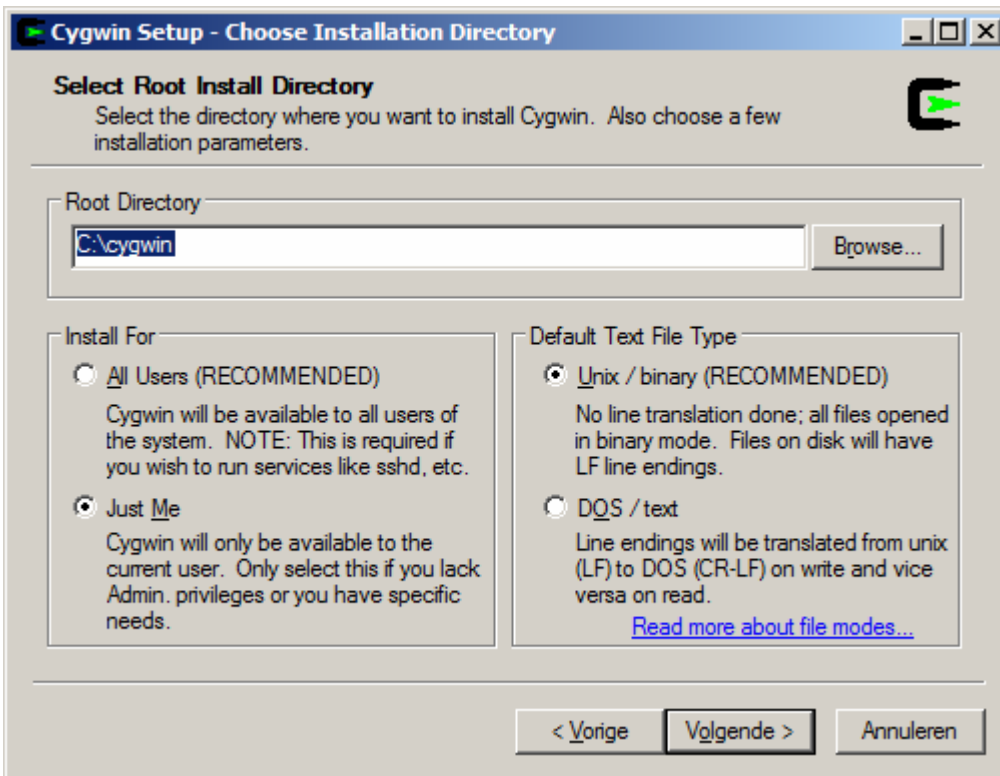
U heeft nu de installatiebestanden gedownload. Deze bestanden kunnen met het setup – programma op een ander medium gezet worden (bijvoorbeeld een USB-stick), welke daarna kunnen worden gekopieerd naar het 'gesloten' systeem. Vervolgens draait u nogmaals de gehele setup op het 'beschermde' systeem vanaf de USB-stick of CD waarop u de bestanden heeft gekopieerd. De volgende figuren geven de schermen weer waardoor u doorheen loopt om de installatie af te ronden. Let op de teksten onder de afbeeldingen, hier is aangegeven wat u moet doen.



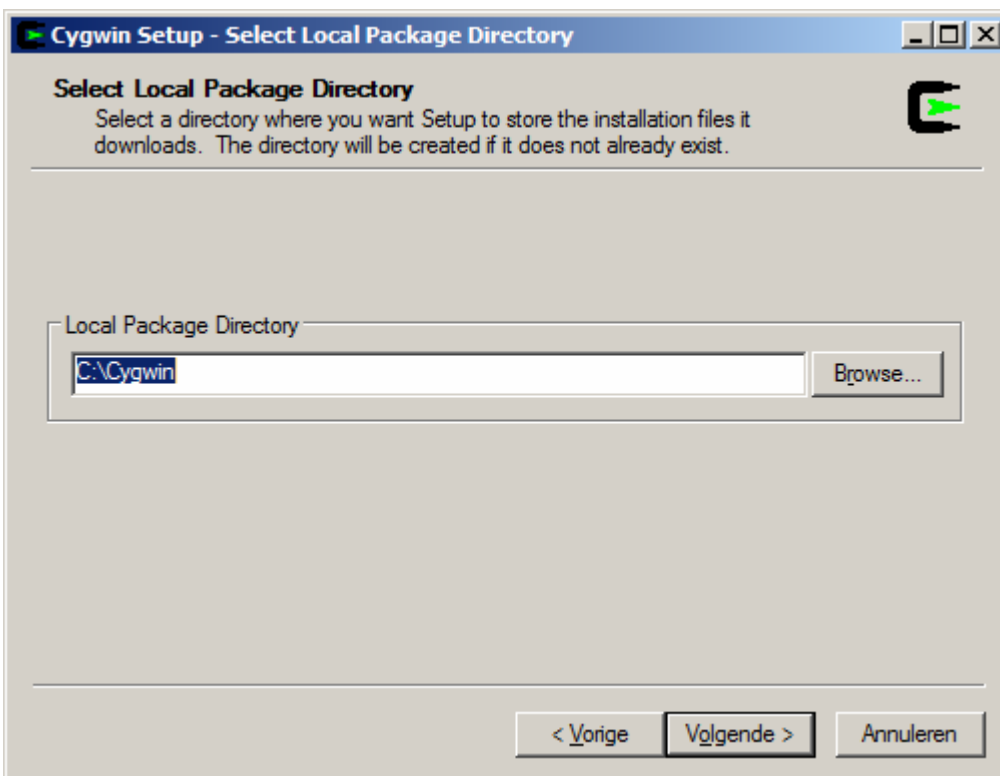
Figuur 3.11 Setup: klik op **Volgende**.



Figuur 3.12 Nu installeert u vanaf het medium waarop u de bestanden gekopieerd heeft. Klik op **Volgende**.

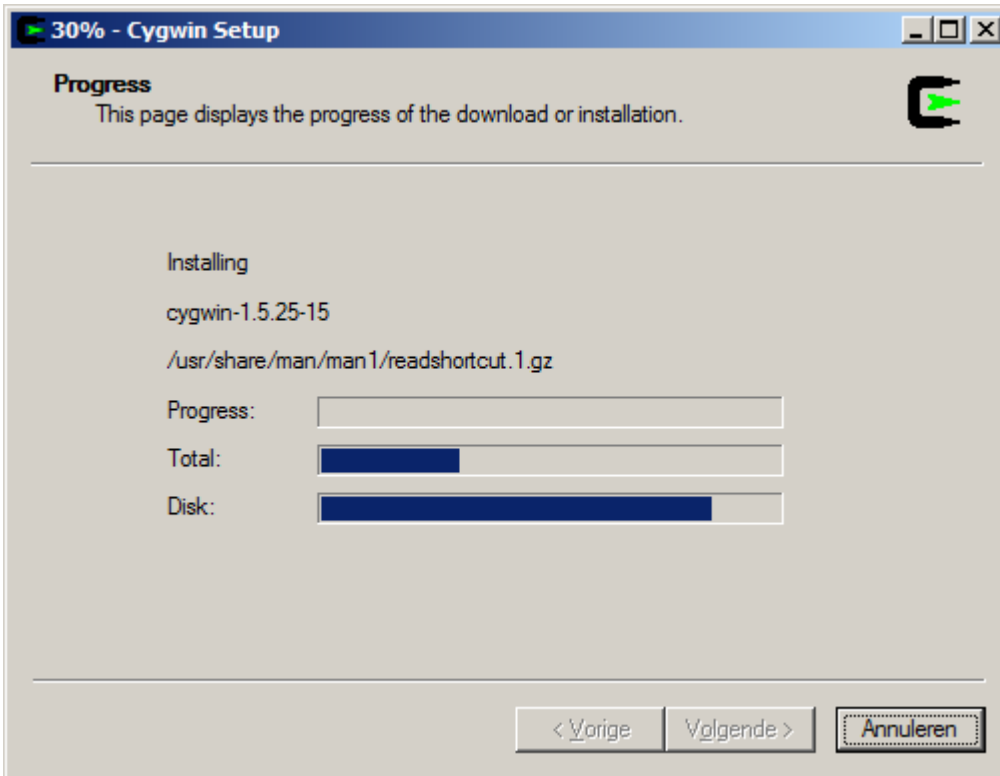


Figuur 3.13 Kies hier de directory van het medium waar u de bestanden die u heeft gedownload heeft staan (USB of CD). Klik op [Volgende](#)

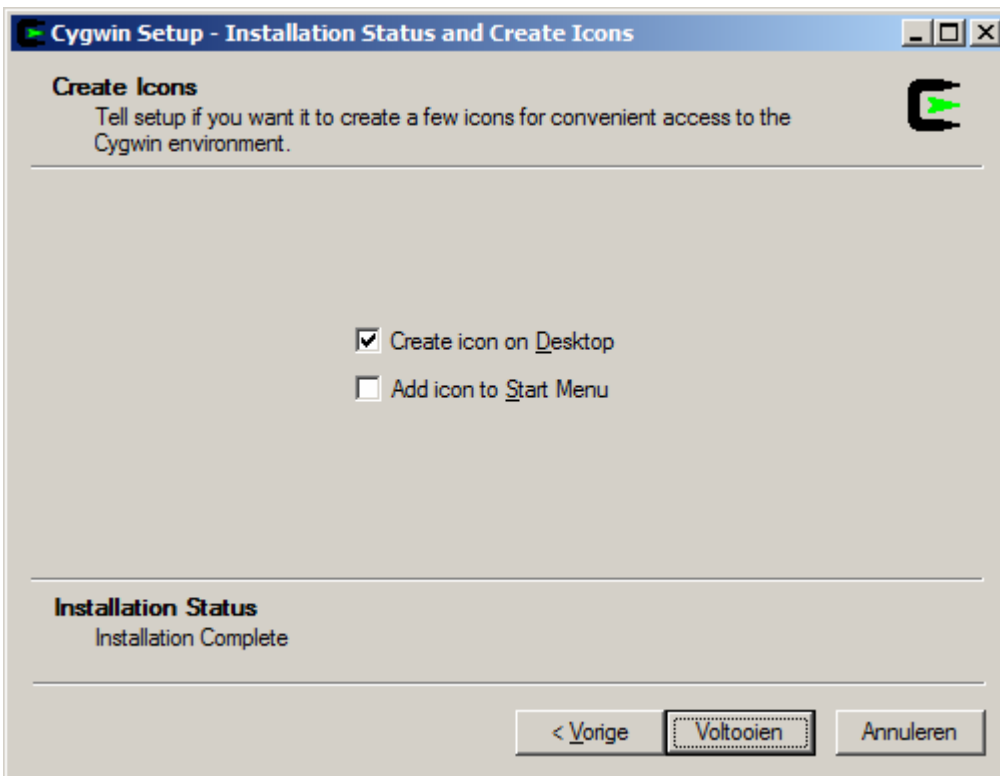


Figuur 3.16 Selecteer nu de directory waar de bestanden naartoe geïnstalleerd gaan worden. Dit is een plek op de PC waarop ook de OSV programmatuur gaat draaien. Klik op [Volgende](#).

Daarna maakt u nogmaals de keuze om een speciaal onderdeel, een 'package' te installeren. In de figuren 3.6, 3.7 en 3.8 is aangegeven hoe dit in zijn werk gaat. Let daarbij op dat OpenSSL geïnstalleerd wordt en klik op [Volgende](#)



Figuur 3.17 Voortgang van het installatieproces. Als het downloaden voltooid is, klikt u weer op [Volgende](#).



Figuur 3.18 Aanmaken van Cygwin icoontjes. Vink hier in ieder geval 'Create icon on Desktop' aan en klik op [Voltooien](#).

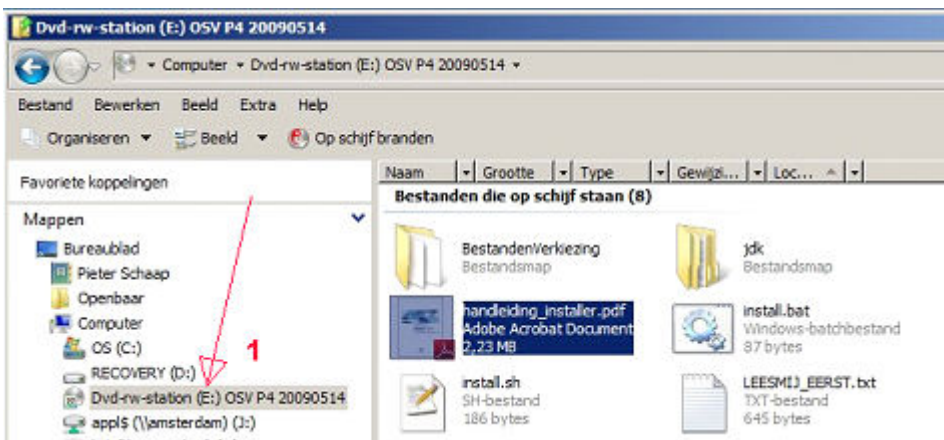
#### 4. Bereken hash-code met Cygwin voor CD of bestand

Na installatie kunt u met de procedure starten om de hash-code te berekenen. Start Cygwin door te dubbelklikken op de snelkoppeling. Er opent zich nu een zwart venster waarin men opdrachten op regelniveau kan invoeren, de zogenaamde 'commando box', zie figuur 4.1.

```

> /cygdrive/e
pssc@Astana ~ 2
$ cd /cygdrive/e
pssc@Astana /cygdrive/e 3
$ find . -type f -exec openssl sha1 {} ';' | cut -f 2 -d " " | sort | openssl
sha1
5a42ce3d249308739ddc7135903f21efa43cd18b
pssc@Astana /cygdrive/e
$
  
```

Figuur 4.1 Cygwin scherm met voorbeeld vaststellen hash-code van een CD.



Figuur 4.2 Vaststellen letter van drive waarin CD zich bevindt.

Hieronder staat aangegeven welke stappen u dient te volgen. Eerst wordt uitgelegd welke stappen men moet volgen voor het berekenen van de hash-code van een CD, daarna volgt de uitleg voor een bestand.

Er zijn 3 stappen die men dient te doorlopen om de hash-code van de CD te bepalen:

1. Bepaal de 'drive'-letter van de cd-dvd speler met daarin de CD met de OSV software (in ons geval E, zie ook figuur 4.2)
2. Vervang de letter 'e' in het volgende commando door de letter van de onder stap 1 vastgestelde letter en voer dit in het invoerscherm in. Commando:

`cd /cygdrive/e` gevolgd door de ENTER-toets.

3. Voor het vaststellen van de **authenticiteit van een CD** type nu het commando :

`find . -type f -exec openssl sha1 {} ';' | cut -f 2 -d " " | sort | openssl sha1`

gevolgd door de ENTER-toets.

Nu gaat het systeem de hash-code van de CD bepalen. Dit proces neemt even in beslag, afhankelijk van de snelheid van uw computer kan dit tussen de 5 en 45 minuten duren voor een CD.

Hieronder staan de 3 stappen die men dient te doorlopen om de hash-code van een **bestand** te bepalen, zie ook figuur 4.3:

1. Stel vast in welke directory het bestand zich bevindt.
2. Navigeer naar dit bestand met de commando's:  
`cd e:` gevolgd door de ENTER-toets. (voor navigatie naar schijf)  
`cd directorypad` gevolgd door de ENTER-toets

**Let op:** een spatie in een directorypad geeft men als volgt aan: '\ ' m.a.w. als men de directory "Program Files" wil selecteren schrijft men 'cd Program\ Files'

3. Voor het vaststellen van de **authenticiteit van een bestand** type nu het commando :

`openssl dgst -sha1 bestandsnaam`

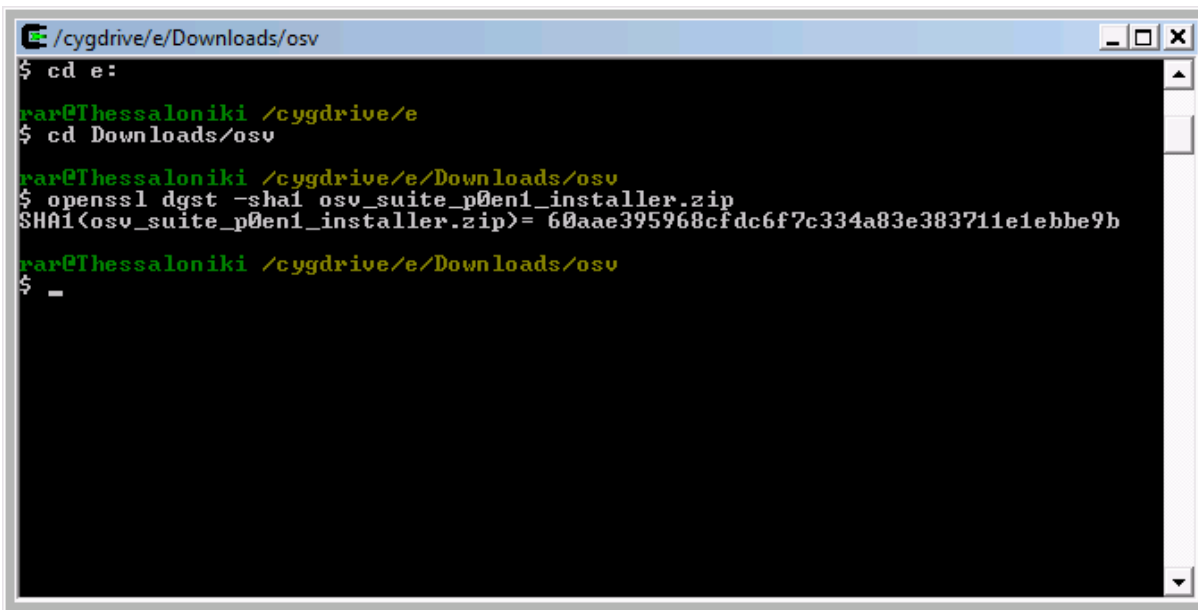
gevolgd door de ENTER-toets.

**Let op:** een spatie in een bestandsnaam geeft men als volgt aan: '\ ' m.a.w. als men de hashcode van het bestand "Deze CD.zip" (er zit een spatie tussen de woorden 'Deze' en 'CD') wil bepalen wordt het commando 'openssl dgst -sha1 Deze\ CD.zip'

Nu gaat het systeem de hash-code van het bestand bepalen. Dit proces neemt even in beslag, afhankelijk van de snelheid van uw computer kan dit tussen de 1 en 5 minuten duren.

In beide gevallen sluit met het Cygwin scherm af met het commando:

`exit`



```
cygdrive/e/Downloads/osv
$ cd e:
par@Thessaloniki /cygdrive/e
$ cd Downloads/osv
par@Thessaloniki /cygdrive/e/Downloads/osv
$ openssl dgst -sha1 osv_suite_p0en1_installer.zip
SHA1(osv_suite_p0en1_installer.zip)= 60aae395968cfdc6f7c334a83e38371e1ebbe9b
par@Thessaloniki /cygdrive/e/Downloads/osv
$ -
$ -
```

Figuur 4.3 Cygwin scherm met voorbeeld vaststellen hash-code van een bestand.

Wanneer de hash-code zoals die getoond wordt in het DOS-scherm identiek is aan de hash-code, zoals die gepubliceerd is in de brief van de Kiesraad (of op de website), heeft u de authenticiteit aangetoond van het ZIP-bestand of van de CD.

Een alternatieve aanpak is om de commando's die ingetoetst dient te worden automatisch in te geven door een shell-script bestand aan te roepen. Waar men dit bestand kan vinden zal aangegeven zijn in de brief van de kiesraad. Het shell-script bestand heet 'AuthenticiteitVanDezeCD.sh'. Zie hfdst. 2 voor een exacte beschrijving voor het aanroepen en uitvoeren van het shell-script bestand.