Hoofdstuk 3

Waardevolle gegevens beveiligen en terughalen

In dit hoofdstuk

> De verdedigingslinie van DOS 6
> Tips, valkuilen en waarheden van Backup
> Belangrijke voorzorgsmaatregelen voor gegevensbeveiliging
> Verloren bestanden en gegevens terughalen
> Definitieve gegevensvernietiging
> Maatregelen tegen virussen
> Een knipoog naar de amusementswereld

De verdedigingslinie van DOS 6

Steeds meer zaken en bedrijven zijn afhankelijk van gegevens in computers. Het verlies van gegevens kan een ramp betekenen. Gelukkig biedt DOS 6 een heel arsenaal aan hulpmiddelen waarmee gegevensverlies kan worden voorkomen en waarmee verloren gegane gegevens kunnen worden teruggehaald.

Hieronder volgt een overzicht van deze hulpmiddelen:

MIRROR. Met de schakeloptie /PARTN wordt er een kopie van de partitietabel van de vaste schijf naar schijf gekopieerd. Dit programma staat op de supplementendiskette van DOS 6.

MSAV. Het anti-virusprogramma van Microsoft voor het opsporen en vernietigen van computervirussen. Dit programma kan worden gestart als een schermgrootte toepassing of met schakelopties vanaf de opdrachtregel.

MSBACKUP. Het backupprogramma van Microsoft voor het maken van backups van bestanden en het weer terugzetten van die kopieën. De opdrachten kunnen niet worden uitgevoerd vanaf de opdrachtregel.

MWAV. De Windows-versie van het anti-virusprogramma. De functionaliteit is gelijk aan die van de DOS-versie maar dit programma

maakt gebruik van de grafische omgeving van Windows.

MWBACKUP. De Windows-versie van het backupprogramma. De functionaliteit is gelijk aan die van de DOS-versie. Beide programma's zijn volledig compatibel.

MWUNDEL. De Windows-versie van het programma waarmee verwijderde gegevens kunnen worden teruggehaald.

UNDELETE. Met dit hulpmiddel vergroot u de kans op het terughalen van verwijderde bestanden

UNFORMAT. Herstelt bestanden en directory's die door formatteren zijn vernietigd.

VSAFE. Dit hulpmiddel laadt het residente anti-virusprogramma dat de schijfactiviteiten controleert, en een bescherming biedt tegen virusinfectie en gegevensbeschadiging.

Zie ook deel 4, *Alle DOS-opdrachten* voor een volledig overzicht van al deze opdrachten.

Wanneer u de Windows-toepassingen installeert, wordt er automatisch een menu Tools aan de File Manager van Windows toegevoegd. In dit menu staan de opdrachten Backup en Anti-Virus. U kunt met SETUP /E zelf het menu aan File Manager toevoegen als Windows na DOS 6 wordt geïnstalleerd.

Gebruikers van Norton Desktop for Windows zullen misschien tot hun ergernis bemerken dat er twee menu's Tools op de menubalk staan. Het meest linkse menu is het standaardmenu Tools van NDW; het andere menu Tools is toegevoegd door DOS 6. Met de gegevens in de sectie [ADDONS] van het bestand WINFILE.INI worden door NDW extra menu's gemaakt. Door het toevoegen van een regel aan de sectie [DEFAULTS] van NDW.INI schakelt u deze optie uit en wordt dit menu Tools van DOS 6 niet aan de menubalk toegevoegd. Deze regel is:

```
MaxWinFileExtensions=0
```

Door het installatieprogramma van DOS 6 wordt er een programmagroep gemaakt met de naam Microsoft Tools. Hiermee kunt u snel de drie Windows-applicaties van DOS 6 starten:

Anti-Virus, Backup en Undelete. Deze groep wordt gedefinieerd in het bestand WINTOOLS.GRP in de DOS-directory. Degenen die met NDW werken, zullen zelf deze groep moeten maken. Hiervoor moeten zij File/New/Group kiezen en met de knop Browse het bestand WNTOOLS.GRP in de DOS-directory selecteren.

Wanneer er met Anti-Virus, Undelete of Backup vanaf een netwerkstation wordt gewerkt, kunnen deze programma's door andere gebruikers zijn aangepast. De standaardinstellingen van deze drie programma's worden gehaald uit respectievelijk MSAV.INI, MWAV.INI, UNDELETE.INI en MSBACKUP.INI.

Door een omgevingsvariabele MSDOSDATA te maken, kunt u opgeven dat het INI-bestand in een bepaalde directory door deze programma's wordt benaderd. Deze omgevingsvariabele dient te worden ingesteld als de directory waarin dat INI-bestand staat. U zou bijvoorbeeld de volgende opdracht aan AUTOEXEC.BAT kunnen toevoegen waarmee DOS wordt gedwongen de INI-bestanden vanuit de directory C:\INIFILES te laden:

```
msdosdata=c:\inifiles
```

Wanneer u vervolgens de configuratie van één van die programma's wijzigt, worden deze wijzigingen opgeslagen in uw eigen INI-bestand.

Tips, valkuilen en waarheden van Backup

De beste manier om niet te worden verrast door het verlies van gegevens, is erop voorbereid te zijn. Dit brengt ons bij de eerste, wrange waarheid:

Waarheid 1: vroeger of later zal er een belangrijk bestand worden vernietigd.

Een verwijderd bestand kan met een utility worden teruggehaald, maar vaak lukt dit niet zodat het bestand voorgoed verloren is. Wanneer u per ongeluk een bestaand bestand overschrijft met een ander bestand, bent u het oorspronkelijke bestand kwijt. Het enige redmiddel is een backup van het overschreven bestand naar de vaste schijf te kopiëren. Hier komt de noodzaak van het maken van backups om de hoek kijken.

Ondanks dat er zeer goede utility's zijn voor het terughalen van verwijderde bestanden, blijft het toch zaak regelmatig backups te maken.

De backupsoftware van DOS 6

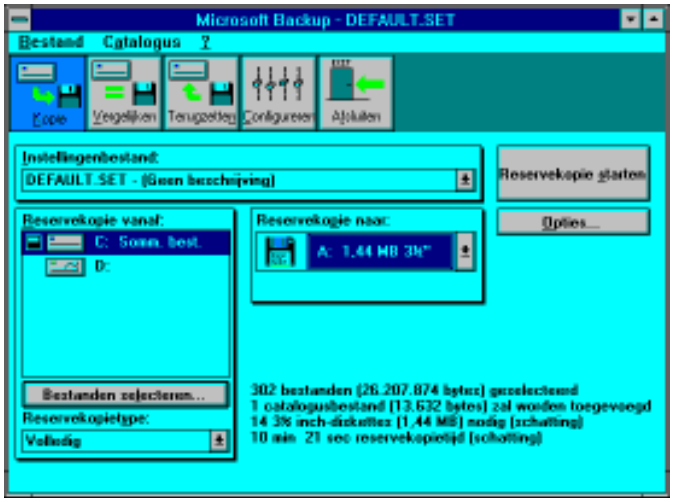
De backup-utility's van DOS 6 zijn een stuk verbeterd, en dat werd tijd. Gelukkig zijn de veel bekritiseerde programma's BACKUP en RESTORE vervangen. Het nieuwe programma komt in twee versies: een DOS- en een Windows-versie.

Het programma RESTORE wordt nog bij DOS 6 geleverd, zodat backups kunnen worden teruggehaald die met het oude programma BACKUP zijn gemaakt.

Een vergelijking tussen MSBACKUP EN MWBACKUP

Het verschil tussen beide programma's is meer kosmetisch dan functioneel. Menu's, terminologie en opties zijn gelijk. Backups die met de ene versie zijn gemaakt, kunnen met de andere versie worden teruggehaald. Afbeelding 3-1 en 3-2 laten de overeenkomsten tussen beide versies zien.

Figuur 3-1: Het dialoogvenster van MSBACKUP, de DOS-versie



Figuur 3-2: MWBACKUP, de Windows-versie

Uw keuze tussen beide versies zal worden bepaald door het gebruiksgemak en niet door de functionaliteit.

De backupprogramma's kunnen alleen op een standaard gegevensdrager van DOS backups maken, zoals een diskettestation, vaste schijf, netwerkstation of een verwisselbare vaste schijf. Een zeer groot nadeel is dat tape streamers niet worden ondersteund. Hopelijk zal deze mogelijkheid wel aanwezig zijn in een volgende versie.

De eerste keer dat u het backupprogramma start, moet u door een configuratieprocedure. Tijdens deze procedure wordt er als test een backup gemaakt op een of twee diskettes. Deze backup wordt vergeleken. Op basis van de verkregen gegevens kan worden bepaald of de procedure goed is uitgevoerd. Zorg dat u twee diskettes bij de hand hebt waarop geen waardevolle gegevens staan.

Bij systemen met twee of meer diskettestations kan een station worden gekozen. Kies het station dat later ook wordt gebruikt voor het maken van backups. Het diskettestation met de grootste capaciteit verdient de voorkeur.

Bestanden selecteren voor de backup

Het is raar maar waar: de meeste mensen hebben moeite met het selecteren van bestanden voor de backup. Het is niet zo dat u alleen het programma start en op de knop Start backup drukt.

De geselecteerde bestanden worden opgeslagen in een SETUP-bestand met de extensie SET. Standaard wordt het bestand DEFAULT.SET geladen.

U moet minstens één bestand hebben geselecteerd voordat u een backup kunt maken. De knop Start Backup is grijs (dus niet beschikbaar) als er geen bestand is geselecteerd.

Op een snelle manier kunt u alle bestanden op een station selecteren. Markeer in het veld Backup From het desbetreffende station (zie afbeelding 3-1 en 3-2) en druk vervolgens op de spatiebalk.

Er zijn twee mogelijkheden om een aantal bestanden te selecteren: aanwijzen en klikken, en de opdrachten include/exclude.

Aanwijzen en klikken

In het dialoogvenster Select Backup Files kunnen vanuit alle directory's bestanden worden geselecteerd. Een volledige directory wordt geselecteerd door deze eerst te markeren en vervolgens op de spatiebalk te drukken. Met Tab selecteert u afzonderlijke bestanden; met Tab wordt ook de selectie van een bestand opgeheven. Door de Exclude options niet te selecteren in het dialoogvenster Special Selections worden ook systeembestanden en verborgen bestanden getoond. Dit dialoogvenster is te openen met de knop Special.

Meerdere directory's die onder elkaar staan, zijn in één handeling te selecteren. Klik op de eerste directory, houd de linker muisknop ingedrukt en sleep over de gewenste directory's. Laat bij de laatste te selecteren directory de muisknop los.

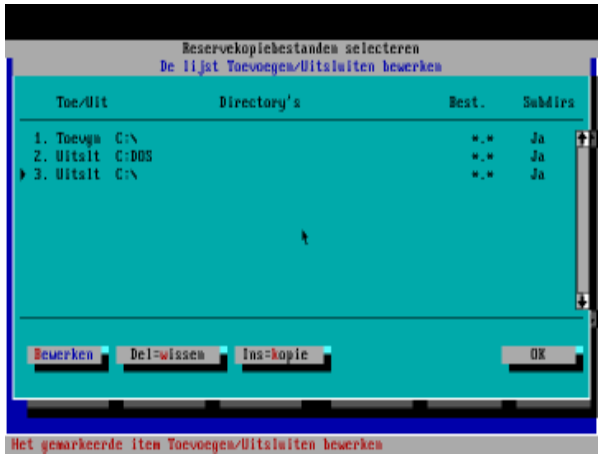
Geselecteerde bestanden worden aangegeven door een vinkje. Wanneer er een punt bij een geselecteerd bestand staat, is dit bestand uitgesloten vanwege een uitsluitingsregel, of omdat het niet overeenkomt met het backuptype. Van bestanden met een punt worden geen backups gemaakt.

Alhoewel beide versies praktisch gelijk zijn, wint de Windows-versie het wat betreft het selecteren van bestanden. Met de toetsen + en - is de directorystructuur in of uit te klappen. Een volledig station kan heel eenvoudig worden geselecteerd door de hoofddirectory in te klappen. Deze optie treft u niet aan in MSBACKUP.

Include en exclude

In het dialoogvenster Edit Include/Edit Exclude, of het dialoogvenster Include/Exclude Files van de Windows-versie, kunnen directory's worden geselecteerd. In de DOS-versie klikt u op de knop Include of Exclude. Vervolgens selecteert u onmiddellijk de knop Edit Include/Exclude List om het volgende dialoogvenster over te slaan. (Dit venster bestaat niet in de Windows-versie.) Zie afbeelding 3-3 voor dit dialoogvenster.

Door bestandsmaskers op te geven kunt u een lijst maken met bestanden waarvan wel, en een lijst met bestanden waarvan geen backup wordt gemaakt. De lijst wordt door het programma van boven naar beneden gelezen. Bij een conflict (bijvoorbeeld een voorwaarde sluit bestanden uit en een andere voorwaarde neemt dezelfde bestanden op) wordt de



Figuur 3-3: Het dialoogvenster Edit Include/Edit Exclude

onderste voorwaarde uitgevoerd. Bekijk de volgende lijst eens:

```
INCLUDE D:\ YES *.*
EXCLUDE D:\ACCESS YES *.*
EXCLUDE
D:\.........................YES *.BAK
```

In bovenstaande lijst worden alle bestanden opgenomen, met uitzondering van de bestanden in de ACCESS-directory en de bijbehorende subdirectory's, en alle bestanden met de extensie BAK.

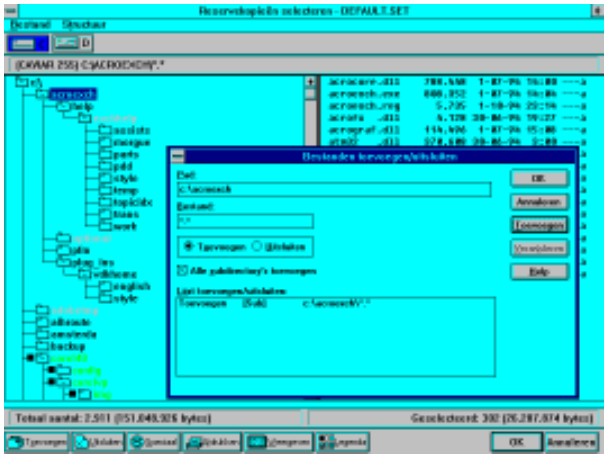
Een andere volgorde van deze lijst heeft consequenties, zoals het volgende voorbeeld illustreert:

```
EXCLUDE D:\ACCESS YES *.*
EXCLUDE
D:\.........................YES *.BAK
INCLUDE D:\ YES *.*
```

De laatste voorwaarde selecteert alle bestanden op station D en overschrijft daarmee de twee voorafgaande voorwaarden. Het resultaat is dat er een backup van alle bestanden op D wordt gemaakt.

Afbeelding 3-4 is het dialoogvenster Include/Exclude Files van de Windows-versie van het backupprogramma. Het zal niet de eerste keer zijn dat een gebruiker een include- en exclude-specificatie verliest door op Enter te drukken. U moet op de knop Add drukken en niet op de toets Enter. Met Enter wordt de knop OK gekozen en wordt het laatste genegeerd wat is ingevoerd.

Nadat bestanden zijn geselecteerd, staat er rechts in het hoofdvenster een overzicht van de geselecteerde bestanden (zie afbeelding 3-1).



Figuur 3-4: Het dialoogvenster Include/Exclude Files

Een selectie kan worden opgeslagen in een SET-bestand. Dit bespaart u de moeite steeds opnieuw bestanden te moeten selecteren. Wanneer u van dezelfde soort bestanden later weer een backup wilt maken, hoeft u alleen het bestand SET te kiezen in het menu File. Met een aantal SET-bestanden wordt het maken van backkups een eenvoudig karwei. Het steeds selecteren van bestanden behoort daarmee tot het verleden.

Backuptype selecteren

Naast het selecteren van bestanden kan een backuptype worden gekozen:

- Full
- Incremental
- Differential

Zoals de naam al aangeeft, wordt er met de optie Full een complete backup gemaakt van alle *geselecteerde* bestanden.

De optie Incremental maakt een backup van alle bestanden die zijn gewijzigd (of toegevoegd) sinds de laatste volledige of incrementele backup. Bij deze optie wordt er aan de hand van de archiefbit bepaald of er van het bestand een backup moet worden gemaakt. Wanneer deze archiefbit is ingesteld, wordt er inderdaad een backup van het bestand gemaakt. Na het maken van een backup worden de archiefbits van de desbetreffende bestanden uitgezet.

Gebruik steeds andere diskettes voor een incrementele backup. U kunt alleen het volledige bestandssysteem terughalen van de vorige, volledige backup en elke opeenvolgende, incrementele backup.

De optie Differential maakt een backup van alle bestanden die zijn gewijzigd sinds de laatste volledige backup. Net zoals bij de incrementele backup bepaalt de differentiële backup door middel van de archiefbit van welke bestanden een backup moet worden gemaakt. Het verschil tussen beide methoden is dat bij een differentiële backup de archiefbit niet wordt uitgezet nadat er een backup is gemaakt. Een volledige reserveset bestaat uit een volledige backup en de laatst differentiële backup.

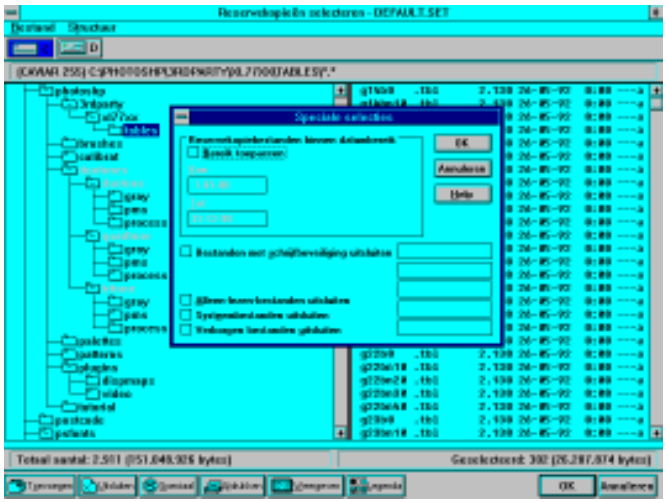
Tussen volledige backups zou u een incrementele of een differentiële backup moeten uitvoeren. Gebruik de laatste twee niet door elkaar. Het terughalen van een volledige set diskettes wordt aanzienlijk bemoeilijkt wanneer u beide methoden hebt gebruikt.

In het veld Backup Type in het hoofdvenster van het programma kan een ander type backup worden gekozen.

Speciale selectie-opties

Voor het selecteren van bestanden is een aantal speciale opties beschikbaar. Hiermee kunt u bijvoorbeeld opgeven dat er alleen een backup wordt gemaakt van bestanden die binnen een bepaald datumbereik vallen, of dat bestanden worden uitgesloten op basis van bestandsattributen.

U opent het dialoogvenster Special Selections met de knop Special in het venster Select Backup Files (zie afbeelding 3-5).



Figuur 3-5: Het dialoogscherm Special Selections

Met uitzonderling van de vijf velden rechtsonder spreekt het dialoogvenster voor zich. In deze velden kunnen tegen kopiëren beveiligde bestanden worden opgegeven waarvan geen backup hoeft te worden gemaakt. Er kunnen maximaal vijf

bestanden uit verschillende directory's worden opgegeven waarvan geen backup zal worden gemaakt. Voorwaarde is dat het veld Copy Protected Files is afgevinkt.

Gelukkig zijn kopieerbeveiligde bestanden niet zo belangrijk meer. Een bestand waarvan eigenlijk geen backup moet worden gemaakt, is het permanente wisselbestand van Windows, 386SPART.PAR. Dit bestand is onmisbaar voor Windows, maar bevat verder geen waardevolle gegevens. Dit bestand kan worden uitgesloten als het wordt gekenmerkt als een kopieerbeveiligd bestand in het dialoogvenster Special Selections.

Zorg ervoor dat de backup goed is

Waarheid 2: veel mensen komen er pas achter dat hun backup waardeloos is, als zij de gegevens willen terughalen.

Beide backupmethoden hebben een optie Compare waarmee de backup wordt vergeleken met de originele gegevens op de vaste schijf. Activeer deze optie, zodat er wordt gecontroleerd of de backup in orde is. Dit controleren kost tijd, maar is die tijd dubbel en dwars waard.

Voer in het begin enkele tests uit met waardeloze gegevens. Zo voorkomt u dat u later fouten maakt met waardevolle gegevens. Maak een backup en plaats de gegevens weer terug op de vaste schijf.

Snelheid verhogen

Hoe sneller de backup, des te beter. Hoe langer een backup duurt, des te minder is men geneigd deze te maken. Met het volgende kunt u sneller backups maken:

- Neem diskettes met een hoge capaciteit.
- Zet de gegevensverificatie in het menu Options uit. Er valt wat te zeggen voor snelheid aan de ene kant en veiligheid aan de andere kant. Controleer eerst enkele malen met Compare of de backups goed zijn. Activeer voor de eerste backup bij nieuwe diskettes de gegevensverificatie.
- Activeer gegevenscompressie. Gegevens comprimeren en naar schijf of diskette schrijven gaat sneller dan het wegschrijven van niet-gecomprimeerde gegevens.

- Zet de foutcorrectie uit. Ook hier moet er een keuze worden gemaakt tussen snelheid en veiligheid. Door informatie over de foutcorrectie op de diskette op te slaan, wordt de kans groter dat gegevens (van een beschadigde diskette) kunnen worden teruggehaald. Deze informatie neemt wel 10 procent extra ruimte in beslag.

- Sluit in de Windows-omgeving zoveel mogelijk programma's. Het maken van backups duurt langer naarmate er meer programma's een beroep doen op de CPU.

Door beide programma's wordt bij het opslaan van gegevens een speciale Error Correction Code (ECC) gebruikt. Deze techniek, die is ontwikkeld door Symantec, vergroot de kans dat gegevens met succes kunnen worden teruggehaald vanaf een beschadigde diskette. Dit kan zich voordoen als de diskette enkele slechte sectoren heeft en de optie Data Verification niet is geselecteerd. Of de diskette raakt beschadigd nadat er een backup is gemaakt.

Het ECC-systeem slaat een aantal sectoren in de laatste cilinder van de diskette op. Bij het terughalen van gegevens kunt u met de sectie ECC maximaal vier beschadigde sectoren repareren.

Zorg ervoor dat het diskettestation niet door andere toepassingen wordt benaderd als u met MWBACKUP werkt; het gevaar bestaat dat gegevens worden vernietigd. Deze beperking geldt voor alle diskettestations en niet alleen voor het station dat voor de backup wordt gebruikt.

Bestanden gemaakt en gebruikt door backup

Een groot aantal bestanden kan worden benaderd door de backupprogramma's. In de volgende lijst staan de belangrijkste bestanden:

- SET
- SLT
- Catalogus
- CAT
- 00*n*
- INI

■ LOG

SET-bestanden. Deze bestanden slaan een volledige definitie van de backup op, waaronder de stations en bestanden waarvan backups worden gemaakt, op welk station deze backups worden geplaatst, het backuptype (volledig of incrementeel) en de speciale opties. SET-bestanden worden in de DOS-directory opgeslagen en zijn ASCII-bestanden. Met File/Print kunt u deze bestanden afdrukken.

SLT-bestanden. In het SLT-bestand staat een lijst met directory's en bestanden die met het toetsenbord en de muis zijn geselecteerd voor de backup (en niet met de lijst Include/Exclude). Het bestand heeft dezelfde naam als het SET-bestand, met dien verstande dat SLT de extensie is.

Calatogusbestanden. Een catalogusbestand wordt voor elke backup gemaakt. Het is een binair bestand met volledige informatie over de structuur van het station (of de stations) waarvan een backup is gemaakt. Een kopie van het bestand wordt in de DOS-directory opgeslagen en een andere kopie aan het einde van de backup op de backupdiskettes.

Bij de naam van het catalogusbestand wordt een eenvoudige conventie gehanteerd. De naam van acht tekens geeft informatie over de backupbron en de gegevens:

Teken 1 De letter van het eerste station waarop de bestanden staan voor de backup.

Teken 2 De letter van het laatste station waarop de bestanden staan voor de backup.

Teken 3-7 De datum waarop de backup is gemaakt. JMMDD is de datumnotatie die hierbij wordt gebruikt. J is het laatste cijfer van het jaar waarin de backup is gemaakt, bijvoorbeeld 3 voor 1993.

Teken 8 Een letter die de volgorde van de backup aangeeft. Dit teken zorgt ervoor dat de naam van het catalogusbestand een unieke naam is. Wanneer er door het programma wordt bemerkt dat er al een catalogusbestand met die naam is, wordt de volgende beschikbare letter van het alfabet op die positie gebruikt.

Als de optie Keep Old Catalogs niet is geselecteerd, is het achtste teken altijd een A en wordt een catalogusbestand met dezelfde naam overschreven.

De extensie van het catalogusbestand geeft het backuptype aan: FUL, INC of DIF.

CAT-bestanden. Voor elke backupset wordt er een hoofdcatalogusbestand (CAT) gemaakt. De bestandsnaam heeft de extensie CAT en bestaat verder uit de eerste acht tekens van de naam van het SET-bestand. In dit (ASCII) bestand wordt bijgehouden wanneer de laatste volledige backup is gemaakt, en het bevat ook een chronologisch overzicht van elke incrementele of differentiële backup. Tijdens het terugplaatsen van gegevens wordt dit bestand benaderd. Bij elke nieuwe volledige backup wordt het bestand gewist en wordt de nieuwe backup als eerste item genoteerd.

00*n*. De bestanden op de backupdiskettes met de extensie 00*n* zijn de reservebestanden waarin de gegevens worden opgeslagen. De eerste backupdiskette krijgt het label 001, de tweede 002, enzovoorts. De bestandsnaam bestaat uit acht tekens en wordt opgebouwd volgens de conventie die ook bij het catalogusbestand wordt toegepast. De datum- en tijdstempel op het bestand geven het tijdstip weer waarop de backup is gemaakt.

Het volumelabel van een backupdiskette levert nog meer informatie op over de backup. Het eerste deel van het label is de naam van het setupbestand (zonder de extensie SET) waarmee de backupopties zijn ingesteld. De laatste drie tekens van dit label geven het backuptype weer: FUL, INC of DIF.

INI-bestanden. Door MSBACKUP wordt het binaire, niet te wijzigen, bestand MSBACKUP.INI gemaakt. Dit bestand bepaalt de primaire backupconfiguratie en de systeemkenmerken (bijvoorbeeld het DMA-transfertype en de geïnstalleerde stations). Wanneer dit bestand ontbreekt, moet u eerst MSBACKUP configureren voordat u ermee kunt werken.

LOG-bestanden. In het tijdelijke bestand MSBACKUP.LOG staat (in binair formaat) de directorystructuur van alle stations die zijn genoteerd tijdens de laatste backup. Dit bestand wordt gemaakt als MSBACKUP meedeelt dat de informatie of schijf wordt gelezen.

Elke diskette die als backupdiskette is gebruikt, kan naderhand weer bij de standaardopdrachten van DOS, zoals kopiëren, worden gebruikt. Wanneer u een nieuwe backup op een oude diskette uitvoert, wordt u gewaarschuwd dat de diskette al bij een vorige backup is gebruikt, zelfs als u de oude reservebestanden hebt verwijderd en het volumelabel hebt gewijzigd.

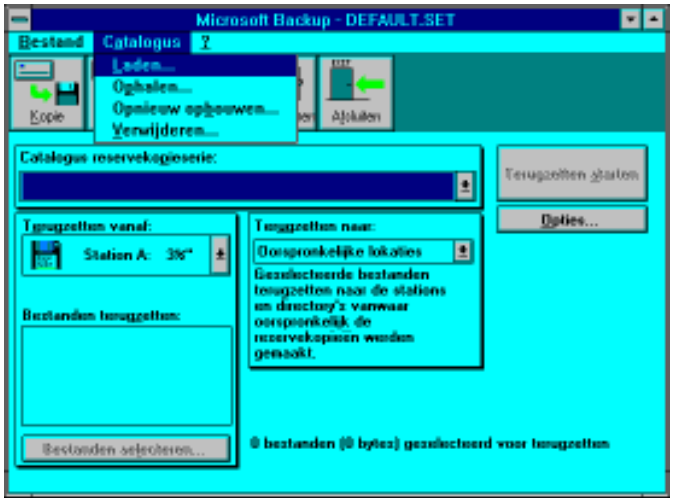
U vraagt zich misschien af hoe het backupprogramma kan weten dat de diskette eerder is gebruikt bij een backup. De bijzonderheden over de backup, SET-naam, datum en tijd en het getal van de diskette, worden opgeslagen in een deel van de bootsector. Dit gedeelte wordt alleen door formatteren verwijderd. Wanneer u een diskette plaatst, wordt er in de bootsector gekeken of deze diskette al is gebruikt bij een backup. Deze controle zorgt ervoor dat tijdens het maken van backups altijd de juiste diskette wordt gebruikt.

Backups terugplaatsen

Waarheid 3: een backup heeft geen zin als u deze niet kunt terugplaatsen.

Bestanden kunnen alleen worden teruggeplaatst als het overeenkomende catalogusbestand door het programma is geladen. Als de backup is gemaakt, wordt er één catalogusbestand in de DOS-directory en de andere op de laatste backupdiskette opgeslagen.

Afbeelding 3-6 is het dialoogvenster Select Calatog met de opties voor het kiezen van een calatog. Dit venster opent u met de knop Catalog in het venster Restore. Alhoewel MSBACKUP dit dialoogvenster niet heeft, kunt u toch dezelfde opties kiezen uit het hoofdmenu van Restore.



Figuur 3-6: Select Catalog in MWBACKUP

Een catalogusbestand is op drie manieren te benaderen:

Load	Het CAT-bestand wordt opgehaald vanaf de vaste schijf.
Retrieve	Het CAT-bestand wordt vanaf de laatste diskette van de backupset teruggeplaatst.
Rebuild	Het backupprogramma controleert de inhoud van elke diskette in de backupset en maakt een nieuw CAT-bestand.

Normaal gesproken moet u proberen het catalogusbestand te laden. Wanneer u het CAT-bestand niet kunt vinden, probeer dit dan vanaf de backupset te laden. U zult een nieuw catalogusbestand moeten maken als dit bestand is beschadigd of als u het niet kunt vinden.

Nadat het catalogusbestand is geladen, worden de bestanden geselecteerd die moeten worden teruggeplaatst. De hierbij gebruikte procedure is dezelfde als bij het maken van backups. Het enige verschil is dat er geen gebruik kan worden gemaakt van include- en exclude-lijsten. Met de knop Select Files in het dialoogvenster van Restore wordt een directorystructuur opgeroepen zoals die was toen de backup werd gemaakt. Het kan zijn dat de huidige structuur verschilt van deze structuur.

Zonder geselecteerde bestanden is de knop Start Restore lichter gekleurd en dus niet beschikbaar.

Standaard worden bepaalde bestanden (alleen-lezen, verborgen en systeem) niet teruggeplaatst. Wanneer u van alle bestanden op de vaste schijf een backup maakt, vervolgens de schijf formatteert en met de standaardinstellingen de bestanden terugplaatst, kan deze schijf niet meer worden opgestart. Dit komt omdat de systeembestanden, verborgen bestanden

Figuur 3-7: Catalog Options in MSBACKUP

en bestanden die alleen kunnen worden gelezen, ontbreken. Selecteer in een dergelijk situatie de knop Special in het dialoogvenster Select Restore Files en deselecteer de optie Exclude Files. Alleen zo worden alle bestanden teruggeplaatst, ongeacht hun bestandsattribuut.

Beperkingen wat betreft grootte

Zowel de DOS-versie als de Windows-versie van het backupprogramma kunnen een backup maken van enkele bestanden tot alle bestanden op de vaste schijf. Er zijn echter enkele beperkingen wanneer u bijvoorbeeld van een fileserver een backup wilt maken.

In onderstaande lijst wordt een overzicht gegeven van de beperkingen van het backupprogramma:

- Het maximum aantal items in een include/exclude-list is 50.
- Er is een maximum per dag van 26 backups van dezelfde stations met hetzelfde backuptype.
- Er kunnen niet meer dan 49 setupbestanden (SET) in een lijst in het dialoogvenster worden weergegeven.
- Er kunnen niet meer dan 1.023 directory's voor een station worden genoteerd.
- Per keer kan er van 'slechts' 65.535 bestanden een backup worden gemaakt.
- 254 diskettes is het maximum aantal voor een enkel bestand. Voor 3.5 inch diskettes (1.44MB) is dit gelijk aan een bestand van 730MB bij maximale compressie. Bij diskettes van 360k zonder compressie zakt deze maximale bestandsgrootte naar 90MB.

Backup van DoubleSpace-stations

Alle bestanden en directory's op een DoubleSpace-station zijn opgeslagen in een enkel (gigantisch) verborgen bestand op het hoststation.

In principe kan er op twee manieren een backup van de DoubleSpace-bestanden worden gemaakt. De eerste manier is een backup van het hoststation

met alle verborgen bestanden. Het nadeel hiervan is dat alle bestanden in één reservebestand worden opgeslagen. Als dit bestand om een of andere reden niet kan worden teruggeplaatst, kan er geen enkel DoubleSpace-bestand meert worden teruggeplaatst. U hebt dan op één paard gewed en verloren.

Een betere manier is van elk bestand op het DoubleSpace-station een backup te maken. Bij een eventuele gegevensfout zult u slechts enkele bestanden niet meer kunnen terugplaatsen.

Een goede backupstrategie

Backups maken zonder dat daar een goede strategie aan ten grondslag ligt, is als een ei zonder zout.

Waarheid 4: hoe ouder de backup, des te waarschijnlijker is het dat u gegevens zult verliezen.

U kunt verschillende strategieën ontwikkelen voor het maken van backups. De frequentie waarmee gegevens worden gewijzigd, zal in het algemeen de frequentie van de backup bepalen. Bij weinig werk is het voldoende eens per maand een volledige backup en eens per week een incrementele backup te maken. Wanneer u dagelijks op de computer werkt, zult u eens per week een volledige backup en elke dag een incrementele of differentiële backup moeten maken. Het hangt van u af hoeveel extra werk u wilt hebben. Hoe langer u met een backup wacht, des te groter de kans dat u veel werk een keer zult moeten overdoen.

Waarheid 5: houd bij het maken van backups een strikte discipline aan.

Blijf realistisch bij het vaststellen van een backuproutine. Twee keer per dag een volledige backup stuit op weerstand. Twee keer per week een volledige backup en dagelijks een differentiële backup behoedt u voor veel narigheid. Daarbij is een differentiële backup te verkiezen boven een incrementele, omdat bij een differentiële backup de volgorde van de diskettes makkelijker is bij te houden en het terugplaatsen van gegevens eenvoudiger is. (Persoonlijk ben ik een voorstander van KISS - Keep It Simple, Stupid.)

Waarheid 6: één backup is niet genoeg.

Het kan voorkomen dat u de verkeerde gegevens hebt gewijzigd en dat bij het maken van een backup de goede gegevens door de verkeerde zijn overschreven. Het enige wat u dan nog rest is het werk overdoen. Beter is om bij gevoelige gegevens (zoals financiële) elke week een nieuwe set te vervaardigen. Na bijvoorbeeld vier weken overschrijft u de oudste set door de nieuwste backup. Zo kunt u in geval van nood altijd teruggrijpen naar de oorspronkelijke gegevens.

Waarheid 7: wie de backupdiskettes vlak bij de computer houdt, vraagt om moeilijkheden.

Berg backupdiskettes altijd op een veilige plaats op, in ieder geval niet bij de andere diskettes. Beter is de backupset te bewaren op een andere plaats, bijvoorbeeld thuis. De kans is wel heel erg klein dat uw eigen huis en het kantoor of bedrijf waar u werkt, tegelijkertijd in vlammen opgaan.

Belangrijke gegevens moeten zeer zorgvuldig worden behandeld. Wees net zo voorzichtig met de backupsets als met uw systeem. Het heeft weinig nut als onbevoegden uw gegevens via de backupset kunnen benaderen. Een kluis bij de plaatselijke bank is een zeer veilige plaats voor backupdiskettes.

Waarheid 8: als backups niet eenvoudig zijn te maken, worden ze nooit gemaakt.

Een vaste schijf van 500MB naar diskettes kopiëren is niet bepaald praktisch. Bij grote schijven moet u naar een andere mogelijkheid zoeken, bijvoorbeeld een tape streamer.

Wanneer u op een netwerk werkt, kunt u een backup van uw gegevens op de netwerkcomputer plaatsen. Als het goed is, zal de netwerkbeheerder hiervan weer een backup maken op tape.

Een verwisselbare vaste schijf is een goed alternatief als u niet op een netwerk bent aangesloten.

Steeds meer gebruikers installeren tape streamers. Op een cassette zo groot als een luciferdoosje kunnen 250 tot 500 megabytes worden opgeslagen. Jammer genoeg worden deze gegevensdragers (nog) niet door DOS ondersteund. Werkt u met veel gegevens, dan zou u kunnen overwegen een tape streamer aan te schaffen.

Belangrijke voorzorgsmaatregelen

Er is geen sterveling die om het kwartier een backup maakt. Door het nemen van enkele voorzorgsmaatregelen kunt u voorkomen dat onverwachte systeemcrashes vervelende gevolgen hebben, bestanden ongewild worden verwijderd en dat virussen uw systeem 'verzieken'.

In de volgende paragrafen worden enkele suggesties aan de hand gedaan die de moeite van het overwegen waard zijn. Het maken van backups is tot nu toe de enige mogelijkheid geen gegevens te verliezen.

Wat te doen tegen onbedoeld gegevensverlies

De grootste oorzaak van gegevensverlies is niet een virus of ander kwaad, een technische storing of wat dan ook. De grootste oorzaak is een menselijke fout: wij verwijderen vaak per ongeluk gegevens.

Voor het menselijke falen biedt DOS 6 een oplossing, namelijk UNDELETE. Dit programma beschermt tegen het verlies van gegevens en kan verwijderde gegevens terughalen. U kunt het als een resident programma laden, waarna het ongeveer 14K RAM in beslag neemt. Vervolgens kunt u het configureren zodat er op de achtergrond wordt gewaakt. Hiervoor zijn twee methoden beschikbaar:

- Delete sentry (sentry is schildwacht)
- Delete tracker (tracker is speurhond)

Bij de methode *delete sentry* worden er in een verborgen directory \SENTRY kopieën van verwijderde bestanden bewaard. Het residente gedeelte van UNDELETE controleert alle activiteiten die te maken hebben met het verwijderen van gegevens, en vervangt het verwijderen door verplaatsen. Deze methode biedt de grootste zekerheid. Een verwijderd bestand kunt u terughalen door het weer naar de oorspronkelijke directory te verplaatsen. Het enige nadeel is dat het enorm veel schijfruimte kost; bestanden worden niet verwijderd maar verplaatst.

De tweede methode *delete tracker* slaat belangrijke informatie voor het terughalen van gegevens op in een verborgen bestand PCTRACKR.DEL in de hoofddirectory van de gecontroleerde schijf. In dit bestand staan de naam van het verwijderde bestand

en een lijst met alle clusters waarin de gegevens van dit bestand waren opgeslagen. Deze methode biedt minder zekerheid dan de eerste, maar heeft het voordeel dat er minder schijfruimte wordt gebruikt. Het nadeel is echter dat de clusters door andere bestanden kunnen worden overschreven. De kans dat een verwijderd bestand kan worden teruggehaald, is groot mits er niet al te veel handelingen zijn verricht sinds de verwijdering van het bestand in kwestie.

Gebruik ASSIGN, JOIN en SUBST niet gelijk met delete tracker.

Maatregelen tegen verwijderen installeren

Wanneer u voldoende schijfruimte over hebt, is delete sentry de beste methode. Met UNDELETE /S wordt deze optie geladen. Om delete sentry bijvoorbeeld voor station C te installeren moet u de volgende regel aan het bestand AUTOEXEC.BAT toevoegen:

```
undelete /sc
```

Kies voor delete tracker als uw vaste schijf bijna vol is. Om delete tracker bijvoorbeeld voor station D te installeren moet u de volgende regel aan het bestand AUTOEXEC.BAT toevoegen:

```
undelete /td
```

Delete tracker houdt de bijzonderheden van slechts een beperkt aantal verwijderde bestanden bij. Het standaardaantal bestanden hangt af van de grootte van de vaste schijf en loopt van 100 op een schijf van 20MB tot 300 op een schijf van 30MB en groter. Een bestand met 300 items neemt minder dan 60K in beslag. Dit aantal items kunt u vaststellen (van 1 tot 999) wanneer u UNDELETE installeert met de itemsyntax. Om het maximum aantal bestanden op station D bij te kunnen houden moet de bovenstaande regel in AUTOEXEC.BAT als volgt worden aangepast:

```
undelete /td-999
```

Wat is UNDELETE.INI?

Bij het installeren van UNDELETE worden de instellingen in het bestand UNDELETE.INI opgeslagen. Het is niet nodig dat u alle schakelopties onthoudt; de instellingen kunt u ook

in dit bestand wijzigen en daarna UNDELETE met de volgende opdracht laden:

```
undelete /load
```

Het volgende bestand is een voorbeeld van een UNDELETE.INI:

```
[configuration]
archive=FALSE
days=7
percentage=20
[sentry.drives]
C=
[mirror.drives]
[sentry.files]
sentry.files=*.* -*.TMP -*.VM?
-*.WOA -*.SWP -*.SPL -*.RMG -*.IMG
-*.THM -*.DOV
[defaults]
d.sentry=TRUE
d.tracker=FALSE
```

In het bestand UNDELETE.INI staan de volgende vijf secties:

```
[configuration]
[sentry.drives]
[sentry.files]
[mirror.drives]
[defaults]
```

In de sectie [configuration] staan drie regels waar wordt bepaald of de archiefbit is ingesteld wanneer de geheime kopie wordt gemaakt, het aantal dagen dat de verwijderde bestanden in de SENTRY-directory worden bewaard en de maximale ruimte in procenten die door de bestanden in deze directory in beslag kan worden genomen.

In de sectie [sentry.drives] wordt bepaald welk station wordt beveiligd door de geïnstalleerde delete sentry. Bij een geïnstalleerde delete tracker wordt deze sectie overgeslagen. Elke stationsletter wordt op een aparte regel aangegeven en wordt gevolgd door een is-gelijk-teken (=). Door de volgende drie regels worden de stations C, D en F beschermd:

```
C=
D=
F=
```

In de sectie [sentry.files] wordt bepaald welke bestanden door delete sentry worden gecontroleerd en beschermd. Normaal gesproken staat er in deze sectie een lijst met bestandsmaskers. Door een

minteken voor een bestandsmasker te plaatsten wordt dit bestandsmasker niet meer beschermd. De volgende specificatie beschermt alle bestanden behalve de bestanden met de extensie BAK of een extensie die begint met TP:

```
*.* -*.BAK -*.TP?
```

In de sectie [mirror.drives] staan de stations die worden beschermd bij een geïnstalleerde delete tracker. De syntax is gelijk aan die van [sentry.drives].

In de sectie [defaults] staat op welke wijze de bescherming is geïmplementeerd wanneer u de opdracht UNDELETE/LOAD invoert. Het ene item moet FALSE zijn, terwijl het andere TRUE is.

```
d.sentry=TRUE
d.tracker=FALSE
```

UNDELETE beschermt altijd de stations die in het bestand UNDELETE.INI zijn opgegeven, zelfs als er bij het laden van UNDELETE minder stations worden gespecificeerd met de schakeloptie /S op /T.

Wanneer u het bestand UNDELETE.INI wilt bewerken, moet UNDELETE eerst worden gesloten met behulp van de schakeloptie /U om daarna opnieuw te worden geladen met de schakeloptie /LOAD. Wanneer er een ander resident programma na UNDELETE is geladen, moet het systeem worden herstart om de nieuwe configuratie door te voeren.

DEFRAG

Zonder UNDELETE als resident programma neemt de kans op het terughalen van verwijderde gegevens toe als de schijf niet is gefragmenteerd. Een bestand dat verspreid op de vaste schijf ligt opgeslagen, is veel moeilijker terug te halen.

Houd bestanden ongefragmenteerd met DEFRAG. Maak er een gewoonte van dit eens per week te doen, bijvoorbeeld aan het einde van de vrijdagmiddag. Niet alleen verwijderde gegevens worden beter teruggehaald, ook de prestaties van het systeem nemen toe. Zie hoofdstuk 4 voor een volledige overzicht van fragmentatie.

Schijven controleren

Laat minstens eens per week CHKDSK los op de vaste schijf, maar liever dagelijks om ervoor te zorgen dat de file allocation table intact is. Hoe eerder een fout in de bestandsstructuur aan het licht komt, des te beter is het.

Jammer genoeg voorziet DOS niet in een echt programma voor het analyseren van schijven. Als aanvulling zou u kunnen overwegen een utility van een andere producent te nemen, bijvoorbeeld de Norton Disk Doctor van Symantec, zowel onder DOS als onder Windows (Norton Desktop for Windows) verkrijgbaar.

De zaak van de vermiste MIRROR

Tot ieders verrassing heeft Microsoft de utility MIRROR weggelaten uit DOS 6. Hiervoor in de plaats zijn andere opdrachten gekomen, maar twee belangrijke functies van MIRROR zijn verdwenen, namelijk de mogelijkheid om een kopie te maken van de partitietabel van de vaste schijf, en om informatie bij te houden waarmee het formatteren van een station ongedaan kan worden gemaakt.

MIRROR staat op de supplementendiskette van DOS 6. Gebruik MIRROR alleen voor een kopie van de partitietabel en voor het ongedaan maken van een formattering.

Eén van de grootste rampen die een systeem kan treffen, is een onbruikbare partitietabel. De oorzaak kan een bug in een programma zijn waardoor naar het verkeerde geheugengebied wordt geschreven, of een ondeskundige gebruiker die met DEBUG schijfsectoren gaat veranderen.

U kunt met het anti-virusprogramma VSAFE uw partitietabel beveiligen tegen onopzettelijke en opzettelijke vernietiging. Dit komt verderop in dit hoofdstuk aan de orde.

Met de volgende MIRROR-opdracht slaat u de partitietabel op:

```
mirror /partn
```

Een kopie van de partitietabel van de vaste schijf wordt zo op een diskette opgeslagen in het bestand PARTNSAV.FIL.

Iedere gebruiker van DOS zou met MIRROR kopieën moeten maken van de FAT en hoofddirectory van iedere vaste schijf. Deze gegevens zijn van vitaal belang voor het terugdraaien van een ongewenste formattering en staat in enkele verborgen bestanden op de vaste schijf.

Met de volgende MIRROR-opdracht in AUTOEXEC.BAT worden de gegevens van de FAT en de hoofddirectory voor station C en D opgeslagen

```
mirror c: d:
```

Verloren bestanden en gegevens terughalen

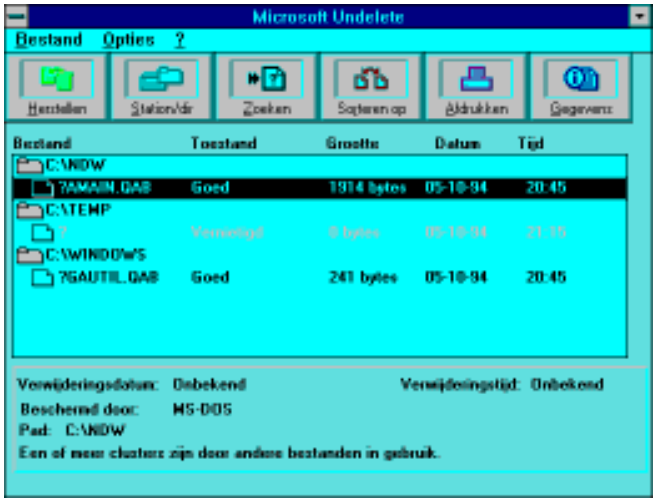
Een ongeluk zit in een klein hoekje. Zelfs als u per ongeluk een bestand verwijdert of een vaste schijf formatteert, of de partitietabel wordt vernietigd, dan nog kunt u met de utility's van DOS de gegevens terughalen.

Verwijderde bestanden terughalen

Het is dan toch gebeurd: u hebt per ongeluk een bestand verwijderd. Zelfs al zou de backup van het bestand een dag oud zijn, dan nog is het de moeite waarde het verwijderde bestand terug te halen. Het bestand betekent misschien wel een dag werk.

De techniek voor het terughalen van een verwijderd bestand is afhankelijk van de beveiligingsmethode die u hebt geïmplementeerd en/of in Windows is geïnstalleerd. In DOS zitten twee programma's waarmee verwijderde bestanden kunnen worden teruggehaald: UNDELETE, een DOS-programma waarmee vanaf de opdrachtregel wordt gewerkt, en MWUNDEL voor gebruikers van Windows. De Windows-versie is veel gebruiksvriendelijker dan de DOS-versie. Verwijderde bestanden kunnen er mee worden opgezocht en er kunnen zowel directory's als bestanden mee worden teruggehaald. Zie deel 4 *Alle DOS-opdrachten* voor een volledige beschrijving van elke opdracht.

Afbeelding 3-8 is het hoofdvenster van MWUNDEL met een opsomming van alle verwijderde bestanden. Met de knop Info kunt u



Figuur 3-8: Een lijst met verwijderde bestanden in MWUNDEL

extra informatie over het geselecteerde bestand oproepen.

Voor elk bestand wordt in het veld Condition aangegeven wat het resultaat is:

Perfect U kunt het verwijderde bestand automatisch terughalen. Deze categorie is gereserveerd voor bestanden die door delete sentry worden beveiligd.

Excellent Omdat alle clusters van het bestand achter elkaar liggen en geen enkele cluster is gebruikt, zal het bestand naar alle waarschijnlijkheid zonder problemen kunnen worden teruggehaald.

Good Het lijkt erop dat alle clusters beschikbaar zijn, hoewel zij niet naast elkaar liggen. U zou het bestand moeten kunnen terughalen.

Poor De eerste cluster van het bestand wordt door een ander bestand gebruikt. De kansen op succes zijn zeer gering.

Destroyed Alle clusters van het bestand zijn weer in gebruik. Het bestand kan niet meer worden teruggehaald.

Recovered Het bestand is teruggehaald.

Geen enkele utility voor het terughalen van verwijderde bestanden kan bestanden uit de categorie poor en destroyed terughalen.

De bestanden waarvan het eerste teken een vraagteken is, werden niet beschermd door delete sentry of delete tracker toen zij werden verwijderd.

Deze bestanden kunnen alleen met de DOS-methode worden teruggehaald en worden nooit beter dan *good* geclassificeerd.

UNDELETE, de DOS-versie waarmee vanaf de opdrachtregel wordt gewerkt, is niet echt scheutig met het verstrekken van informatie over verwijderde bestanden. Door twee schakelopties te combineren kunt u echter een lijst laten genereren met verwijderde bestanden per categorie. Met de volgende opdracht krijgt u een lijst te zien met alle verwijderde bestanden die alleen met de DOS-methode kunnen worden teruggehaald:

```
undelete /list /dos
```

Bestandsnamen waarvoor twee asterisken staan, kunnen niet worden teruggehaald. Vervang de schakeloptie /DOS door /DS of /DT voor een lijst met bestanden die worden beveiligd door respectievelijk delete sentry en delete tracker.

Een formattering ongedaan maken

Wanneer u per ongeluk een schijf formatteert, kunt u dit proberen ongedaan te maken met UNFORMAT. U hoeft alleen deze opdracht in te geven met de letter van het station:

```
unformat a:
```

Er bestaat een mogelijkheid dat u het formatteren van een schijf ongedaan kunt maken als er geen verborgen, niet-formatterende bestanden op staan. Door UNFORMAT wordt geprobeerd de verloren gegane gegevens terug te halen. Verwacht geen wonderen, want het programma is verre van goed. De DOS-opdracht UNFORMAT is minder betrouwbaar dan menige tegenhanger, zoals PC Tools en The Norton Utilities. Al deze programma's maken gebruik van dezelfde techniek, maar de een is wat slimmer dan de ander. Wanneer de gegevens belangrijk zijn en u weet dat er geen spiegelbestand bestaat, moet u zeker overwegen in plaats van UNFORMAT één van deze andere programma's te gebruiken.

Met de schakeloptie /J kunt u heel makkelijk bepalen of er spiegelbestanden op de schijf staan. De volgende opdracht controleert of er op de diskette in station A de benodigde informatie staat:

```
unformat a: /j
```

UNFORMAT moet trachten de FAT opnieuw te construeren. Eerst wordt de schijf cluster voor cluster afgezocht naar gegevens die op een directorybestand lijken. Voor een diskette kan dit wel 30 minuten duren. Vervolgens worden de directorybestanden teruggehaald. Jammer genoeg worden alle directorynamen op hoofdniveau door UNFORMAT vernietigd. Deze namen worden vervangen door SUBDIR1, SUBDIR2, enzovoorts. Alle namen van subdirectory's op lager niveau kunnen worden teruggehaald.

Nadat de directory's zijn teruggehaald, worden door UNFORMAT met dezelfde technieken als bij UNDELETE de bestanden in elke directory teruggehaald. UNFORMAT kan geen bestanden in de hoofddirectory of gefragmenteerde bestanden terughalen. Waarmee nogmaals wordt gezegd dat u uw schijven ongefragmenteerd moet houden.

Wanneer u met UNFORMAT een schijf behandelt waarop geen spiegelbestanden staan, zou u de schakeloptie /TEST kunnen toepassen. Deze schakeloptie zorgt ervoor dat FORMAT een proefpoging doet en geen wijzigingen aanbrengt. Zo kunt u bepalen of de bewerking enig succes zal hebben.

Enkele beperkingen van UNFORMAT staan in het volgende overzicht:

- U kunt de formattering van een schijf niet ongedaan maken als deze met de schakeloptie /U is geformatteerd.
- U kunt alleen de formattering ongedaan maken van stations met 512, 1024 of 2046 bytes per sector. De sectorgrootte van een station kan met MSD worden bepaald.
- U kunt de formattering van netwerkstations niet ongedaan maken.

Partitiegegevens van de vaste schijf terughalen

Wanneer u met MIRROR een kopie maakt van de partitietabel van de vaste schijf (eerder in dit hoofdstuk besproken), kunt u deze kopie terughalen met UNFORMAT en de schakeloptie /PARTN. In de meeste gevallen zal een systeem met een beschadigde partitietabel niet opstarten. Bewaar het partitiebestand PARTNSAV.FIL en UNFORMAT.COM dus op een opstartdiskette.

Met de volgende opdracht wordt de partitietabel teruggehaald:

```
unformat /partn
```

Vervolgens moet u het systeem herstarten en werkt als het goed is, alles weer als vanouds.

Opzettelijke gegevensvernietiging

Om bestanden met vertrouwelijke of persoonlijke gegevens te vernietigen is er meer nodig dan deze te verwijderen of de diskette te formatteren. Zoals u in het voorafgaande hebt kunnen lezen, zijn er altijd manieren om verwijderde gegevens terug te halen.

Een afdoende manier om gegevens te vernietigen is bijvoorbeeld Shredder in Norton Desktop for Windows. Wat een papiervernietiger doet met papier, doet Shredder met gegevens. Bestanden die u door Shredder laat verwijderen, zijn op geen enkele manier meer terug te halen. Zoals Norton zelf zegt, is alles wat door Shredder wordt aangeraakt, binaire spaghetti.

Maatregelen tegen virussen

Net zoals bij een dieet wordt er over virussen meer gesproken dan er daadwerkelijk aan wordt gedaan. Eenieder zal wel eens verhalen over dodelijke virussen hebben horen vertellen. Virussen zijn een reëel gevaar en vernietigen gegevens, maar er gaan meer gegevens verloren door menselijke fouten dan door virussen. Ondanks dat zou iedereen die met computers werkt, voorzorgsmaatregelen moeten nemen. DOS 6 maakt het ons makkelijk met de volgende programma's:

MSAV Het anti-virusprogramma van Microsoft waarmee virussen worden opgespoord en vernietigd. U kunt de DOS-versie als een normaal programma starten of vanuit de opdrachtregel met schakelopties werken.

MWAV De Windows-versie is qua functionaliteit gelijk aan het DOS-broertje, maar is gebruiksvriendelijker en biedt enkele mogelijkheden meer.

VSAFE Dit residente anti-virusprogramma controleert de schijfactiviteit op virussen. Wijzigingen aan zeer belangrijke gegevensgebieden, zoals de bootsector en de FAT van een schijf, worden verhinderd.

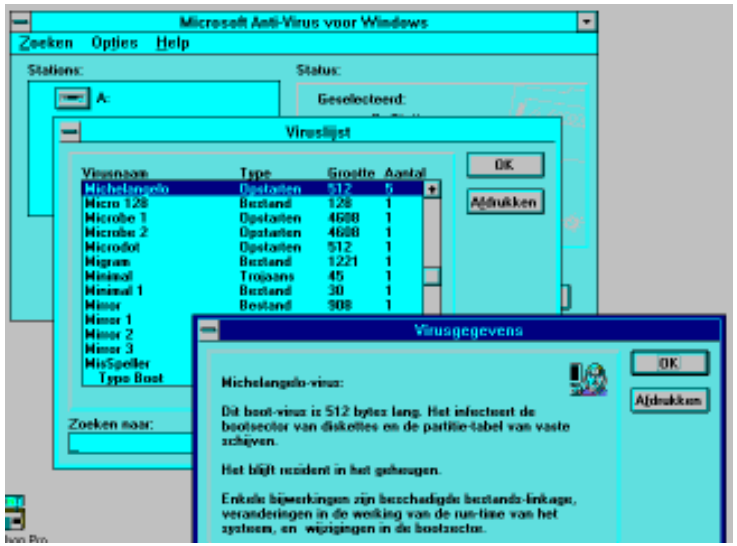
Het fenomeen virus

Eenvoudig gesteld is een *computervirus* een programma dat zich op slinkse wijze voortplant van systeem naar systeem. Aan het vermogen zich voort te planten dankt het virusprogramma zijn naam. Bepaalde gebeurtenissen, bijvoorbeeld een datum of het aantal keren dat een programma wordt gestart, activeren een virus. Dit kan variëren van een eenvoudig bericht tot een complete formattering van de vaste schijf.

Goedaardige of onschuldige virussen bestaan niet. Virussen doen iets waar u en ik niet op zitten te wachten. De makers van virussen zouden vervolgd en bestraft moeten worden. Een sprekend voorbeeld is de besmette computer van een apotheker die een tien maal grotere dosering van een gevaarlijk medicijn voorschreef.

Op dit moment zijn er ongeveer 1200 virussen bekend. De bestrijdingsprogramma's worden beter; daarentegen worden de virussen ook gemener.

Voor een overzicht van de verschillende virussporen start u MWAV in Windows en selecteert u Scan/Virus List in het menu. Er wordt een lijst afgebeeld met alle virussen die door het programma kunnen worden opgespoord. Met de knop Info vraagt u een volledige beschrijving op van het gemarkeerde item (zie afbeelding 3-9).



Figuur 3-9: De lijst met informatie over virussen in MWAV

Hoe virussen zich verspreiden

Wanneer een besmet programma wordt gestart, wordt het virus te zamen met het programma in het geheugen geladen. Nadat het virus in het geheugen is geïnstalleerd, kan het net zoals elk ander programma stations, bestanden en printers benaderen. Het virus probeert zich gewoonlijk te hechten aan andere programmabestanden, waarna deze bestanden besmet raken. Als deze besmette programma's worden gestart, kunnen ze op hun beurt weer andere programma's besmet raken. Op deze manier wordt het virus verspreid.

Een algemeen verbreide misvatting is dat virussen alleen EXE- en COM-bestanden kunnen infecteren. Virussen worden in alle soorten uitvoerbare codes gevonden, waaronder de EXE- en COM-bestanden, SYS-stuurprogramma's, DLL-bestanden van Windows en overlay-bestanden (vaak met de letter *O* of *V* in de extensie). Virussen kunnen zich niet in niet-uitvoerbare bestanden verspreiden, zoals ASCII-bestanden.

Een virus verspreidt zich alleen als de besmette code wordt gestart. In feite kan uw systeem alleen worden besmet als u programma's uit andere bronnen start. Wanneer u nooit nieuwe software installeert of programma's start vanaf diskettes, netwerken of via een modem, kan uw systeem eenvoudigweg niet besmet raken. De realiteit is echter anders. Bijna iedereen installeert nieuwe software, werkt met diskettes, laadt software via een modem of werkt op een netwerk, hetgeen een bron van infectie kan zijn.

MWAV identificeert de verschillende verspreidingsmethoden in de kolom Type (zie afbeelding 3-9). Elk virus wordt onderverdeeld in één van de volgende categorieën:

File Dit type virus hecht zich aan uitvoerbare programma's, zoals COM-, EXE- en DLL-bestanden. Sommige virussen overschrijven de bestaande programmacode in plaats van dat zij aan het einde van het programma worden toegevoegd.

Boot Een bootvirus hecht zichzelf aan de bootsector van een vaste schijf of opstartdiskette. Als het systeem wordt gestart, wordt het virus in het geheugen geladen, waar het zich kan verspreiden naar andere schijven of diskettes.

Wanneer u van iemand een opstartdiskette krijgt, controleer deze diskette dan eerst op eventuele virussen voordat u uw systeem met deze diskette start. Wanneer er een diskette in het station zit waarmee het systeem niet kan worden gestart, en u zet het systeem aan, moet u het volgende doen. Druk geen toets in en probeer het systeem weer te starten als u de foutmelding "non-system disk" ziet. Verwijder onmiddellijk de diskette, zet het systeem uit en probeer het opnieuw. Zelfs een afgebroken startprocedure kan een systeem besmetten.

Trojan Een Trojaans paard is technisch gesproken geen virus. Het is een programma dat zijn ware (vernietigende) aard verbergt achter andere functies. Een onschuldig programma kan bijvoorbeeld een code zijn om de vaste schijf te wissen.

Mogelijke schade door een virus

Een virus kan een systeem op twee manieren beschadigen. Ten eerste kan de code waarmee het virus wordt verspreid, een bootsector of een programma wijzigen en de functionaliteit en prestatie nadelig beïnvloeden. Zelfs als het virus is verwijderd, kan het programma slecht werken. Deze vorm van beschadiging is een bijprodukt van de verspreiding.

Ten tweede kan een virus een systeem beschadigen wanneer het door een andere handeling wordt geactiveerd. De meeste kwaadaardige virussen proberen op één van de volgende manieren een systeem te beschadigen: vernietiging van de partitietabel van de vaste schijf, vernietiging of beschadiging van de FAT of het overschrijven van bestanden met onzin. Onnodig te zeggen dat dit alles een vernietigende werking heeft op gegevens.

Virussen opsporen en bestrijden

Omdat een virus zich onopgemerkt moet verspreiden voordat er wordt geprobeerd een systeem te beschadigen, bestaat er een goede kans dat u de besmetting kunt identificeren voordat er schade is toegebracht.

De volgende symptomen zijn een indicatie van een virusbesmetting:

- Het beschikbare geheugen wordt minder.
- Bestaande programma's worden groter en nemen kostbare schijfruimte in beslag.
- Uw systeem wordt trager, minder stabiel en crasht steeds vaker.

Het regelmatig scannen van uw systeem op virussen is zeker geen overbodige luxe. Het kan u veel narigheid besparen.

Virusinfecties opsporen

Zowel MSAV als MWAV controleren systemen op virussen. Selecteer de knop Detect om het geselecteerde station op virussen te controleren.

De meeste bekende virussen laten een bepaald patroon van bytes na in een besmet bestand, dat wel eens wordt betiteld als de *virus signatures*. Tijdens het scannen zoekt het programma in alle bestanden op het geselecteerde station of stations naar deze signatures.

U dient minstens één keer per week te scannen op virussen. Voer de controle zeker uit voordat er een volledige backup wordt gemaakt.

Wanneer virussporen wordt geanalyseerd, worden nieuwe signatures geïdentificeerd en aan de lijst toegevoegd. U kunt deze lijst via een modem bijwerken. De benodigde gegevens hiervoor zijn op te vragen bij een bulletin board van Microsoft. Zie appendix D van de gebruikershandleiding van MS-DOS voor verdere bijzonderheden.

Met de anti-virusprogramma's van DOS kan niet, zoals bij Norton Anti Virus het geval is, een aparte directory worden gescand. De Windows-versie MWAV ondersteund echter een beperkte selectie van bestanden. Om één of meerdere bestanden op virussen te controleren moeten in Bestandsbeheer de bestanden worden geselecteerd. Vervolgens kunt u de geselecteerde bestanden naar het Anti-Virus pictogram in de groep Microsoft Tools slepen en daar laten 'vallen'. MWAV wordt gestart, controleert eerst het geheugen op virussen en daarna de bestanden die u naar het pictogram hebt gesleept.

Waar komen de bestanden CHKLIST.MS vandaan

Door het scannen van signatures worden alleen bekende virussen opgespoord. Het anti-virusprogramma maakt gebruik van een zeer slimme methode, checksums, waarmee verdachte activiteiten worden gecontroleerd. Een checksum is een getal dat wordt afgeleid door een speciale algoritme toe te passen op de afzonderlijke waarden in een bestand. Wanneer een bestand wordt veranderd, verandert ook de checksum. Door de huidige berekende checksum van een bestand te vergelijken met een eerder gemaakte checksum, wordt vastgesteld of het bestand is veranderd.

Selecteer Options om het scannen met een checksum te activeren, en selecteer ook de opties Verify Integrity en Create New Checksums.

De instellingen van de optie worden opgeslagen in een INI-bestand in de DOS-directory. De anti-virus programma's hebben niet dezelfde instellingen. De instellingen van de DOS-versie worden opgeslagen in MSAV.INI en die van de Windows-versie in MWAV.INI.

Wijzig de opties liever vanuit het hoofdprogramma en niet direct in het INI-bestand.

De volgende keer dat u een station scant, wordt er door het anti-virusprogramma in elke directory een bestand gemaakt met de naam CHKLIST.MS. In dit bestand staat een checksumwaarde voor elk bestand waarin een uitvoerbare code staat (bijvoorbeeld EXE-, COM- of DLL-bestanden). Tijdens latere scans wordt de checksum in het bestand CHKLIST.MS vergeleken met de nieuw berekende checksum.

Sommige virussen maken gebruik van een techniek Stealth (stiekem) genaamd, waardoor zij minder snel worden opgespoord. (Stealth heeft niets te maken met QEMM Stealth.) Het anti-virusprogramma kan een zeer grondige scan uitvoeren wanneer Anti-Stealth wordt geselecteerd in het dialoogvenster Options.

Checksumbestanden verwijderen

De bestanden CHKLIST.MS leveren een zeer waardevolle anti-virus functie, die u echter kunt verwijderen. Hiervoor hoeft u niet elke directory en elk bestand af te gaan. Er is een makkelijke manier

om deze bestanden te verwijderen: selecteer de optie Scan/Delete CHKLIST Files wanneer u in Windows werkt.

Bescherming tegen dodelijke virussen

U kunt het programma VSAFE resident in het geheugen laden om zo alle activiteiten te kunnen controleren. VSAFE controleert niet op bepaalde virussen, maar beschermt de gebieden die gewoonlijk door virussen worden besmet en biedt een algemene bescherming tegen alle virussen.

Zie hiervoor ook deel 4 *Alle DOS-opdrachten* voor een compleet overzicht van alle schakelopties.

Wanneer een programma op een verdachte manier probeert een schijf te wijzigen, bijvoorbeeld het veranderen van de bootsector of een EXE-bestand, verschijnt er een dialoogvenster met een waarschuwing en wordt u gevraagd of de verandering mag worden uitgevoerd. Wanneer VSAFE is geïnstalleerd en u werkt met Windows, moet MSAVTSR.EXE van DOS 6 zijn geladen. Dat programma zorgt ervoor dat VSAFE het dialoogvenster in de stijl van Windows laat verschijnen. Het beste zou zijn als u de volgende opdracht aan WIN.INI zou toevoegen, waardoor het programma automatisch wordt geladen als Windows wordt gestart:

```
load=c:\dos\msavtsr.exe
```

Deselecteer altijd optie 3 van VSAFE als u met Windows werkt. Deze optie onderschept alle schrijfactiviteiten naar schijf en vraagt om uw toestemming voordat er verder wordt gegaan. Windows schrijft regelmatig naar de vaste schijf; als deze optie actief is, zult u meer tijd besteden aan het geven van uw toestemming dan aan uw werk.

Virussen uit een besmet systeem verwijderen

Beide programma's kunnen een besmet systeem weer gezond maken. Dit proces wordt *cleaning* (schoonmaken) genoemd. Selecteer de knop Detect and Clean waarna eventuele virussen uit het systeem worden verwijderd.

Wanneer het anti-virusprogramma een virus in het geheugen opmerkt, moet u het volgende doen:

1. Zet de computer uit.

2. Start de computer met een opstartdiskette die gegarandeerd virusvrij moet zijn.

   U moet eigenlijk dus altijd een opstartdiskette bij de hand hebben. Wanneer er op uw vaste schijven stuurprogramma's staan voor DoubleSpace, moeten er op deze diskette ook de juiste stuurprogramma's voor DoubleSpace staan (zie hoofdstuk 4). Kopieer ook de bestanden MSAV.EXE, MSAV.INI en VSAFE.EXE. Controleer de diskette met MSAV om er zeker van te zijn dat deze virusvrij is en maak de diskette schrijfbeveiligd.

3. Start MSAV vanaf de diskette en selecteer de optie Detect and Clean.

4. Herstart de computer vanaf de vaste schijf, plaats de opstartdiskette en installeer vanaf deze diskette VSAFE in het geheugen.

5. Sommige besmette bestanden kunnen beschadigd en onbruikbaar zijn. Vervang de bestanden door de backups die op een backupdiskette staan. Deze backups kunnen ook besmet raken. Zodra deze reservebestanden zijn teruggeplaatst, moet u ze aan een grondige scan onderwerpen.

6. Controleer al uw diskettes op virussen.

7. Waarschuw andere gebruikers met wie u in contact bent geweest, vooral die gebruikers waarmee u bestanden hebt uitgewisseld. Waarschuw bij een netwerk de netwerkbeheerder.

Controleer zeker enkele weken lang met VSAFE op besmetting vanuit dezelfde bron en kies de grondigste controle. Controleer ook dagelijks uw vaste schijf/schijven. Dit lijkt misschien wat overtrokken, maar is het zeker niet. Een besmet systeem kan u heel wat hoofdbrekens bezorgen.

Een vergelijking tussen MSAV en MWAV

De twee anti-virusprogramma's zijn vrijwel gelijk aan elkaar. De verschillen tussen beide zijn de volgende:

- Vanaf de opdrachtregel kan er met MSAV worden gewerkt. Een groot aantal schakelopties

wordt ondersteund voor een automatische uitvoering. Deze mogelijkheid maakt MSAV uitermate geschikt om op te nemen in AUTOEXEC.BAT.

- MSAV kan met de schakeloptie /R informatie in een rapport opnemen.

- In MWAV kunnen met een enkele optie alle checksumbestanden van een station worden verwijderd.

On-line informatie over virussen

Wanneer u meer wilt weten over virussen en u bent lid van CompuServe Information Service, krijgt u met de opdracht GO VIRUSFORUM toegang tot allerlei interessante wetenswaardigheden. De nieuwste updates van MSAV en MWAV komen van Central Point Software en kunnen worden opgevraagd met GO CENTRAL.

Een knipoog naar de amusementswereld

Het kwijtraken van gegevens is iets waar we veel te licht over denken. Mocht u echter eens een belangrijk bestand verliezen, dan zijn er zelfs films of titels van CD's die u daaraan helpen herinneren:

Indiana Jones and the PC of Doom
Discablanca
Star Wars: The Virus Strikes Back
Crashanova

Natuurlijk zijn er ook muziekstukken die u het verlies onder de neus kunnen wrijven:

Fifty Ways to Lose Your Data van Paul Simon
Bit out of Hell van Meat Loaf
Pray van Hammer
Get Back(up) van The Beatles
Backing Up is Hard to Do van Neil Sedaka

Tenslotte blijken ook Nederlandse artiesten hier weg mee te weten:

Waarheen, Waarvoor van Mieke Telkamp

Kom van die disk af van Peter en z'n Rockets

Samenvatting

In dit hoofdstuk worden voorzorgsmaatregelen aan de hand gedaan waarmee u het verlies van gegevens kunt voorkomen, en verloren gegevens kunt terughalen. De volgende onderwerpen zijn aan bod geweest:

- Het selecteren van bestanden voor de backup.
- Het belang van de optie Compare voor het controleren van de integriteit van een backup.
- Het terughalen van bestanden met de backupcatalogus en het opnieuw laden en samenstellen van een catalogus die van de vaste schijf is verwijderd.
- Belangrijke maatregelen tegen het verlies van gegevens, zoals UNDELETE, en het bewaren van de partities van de vaste schijf met MIRROR.
- Het terughalen van gegevens met UNDELETE, UNFORMAT en MIRROR.
- Een uitleg over de verspreiding van virussen en hoe met MSAV en MWAV virussen kunnen worden opgespoord en vernietigd.

Hoofdstuk 4 *Geheime wapens voor uw hardware* is het eerste hoofdstuk van deel 2. In dit hoofdstuk wordt de vaste schijf onder de loep genomen en worden alle nieuwe compressiemogelijkheden van DoubleSpace behandeld.