Registry reasoning

Andrew Ward sorts out problems with hives, common-sense printing and ghostly desktops.

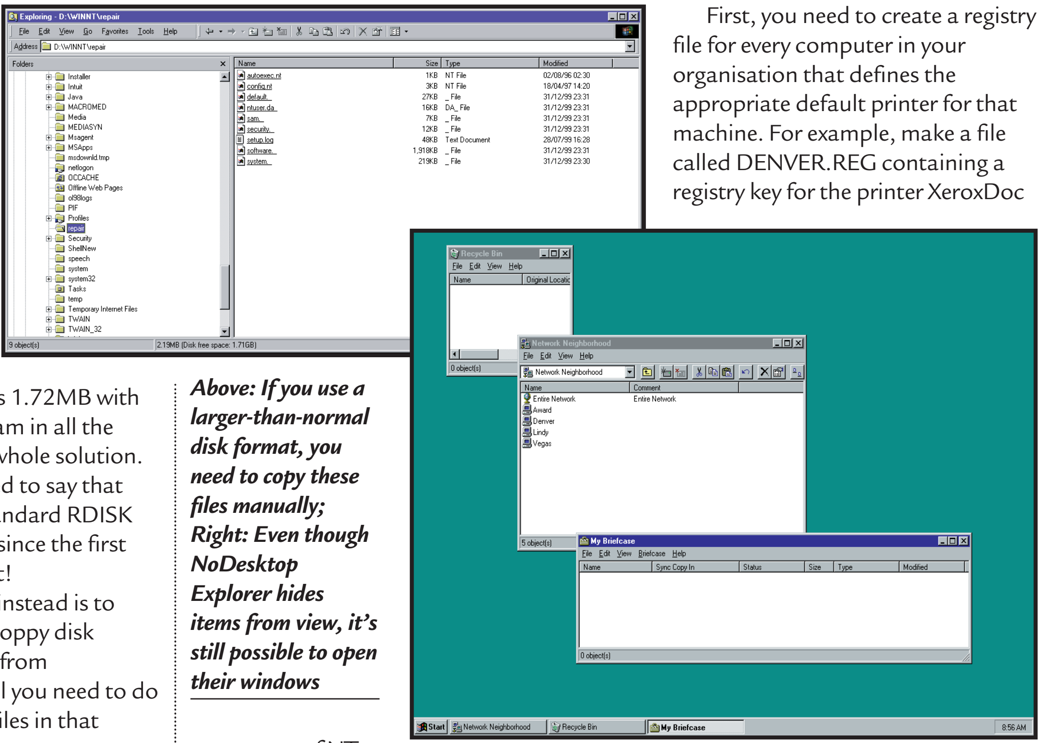
Last month I discussed ways of cramming all the files of an emergency repair disk (ERD) – whose contents are bigger than 1.44MB – onto a standard floppy. But Alan Bailey has written in to point out that reformatting a floppy disk to larger sizes such as 1.72MB with WinImage, in order to cram in all the necessary files is not the whole solution. He's quite right – I omitted to say that you can't then use the standard RDISK utility to create this disk, since the first thing it does is reformat it!

What you have to do instead is to copy the files onto your floppy disk manually. The files come from %systemroot%\repair – all you need to do is make a copy of all the files in that directory. If you still have a space problem, you can delete some of the entries in the setup.log file. Locate the [Files.WinNt] section, and delete any of the lines within it that don't belong with %systemroot%\SYSTEM32\.

If the files still won't fit on a single disk, no matter how large it is, just copy them onto more than one disk. However, you will also need to copy setup.log onto each disk. Without the presence of setup.log, the startup disks won't recognise the floppy as an ERD.

When you come to effect an emergency recovery of the registry, you recover from each disk in turn, and for each disk only check the hives that are present on that disk.

From a personal point of view, however, I've never found the ERD recovery procedure for restoring registry hives to be satisfactory. Recovery attempts have always resulted in the error message saying that the registry couldn't be repaired. The other recovery methods I've described in this column in the past are usually much more reliable, such as backing these files up onto another medium, and then either booting with a spare copy of NT, or carrying out a fresh install, and then recovering the files.



Exploring - D:\WINNT\repair

Address: D:\WINNT\repair

Name	Size	Type	Modified
autoexec.nt	1KB	NT File	02/08/96 02:30
config.nt	3KB	NT File	18/04/97 14:20
default._	27KB	_ File	31/12/99 23:31
ntuser.da_	16KB	DA_ File	31/12/99 23:31
sam._	7KB	_ File	31/12/99 23:31
security._	12KB	_ File	31/12/99 23:31
setup.log	48KB	Text Document	28/07/99 16:28
software._	1,918KB	_ File	31/12/99 23:31
system._	219KB	_ File	31/12/99 23:30

9 object(s) 2.19MB (Disk free space: 1.71GB)

***Above:** If you use a larger-than-normal disk format, you need to copy these files manually; **Right:** Even though NoDesktop Explorer hides items from view, it's still possible to open their windows*

Printing locally

Stephen O'Connell returns us to the problem that the default printer is based on the user who logs into a PC and not the PC itself. This results in printing taking place on a device that could be in a completely different building, unless the printer is changed every single time a user logs on. The solution he's opted for is based on using regedit to import the new printer setting from a .REG file. This is carried out automatically at each logon, so users always print to the most convenient physical printer.

FIG 1

Specify a printer

```
    REGEDIT4
    [HKEY_CURRENT_USER\✓
Software\Microsoft\Windows ✓
NT\CurrentVersion\Windows]
    "Device"="\\\\VEGAS\\✓
XeroxDoc,,LPT1:"
```

(*Key:* ✓ *code string continues*)

First, you need to create a registry file for every computer in your organisation that defines the appropriate default printer for that machine. For example, make a file called DENVER.REG containing a registry key for the printer XeroxDoc on computer VEGAS, as outlined in Fig 1.

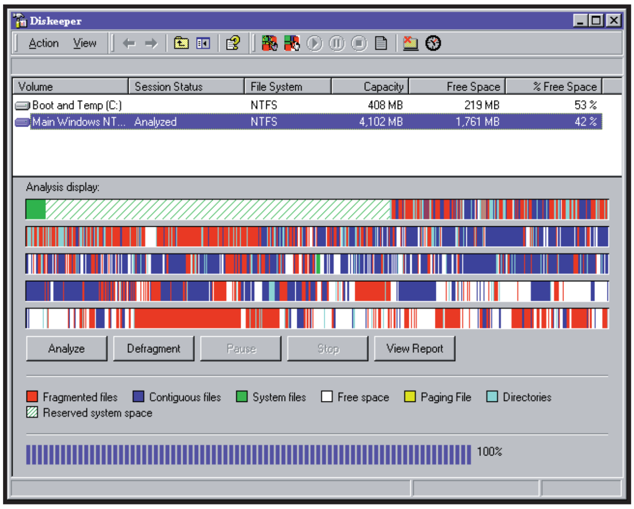
You'll also need to set up a logon script for every user, to cause this file to be imported into the registry. The following command will accomplish what you need:

```
If exist "%LogonServer%✓
\Netlogon\%ComputerName%.✓
REG" regedit /S "%Logon✓
Server%\Netlogon\%Computer✓
Name%.REG"
```

Phantom desktop

Nick Lee points out that the NoDesktop Explorer policy doesn't really provide that much security after all. At his school, this technique is used to hide desktop items such as the Network Neighborhood, and it certainly works – the icons aren't visible on the desktop. However, they are still there and – more worryingly – they are still active.

If you press Ctrl & Esc to bring up the Start menu and then press Esc again, the Start button stays selected. Pressing the Tab key twice (or three times, if you have IE4 with the Quicklaunch pad activated)



Volume	Session Status	File System	Capacity	Free Space	% Free Space
Boot and Temp (C:)		NTFS	408 MB	219 MB	53 %
Main Windows NT...	Analyzed	NTFS	4,102 MB	1,761 MB	42 %

Diskeeper can help prevent disk fragmentation, which still occurs in Windows NT

will bring the focus to the desktop. By using the cursor keys, you can then move around the desktop items – pressing Enter will open whichever one is currently selected. Of course, you can't see which one is selected since they are invisible, but you can get to the Network Neighborhood and so on by trial and error.

Unfortunately, one or two of Nick's users are aware of this, and have used this back door to install Quake on various systems, and to make changes to Windows and Microsoft Office configuration settings.

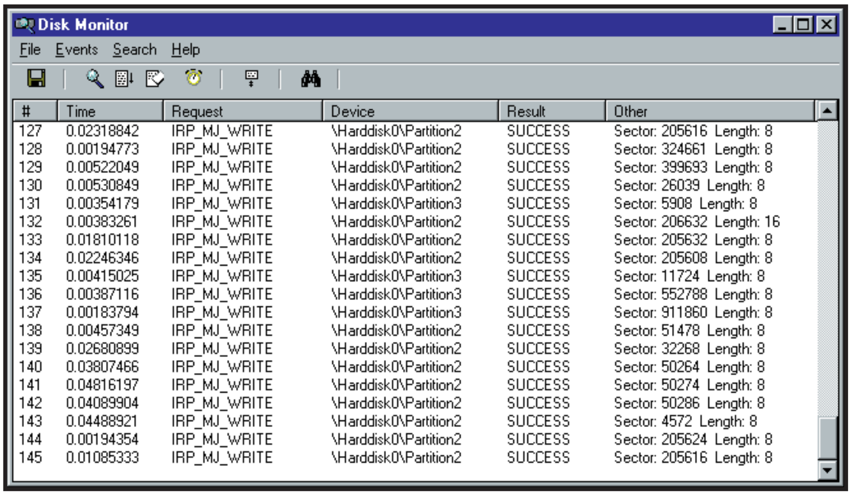
Adding RestrictRun to the list of policies in force may help a bit, but as I've said before, that isn't watertight either. Neither is NoDrives. So while using all these policies do result in a system that is a fiddle to crack, it's still by no means fully secure.

To be fair to Microsoft, the official explanation of the registry key doesn't include anything about disabling the desktop items – only that they are hidden: 'Hides all desktop items regardless of menus, folders, and shortcuts defined either by profiles or by other pointers in the policy file for custom program folders, custom desktop icons, and so on.'

Disk defragmentation

Alex Taperek is concerned about his disks becoming fragmented, and he's every right to be worried. In theory, NTFS is self-healing, and shouldn't need defragmentation. In practice, this isn't so, and a badly fragmented disk will not only slow things down considerably but could cause a system to fail altogether in extreme circumstances. Even Microsoft concedes that defragmentation is necessary, and ships Diskeeper Lite with Windows 2000.

There are several disk defragmenters available for Windows NT4, and I've covered them all before in this column at some point in the dim and distant past. They all have their pros and cons, and they all have their ardent supporters. Diskeeper, from Executive Software, does have the prestige of being the first-ever utility (and only about the third piece of software altogether) to have achieved Windows 2000 logo certification. This is the product I use at the moment.



#	Time	Request	Device	Result	Other
127	0.02318842	IRP_MJ_WRITE	\Harddisk0\Partition2	SUCCESS	Sector: 205616 Length: 8
128	0.00194773	IRP_MJ_WRITE	\Harddisk0\Partition2	SUCCESS	Sector: 324661 Length: 8
129	0.00522049	IRP_MJ_WRITE	\Harddisk0\Partition2	SUCCESS	Sector: 399693 Length: 8
130	0.00530849	IRP_MJ_WRITE	\Harddisk0\Partition2	SUCCESS	Sector: 26039 Length: 8
131	0.00354179	IRP_MJ_WRITE	\Harddisk0\Partition3	SUCCESS	Sector: 5908 Length: 8
132	0.00383261	IRP_MJ_WRITE	\Harddisk0\Partition2	SUCCESS	Sector: 206632 Length: 16
133	0.01810118	IRP_MJ_WRITE	\Harddisk0\Partition2	SUCCESS	Sector: 205632 Length: 8
134	0.02246346	IRP_MJ_WRITE	\Harddisk0\Partition2	SUCCESS	Sector: 205608 Length: 8
135	0.00415025	IRP_MJ_WRITE	\Harddisk0\Partition3	SUCCESS	Sector: 11724 Length: 8
136	0.00387116	IRP_MJ_WRITE	\Harddisk0\Partition3	SUCCESS	Sector: 552788 Length: 8
137	0.00183794	IRP_MJ_WRITE	\Harddisk0\Partition3	SUCCESS	Sector: 911860 Length: 8
138	0.00457349	IRP_MJ_WRITE	\Harddisk0\Partition2	SUCCESS	Sector: 51478 Length: 8
139	0.02680899	IRP_MJ_WRITE	\Harddisk0\Partition2	SUCCESS	Sector: 32268 Length: 8
140	0.03807466	IRP_MJ_WRITE	\Harddisk0\Partition2	SUCCESS	Sector: 50264 Length: 8
141	0.04816197	IRP_MJ_WRITE	\Harddisk0\Partition2	SUCCESS	Sector: 50274 Length: 8
142	0.04089904	IRP_MJ_WRITE	\Harddisk0\Partition2	SUCCESS	Sector: 50286 Length: 8
143	0.04488921	IRP_MJ_WRITE	\Harddisk0\Partition2	SUCCESS	Sector: 4572 Length: 8
144	0.00194354	IRP_MJ_WRITE	\Harddisk0\Partition2	SUCCESS	Sector: 205624 Length: 8
145	0.01085333	IRP_MJ_WRITE	\Harddisk0\Partition2	SUCCESS	Sector: 205616 Length: 8

Diskmon can find out what's causing unnecessary accesses to the hard disk

In its latest incarnation, version 5, Diskeeper can defragment both the MFT (Master File Table) and the paging file, in addition to ordinary disk files. These system files are only defragmented at system boot time, obviously, and not while the system is running. However, in addition, Diskeeper can operate at run-time to help prevent these files becoming fragmented in the first place. Interestingly, there is no executable file or user interface for Diskeeper. Instead, it is controlled through the Microsoft Management Console.

Another advantage of Diskeeper is that you can download a trial version for free from www.execsoft.co.uk.

Active disks

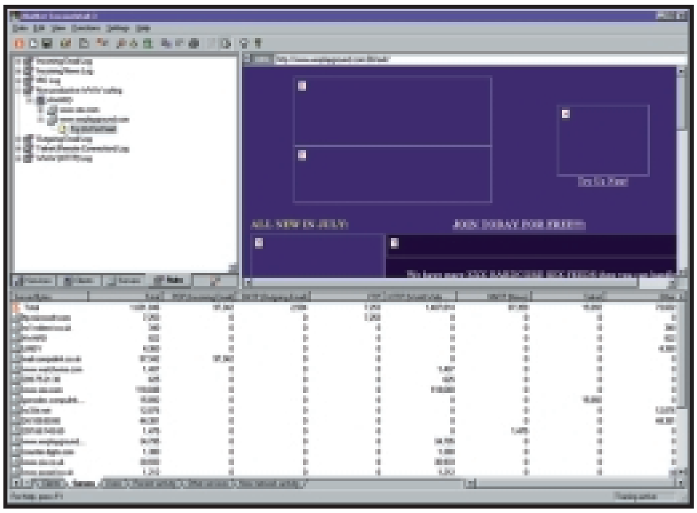
Stuart Taylor wrote in to complain that his hard-disk light illuminated at frequent and regular intervals. Worried about any unnecessary disk thrashing, he downloaded the utilities Filemon and Diskmon to find out what was causing the accessing. It turned out that it was the Background Status Monitor utility for an Epson Stylus Colour printer. Turning this off returned hard-disk activity to more normal levels. Thanks for the tip, Stuart!

Diskmon and Filemon are both available for download at: http://sysinternals.ovb.ch.

While on the subject of hard disks, various Windows NT mailing lists and newsletters carried a warning before the new year, that servers shouldn't be shut down over the holiday – in order to avoid any millennium bug or virus problems – and then restarted when people went back to work. If they were, the hard drives might fail.

The theory is that the heads on a hard drive build up a thin film of rubbish as they fly over the disk surface. This doesn't affect normal operation, but when the disk stops and the heads touch down (in normal operation, they aren't in contact with the disk itself, but literally float above it, with a tiny gap), the gunk that has built up can actually glue the heads to the drive. When you come in to restart the drives, they won't work.

These warnings initiated a flurry of



SessionWall 3 can be used both to monitor and control traffic on a network

claim and counterclaim, but experienced Windows NT network managers confirmed that there is a great deal of truth in this story. For example, one administrator who'd had to shut down all his servers in order to move them to another site, said quite a few hard drives failed to restart.

There is a way to avoid this problem. It involves shutting systems down for a very short interval – maybe 30 seconds – and then starting them up again. The idea is that this is long enough to clean some of the dirt off, but not long enough for the heads to stick down fatally.

When you shut a drive down, the heads are parked on an area of the disk known as the landing zone, which is supposed to be roughened and hence will clean off some of the dirt. After following this procedure, you can then turn the system off again for a longer interval, with a greater chance of the hard drive restarting.

You can use SessionWall to block access to porn sites or stop people playing Quake

Network traffic

Russell Howe would like to be able to monitor traffic on a network for data that is destined for port 139. He wants to be able to monitor the network using any machine on it – logging the source IP, to find out who keeps using WinNuke on the school network!

There's network monitoring software included with Windows NT4 Server, but it will only allow you to monitor traffic to and from that server, for security reasons. Full network-monitoring software is included with things such as Microsoft Systems Management Server (SMS) and with Network Associates' Total Network Solution, but these are expensive. SessionWall 3 is by far the best and easiest-to-use software that I've seen, but it's not cheap either. However, you can download a trial version to test it out before you buy.

SessionWall 3 can be used by a network administrator to monitor network traffic and track down particular problems such as Russell's, but it has other uses too. It can actually limit or disable certain types of network traffic altogether – at particular times, from specific machines, or to specific Internet hosts – so can be used to implement all sorts of Internet access policies. You can use it to block access to porn websites, to stop people from playing Quake or to scan incoming mail for viruses. It can also help monitor intrusion-detection attempts on your network.

A trial version of SessionWall 3 is available for download from: www.sessionwall.com.

Shell extensions

Alex Taperek has also asked about the EnforceShellExtensionSecurity policy. This is to restrict those shell extensions (extensions to Windows NT Explorer) that are allowed to run. Many applications today, such as WinZip and ArcServe, install their own extensions to Explorer functionality. With EnforceShellExtensionSecurity, you can control which of these (if any) are allowed to run.

According to Microsoft, if the EnforceShellExtensionSecurity policy is turned on, the shell will only run shell extensions that are registered under the Approved key. However, if the same EnforceShellExtensionSecurity policy is turned off, any shell extension can be run, whether or not it is registered under the Approved key.

The relevant registry key is: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer].

In order to enable shell extension security, add the value: EnforceShellExtensionSecurity and set it to one. The CLSIDs of any shell extensions that you want to allow then need to be explicitly added to the following key: [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved].

Home again

Finally, a quick comment on home directories – which also comes from the prolific Mr Taperek. If your client systems are running Windows 98, then setting a default home directory for users to store their data in should be straightforward.

First, create a data folder within the home directory on the Windows NT server, and then share it, giving full or change permissions to the user. Next, change the properties of the My Documents folder on the Windows 98 desktop to point to that directory (using the UNC path \\Server\Share\Folder). Normally, the My Documents folder points to C:\My Documents or C:\Windows\Profiles\username\My Documents.

When this is done, the many newer 32bit applications that default to storing documents in the My Documents folder will automatically use the data folder on the server that you have created.

CONTACTS

Andrew Ward welcomes your comments on the Windows NT column. Contact him via the *PCW* editorial office or email **nt@pcw.co.uk**