Global Information Assurance Certification Paper

Part 1 - Option 1: Forensic Analysis on a System

1. Description of system under analysis.

An Internet PC used for research by the Project Management Dept. Tagged as part of internal fixed asset register.

(a)**Software:** Windows 98 (Second Edition).

Norton anti-virus software
XXX ISP. Dynamic IP addresses allocated in the range X.X.X.X to X.X.X.X.

(b)**Hardware:** Compaq Presario computer system.

Midi tower chassis.
64MB RAM Internal
3.5" floppy disk drive.
Compact Disk drive.
Conexant HCF V90 56K Data/FAX PCI modem

Item seized: tagged as H_PSO_1: Western Digital WD272AW 20GB Hard disk drive.
S/N: WMA0C 103 3467

2. Synopsis of Case Facts

The Project Management department has several standalone PCs which are used for dedicated project support tasks. Two of the PCs also have dial-up internet access to allow staff to browse and cut-n-paste from web-sites related to their particular tasks. These machines are essentially "unsupported"by the IT department in terms of their software build.

On 29th April 2002, a colleague from the Project Management department came to see me because he was having problems with his PC. He explained that several days ago his anti-virus software had detected an infection on the PC. He had attempted to use the software to remove the virus but now the PC would not boot-up properly. He did not know how the machine could have been infected, nor could he remember the name of the virus. My colleague did not suspect any malicious intent on the behalf of the other members of the team who also used the PC, nor did he believe that there was any reason for his PC to be targeted for attack by internet denizens. A number of attempts had been made to get the PC to start correctly over the last few days since the virus infection had occurred.

Normally I would not spend more than a cursory few minutes on problems with this kind of system, but this seemed like an ideal subject for forensic analysis.

3. Media Imaging

The Hard disk was removed from the suspect machine and two separate images were made. The imaging machine is a full tower Systemax PC with 3.5" floppy, 250MB zip, DVD-ROM and Adaptec 7190 SCSI card. There are 4removable drive bays: 2 x IDE and 2 x SCSI. 256MB of RAM is installed.

(a)**dd image**.

The dd utility is an incredibly versatile and widely used tool which makes it attractive for use in forensic imaging. dd images are now recognised standard format, making exchange of data with other investigators straightforward. For example, Guidance Software's Encase product accepts dd raw images.

Imaging software build: RedHat LINUX 7.2 standard installation onto Western Digital 272AW 27.2 GB hard disk. Disk connected to primary IDE channel. External jumper set to Master. Kernel 2.4.7, dd version 4.1. md5sum version 2.0.14.

Imaging process:

i)The suspect disk was connected to the second IDE channel with its external jumper set to slave to ensure the disk was not booted from at system startup. The machine had first been booted with another blank IDE disk set as a slave in this position on the IDE channel to verify correct system initiation. A brand new Seagate 40GB SCSI disk was used as the target device to store the image.

ii)After booting the system, the /var/log/dmesg file was examined to determine which /dev device node was allocated to which disk. Extracts are listed below

```
ide: Assuming 33MHz PCI bus speed for PIO modes; override with idebus=xx
VP_IDE: VIA vt82c686b (rev 40) IDE UDMA100 controller on pci00:07.1
    ide0: BM-DMA at 0xc000-0xc007, BIOS settings: hda:DMA, hdb:DMA
    ide1: BM-DMA at 0xc008-0xc00f, BIOS settings: hdc:DMA, hdd:DMA
hda: QUANTUM FIREBALL EX6.4A, ATA DISK drive
hdb: Pioneer DVD-ROM ATAPIModel DVD-106S 010, ATAPI CD/DVD-ROM drive
hdc: WDC WD200BB-32CLB0, ATA DISK drive
hdd: IOMEGA ZIP 250 ATAPI, ATAPI FLOPPY drive
ide0 at 0x1f0-0x1f7,0x3f6 on irq 14
ide1 at 0x170-0x177,0x376 on irq 15
hda: 12594960 sectors (6449 MB) w/418KiB Cache, CHS=833/240/63, UDMA(33)
hdc: 39102336 sectors (20020 MB) w/2048KiB Cache, CHS=38792/16/63, UDMA(33)
ide-floppy driver 0.97
hdd: No disk in drive
hdd: 0kB, 0/64/32 CHS, 4096 kBps, 512 sector size, 2941 rpm
ide-floppy: hdd: I/O error, pc = 5a, key =  5, asc = 24, ascq =  0
Partition check:
 hda: hda1 hda2 hda3 hda4 < hda5 hda6 hda7 >
 hdc: [PTBL] [2586/240/63] hdc1 hdc2 < hdc5 >
<snip>
SCSI subsystem driver Revision: 1.00
```

```
PCI: Found IRQ 11 for device 00:0a.0
PCI: Sharing IRQ 11 with 00:07.5
(scsi0) <Adaptec AIC-7892 Ultra 160/m SCSI host adapter> found at PCI
0/10/0
(scsi0) Wide Channel, SCSI ID=7, 32/255 SCBs
(scsi0) Downloading sequencer code... 396 instructions downloaded
scsi0 : Adaptec AHA274x/284x/294x (EISA/VLB/PCI-Fast SCSI) 5.2.4/5.2.0
       <Adaptec AIC-7892 Ultra 160/m SCSI host adapter>
  Vendor: SEAGATE   Model: ST318417N         Rev: 0105
  Type:   Direct-Access                      ANSI  SCSI revision: 03
Attached scsi disk sda at scsi0, channel 0, id 0, lun 0
(scsi0:0:0:0) Synchronous at 20.0 Mbyte/sec, offset 31.
SCSI device sda: 35937500 512-byte hdwr sectors (18400 MB)
 sda: sda1
```

iii)An md5 checksum was taken of the disk before the imaging process was started:

```
madge# md5sum /dev/hdc

    c62e6ec989080a735e3fc5f5e9858dd4  /dev/hdc
```

iv)Even though it was brand new, the target SCSI disk was wiped to ensure no possible contamination of the image can occur:

```
madge# dd if=/dev/zero of=/dev/sda; sync
```

This process was verified. The following command should not have (and did not) return any lines:

```
madge# dd if=/dev/sdb | xxd | grep -v "0000 0000 0000 0000
0000 0000 0000 0000"
```

v)A new partition was created spanning the entire target disk using fdisk. An ext2 filesystem was then created using mkfs. This partition was then mounted:

```
madge# mount /dev/sda1 /mnt/images
```

vi) The partition information from the suspect disk was recorded[1]:

```
madge# fdisk -l /dev/hdc > /mnt/images/H_PSO_1_200402.fdisk
```

The contents of this file were as follows:

```
Disk /dev/hdb: 240 heads, 63 sectors, 2586 cylinders
```

1 An explanation of the image file and case naming convention used: <Disk type>_<dept>_x_<date>_<format> where *x* is sequence number relating to images from machines from a specific department *dept*.
Disk type can be:
H - PC IDE hard disk,
S - PC SCSI hard disk,
L - Laptop IDE hard disk
P - Palm or other PDA.

```
Units = cylinders of 15120 * 512 bytes

   Device Boot    Start       End    Blocks   Id  System
/dev/hdc1   *         1      1033   7809448+   c  Win95 FAT32
(LBA)
/dev/hdc2          1034      1292   1958040    f  Win95 Ext'd
(LBA)
/dev/hdc5          1034      1292   1958008+   b  Win95 FAT32
```

vii) Finally the entire suspect disk was imaged:

```
madge# dd conv=noerror bs=512k if=/dev/hdc
of=/mnt/images/H_PSO_1_290402.dd

38185+1 records in
38185+1 records out
```

Typically this file will only play a small part in the analysis process so it was compressed to preserve disk space.

viii) md5 hash checksums of each partition were calculated:

```
madge# md5sum /dev/hdc1 > md5_1
madge# more md5_1

601899fccd63ee731ac93aa78ab97b61  /dev/hdc1

madge# md5sum /dev/hdc2 > md5_2
madge# more md5_2

fe94ae334b97e0244de0d1b1adefc83e  /dev/hdc2

madge# md5sum /dev/hdc5 > md5_5
madge# more  md5_5

57a57136e3c4e83105a2420574135193  /dev/hdc5
```

ix) Then each partition was imaged separately:

```
madge# dd conv=noerror bs=512k if=/dev/hdc1
of=/mnt/images/H_PSO_1_290402_p1.dd

15252+1 records in
15252+1 records out

madge# dd conv=noerror bs=512k if=/dev/hdc2
of=/mnt/images/H_PSO_1_290402_p2.dd

3824+1 records in
```

```
3824+1 records out
```

x)All md5 checksums were compared:

```
c62e6ec989080a735e3fc5f5e9858dd4
/mnt/images/H_PSO_1_290402.dd

601899fccd63ee731ac93aa78ab97b61
/mnt/images/H_PSO_1_290402_1.dd

57a57136e3c4e83105a2420574135193
/mnt/images/H_PSO_1_290402_5.dd
```

(b)Encase image.

The same hardware was used to make this image. The imaging software build was a Guidance Software's Encase boot-disk Version 3.

Imaging process

i) The BIOS configuration of the imaging machine was altered such that booting from the hard disk was disabled to permit floppy booting only. The suspect disk was connected to the secondary IDE channel with its external jumper set to slave. A brand new Western Digital 272AW 27.2GB IDE disk was used as the target device to store the image. A FAT32 partition spanned this entire disk. This was connected to the SCSI chain. The machine was first booted with another blank IDE disk set as a slave in the suspect disk position on the IDE channel to verify correct system initiation from floppy disk.

ii) The imaging machine was booted from the floppy and the en.exe application started. The “Hash” option was selected and an MD5 checksum calculated for the disk:

```
The hash value of 0 from sector 0 to 39102335 is:
C62E6EC989080A735E3FC5F5E9858DD4
Completed on: 04/29/2002 07:29:46pm
Elapsed time: 2:39:00
```

This is exactly the same value as obtained using Linux's md5sum.

iii) Taking care to ensure the correct disks were selected as master and target, the imaging process was started via the GUI. Encase creates a complete bit-stream forensic image of a target drive. The image was compressed to save disk space, although this did slow the imaging process.

iv) The Encase Evidence file is a secure, self-verifying and fully integrated forensic image. Every byte of the file is verified using a 32-bit Cyclical Redundancy Check (CRC) which is generated as the image is produced. In fact Encase actually

computes a CRC value for every block of 64 sectors that it writes to the target disk. An MD5 checksum is automatically calculated for all the data contained within the bit-stream as it is created. This value and the CRC values are stored within the proprietary Encase image format[2]. Each time the Encase image is opened for analysis though the software GUI the MD5 checksum and CRC values are automatically verified (See section 4 below).

3. Media Analysis

The analysis machine is a full tower Systemax PC with 3.5" floppy, 250MB zip, Panasonic DVD-RAM, DVD-ROM and Adaptec 7190 SCSI card. There are 3 removable drive bays; 2 x IDE and 1 SCSI. Analysis was performed using three software tools: Guidance Software's Encase, the TASK from @stake.com and Norton's Diskedit. The discovery process was completed using all three tools in parallel, often cross-referencing results obtained between applications. For clarity, the analysis and deductions are described in sections relating to the tools used. This does not necessarily represent the actual sequence of actions performed as part of the analysis.

(a) **The @stake Sleuth Kit (TASK).[3]**

i. A RedHat Linux 7.2 build was used for this part of the analysis, running on the same analysis hardware as described above. Typically KDE was used for TASK and the Autopsy Forensic Browser[4], an HTML-based graphical interface to TASK. A custom kernel is available for selection at boot-time. Pertinent compilations options selected include >2GB file support for Perl, support for NTFS, UDF and Mac filesystems, and an increased timeout for SCSI devices

ii. TASK is based on the code and design of The Coroner's Toolkit (TCT) and TCTUTILs. Previous versions of these tools only supported UNIX file systems, but TASK version 1.0 includes support for Windows-based file systems. The ability to build a MACTime chronology for a disk partition is an invaluable tool for forensic analysis and the resulting file can form the basis of deductions and assumptions which can be investigated further with other utilities. The inclusion of data related to deleted files within this timeline also provides a first-look at potentially malicious activity.

iii. A FAT filesystem stores file content in clusters, which are just a grouping of many sectors (typically 512-bytes each). Because the "first" cluster does not necessarily start at the beginning of the partition, it is non-trivial to use clusters as addressable units as there is no way to identify the non-"data area" sectors. TASK solves this problem[5] by using the sector as the

2 See the Encase Software manual for more details. www.encase.com
3 TASK version 1.0 10th April 2002. Available from www.atstake.com/research/tools/task
4 The Autopsy Forensic Browser version 1.5 10th April 2002. Available from www.atstake.com/research/tools/autopsy
5 Paraphrased from the TASK documentation (included with the tar file available from @stake.

addressable unit. When a "file" is described (using 'istat' for example), the sector addresses are given. A further complication in applying UNIX filesystem techniques to FAT is that the Windows filesystem has no notion of an "inode". FAT describes its files in a directory entry structure (contained in the sectors allocated by the parent directory). The directory entry structures have a fixed size of 32-bytes and are roughly comparable to a UNIX inode. Unfortunately they are not numbered and can exist anywhere on the disk. This problem can be overcome by treating each sector in the "data area" as though it could be full of directory entries; as each sector is 512-bytes and each directory entry is 32-bytes, each sector could contain 16 entries. The root directory is given the value of 2 (and its meta-data is set to 0). The first 32-bytes of the first sector in the data area are then addressed as 3, the second 32-bytes of the sector as 4 and so on.. This allows identification of the location of a meta-data structure given only its address. It also places a limit on the size of the partition that can be analyzed: 2^32 / 16 = 2^28 sectors => partitions of 137,438,953,472 bytes. Our disk images were less than 20GB so no problems should be encountered using TASK.

iv. The SCSI disk containing the previously created dd image was mounted.

```
[Zerot@Anna zerot]$  ls -l /mnt/images

total 17352356

-rw-r--r--    1 root     root          627 Jun 28 12:41 fsmorgue
-rw-r--r--    1 root     root     3085459222 May  2 18:37
H_PSO_1_020502.dd.gz
-rw-r--r--    1 root     root     7996874752 Jun 27 23:08
H_PSO_1_290402_1.dd
-rw-r--r--    1 root     root     2005000192 Jun 27 22:56
H_PSO_1_290402_5.dd
drwxr-xr-x    2 root     root         4096 May 30 17:37 lost+found
-rw-r--r--    1 root     root           44 Jun 27 22:49 md5_1
-rw-r--r--    1 root     root           66 Jun 27 23:23 md5_1_c opy
-rw-r--r--    1 root     root           44 Jun 27 22:53 md5_5
-rw-r--r--    1 root     root           66 Jun 27 23:11 md5_5_copy
-rw-r--r--    1 root     root           43 Jun 27 22:34 md5_all
-rw-r--r--    1 root     root           66 Jun 27 23:51 md5 _all_copy
```

v. To verify that useful images had been created, they were mounted as loop devices. From the previous fdisk results, it was known that the filesystem was FAT32 and so the appropriate -t option must be passed to the mount command:

```
[Zerot@Anna zerot]$ mount -t vfat -o ro,loop,noatime,noexec,nodev
/mnt/images/H_PSO_1_290402_1.dd /mnt/susp1
```

vi. Typical files you would expect to see for a Windows installation could then be viewed:

```
[Zerot@Anna zerot]$ ls -l /mnt/susp1

total 112128
```

```
drwxr-xr-x    3 root     root         4096 Feb 25  2001 Acrobat3
drwxr-xr-x    5 root     root         4096 Nov 11  2000 Adobe Albums
-rwxr-xr-x    1 root     root          194 Apr 26 15:33 autoexec.bak
-rwxr-xr-x    1 root     root          194 Apr 26 15:33 autoexec.bat
-rwxr-xr-x    1 root     root          194 Apr  7  2001 autoexec.nai
-rwxr-xr-x    1 root     root          194 Dec 12  2001 autoexec.nu4
-rwxr-xr-x    1 root     root        69221 Apr 26 15:52 bootlog.prv
-rwxr-xr-x    1 root     root        70324 Apr 26 16: 10 bootlog.txt
-r-xr-xr-x    1 root     root        93040 Jun  8  2000 command.com
-rwxr-xr-x    1 root     root          967 Aug  2  2000 command.pif
drwxr-xr-x    7 root     root         4096 Oct 19  2000 compaq
-rwxr-xr-x    1 root     root            0  Apr 26 15:33 config.bak
-rwxr-xr-x    1 root     root            0 Apr 26 15:33 config.sys
drwxr-xr-x    9 root     root         4096 Aug  2  2000 cpqdrv
drwxr-xr-x    8 root     root         4096 Aug  9  2000 Cpqs
-rwxr-xr-x    1 root     root        325 08 Oct 19  2000 detlog.txt
-rwxr-xr-x    1 root     root         2755 Apr 10 19:48 frontpg.log
-r-xr-xr-x    1 root     root       110080 Jun  8  2000 io.sys
-rwxr-xr-x    1 root     root       129078 Jun  8  2000 logo.sys
-rwxr-xr-x    1 root     root            0 Apr  3 21:55 Log.txt
-r-xr-xr-x    1 root     root         1660 Oct 19  2000 msdos.sys
dr-xr-xr-x   18 root     root         4096 Aug  2  2000 My Documents
drwxr-xr-x    2 root     root         4096 Dec 12  2001 ncdtree
-rwxr-xr-x    1 root     root         2941 Oct 19  2000 netlog.txt
drwxr-xr-x   48 root     root         4096 Aug  2  2000 Program Files
-rwxr-xr-x    1 root     root          547 Mar  8  1999 QT_YES.txt
drwxr-xr-x    3 root     root        12288 Aug  2  2000 recycled
drwxr-xr-x    7 root     root         4096 Oct 19  2000 _restore
-rwxr-xr-x    1 root     root          615 Apr 26 15:11 scandisk.log
-rwxr-xr-x    1 root     root          832 Nov 11  2000 setupxlg.txt
-rwxr-xr-x    1 root     root       938013 Mar  2 23:10 stub.log
drwxr-xr-x    2 root     root         4096 Aug  2  2000 system.sav
-rwxr-xr-x    1 root     root    113246208 Apr 26 16:10 win386.swp
drwxr-xr-x   55 root     root        16384 Aug  2  2000 windows
-rwxr-xr-x    1 root     root           63 Nov 27  2000 WI NDOWSWinHlp32.BMK
```

vii. The Windows swap file win386.swp is often a fruitful source of forensic information so all human-readable strings were extracted:

```
[Zerot@Anna zerot]$ strings < /mnt/susp1/win386.swp >
/mnt/images/H_PSO_1_290402_1.swp.str
```

viii. Snooping around the loop-mounted imaged revealed that the following software had been installed on the PC:

```
Aug 2 2000 Adobe
Apr 26 15:51 ahead
Feb 25 2001 Borland
Oct 19 2000 BT Click
Nov 16 2000 BT Internet
Oct 19 2000 Compaq
Oct 19 2000 CompaqNET.co.uk
Feb 25 2001 Corel
Oct 19 2000 Freeserve
Nov 11 2000 Hewlett-Packard
Nov 11 2000 HP DeskJet 840C Series
Oct 19 2000 Indigo
Oct 19 2000 InstallShield Installation Information
Aug 2 2000 Internet Explorer
```

```
Nov 16 2000 Inverse IP InSight
Apr 7 2001 McAfee
Apr 7 2001 McAfee VirusScan Retail Licensed
Oct 19 2000 Mediamatics
Aug 2 2000 Messenger
Nov 16 2000 Microsoft Chat
Mar 20 2001 Microsoft FrontPage
Nov 16 2000 Microsoft FrontPage Express
Aug 2 2000 Microsoft Office
Aug 2 2000 Microsoft Visual Studio
Aug 2 2000 Microsoft Works
Aug 2 2000 Movie Maker
Aug 2 2000 MSN Gaming Zone
Dec 24 2000 Napster
Aug 2 2000 NetMeeting
Dec 26 2000 Network Associates
Dec 12 2001 Norton SystemWorks
Sep 23 2001 Ocad7
Aug 2 2000 Online Services
Aug 2 2000 Outlook Express
Jan 5 2001 QuickTime
Mar 20 2001 Snapshot Viewer
Dec 12 2001 Symantec
Oct 19 2000 via
Aug 2 2000 Web Publish
Feb 25 2001 WexTech
Aug 2 2000 Windows Media Player
```

ix. The location of the image file was added to TASK's main configuration file; fsmorgue which was created in the Autopsy software's morgue directory /mnt/images. Autopsy was then initialised on port 8888 and the generated URL pointer copied into the analysis machine's browser's address line. The contents of the fsmorgue file at the end of the analysis are shown below:

```
H_PSO_1_290402_1.dd  fat       /          GMT
H_PSO_1_290402_5.dd  fat       /          GMT
H_PSO_1_290402_1.body          body
H_PSO_1_290402_1.tl  timeline
H_PSO_1_290402_5.body          body
H_PSO_1_290402_5.tl  timeline
```

x. MACTime Analysis

A. The TASK browser interface provides a simple mechanism to create a timeline from the partition image. First a 'body' file was created from the image. This action is actually performed by the **fls** command which gathers data related to allocated and unallocated files . Next a timeline was extracted from the 'body' data using **ils -m**.

B. The timeline for the smaller 'recovery' partition was likely to provide a useful indication of when the system was actually built and the operating system installed. The MACTime file is listed below:

```
[Zerot@Anna /mnt/images]$ more H_PSO_1_290402_.tl
```

```
Jan 01 1970 00:00:00        1 m.. -rwxrwxrwx 0        0                <H_PSO_1_290402_5.dd-
_0000000.DAT-dead-29421318>
                            1 .a. -rwxrwxrwx 0        0                <H_PSO_1_290402_5.dd-
_0000000.DAT-dead-29421318>
                            1 ..c -rwxrwxrwx 0        0                <H_PSO_1_290402_5.dd-
_0000000.DAT-dead-29421318>
Oct 19 2000 00:00:00     4096 .a. d/dr-xr-xr-x 0        0        8        /_Restore (_RESTORE)
Oct 19 2000 19:22:04     4096 ..c d/dr-xr-xr-x 0        0        8        /_Restore (_RESTORE)
Oct 19 2000 19:22:06     4096 m.. d/dr-xr-xr-x 0        0        8        /_Restore (_RESTORE)
Nov 11 2000 00:00:00     4096 .a. d/dr-xr-xr-x 0        0        10       /Recycled (RECYCLED)
Nov 11 2000 21:18:40     4096 ..c d/dr-xr-xr-x 0        0        10       /Recycled (RECYCLED)
                           20 ..c -/-r-xr-xr-x 0        0        29385223 /RECYCLED/INFO2
Nov 11 2000 21:18:42     4096 m.. d/dr-xr-xr-x 0        0        10       /Recycled (RECYCLED)
Dec 12 2001 00:00:00     4096 .a. d/dr-xr-xr-x 0        0        29385224 /RECYCLED/NPROTECT
Dec 12 2001 19:54:12        1 ..c -rwxrwxrwx 0        0        29421318 <H_PSO_1_290402_5.dd-
_0000000.DAT-dead-29421318>
                            1 ..c -/-rwxrwxrwx 0        0        29421318
/RECYCLED/NPROTECT/_0000000.DAT (deleted)
Dec 12 2001 19:54:14        1 m.. -rwxrwxrwx 0        0        29421318 <H_PSO_1_290402_5.dd-
_0000000.DAT-dead-29421318>
                            1 m.. -/-rwxrwxrwx 0        0        29421318
/RECYCLED/NPROTECT/_0000000.DAT (deleted)
Dec 12 2001 22:40:36   646528 ..c -/-rwxrwxrwx 0        0        29421317
/RECYCLED/NPROTECT/NPROTECT.LOG
                       4096 ..c d/dr-xr-xr-x 0        0        29385224 /RECYCLED/NPROTECT
Dec 12 2001 22:40:38     4096 m.. d/dr-xr-xr-x 0        0        29385224 /RECYCLED/NPROTECT
Apr 01 2002 21:34:00       65 ..c -/-r-xr-xr-x 0        0        29385222
/RECYCLED/desktop.ini (DESKTOP.INI)
Apr 01 2002 21:34:02       65 m.. -/-r-xr-xr-x 0        0        29385222
/RECYCLED/desktop.ini (DESKTOP.INI)
Apr 25 2002 18:27:46        1 ..c -/-rwxrwxrwx 0        0        29385093
/_RESTORE/SRDISKID.DAT
Apr 25 2002 18:27:54        1 m.. -/-rwxrwxrwx 0        0        29385093
/_RESTORE/SRDISKID.DAT
Apr 26 2002 00:00:00        1 .a. -/-rwxrwxrwx 0        0        29385093
/_RESTORE/SRDISKID.DAT
                            0 .a. -/-rwxrwxrwx 0        0        14       /_SI2233.TMP
(deleted)
                           20 .a. -/-r-xr-xr-x 0        0        29385223 /RECYCLED/INFO2
                            1 .a. -rwxrwxrwx 0        0        29421318 <H_PSO_1_290402_5.dd-
_0000000.DAT-dead-29421318>
                            1 .a. -/-rwxrwxrwx 0        0        29421318
/RECYCLED/NPROTECT/_0000000.DAT (deleted)
                            0 .a. -rwxrwxrwx 0        0        14       <H_PSO_1_290402_5.dd-
_SI2233.TMP-dead-14>
Apr 26 2002 13:39:22       20 m.. -/-r-xr-xr-x 0        0        29385223 /RECYCLED/INFO2
Apr 26 2002 15:50:34        0 ..c -rwxrwxrwx 0        0        14       <H_PSO_1_290402_5.dd-
_SI2233.TMP-dead-14>
                            0 ..c -/-rwxrwxrwx 0        0        14       /_SI2233.TMP
(deleted)
Apr 26 2002 15:50:36        0 m.. -rwxrwxrwx 0        0        14       <H_PSO_1_290402_5.dd-
_SI2233.TMP-dead-14>
                            0 m.. -/-rwxrwxrwx 0        0        14       /_SI2233.TMP
(deleted)
Apr 27 2002 00:00:00       65 .a. -/-r-xr-xr-x 0        0        29385222
/RECYCLED/desktop.ini (DESKTOP.INI)
Apr 27 2002 00:00:00   646528 .a. -/-rwxrwxrwx 0        0        29421317
/RECYCLED/NPROTECT/NPROTECT.LOG
Apr 27 2002 17:58:26   646528 m.. -/-rwxrwxrwx 0        0        29421317
/RECYCLED/NPROTECT/NPROTECT.LOG
```

The earliest timestamp found on this partition, on the _Restore directory (which is created by the installation process) is Oct 19 2000. This provided a good starting point for identifying the build time of the system. Returning to the main disk partition, examination of the Microsoft Task scheduler file schedlog.txt (which is created at installation time and less likely to be modified/re-created during the life of a PC) showed that the Created/changed date on the file was also Oct 19th 2000.

```
Oct 19 2000 19:21:46    32656 ..c  -/-rwxrwxrwx 0 0 65460297
/WINDOWS/SchedLog.Txt (SCHEDLOG.TXT)

Apr 26 2002 16:10:46    32656 m..  -/-rwxrwxrwx 0 0 65460297
/WINDOWS/SchedLog.Txt (SCHEDLOG.TXT)
```

C.Turning to the larger partition, a much larger timeline was created , ranging from:

```
Jan 01 1970 00:00:00          m..                                <H_PSO_1_29 0402_1.dd-
_ROGMAN.EXE-dead-230126346>
                              .a.                                <H_PSO_1_290402_1.dd -
_ROGMAN.EXE-dead-230126346>
                              ..c                                <H_PSO_1_290402_1.dd -
_ROGMAN.EXE-dead-230126346>
Mar 19 1988 07:00:00      612 m.c  -/-rwxrwxrwx 0        0        65587953
/PROGRA~1/NORTON~1/NORTON~1/QuarOpts.dat (QUAROP TS.DAT)
Jun 17 1992 13:44:46        2 m..  -/-rwxrwxrwx 0        0        65583780
/PROGRA~1/HEWLET~1/HPPREC~1/ISTECH/OCR/trkphon.env (TRKPHON.ENV)
Oct 14 1993 14:47:18        2 m..  -/-rwxrwxrwx 0        0        65583868
/PROGRA~1/HEWLET~1/HPPREC~1/ISTECH/ OCR/hunphon.env (HUNPHON.ENV)
Oct 14 1993 14:48:14        2 m..  -/-rwxrwxrwx 0        0        65583950
/PROGRA~1/HEWLET~1/HPPREC~1/ISTECH/OCR/slkphon.env (SLKPHON.ENV)
Oct 14 1993 14:49:00        2 m..  -/-rwxrwxrwx 0        0        65583954
/PROGRA~1/HEW LET~1/HPPREC~1/ISTECH/OCR/slnphon.env (SLNPHON.ENV)
Nov 17 1994 03:34:22   474624 m..  -/-rwxrwxrwx 0        0        65588218
/PROGRA~1/NORTON~1/NORTON~3/PGNORTON.DLL
Feb 16 1995 19:28:48   189440 m.c  -/-rwxrwxrwx 0        0        65517839
/PROGRA~1/COMMO N~1/MICROS~1/TEXTCONV/TXTLYT32.CNV
```

to

```
Apr 26 2002 16:10:34   147456 m..  -/-rwxrwxrwx 0        0        65468550
/WINDOWS/COOKIES/index.dat (INDEX.DAT)
                     12337152 m..  -/-rwxrwxrwx 0        0        65672582
/WINDOWS/TEMPOR~1/CONTENT.IE 5/index.dat (INDEX.DAT)
                       950272 m..  -/-rwxrwxrwx 0        0        65709321
/WINDOWS/HISTORY/HISTORY.IE5/index.dat (INDEX.DAT)
Apr 26 2002 16:10:40        5 m..  -/-rwxrwxrwx 0        0        65710856
/WINDOWS/ALLUSE~1/APPLIC~1/SYMANT EC/NORTON~1/NavProxy.dat (NAVPROXY.DAT)
Apr 26 2002 16:10:42   958496 m..  -/---x--x--x 0        0        65460456
/WINDOWS/USER.DAT
Apr 26 2002 16:10:44       52 m..  -/-r-xr-xr-x 0        0        65465610
/_RESTORE/DSINFO.DAT
                        6763  m..  -/-rwxrwxrwx 0        0        65473158
/WINDOWS/APPLOG/APPLOG.ind (APPLOG.IND)
Apr 26 2002 16:10:46    32656 m..  -/-rwxrwxrwx 0        0        65460297
/WINDOWS/SchedLog.Txt (SCHEDLOG.TXT)
                           50 m..  -/-rwxrwxrwx 0        0         65460279
/WINDOWS/wiaservc.log (WIASERVC.LOG)
```

D. Further examination of this timeline revealed significant activity around our suspected installation date, with a large number of system files and drivers being created. An extract is listed below:

```
Oct 10 2000 16:12:46   139264 m.c -/-rwxrwxrwx 0        0        4433715
/PROGRA~1/AHEAD/NERO/MPGEnc.dll (MPGENC.DLL)
Oct 19 2000 00:00:00     4096 .a. d/drwxrwxrwx 0        0        65461131 /COMPAQ/RowIsp
(ROWISP)
                         4096 .a. d/drwxrwxrwx 0        0        65596170
/COMPAQ/LUTIL/HTML/images (IMAGES)
                         4096 .a. d/drwxrwxrwx 0        0        65494398
```

```
/CPQDRV/NVIDIA/setupdir (SETUPDIR)
                        4096 .a. d/drwxrwxrwx 0        0        65596168
/COMPAQ/LUTIL/HTML/NaFrench (NAFRENCH)
                        4096 .a. d/drwxrwxrwx 0        0        65512077
/PROGRA~1/COMPAQ/Compaq Hardware Discovery (COMPAQ~1)
                        4096 .a. d/drwxrwxrwx 0        0        65581958
/PROGRA~1/COMPAQ/EASYAC~1/Desktops (DESKTOPS)
                        4096 .a. d/drwxrwxrwx 0        0        65512204
/PROGRA~1/INSTAL~1/{C1A9EFC0-1C2E-11D4-892F-0008C73FDA66} ({C1A9E~1)
                        4096 .a. d/drwxrwxrwx 0        0        65596446
/COMPAQ/LUTIL/HTML/IMAGES/NaEnglish (NAENGL~1)
                        4096 .a. d/drwxrwxrwx 0        0        65595672 /COMPAQ/LUTIL/html
(HTML)
                        4096 .a. d/drwxrwxrwx 0        0        65583114
/PROGRA~1/MEDIAM~1/DVDEXP~1/Migrate (MIGRATE)
                        4096 .a. d/drwxrwxrwx 0        0        65583366
/PROGRA~1/MEDIAM~1/DVDEXP~1/DVD/Help (HELP)
                        4096 .a. d/drwxrwxrwx 0        0        65461060 /PROGRA~1/Indigo
(INDIGO)
                        4096 .a. d/drwxrwxrwx 0        0        65500687
/CPQDRV/NVIDIA/SETUPDIR/0013
                        4096 .a. d/drwxrwxrwx 0        0        65512071
/PROGRA~1/COMPAQ/Easy Access Button Support (EASYAC~1)
                        4096 .a. d/drwxrwxrwx 0        0        65597575 /CPQS/SUPPORT/rooms
(ROOMS)
                        4096 .a. d/drwxrwxrwx 0        0        65498247
/CPQDRV/ADI/SETUPDIR/0009
                        4096 .a. d/drwxrwxrwx 0        0        65512212
/PROGRA~1/INSTAL~1/{DEBD6FD4-146B-11D4-8CE7-0008C71345FC} ({DEBD6~1)
                        4096 .a. d/drwxrwxrwx 0        0        65500679
/CPQDRV/NVIDIA/SETUPDIR/0009
                        4096 .a. d/drwxrwxrwx 0        0        65498256
/CPQDRV/ADI/SETUPDIR/0014
                        4096 .a. d/drwxrwxrwx 0        0        65497627 /CPQDRV/ADI/setupdir
(SETUPDIR)
                        4096 .a. d/drwxrwxrwx 0        0        65500688
/CPQDRV/NVIDIA/SETUPDIR/0014
                        4096 .a. d/drwxrwxrwx 0        0        65470982
/WINDOWS/CPQDIAG/cpqdiags (CPQDIAGS)
                        4096 .a. d/drwxrwxrwx 0        0        65597830 /CPQS/BACKWEB/Data
(DATA)
                        4096 .a. d/drwxrwxrwx 0        0        65597843 /CPQS/BACKWEB/tmp
(TMP)
                        4096 .a. d/drwxrwxrwx 0        0        65461127 /COMPAQ/lutil
(LUTIL)
                        8192 .a. d/drwxrwxrwx 0        0        65460747 /CPQDRV/nvidia
(NVIDIA)
                        4096 .a. d/drwxrwxrwx 0        0        65498261
/CPQDRV/ADI/SETUPDIR/001e (001E)
                        4096 .a. d/drwxrwxrwx 0        0        65598725 /CPQS/BACKWEB/DATA/1
                        4096 .a. d/drwxrwxrwx 0        0        65597446 /CPQS/QUICKSR/QRWIN
                        4096 .a. d/drwxrwxrwx 0        0        65500691
/CPQDRV/NVIDIA/SETUPDIR/001d (001D)
                        4096 .a. d/drwxrwxrwx 0        0        65498259
/CPQDRV/ADI/SETUPDIR/001d (001D)
                        4096 .a. d/drwxrwxrwx 0        0        65512208
/PROGRA~1/INSTAL~1/{87D2A4AC-FF34-11D3-892C-0008C73FDA66} ({87D2A~1)
                        4096 .a. d/drwxrwxrwx 0        0        65583624
/PROGRA~1/MEDIAM~1/DVDEXP~1/DVD/HELP/DlgImg (DLGIMG)
                        4096 .a. d/drwxrwxrwx 0        0        65497616 /CPQDRV/ADI/SE
                        4096 .a. d/dr-xr-xr-x 0        0        65461052
/PROGRA~1/InstallShield Installation Information (INSTAL~1)
                        4096 .a. d/drwxrwxrwx 0        0        65500677
```

E. However when activity slightly further back in time was examined, file accesses inconsistent with an Oct 19 installation were identified. Files under a user's profile directory had been modified on June 8th. No user or machine specific files should have a timestamp earlier than the installation date. The most likely explanation for this inconsistency is that Oct 19th was not the *first* time the operating system was built, but rather an occasion

when the PC configuration had to be restored from the recovery CD and partition.

```
Jun 08 2000 17:00:00    27925 m.. -/-rwxrwxrwx 0        0        65610379
/WINDOWS/HELP/MIT/TRAINING/WINMIL/CONTENT/CBZ/L6_CA.CBZ
                         9828 m.. -/-rwxrwxrwx 0        0        65608880
/WINDOWS/HELP/MIT/TRAINING/WINMIL/CONTENT/LIB/L12_B.LDZ
                      3440660 m.. -/-rwxrwxrwx 0        0        65611810
/WINDOWS/SYSTEM32/DRIVERS/GM.DLS
                         9828 m.. -/-rwxrwxrwx 0        0        65608878
/WINDOWS/HELP/MIT/TRAINING/WINMIL/CONTENT/LIB/L11_G.LDZ
                        33873 m.. -/-rwxrwxrwx 0        0        65461743
/WINDOWS/SYSTEM/VJOYD.VXD
                        20480 m.. -/-rwxrwxrwx 0        0        65461271 /
/WINDOWS/PROFILES/MARILYN/APPLIC~1/MICROS~1/INTRO/YLOBCKGD.JPG
                       528384 m.c -/-rwxrwxrwx 0        0        65460226
/WINDOWS/KODAKIMG.EXE
                        74422 m.. -/-rwxrwxrwx 0        0        65609371
/WINDOWS/HELP/MIT/TRAINING/WINMIL/CONTENT/LIB/TopInstallingSystemUpdates.swf (TOPINS~1.SWF)
                         7352 m.. -/-rwxrwxrwx 0        0        65503626
/MYDOCU~1/TIM'SM~1/beck.bmp (BECK.BMP)
```

F. It was already known from the user of the system when the problems he encountered with the PC began: around the 20th April 2002. Therefore a smaller timeline snippet centred on this date can be created. The full listing of this (with irrelevant permissions column removed) is available in Appendix B.

G. On 19th April significant activity could be seen around the AV software. Tests on another Windows machine running this package suggest this is symptomatic of an update of the AV definitions being automatically performed via the internet.

H. There is no MACTime data produced for April 20th.

I. On April 21st there was an interesting period of activity

- 21:43:48- The first of a number of file accesses associated with internet activity .
- 21:49:42- A file “Internet Security Update.dat” was cached.
- 21:50:02- The Symantec/Norton auto-update file was modified. More activity consistent with virus definition updates being downloaded begins.
- 21:55:02- The file q216309.exe was deleted from the My Documents folder.
- Accessed attribute; No time available- Two executables from the Norton quarantine directory are deleted. These filenames, ap0.exe and ap1.exe are consistent with the names used by Norton when it segregates a file it believes to be infected. No times are provided by Windows for these actions so it is a matter of supposition at exactly which time these file accesses took place.
- 21:56:04- Last activity that day.

J.The MACTime chronology generated by TASK is in a useful format for

determining when a large number of changes were made to the system (for example at installation time or when an intruder installs a rootkit or other malicious software). However file modifications all occurring at the same time do not have an individual date/time entry in the left hand column of the chronology. This can be a handicap when performing keyword (grep) searches of the file, when the intention is to list only lines which contain a particular string as not every line will have a date/timestamp. This problem iwas overcome by creating a second chronology file from the first, with each line having the appropriate date/time. This was achieved using a simple awk script:

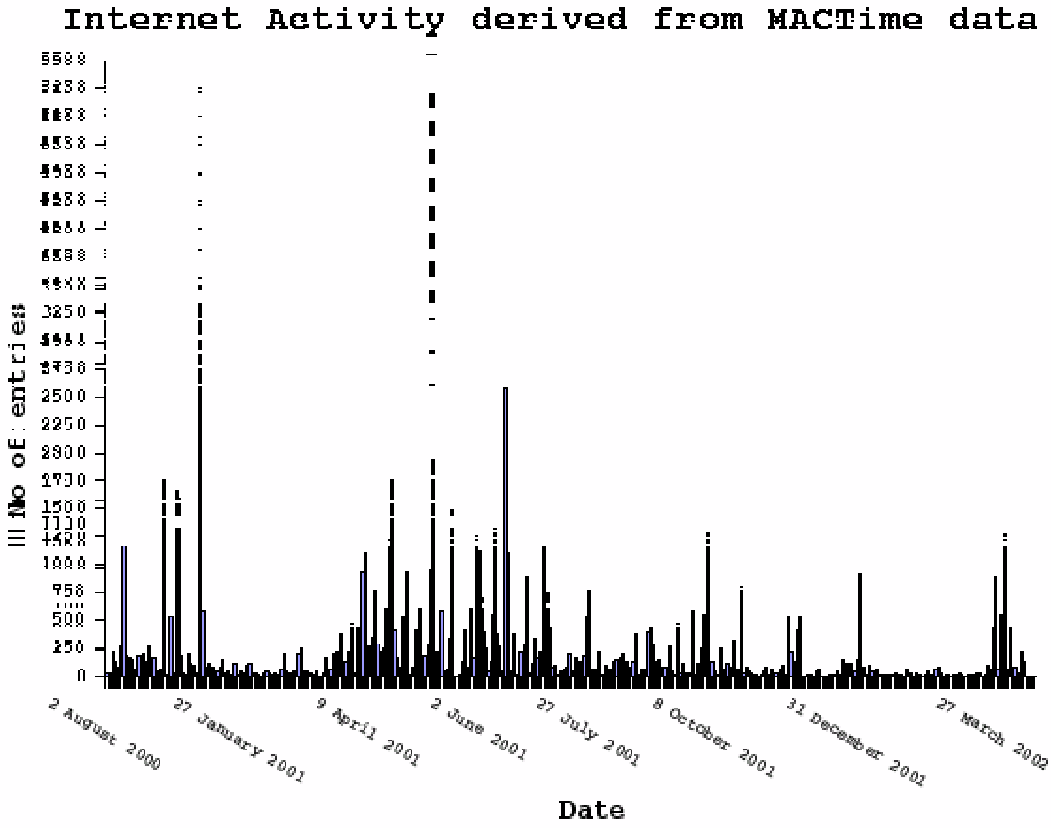
```
#run with awk -f
BEGIN {
            df = ""
}
{
            s = substr ($0, 1, 20)
            r = substr ($0, 21)

            if (s == "                    ") {
                        print df""r
            } else {
                        df = s
                        print
            }
}
```

K. Using this new file, it was possible to develop a picture of the internet activity on this machine. Grep searching for “TEMPOR~1/CONTENT” provided a list of each recorded MAC alteration to these cache files. An approximate picture of the users' surfing habits could then be constructed by counting the total number of MACTime entries for each day. Once again this was achieved using a simple awk script.

```
{
            for (i=1;i <= NF; i++)
            freq[$i]++
}
END {
            for (word in freq)
{
            MON = substr(word,1,3)
            DAY = substr(word,4,2)
            YR = substr(word,6,4)
            print DAY"-"MON"-"YR","freq[word]
}
}
```

L. The search produced 123859 lines with the first recorded surfing on April 02nd 2000. Then there is a jump until Nov 02nd 2000. Regular internet use continues up until present day, with certain peaks of activity (5th January - first day back at work after the Christmas holiday - being the largest).



M. It was known that the machine was used for internet research. Search engines typically have a distinctive URL which is often cached as part of search activity. Searching the strings extracted by the image file via TASK for "google.com/search?" reveals the a number of queries made at Google[6]. These are listed in Appendix A.

N. The user of the system reported that his anti-virus software, which was up-to-date, had located an infection but after the cleaning process the workstation would not boot correctly. Therefore a search was made for any log files associated with the anti-virus software. Norton's Activity.log file was found and, because it is not actually an ascii text file, strings extracted. Of particular interest was the following:

```
Virus scan started.
COMPUTER
marilyn
The file C:\WINDOWS\SYSTEM\kdll.dll is infected with the  W32.Badtrans.B@mm virus.
The file was quarantined.
Virus scan started.
COMPUTER
marilyn
The file C:\WINDOWS\Temporary Internet Files\Content.IE5\L5YZBWU7\Mail delivery
failed_ returning message to sender.txt is infected with the  W32.Badtrans@mm.enc
```

6 www.google.com

```
virus.
The file was quarantined.
Virus scan started.
COMPUTER
marilyn
The file C:\WINDOWS\Temporary Internet Files\Content.IE5\L5YZBWU7\Delivery-Report
(failure).dat is infected wit h the W32.Badtrans@mm.enc virus.
The file was quarantined.
```

Similar entries were also found relating to temporary internet folders ZC4GC6V, EGP73Y04 and C0J2D2DZL. The log revealed more:

```
marilyn
Unable to repair this file.^
The file
C:\recycled\NPROTECT\00000425.DLL
is infected with the W32.Badtrans.B@mm virus.%
C:\recycled\NPROTECT\00000425.DLL
COMPUTER
marilyn
W32.Badtrans.B@mm
Windows Auto-Protect
The file was deleted._
The file
C:\recycled\NPROTECT\00000425.DLL
was infected with the W32.Badtrans.B@mm virus.%
C:\recycled\NPROTECT\00000425.DLL
COMPUTER
marilyn
W32.Badtrans.B@mm
Windows Auto-Protect
Virus scan started.
```

W32.Badtrans.B@mm was not the only infection that Norton had detected:

```
COMPUTER
marilyn
This script was stopped.|
Script Blocking detected suspicious activity.
File: IEXPLORE.EXE
Object: FileSystem Object
Activity: GetSpecialFolder
COMPUTER
marilyn
Virus scan started.
COMPUTER
marilyn

COMPUTER
marilyn
Unable to repair this file.R
The file
C:\My Documents\q216309.exe
is infected with the W32.Gibe@mm virus.
C:\My Documents\q216309.exe
COMPUTER
marilyn
W32.Gibe@mm
Windows Auto-Protect
Unable to repair this file.R
The file
C:\My Documents\q216309.exe
```

```
is infected with the W32.Gibe@mm virus.
C:\My Documents\q216309.exe
COMPUTER
marilyn
W32.Gibe@mm
Windows Auto-Protect
The file was quarantined.S
The file
C:\My Documents\q216309.exe
was infected with the W32.Gibe@mm virus.
C:\My Documents\q216309.exe
COMPUTER
marilyn
W32.Gibe@mm
Windows Auto-Protect
Unable to delete this file.R
The file
C:\My Documents\q216309.exe
is infected with the W32.Gibe@mm virus.
C:\My Documents\q216309.exe
COMPUTER
marilyn
W32.Gibe@mm
Windows Auto-Protect
Unable to quarantine this file.R
The file
C:\My Documents\q216309.exe
is infected with the W32.Gibe@mm virus.
C:\My Documents\q216309.exe
COMPUTER
marilyn
W32.Gibe@mm
Windows Auto-Protect
The file was excluded from future virus checks.
```

O. None of the temporary internet folders referenced in this file were still in existence on the hard disk, even in the unallocated sectors. Research at the Sophos web-site[7] confirms that the W32.Gibe@mm virus was highly prevalent at this time (April 2002) and that the q216309.exe file is the usual infecter. A grep search through the strings extracted from the swapfile revealed:

```
nq216309.exe
q216309.lnk
uments\q216309.exe
gC:\My Documents\q216309.exe
```

xi. Recovery of Deleted data.

A. From the anti-virus software logfile it was known that executable associated with the worm W32.Gibe-A is q216309.exe, so it would assist the investigation to examine this file to ensure that it was indeed this variant that the machine was infected and not a new or custom mutation specifically designed to target this user.

B. Unfortunately, TASK listed this file as deleted but with zero (0) bytes and

7www.sophos.com/virusinfo/analyses/w32gibea.html

therefore could not recover the file. Although the FAT32 filesystem directory remains, the actual physical areas of the disk may have been overwritten.

C. To confirm that recovery of deleted files was possible, the "All deleted files" (see illustration 1) link was selected via TASK and the ascii text of a number of files which had been deleted from the suspect disk viewed. The same result could have been obtained manually using the component commands behind TASK and previously included as part of The Coroners Toolkit (TCT) and TCTutils.

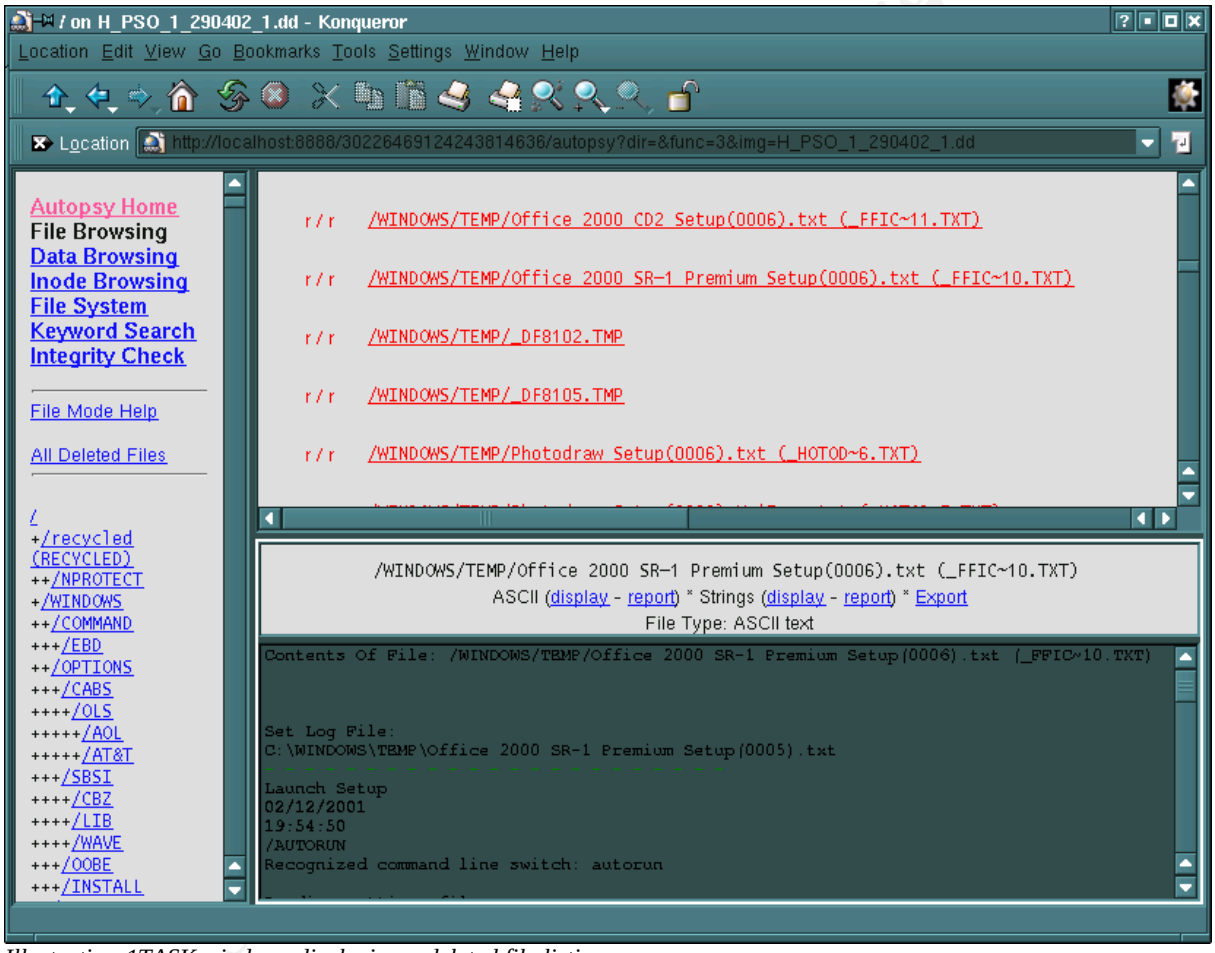


Illustration 1TASK windows displaying a deleted file listing

xii. The Sophos[8] information indicates that W32.Gibe-A usually spreads via e-mail. Therefore it is possible that the message carrying the payload remains in the inbox of the user who received it. Hunting through the mounted loop device filesystem revealed that Microsoft Office 2000 had been installed (the deleted installation logfile recovered earlier as shown in illustration1 confirms

8 http://www.sophos.com/virusinfo/analyses/w32gibea.html

this). It is likely that Outlook or Outlook Express (OE5) was used as the e-mail client. The user confirmed that OE5 was used and so the default location of this application's mailboxes was researched. A useful document[9] explains the typical location. Unlike Windows NT/W2K/XP or Unix systems, Windows 98 has no true concept of individual users. Although people may setup individual accounts on the system, there is no dedicated /etc/passwd file or SAM database which acts as the master repository for user authentication information. However this PC was known to be a multi-user system, primarily for the purposes of e-mail correspondence outside formal company channels. A number of apparently active mailboxes each resident in subdirectories under a tree hierarchy identified by a System ID (SID) relating to each user of the machine were found

```
total 36
drwxr-xr-x    3 root     root         4096 Feb  2  2001 {3790124A-79DF-
4740-96AC-0E68C6EBE1FD}
drwxr-xr-x    3 root     root         4096 Feb  4  2001 {40DD34D6-F459-
4E01-9A36-BEBF81E675B2}
drwxr-xr-x    3 root     root         4096 Apr 17  2001 {560CA6E5-983C-
48BE-BCE7-26E1C6F71A25}
drwxr-xr-x    3 root     root         4096 Dec 20  2000 {62862BFC-AE69-
4208-B2E2-8312627B9956}
drwxr-xr-x    3 root     root         4096 Dec 20  2000 {686CFE2E-3498-
4265-A806-1380F7010C89}
drwxr-xr-x    3 root     root         4096 Aug  2  2000 {71178F04-098D-
49FE-8FD3-5026B89CC982}
drwxr-xr-x    3 root     root         4096 Feb 13  2001 {776D126E-BFCE-
4E58-BCEF-E774EEFF2762}
drwxr-xr-x    3 root     root         4096 Apr 15  2001 {C7496789-B5CE-
4572-AAA4-91D0F8E92E49}
drwxr-xr-x    3 root     root         4096 Nov 26  2000 {E236B507-2893-
4C69-8EEC-8877E5AFA19B}
```

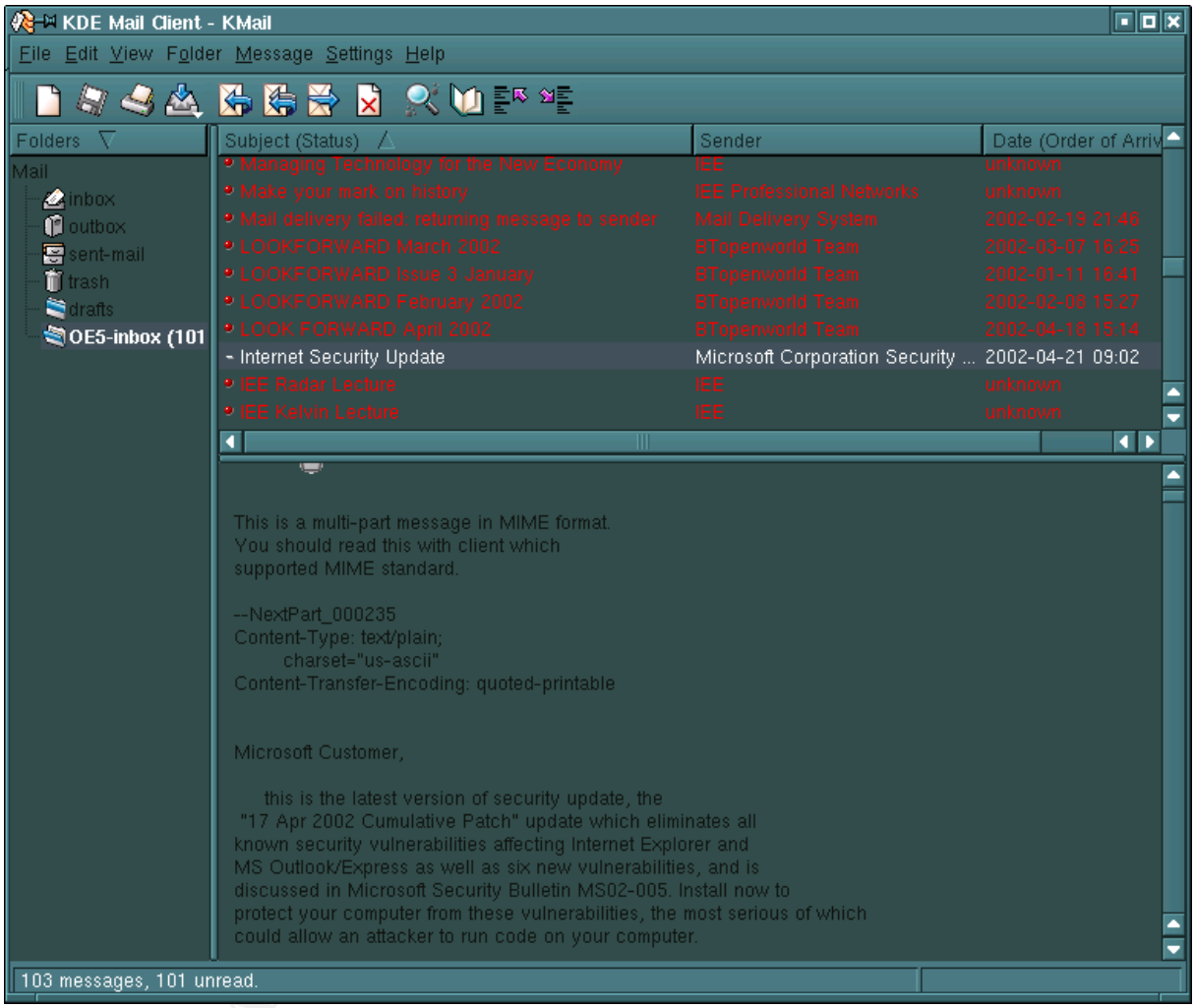
xiii. Fortunately the exact mailbox of interest could be pinpointed by associating real world usernames with their SID. This was performed using Encase to interrogate the registry file (see illustration 3 below). Once the specific mailbox (OE5 stores messages in .dbx files) was known, it was exported from the image via TASK.

```
[Zerot@Anna /mnt/images]$ ls -l /mnt/susp/windows/Application
Data/Identities/{71178F04-098D-49FE-8FD3-5026B89CC982}/Microsoft/Outlook
Express

total 2160
-rwxr-xr-x    1 root     root        44733 Apr 22 03:36 cleanup.log
-rwxr-xr-x    1 root     root        60116 Apr 22 03:36 Deleted Items.dbx
-rwxr-xr-x    1 root     root        60116 Apr 22 03:21 Drafts.dbx
-rwxr-xr-x    1 root     root        74720 Apr 22 03:36 Folders.dbx
-rwxr-xr-x    1 root     root      1346416 Apr 22 23:17 Inbox.dbx
-rwxr-xr-x    1 root     root         9656 Apr 22 03:36 Offline.dbx
-rwxr-xr-x    1 root     root       191188 Apr 22 23:17 Outbox.dbx
-rwxr-xr-x    1 root     root         9404 Apr 22 03:36 Pop3uidl.dbx
-rwxr-xr-x    1 root     root        39344 Apr 22 03:25 Sent Items.dbx
```

9 mailservices.web.cern.ch/MailServices/docs/clients/outlook -express/configuration.html

xiv. KDE's Kmail client has the ability to import dbx mailboxes so this application was used to view the mailbox. Scrolling through the messages, the subject line reported by Sophos could quickly be found. The extracted text of this message is included as Appendix D.



xv. At this stage the morgue directory to view the files created as part of the analysis process was examined. To ensure the integrity of the investigation if the data was subsequently re-visited, it was necessary to calculate md5 checksums for each of these component files, either through the TASK interface or via the command line. For storage purposes an individual checksum was calculated for each file and this information added to the morgue directory in a text file. Another checksum was taken for the whole directory which was then added to a tar archive along with the morgue directory contents. This archive was then compressed and yet another

checksum calculated for this file. The tar.gz file was finally written to backup medium (a DLT) and the checksum value recorded in a hardcopy log book.

```
total 17352356

-rw-r--r--    1 root     root          627 Jun 28 12:41 fsmorgue
-rw-r--r--    1 root     root     3085459222 May  2 18:37
H_PSO_1_020502.dd.gz
-rw-r--r--    1 root     root      9685785 Jun 28 10:58
H_PSO_1_290402_1.body
-rw-r--r--    1 root     root     7996874752 Jun 27 23:08
H_PSO_1_290402_1.dd
-rw-r--r--    1 root     root     3043557586 Jun 28 16:14
H_PSO_1_290402_1.dd.str
-rw-r--r--    1 root     root     37607881 Jun 28 17:52
H_PSO_1_290402_1.swp.str
-rw-r--r--    1 root     root     25265893 Jun 28 12:25 H_PSO_1_290402_1.tl
-rw-r--r--    1 root     root        33054 Jun 28 12:40
H_PSO_1_290402_5.body
-rw-r--r--    1 root     root     200500019 2 Jun 27 22:56
H_PSO_1_290402_5.dd
-rw-r--r--    1 root     root         3765 Jun 28 12:41 H_PSO_1_290402_5.tl
drwxr-xr-x    2 root     root         4096 May 30 17:37 lost+found
-rw-r--r--    1 root     root           44 Jun 27 22:49 md5_1
-rw-r--r--    1 root     root           66 Jun 27 23:23 md5_1_copy
-rw-r--r--    1 root     root           44 Jun 27 22:53 md5_5
-rw-r--r--    1 root     root           66 Jun 27 23:11 md5_5_copy
-rw-r--r--    1 root     root           43 Jun 27 22:34 md5_all
-rw-r--r--    1 root     root           66 Jun 27 23:51 md5_all_copy
```

MD5 hashes:

```
d5cc9933b466b42bbcc95b0882047bd0  H_PSO_1_290402_1.body
601899fccd63ee731ac93aa78ab97b61  H_PSO_1_290402_1.dd
fcc8de36455ee5ce2e9efc408fe5485d  H_PSO_1_290402_1.dd.str
9119cc4bd4762ca64 904a97aa24d5584  H_PSO_1_290402_1.swp.str
09e7d0a843e0ae6d8bdbfd58ebe827f1  H_PSO_1_290402_1.tl
525a0b96b479d21aa2ef226dd1584dd1  H_PSO_1_290402_5.body
57a57136e3c4e83105a2420574135193  H_PSO_1_290402_5.dd
7de46f08ebde62c7e9189e758e4030f8  H_PSO_1_290402_5 .tl
```

(b)Encase

i. Encase is the market leading forensic software with a good track record with Law Enforcement cases worldwide. This widespread adoption of the software by the computer forensics community serves as a crucial factor for authentication of Encase evidence. It is excellent for cases involving graphical evidence and provides a number of automated processes to assist the analyst when dealing with large disk images. It is especially well-suited to dealing with Microsoft Windows PCs.

ii. Once again version 3.15A was used, but this time in full analysis mode, having booted from a Windows 98(SE) disk. A second hard disk containing the image created earlier was accessed through the second IDE bay. In

order to read and write to ext2 filesystems, Paragon Ext2 Anywhere[10] V2.5 software was used.

iii. A new case H_PSO_290402.cas was opened and the previously created (by Encase in 3.b.iv above) image file added to this case. The software automatically begins comparing the checksum calculated at the time of imaging with the current state of the image. This process continues in the background each time a case is opened unless manually canceled by the examiner.

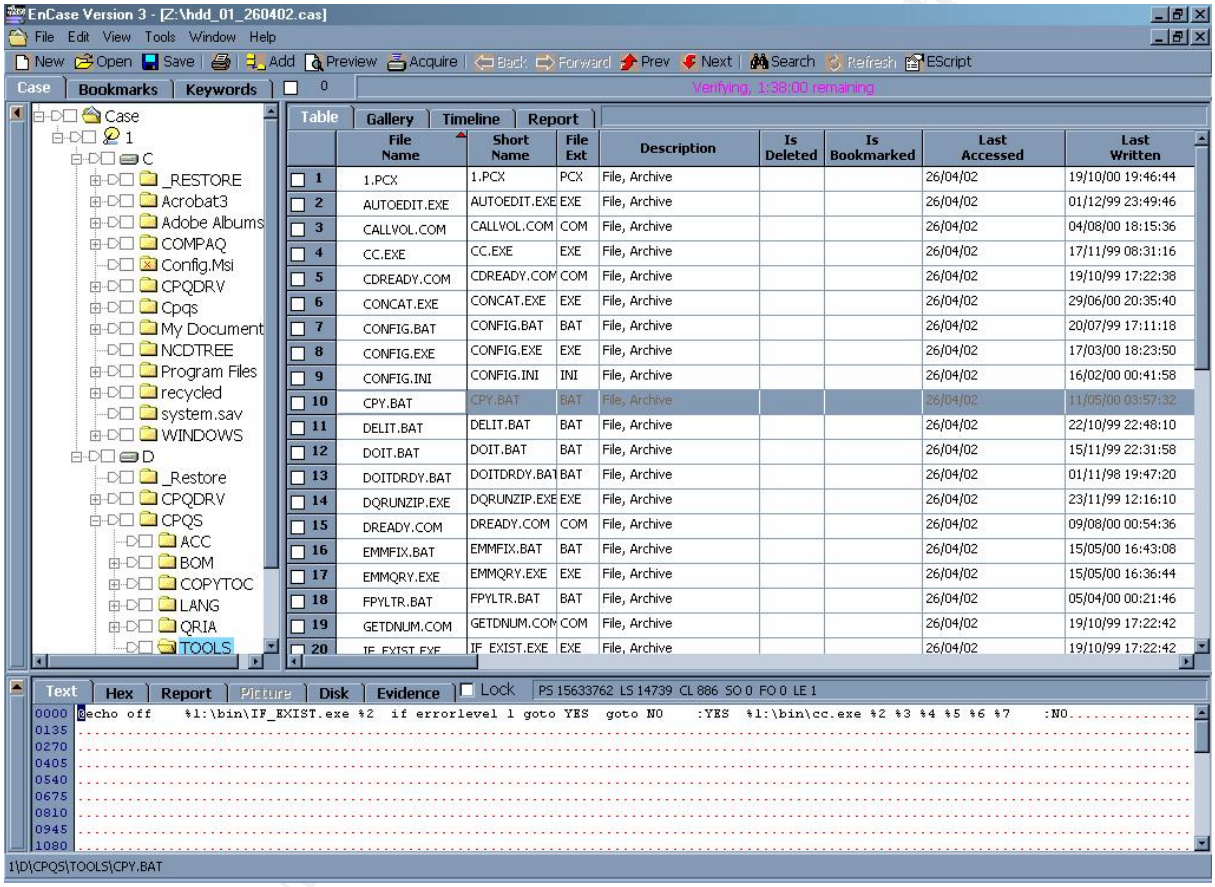


Illustration 2Encase verifying hash of image file.

iv. As already discovered using fdisk as part of the dd imaging process, the disk consisted of 3 partitions, a FAT32 primary and an extended partition containing only another single FAT32 partition. These are shown in the right-hand Encase frame of illustration 2 as C and D drives. Typically Compaq Pcs, such as the one being analysed are sold with the home user market in mind and have the operating system partially pre-loaded. The smaller disk partition contained remnant information from this process which can be re-used in the event of system problems and the need to restore the configuration using the supplied recovery CD.

10 www.partition-manager.com/n_ext2fs_main.htm

v.Concentrating on the larger partition, it had already been established from the swap-file searching carried out under Linux analysis that the infected executable had, at some point, been resident in the “My Documents” directory. Encase should display any deleted files which it can establish were previously stored on the disk, however just like TASK, it could not retrieve q216309.exe.

vi.In order to correlate activity and file ownership with particular people, it is helpful to associate specific Microsoft Windows SIDs with particular members of the department and users of the PC. This mapping information is contained within the registry. Fortunately Encase is able to interrogate windows registry “databases” (in this case user.dat) directly (right-click on the file and select “view file structure”). The mapping values were then found under the SID sub-key, under the Identities key. Note this same technique can be used with OE5 mailboxes and was carried out on all mailboxes found (see 3.a.xiii).

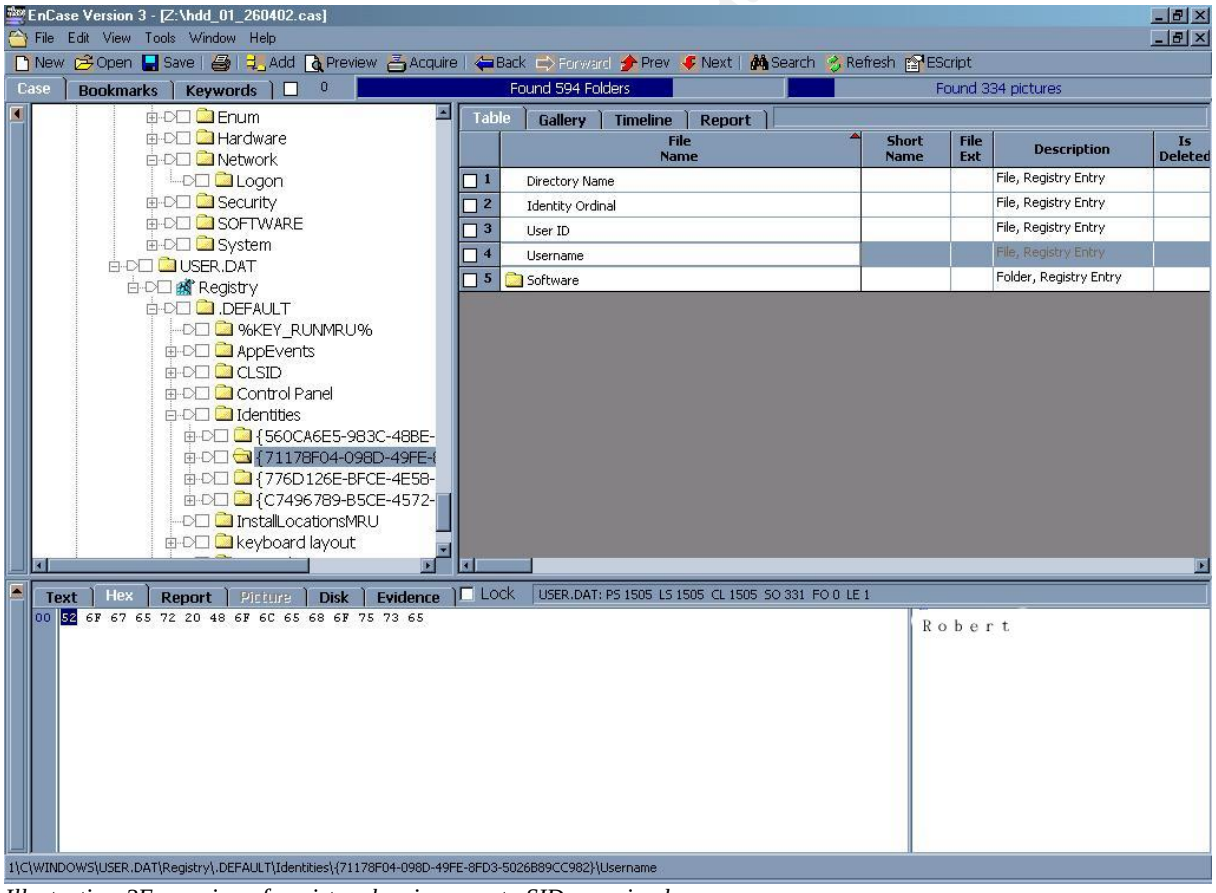


Illustration 3Expansion of registry showing user to SID mapping key

(b)Recovery of Deleted data.

xi.Encase allows the recovery of deleted folders via the GUI. This process

trawls through the unallocated clusters of an evidence file looking for the "..”" string which indicates the existence of a previously deleted folder. Although it will not recover the folder name, it should recover the contents (ie: files and other directories) . Once found, the software rebuilds the folder and adds it to the evidence case file. Running against the entire image, Encase found and retrieved 647 deleted folders.

xii. Encase also has its own programming language allowing the analyst to create scripts to automate various forensic tasks. One such script trawls the image searching for temporary internet files and folders. The results of running the Internet History Parser are shown in the table below. This index html file was created with each link pointing to a recovered cache or cookie index file. By scrutinising these files it was possible to construct a profile of the surfing habits of the user of the machine.

1	1\C\WINDOWS\Cookies\index.dat
2	1\C\WINDOWS\History\History.IE5\MSHist012001020520010206\index.dat
3	1\C\WINDOWS\History\History.IE5\MSHist012002040120020408\index.dat
4	1\C\WINDOWS\History\History.IE5\MSHist012002040820020415\index.dat
5	1\C\WINDOWS\History\History.IE5\MSHist012002041520020422\index.dat
6	1\C\WINDOWS\History\History.IE5\MSHist012002042220020423\index.dat
7	1\C\WINDOWS\History\History.IE5\MSHist012002042520020426\index.dat
8	1\C\WINDOWS\History\History.IE5\MSHist012002042620020427\index.dat
9	1\C\WINDOWS\History\History.IE5\index.dat
10	1\C\WINDOWS\Profiles\marilyn\Cookies\index.dat
11	1\C\WINDOWS\Profiles\marilyn\History\History.IE5\MSHist012001020520010206\index.dat
12	1\C\WINDOWS\Profiles\marilyn\History\History.IE5\MSHist012001020520010212\index.dat
13	1\C\WINDOWS\Profiles\marilyn\History\History.IE5\MSHist012001021220010219\index.dat
14	1\C\WINDOWS\Profiles\marilyn\History\History.IE5\MSHist012001021920010226\index.dat
15	1\C\WINDOWS\Profiles\marilyn\History\History.IE5\MSHist012001022620010227\index.dat
16	1\C\WINDOWS\Profiles\marilyn\History\History.IE5\MSHist012001022720010228\index.dat
17	1\C\WINDOWS\Profiles\marilyn\History\History.IE5\MSHist012001022820010301\index.dat
18	1\C\WINDOWS\Profiles\marilyn\History\History.IE5\MSHist012001030420010305\index.dat
19	1\C\WINDOWS\Profiles\marilyn\History\History.IE5\MSHist012001032420010325\index.dat
20	1\C\WINDOWS\Profiles\marilyn\History\History.IE5\index.dat
21	1\C\WINDOWS\Profiles\robert\Cookies\index.dat
22	1\C\WINDOWS\Profiles\robert\History\History.IE5\MSHist012001020520010206\index.dat
23	1\C\WINDOWS\Profiles\robert\History\History.IE5\MSHist012001020520010212\index.dat
24	1\C\WINDOWS\Profiles\robert\History\History.IE5\MSHist012001021220010219\index.dat
25	1\C\WINDOWS\Profiles\robert\History\History.IE5\MSHist012001021920010226\index.dat
26	1\C\WINDOWS\Profiles\robert\History\History.IE5\MSHist012001022620010227\index.dat
27	1\C\WINDOWS\Profiles\robert\History\History.IE5\MSHist012001022620010305\index.dat
28	1\C\WINDOWS\Profiles\robert\History\History.IE5\MSHist012001022720010228\index.dat
29	1\C\WINDOWS\Profiles\robert\History\History.IE5\MSHist012001022820010301\index.dat
30	1\C\WINDOWS\Profiles\robert\History\History.IE5\MSHist012001030520010312\index.dat
31	1\C\WINDOWS\Profiles\robert\History\History.IE5\MSHist012001031220010319\index.dat
32	1\C\WINDOWS\Profiles\robert\History\History.IE5\MSHist012001031920010320\index.dat
33	1\C\WINDOWS\Profiles\robert\History\History.IE5\MSHist012001032020010321\index.dat
34	1\C\WINDOWS\Profiles\robert\History\History.IE5\MSHist012001032120010322\index.dat
35	1\C\WINDOWS\Profiles\robert\History\History.IE5\MSHist012001032220010323\index.dat
36	1\C\WINDOWS\Profiles\robert\History\History.IE5\MSHist012001032420010325\index.dat
37	1\C\WINDOWS\Profiles\robert\History\History.IE5\index.dat
38	1\C\WINDOWS\Temporary Internet Files\Content.IE5\index.dat

xiii. In this case it was established that the most frequently visited sites included

Gartner[11], Microsoft[12], Apple[13], BBC[14] and Google[15]. Robert and Marilyn were the only users whose profiles contained specific internet history files.

xiv. In order to search for evidence of the W32.Gibe virus a keyword list relating to the files normally associated with infection from this malicious software was created:

gfxacc.exe
bctool.exe
q216309.exe
winnetw.exe
02_n802.dat

xv. Variations of these filenames (for example, omitting the first character or without the extension) were also added to the keyword list. The Encase GUI was then used to activate a search, ensuring the "unallocated sectors" and "file slack space" boxes were checked. Only the actual dropper executable itself yielded any (92) hits. Some of the interesting results are shown below. The references to the file in the swap file, user OE5 mailbox and Norton activity log already described were, as expected, also found by Encase.

```
Hit Text   File Name  Is Deleted Physical Location    Full Path
216309     WIN386.SWP           PS:41330, SO:509: LE:6
           1\C\WIN386.SWP

216309     Unallocated Clusters          PS:245959, SO:173: LE:6
           1\C\Unallocated Clusters
216309     Unallocated Clusters          PS:245959, SO:497: LE:6
           1\C\Unallocated Clusters

216309     Orienteering.dat              PS:244308, SO:479: LE:6
           1\C\WINDOWS\Temporary Internet
Files\Content.IE5\W12FWT6B\Orienteering.dat
216309     Orienteering.dat              PS:244310, SO:182: LE:6
           1\C\WINDOWS\Temporary Internet
Files\Content.IE5\W12FWT6B\Orienteering.dat
216309     Orienteering.dat              PS:244310, SO:276: LE:6
           1\C\WINDOWS\Temporary Internet
Files\Content.IE5\W12FWT6B\Orienteering.dat
216309     Internet Security Update.dat             PS:244331, SO:257: LE:6
           1\C\WINDOWS\Temporary Internet
Files\Content.IE5\W12FWT6B\Internet Security Update.dat

216309     Internet Security Update (1).dat                    PS:244339,
SO:257: LE:6         1\C\WINDOWS\Temporary Internet
Files\Content.IE5\W12FWT6B\Internet Security Update (1).dat
216309     16C44529.exe                  PS:245447, SO:429: LE:6
           1\C\Program Files\Norton SystemWorks\Norton
```

11 www3.gartner.com/Init
12 www.microsoft.com
13 www.apple.com/creative
14 www.bbc.co.uk/news
15 www.google.com

AntiVirus\Quarantine\16C44529.exe

```
216309     _0008092.EXE          •          PS:245671, SO:341: LE:6
           1\C\recycled\NPROTECT\_0008092.EXE
216309     _0008091.EXE          •          PS:245935, SO:341: LE:6
           1\C\recycled\NPROTECT\_0008091.EXE
216309     Inbox.dbx             PS:6897408, SO:463: LE:6
           1\C\WINDOWS\Application Data\Identities\{71178F04-098D-49FE-8FD3-
5026B89CC982}\Microsoft\Outlook Express\Inbox.dbx
216309     Inbox.dbx             PS:6897410, SO:198: LE:6
           1\C\WINDOWS\Application Data\Identities\{71178F04-098D-49FE-8FD3-
5026B89CC982}\Microsoft\Outlook Express\Inbox.dbx
216309     Inbox.dbx             PS:6897410, SO:292: LE:6
           1\C\WINDOWS\Application Data\Identities\{71178F04-098D-49FE-8FD3-
5026B89CC982}\Microsoft\Outlook Express\Inbox.dbx
216309     USER.DAT              PS:290269, SO:147: LE:6
           1\C\WINDOWS\USER.DAT
216309     USER.DAT              PS:290271, SO:40: LE:6
           1\C\WINDOWS\USER.DAT
216309     USER.DAT              PS:293131, SO:29: LE:6
           1\C\WINDOWS\USER.DAT
216309     USER.DAT              PS:293131, SO:55: LE:6
           1\C\WINDOWS\USER.DAT
216309     My Documents                     PS:4121847, SO:161: LE:6
           1\C\My Documents
216309     recent                PS:4122037, SO:65: LE:6
           1\C\WINDOWS\recent
216309     vxdsfp.log            PS:4255539, SO:233: LE:6
           1\C\_RESTORE\LOGS\vxdsfp.log
216309     Activity.log                     PS:4854808, SO:491: LE:6
           1\C\Program Files\Norton SystemWorks\Norton
AntiVirus\Activity.log
216309     Activity.log                     PS:4854809, SO:51: LE:6
           1\C\Program Files\Norton SystemWorks\Norton
AntiVirus\Activity.log

216309     Unallocated Clusters             PS:1564, SO:29: LE:6
           1\C\WINDOWS\USER.DAT\Registry\Unallocated Clusters
216309     Unallocated Clusters             PS:1564, SO:55: LE:6
           1\C\WINDOWS\USER.DAT\Registry\Unallocated Clusters
216309     g                     PS:422, SO:147: LE:6
           1\C\WINDOWS\USER.DAT\Registry\.DEFAULT\Software\Microsoft\Windows
\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\•\g
216309     h                     PS:424, SO:40: LE:6
           1\C\WINDOWS\USER.DAT\Registry\.DEFAULT\Software\Microsoft\Windows
\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\EXE\h


216309     Internet Security Update                  PS:1078127, SO:0: LE:6
           1\C\WINDOWS\Application Data\Identities\{71178F04-098D-49FE-8FD3-
5026B89CC982}\Microsoft\Outlook Express\Inbox.dbx\DBX Volume\Internet
Security Update
216309     Internet Security Update                  PS:1078854, SO:0: LE:6
           1\C\WINDOWS\Application Data\Identities\{71178F04-098D-49FE-8FD3-
5026B89CC982}\Microsoft\Outlook Express\Inbox.dbx\DBX Volume\Internet
Security Update
216309     Internet Security Update                  PS:1078948, SO:0: LE:6
           1\C\WINDOWS\Application Data\Identities\{71178F04-098D-49FE-8FD3-
5026B89CC982}\Microsoft\Outlook Express\Inbox.dbx\DBX Volume\Internet
Security Update
```

xvi. Of particular interest was the file reported in the Norton quarantine area. It appears that the anti-virus software was successful in detecting and preserving the worm executable. The top few lines of this (binary) file confirm this:

```
Í ªª
ý¿@§`
16C44529.exe
C:\My Documents\q216309.exe
marilyn
COMPUTER
W32.Gibe@mm
ö¿4øf
```

xvii. Encase contains a database of file signatures. System files contained within the image file can be compared to these fingerprints to detect possibly subverted or trojanised files, or those renamed to conceal illicit activity. Having run the comparison process against this image, no inexplicable mismatches were detected.

(c)Diskedit

i. Norton's Diskedit has been a staple tool of forensic analysts since the infancy of the science. One drawback is that the software works on real, physical disks although it does enable the analyst to examine the disk at the lowest possible software level. Therefore a working copy (WC) must be created for use with Diskedit. In this case, the "restore disk" functionality of Encase was used to re-create the suspect disk on a new disk (verified as clean using the steps described in 3.a.iv above. The WC disk is then replaced into the imaging machine and interrogated under Linux. The integrity is verified using md5sum:

```
madge# md5sum /dev/hdc

  c62e6ec989080a735e3fc5f5e9858dd4  /dev/hdc
```

ii. Back at the analysis machine, the WC disk was inserted and the PC booted from the Norton utilities CD containing the latest version of Diskedit. Initially the Boot sector of the disk was displayed as shown in Appendix C. The partition table (c.f: the data from fdisk) is shown below:

```
Physical Sector: Absolute Sector 0
+------+----+-------------------+-------------------+-----------+-----------+
|      |    | Starting Location |  Ending Location  |  Relat ive | Number of |
|System|Boot|Side Cylinder Sector|Side Cylinder Sector|  Sectors  |  Sectors  |
+------+----+-------------------+-------------------+-----------+-----------+
|FAT32x| Yes|   1      0       1  | 239   1023      63  |        63|  15618897  |
|EXTNDx| No |   0   1023       1  | 239   1023      63  |  15618960|   3916080|
|unused| No |   0      0       0  |   0      0       0  |         0|         0|
|unused| No |   0      0       0  |   0      0       0  |         0|         0|
+------+----+-------------------+-------------------+-----------+-----------+
```

iii. Intrigued by the references to `C\recycled\NPROTECT\_0008092.EXE` and `\_0008091.EXE` revealed by the Encase keyword, Diskedit was used to attempt to recover the files along with q216309.exe. Diskedit was first used to display the "My Documents" directory where the remains of this latter file can be seen. Note that the first character of the filename "q" has been replaced by 0xE5 indicating to the windows operating system that this 32 byte directory entry is available for re-use. This is the only modification made to the entry. Any directory listing (either at the command line or via Explorer) under Windows will not show any trace of such files, even though the data contents may still reside on the disk.

```
Physical Sector: Absolute Sector 4,121,847
00000000: 2E 20 20 20 20 20 20 20   - 20 20 20 10 00 AF E4 5B   .          ....[
00000010: 02 29 02 29 07 00 E5 5B   - 02 29 B7 CD 00 00 00 00   .).)...[ .).....
00000020: 2E 2E 20 20 20 20 20 20   - 20 20 20 10 00 AF E4 5B   ..         ....[
00000030: 02 29 02 29 00 00 E5 5B   - 02 29 00 00 00 00 00 00   .).)...[.).....
00000040: 41 54 00 69 00 6D 00 27   - 00 73 00 0F 00 42 20 00   AT.i.m.'.s...B .
00000050: 4D 00 75 00 73 00 69 00   - 63 00 00 00 00 00 FF FF   M.u.s.i.c.......
00000060: 54 49 4D 27 53 4D 7E 31   - 20 20 20 10 00 20 38 5C   TIM'SM~1   .. 8 \
00000070: 02 29 02 29 07 00 39 5C   - 02 29 05 CF 00 00 00 00   .).)..9 \.).....
00000080: E5 71 00 32 0 0 31 00 36  - 00 33 00 0F 00 AB 30 00   .q.2.1.6.3....0.
00000090: 39 00 2E 00 65 00 78 00   - 65 00 00 00 00 00 FF FF   9...e.x.e.......
000000A0: E5 32 31 36 33 30 39 20   - 45 58 45 20 00 8B B4 AE   .216309 EXE  ....
000000B0: 95 2C 95 2C 00 00 E1 AE   - 95 2C 00 00 00 00 00 00   .,.,.....,......
000000C0: 41 43 00 43 00 57 00 69   - 00 6E 00 0F 00 7B 39 00   AC.C.W.i.n...{9.
000000D0: 00 00 FF FF FF FF FF FF   - FF FF 00 00 FF FF FF FF   ................
000000E0: 43 43 57 49 4E 39 20 20   - 20 20 20 10 00 28 E1 98   CCWIN9     ..(..
000000F0: 59 2A 59 2A 07 00 E2 98   - 59 2A 06 CF 00 00 00 00   Y*Y*....Y*......
00000100: 42 54 00 49 00 4F 00 4E   - 00 00 00 0F 00 5A FF FF   BT.I.O.N.....Z..
00000110: FF FF FF FF FF FF FF FF   - FF FF 00 00 FF FF FF FF   ........ ........
00000120: 01 48 00 45 00 41 00 54   - 00 49 00 0F 00 5A 4E 00   .H.E.A.T.I...ZN.
00000130: 47 00 20 00 51 00 55 00   - 4F 00 00 00 00 54 00 41   G. .Q.U.O...T.A.
00000140: 48 45 41 54 49 4E 7E 31   - 20 20 20 10 00 C6 A3 7C   HEATIN~1   ....|
00000150: 35 2A 35 2A 07 00 A4 7C   - 35 2A 07 CF 00 00 00 00   5*5*...|5*......
00000160: 41 4F 00 75 00 72 00 20   - 00 57 00 0F 00 E8 65 00   AO.u.r. .W....e.
00000170: 62 00 73 00 00 00 FF FF   - FF FF 00 00 FF FF FF FF   b.s.............
00000180: 4F 55 52 57 4 5 42 7E 31  - 20 20 20 10 00 0F 27 5D   OURWEB~1   ...']
00000190: 9C 2A 9C 2A 07 00 28 5D   - 9C 2A 08 CF 00 00 00 00   .*.*..(].*......
000001A0: 42 6C 00 65 00 73 00 00   - 00 FF FF 0F 00 5F FF FF   Bl.e.s......._..
000001B0: FF FF FF FF FF FF FF FF   - FF FF 00 00 FF FF FF FF   ................
000001C0: 01 43 00 6F 00 72 00 65   - 00 6C 00 0F 00 5F 20 00   .C.o.r.e.l..._ .
000001D0: 55 00 73 00 65 00 72 00   - 20 00 00 00 46 00 69 00   U.s.e.r. ...F.i.
000001E0: 43 4F 52 45 4C 55 7E 31   - 20 20 20 10 00 A5 11 99   CORELU~1   .....
000001F0: 59 2A 59 2A 07 00 12 99   - 59 2A 09 CF 00 00 00 00   Y*Y*....Y*......
```

iv. Changing to Directory view in Diskedit revealed that this file is gone for good. No file size could be reported, but more importantly no starting cluster was available. Presumably, this is why Encase does not even list this as a deleted file (although it does report the presence of the text string in unallocated sectors).

```
Physical Sector: Absolute Sector 4,121,847
Name     .Ext ID         Size      Date      Time    Cluster    76 A R S H D V
-------------------------------------------------------------------------------
.             Dir            0   8 -02-00  11:31 am      52663      - - - - D -
..            Dir            0   8 -02-00  11:31 am          0      - - - - D -
Tim's Music   LFN                                           0      - R S H - V
TIM'SM~1      Dir            0   8 -02-00  11:33 am      52997      - - - - D -
```

```
q216309.exe    Del LFN                                          0       - R S H - V
å216309  EXE   Erased        0   4 -21-02   9:55 pm           0      A  - - - - - -
CCWin9         LFN                                            0       - R S H - V
CCWIN9         Dir           0   2 -25-01   7:07 pm       52998       - - - - D -
TION           LFN                                            0       - R S H - V
HEATING QUOTA LFN                                             0       - R S H - V
HEATIN~1       Dir           0   1 -21-01   3:37 pm       52999       - - - - D -
Our Webs       LFN                                            0       - R S H - V
OURWEB~1       Dir           0   4 -28-01  11:41 am       53000       - - - - D -
les            LFN                                            0       - R S H - V
Corel User Fi LFN                                             0       - R S H - V
CORELU~1       Dir           0   2 -25-01   7:08 pm       53001       - - - - D -
```

v. Turning to the C:\recycled\nprotect directory:

```
Cluster 511,446, Sector 4,122,039
00000000: E5 30 30 30 38  30 38 32   - 44 41 54 00 00 30 CC A2   .0008082DAT..0..
00000010: 8B 2C 9A 2C 00 00 00 48   - 8A 2C 86 4A 52 13 01 00   .,.,...H.,.JR...
00000020: E5 30 30 30 38 30 38 33   - 44 41 54 00 00 7F CC A2   .0008083DAT.. ..
00000030: 8B 2C 9A 2C 00 00 00 48   - 8A 2C C4 4C AF E7 06 00   .,.,...H.,.L....
00000040: E5 30 30 30 38 30 38 34   - 44 41 54 00 00 7D CD A2   .0008084DAT..}..
00000050: 8B 2C 9A 2C 00 00 00 48   - 8A 2C 2A 89 EF 25 06 00   .,.,...H.,*..%..
00000060: E5 30 30 30 38 30 38 35   - 49 4E 46 00 00 4A CE  A2   .0008085INF..J..
00000070: 8B 2C 9A 2C 00 00 00 48   - 8A 2C 46 6E FC 9E 01 00   .,.,...H.,Fn....
00000080: E5 30 30 30 38 30 38 36   - 54 58 54 00 00 7B CE A2   .0008086TXT..{..
00000090: 8B 2C 9A 2C 00 00 00 48   - 8A 2C 44 6F A8 7A 00 00   .,.,...H., Do.z..
000000A0: E5 30 30 30 38 30 38 37   - 54 58 54 00 00 86 CE A2   .0008087TXT.....
000000B0: 8B 2C 9A 2C 00 00 00 48   - 8A 2C 4C 6F 4F 19 00 00   .,.,...H.,LoO...
000000C0: E5 30 30 30 38 30 38 38   - 54 58 54 00 00 A2 CE A2   .0008088TXT.....
000000D0:  8B 2C 9A 2C 00 00 00 48   - 8A 2C 4E 6F 70 14 00 00   .,.,...H.,Nop...
000000E0: E5 30 30 30 38 30 38 39   - 44 41 54 00 00 29 CF A2   .0008089DAT..)..
000000F0: 8B 2C 9A 2C 00 00 00 48   - 8A 2C 62 6F 94 00 00 00   .,.,...H.,bo....
00000100: E5 30 30 30 38  30 39 30   - 44 41 54 00 00 39 CF A2   .0008090DAT..9..
00000110: 8B 2C 9A 2C 00 00 00 48   - 8A 2C 64 6F A4 24 00 00   .,.,...H.,do.$..
00000120: E5 30 30 30 38 30 39 31   - 45 58 45 20 00 98 B4 AE   .0008091EXE  ....
00000130: 95 2C 9A 2C 00 00 B5 AE   - 95 2C 2E 69 40 FF 01 00   .,.,.....,.i@...
00000140: E5 30 30 30 38 30 39 32   - 45 58 45 20 00 9D B4 AE   .0008092EXE ....
00000150: 95 2C 9A 2C 00 00 B5 AE   - 95 2C 0D 69 40 FF 01 00   .,.,.....,.i@...
00000160: E5 30 30 30 38 30 39 33   - 44 41 54 20 00 00 24  5F   .0008093DAT ..$_
00000170: CC 2A 9A 2C 00 00 24 5F   - CC 2A 75 B0 4C 00 00 00   .*.,..$_.*u.L...
00000180: E5 30 30 30 38 30 39 34   - 48 54 54 26 00 70 73 AE   .0008094HTT&.ps.
00000190: 95 2C 9A 2C 00 00 74 AE   - 95 2C 10 69 1E 0A 00 00   .,.,..t.., .i....
000001A0: E5 30 30 30 38 30 39 35   - 4C 44 42 20 00 20 5B AF   .0008095LDB . [.
000001B0: 95 2C 9A 2C 00 00 60 AF   - 95 2C 60 68 40 00 00 00   .,.,..`..,`h@...
000001C0: E5 30 30 30 38 30 39 36   - 48 54 54 26 00 6C 46 AF   .0008096HTT&.lF.
000001D0:  95 2C 9A 2C 00 00 47 AF   - 95 2C D7 60 1E 0A 00 00   .,.,..G..,.`....
000001E0: E5 30 30 30 38 30 39 37   - 48 54 54 26 00 AB 78 B0   .0008097HTT&..x.
000001F0: 95 2C 9A 2C 00 00 79 B0   - 95 2C B7 60 F4 10 00 00    .,.,..y..,.`....
```

vi. Starting with 00008091.exe, the starting cluster for both files was determined from the Diskedit directory view: 26926 and 26893

```
Cluster 511,446, Sector 4,122,039
Name     .Ext ID        Size      Date      Time    Cluster    76 A R S H  D
V
-------------------------------------------------------------------------
----
å0008091 EXE  Erased    130880   4 -21-02   9:53 pm      26926     A - - - -
-
å0008092 EXE  Erased    130880   4 -21-02   9:53 pm      26893     A - - - -
```

vii. The clusters around 26926 & 26893 were then selected for inspection from within the File Allocation Table (FAT) on the disk. When a file has been deleted, the FAT entry is zeroed out to indicate that this cluster is available for use.

```
Sector 242
Clusters 26,882 - 27,007
 [ 0]     26881    [ 0]     26882    [ 0]     26883    [ 0]     26884
 [ 0]     26885    [ 0]     26886    [ 0]     26887    [ 0]     26888
 [ 0]     26889    [ 0]     26890    [ 0]     26891    [ 0]     26892
 [ 0]     26897    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]     26898    [ 0]     26899    [ 0]     26900
 [ 0]     <EOF>    [ 0]     <EOF>    [ 0]     <EOF>    [ 0]     <EOF>
 [ 0]     <EOF>    [ 0]     <EOF>    [ 0]     26943    [ 0]     <EOF>
 [ 0]     26909    [ 0]     26910    [ 0]     26911    [ 0]     26912
 [ 0]     26913    [ 0]     26914    [ 0]     26915    [ 0]     26916
 [ 0]     26917    [ 0]     26918    [ 0]     26919    [ 0]     26920
 [ 0]     26921    [ 0]     26922    [ 0]     26923    [ 0]     <EOF>
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]    796133    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]     26944
 [ 0]     26947    [ 0]         0    [ 0]         0    [ 0]     27102
 [ 0]         0    [ 0]     <EOF>    [ 0]     26951    [ 0]     26952
 [ 0]     26953    [ 0]     26954    [ 0]     26955    [ 0]     26956
 [ 0]     26957    [ 0]     <EOF>    [ 0]     27122    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0

Sector 243
Clusters 27,010 - 27,135
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
 [ 0]         0    [ 0]         0    [ 0]         0    [ 0]         0
```

```
[ 0]          0    [ 0]          0    [ 0]          0    [ 0]          0
[ 0]          0    [ 0]          0    [ 0]          0    [ 0]          0
[ 0]          0    [ 0]          0    [ 0]          0    [ 0]          0
[ 0]          0    [ 0]          0    [ 0]          0    [ 0]          0
[ 0]          0    [ 0]          0    [ 0]          0    [ 0]          0
[ 0]          0    [ 0]          0    [ 0]          0    [ 0]          0
[ 0]          0    [ 0]          0    [  0]         0    [ 0]          0
[ 0]          0    [ 0]          0    [ 0]          0    [ 0]          0
[ 0]      <EOF>    [ 0]          0    [ 0]      27103    [ 0]      27778
[ 0]      27105    [ 0]      27106    [ 0]      27107    [ 0]      27108
[ 0]      27109    [ 0]      27110    [ 0]      27111    [ 0]      27112
[ 0]      27113    [ 0]      27149    [ 0]          0    [ 0]          0
[ 0]          0    [ 0]          0    [ 0]          0    [ 0]          0
[ 0]          0    [ 0]          0    [ 0 ]     27123    [ 0]      27124
[ 0]      27125    [ 0]      27126    [ 0]      27127    [ 0]      27128
[ 0]      27129    [ 0]      27130    [ 0]      27131    [ 0]      27132
[ 0]      27133    [ 0]      27134    [ 0]      27140    [ 0]      27136
```

viii. When recovering files, it is necessary to replace the 0xE5 in the directory entry with a valid character. Following the Encase convention an underscore (_) 0x2D was used as the replacement. Next, the FAT must be modified. Because the file size was 130880 for both files, this means that 130880/512= 255.625 -> 256 clusters[16]. These clusters must now be chained together in the FAT so that the file data is in the proper sequence. This is a tedious manual process! Each cluster in the chain must point to the next until the final cluster is reached. The final cluster should be changed to an E for the End of File Marker (EOF).

ix. Initially it was assumed that the clusters were relatively contiguous. However, as can be seen by the FAT clusters displayed above, other file data must be interspersed with the two executables, including each other!

x. Tools such as Encase and Norton's Unerase can quickly chain the FAT for long files, however the software has no method of establishing for certain which clusters must be included if the data occupies a non-contiguous region. The tool will search and allocate unallocated clusters until the quota needed for the file is reached. Both of the applications mentioned were used in an attempt to restore the files, but neither was able to restore a functional executable. The manual method, selecting different clusters at other file boundaries, was then tried but time constraints prohibited a prolonged attempt. This is especially difficult when dealing with a binary file - files containing a reasonable amount of textual information are easier as clues can be found by examining data contained within the clusters and matching up sentences which overspill from one cluster to the next in the chain.

4. Conclusions.

The machine under examination was a Windows 98 PC primarily used for internet research and e-mail correspondence in connection with project support work. The

16 512 bytes is the disk cluster size

system had, over the course of its life, supported at least 9 accounts. However since it appears that the PC operating system was restored in October 2000 it is possible that some of the e-mail account folders were duplicated/ re-created for pre-existing users.

The late night access times for files related to internet activity suggest that the PC was mostly, although not exclusively, used by shift workers on the Project support team who deal with overseas offices.

Some users of the machine were involved in small scale programming projects using Borland and Microsoft Visual Studio. The PSO corporate intranet pages were prepared on this PC using Microsoft Frontpage. Analysis of photographic images was performed using software installed on the machine.

The machine was subject to considerable internet use.

The music sharing software Napster was installed on the PC but no MP3 or other digital music files were found.

Security of the PC was fairly good: the anti-virus software installed was kept up-to-date. However the system was vulnerable to attack when connected to the internet due to the absence of any personal firewall software.

Despite (or perhaps the reason for), the current good AV practice, the machine was infected with the W32.Badtrans mass-mailing worm although no substantive trace of this infection could be found. Most recently, the user named Robert had received an e-mail message purporting to be an internet security update from Microsoft. The attached executable was in fact the W32.Gibe worm. Fortunately the evidence suggests that this was detected by the the memory resident Norton anti-virus software and quarantined before the machine could be infected. At the time the infected e-mail was received, Norton anti-virus was in the process of completing an automatic update. Activation of the memory resident program into the foreground may have caused the program (or perhaps the whole PC) to hang or crash. Damage sustained during this incident caused the PC to subsequently have problems when booting up. These problems were rectified using the recovery CD supplied with the PC and no user data was lost. It is planned to upgrade this machine to Windows XP in the near future.

Incident Response procedures for all internet-connected machines have been updated to specifically deal with virus infection. The new documents, issued to all users emphasise the need to preserve data in the event of such an incident. In this case the users had potentially eradicated valuable forensic evidence in their attempts to remedy the problems they were encountering.

Bibliography

SANS GCFA 2002 course notes

Handbook of computer crime investigation *Eoghan Casey* (Ed)
www.amazon.co.uk/exec/obidos/ASIN/0121631036/qid=1026245082/sr=2-1/ref=sr_2_3_1/026-0845379-5262019

Criminalistics 7th Ed *Richard Saferstein*
www.amazon.co.uk/exec/obidos/ASIN/0130138274/026-0845379-5262019

Cyber Crime Investigator's Field Guide *Bruce Middleton*
www.amazon.co.uk/exec/obidos/ASIN/0849311926/026-0845379-5262019

Encase: Guidance Software's Encase manual. Available when the product is purchased. www.encase.com

TASK version 1.0 . Available from www.atstake.com/research/tools/task

The Autopsy Forensic Browser version 1.5.
www.atstake.com/research/tools/autopsy

W32.Gibe-A worm information from Sophos at
www.sophos.com/virusinfo/analyses/w32gibea.html

and Symantec at
securityresponse.symantec.com/avcenter/venc/data/w32.gibe@mm.html

Paragon Ext2 Anywhere available from
www.partition-manager.com/n_ext2fs_main.htm

OE5 mailbox information from
mailservices.web.cern.ch/MailServices/docs/clients/outlook-express/configuration.html

Appendix A: Recovered Google searches

```
 :2002040820020415:
marilyn@http://www.google.com/search?hl=en&q=apple+mac+UK
:2002040820020415:
marilyn@http://www.google.com/search?hl=en&q=Computer+Sellers+UK
:2002040820020415: marilyn@http://www.google.com/search?hl=en&q=quarkXpress
:2002040820020415: marilyn@http://www.google.com/search?hl=en&q=used+i+mac
:2002040820020415:
marilyn@http://www.google.com/search?hl=en&q=used+imac+UK
:2002040820020415:
marilyn@http://www.google.com/search?hl=en&q=%28graphics+solutions%29+Compu
ter+suppiers&btnG=Google+Search :2002040820020415:
marilyn@http://www.google.com/search?hl=en&q=Computer+suppliers+Hampshire+U
K&btnG=Google+Search :2002040820020415:
marilyn@http://www.google.com/search?hl=en&q=Apple+mac+i+book
:2002040820020415:
marilyn@http://www.goog le.com/search?q=Apple+mac+suppliers+Hampshire+UK&hl=
en&start=10&sa=N :2002040820020415:
marilyn@http://www.google.com/search?hl=en&q=graphics+solutions+Computer+su
ppiers&btnG=Google+Search :2002040820020415:
marilyn@http://www.google.com/search?hl=en&q=App le+mac+suppliers+Hampshire+
UK&btnG=Google+Search :2002040820020415:
marilyn@http://www.google.com/search?hl=en&q=second+hand+Apple+mac+i+book
:2002040820020415:
marilyn@http://www.google.com/search?q=Apple+mac+i+book&hl=en&start=10&sa=N
:2002040820020415:
marilyn@http://www.google.com/search?hl=en&q=graphic+solutions+Uk
:2002040820020415:
marilyn@http://www.google.com/search?hl=en&q=Apple+Mac++Sellers+UK
:2002040820020415: marilyn@http://www.google.com/search?hl=en&q=i+book
:2002040820020415:
marilyn@http://www.google.com/search?hl=en&q=second+hand+Apple+mac+UK
:2002040820020415:
marilyn@http://www.google.com/search?hl=en&q=second+hand+mac+UK  Google -
Visited:
marilyn@http://www.google.com/search?hl=en&q=Accomadation+Rental+UK+Hampshi
re&btnG=Google+Search Visited:
marilyn@http://www.google.com/search?q=Accomadation+Rental+Hampshire+UK&hl=
en&start=10&sa=N Visited:
marilyn@http://www.google.com/search?hl =en&q=Accomadation+Rental+Hampshire+
UK&btnG=Google+Search Visited:
marilyn@http://www.google.com/search?hl=en&q=Hampshire+UK+Rental+Accomadati
on&btnG=Google+Search Visited:
marilyn@http://www.google.com/search?q=Hampshire+UK+Rental+Accomadation&hl=
en&start=10&sa=N Visited:
marilyn@http://www.google.com/search?q=Hampshire+UK+Rental+Accomadation&hl=
en&start=20&sa=N Visited:
marilyn@http://www.google.com/search?hl=en&q=Hampshire+UK++Accomadation+Age
ncies Visited:
marilyn@http://www.google.com/search?hl=en&q=Es tate+Agents+UK+Rental
Visited:
marilyn@http://www.google.com/search?hl=en&q=Jacobs++and+Hunt+rental
Visited: marilyn@http://www.google.com/search?hl=en&q=Jacobs++and+Hunt
Visited:
marilyn@http://www.google.com/search?hl=en&q=Jacobs++and+Hunt+accommadation
Visited: marilyn@http://www.google.com/search?hl=en&q=Peterfield+Post
Visited: marilyn@http://www.google.com/search?hl=en&q=Peterfield+Post+UK
```

```
Visited:
marilyn@http://www.google.com/search?hl=en&q=Peterfield+Post+UK+Newspaper
Visited:
marilyn@http://www.google.com/search?hl=en&q=Peterfield+Herald+UK+Newspaper
Visited: marilyn@http://www.google.com/search?hl=en&q=Peterfield+Herald+
Visited:
marilyn@http://www.google.com/search?hl=en&q=Hampshire+Classified+Adverts
Visited: marilyn@http://www.google.com/search ?hl=en&q=apple+mac+UK Visited:
marilyn@http://www.google.com/search?hl=en&q=used+i+mac Visited:
marilyn@http://www.google.com/search?hl=en&q=quarkXpress Visited:
marilyn@http://www.google.com/search?hl=en&q=second+hand+mac+UK Visited:
marilyn@http://www.google.com/search?hl=en&q=graphic+solutions+Uk Visited:
marilyn@http://www.google.com/search?hl=en&q=used+imac+UK Visited:
marilyn@http://www.google.com/search?hl=en&q=Computer+Sellers+UK Visited:
marilyn@http://www.google.com/search?hl=en&q=i+book Visited:
marilyn@http://www.google.com/search?hl=en&q=Apple+Mac++Sellers+UK Visited:
marilyn@http://www.google.com/search?hl=en&q=Apple+mac+i+book Visited:
marilyn@http://www.google.com/search?q=Apple+mac+i+book&hl=en&start=10&sa=N
Visited:
marilyn@http://www.google.com/search?hl=en&q=second+hand+Apple+mac+i+book
Visited:
marilyn@http://www.google.com/search?hl=en&q=second+hand+Apple+mac+UK
Visited:
marilyn@http://www.google.com/search?hl=en&q=graphics+solutions+Computer+su
ppiers&btnG=Google+Search Visited:
marilyn@http://www.google.com/search?hl=en&q=%28graphics+solutions%29+Compu
ter+suppiers&btnG=Google+Search Visited:
marilyn@http://www.google.com/search?hl=en&q=Computer+suppliers+Hampshire+U
K&btnG=Google+Search Visited:
marilyn@http://www.google.com/search?q=Appl e+mac+suppliers+Hampshire+UK&hl=
en&start=10&sa=N Visited:
marilyn@http://www.google.com/search?hl=en&q=Apple+mac+suppliers+Hampshire+
UK&btnG=Google+Search
marilyn@http://www.google.com/search?hl=en&q=Jacobs++and+Hunt+rental
:2002040120020408:
marilyn@http://www.google.com/search?q=Hampshire+UK+Rental+Accomadation&hl=
en&start=10&sa=N :2002040120020408:
marilyn@http://www.google.com/search?hl=en&q=Accomadation+Rental+Hampshire+
UK&btnG=Google+Search :2002040120020408:
marilyn@http://www.google.com/search?hl=e n&q=Peterfield+Post+UK+Newspaper
:2002040120020408:
marilyn@http://www.google.com/search?q=Accomadation+Rental+Hampshire+UK&hl=
en&start=10&sa=N :2002040120020408:
marilyn@http://www.google.com/search?hl=en&q=Peterfield+Herald+
:2002040120020408:
marilyn@http://www.google.com/search?hl=en&q=Hampshire+UK+Rental+Accomadati
on&btnG=Google+Search :2002040120020408:
marilyn@http://www.google.com/search?hl=en&q=Peterfield+Post
:2002040120020408:
marilyn@http://www.google.com/search?hl=en&q=Peterfield+Herald+UK+News paper
:2002040120020408:
marilyn@http://www.google.com/search?hl=en&q=Jacobs++and+Hunt+accommadation
:2002040120020408:
marilyn@http://www.google.com/search?hl=en&q=Accomadation+Rental+UK+Hampshi
re&btnG=Google+Search :2002040120020408:
marilyn@http://www.google.com/search?hl=en&q=Hampshire+UK++Accomadation+Age
ncies :2002040120020408:
marilyn@http://www.google.com/search?hl=en&q=Peterfield+Post+UK
:2002040120020408:
```

```
marilyn@http://www.google.com/search?hl=en&q=Jacobs++and+Hunt
:2002040120020408:
marilyn@http://www.google.com/search?q=Hampshire+UK+Rental+Accomadation&hl=
en&start=20&sa=N :2002040120020408:
marilyn@http://www.google.com/search?hl=en&q=Hampshire+Classified+Adverts
:2002040120020408:
marilyn@http://www.google.com/search?hl=en&q=Estate+Agents+UK+Re ntal
:2002040820020409: marilyn@http://www.google.com/search?hl=en&q=quarkXpress
:2002040820020409:
marilyn@http://www.google.com/search?hl=en&q=apple+mac+UK
```

Appendix B: Full MACTime timeline for 19-21 April 2002.

```
Apr172002 23:39:06 0 m.. 96871108 <H_PSO_1_290402_1.dd-_VX~0000.TMP-dead-96871108>
Apr172002 23:39:06 0 m.. 96871108
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020412.021/_VX~0000.TMP(deleted)
Apr192002 09:00:00 98048 m.. 80683526
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/naveng.exp(NAVENG.EXP)
Apr192002 09:00:00 406284 m.. 80683575
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/virscan9.dat(VIRSCAN9.DAT)
Apr192002 09:00:00 1957 m.. 80683540
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/tinfl.dat(TINFL.DAT)
Apr192002 09:00:00 224 m.. 80683553
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/zdone.dat(ZDONE.DAT)
Apr192002 09:00:00 741888 m.. 80683532
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/navex32a.dll(NAVEX32A.DLL)
Apr192002 09:00:00 702493 m.. 80683567
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/virscan1.dat(VIRSCAN1.DAT)
Apr192002 09:00:00 925 m.. 80683563
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/symaveng.inf(SYMAVENG.INF)
Apr192002 09:00:00 106236 m.. 80683577
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/virscan.inf(VIRSCAN.INF)
Apr192002 09:00:00 1179 m.. 80683542
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/tscan1hd.dat(TSCAN1HD.DAT)
Apr192002 09:00:00 28279 m.. 80683579
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/whatsnew.TXT(WHATSNEW.TXT)
Apr192002 09:00:00 148 m.. 80683585
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/tinfidx.dat(TINFIDX.DAT)
Apr192002 09:00:00 70482 m.. 80683571
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/virscan5.dat(VIRSCAN5.DAT)
Apr192002 09:00:00 9380 m.. 80683587
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/tscan1.dat(TSCAN1.DAT)
Apr192002 09:00:00 1253 m.. 80683565
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/catalog.dat(CATALOG.DAT)
Apr192002 09:00:00 7485 m.. 80683536
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/symaveng.cat(SYMAVENG.CAT)
Apr192002 09:00:00 354132 m.. 80683548
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/virscan6.dat(VIRSCAN6.DAT)
Apr192002 09:00:00 140800 m.. 80683528
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/naveng32.dll(NAVENG32.DLL)
Apr192002 09:00:00 453 m.. 80683538
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/tinf.dat(TINF.DAT)
Apr192002 09:00:00 804736 m.. 80683555
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/navex15.exp(NAVEX15.EXP)
Apr192002 09:00:00 57488 m.. 80683534
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/scrauth.dat(SCRAUTH.DAT)
Apr192002 09:00:00 308550 m.. 80683546
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/virscan4.dat(VIRSCAN4.DAT)
Apr192002 09:00:00 118865 m.. 80683561
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/naveng.vxd(NAVENG.VXD)
Apr192002 09:00:00 6479 m.. 80683581
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/ncsacert.txt(NCSACERT.TXT)
Apr192002 09:00:00 586816 m.. 80683530
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/navex15.sys(NAVEX15.SYS)
Apr192002 09:00:00 774217 m.. 80683557
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/navex15.vxd(NAVEX15.VXD)
Apr192002 09:00:00 459787 m.. 80683573
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/virscan7.dat(VIRSCAN7.DAT)
Apr192002 09:00:00 140268 m.. 80683569
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/virscan3.dat(VIRSCAN3.DAT)
Apr192002 09:00:00 466368 m.. 80683544
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/virscan2.dat(VIRSCAN2.DAT)
Apr192002 09:00:00 65920 m.. 80683559
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/naveng.sys(NAVENG.SYS)
Apr192002 09:00:00 536010 m.. 80683550
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/virscan8.dat(VIRSCAN8.DAT)
Apr192002 09:00:00 5232 m.. 80683583
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/technote.txt(TECHNOTE.TXT)
Apr212002 00:00:00 0 .a. 65590920
/PROGRA~1/NORTON~1/NORTON~1/QUARAN~1/INCOMING/AP1.exe(_P1.EXE)(deleted)
Apr212002 00:00:00 4096 .a. 65532318 /PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005
Apr212002 00:00:00 4096 .a. 65532317
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/tmp32B4.TMP(_MP32B4.TMP)(deleted)
Apr212002 00:00:00 4096 .a. 65532317 <H_PSO_1_290402_1.dd-_MP32B4.TMP-dead-65532317>
```

```
Apr212002 00:00:00 0 .a. 65460872 /MYDOCU~1/q216309.exe(_216309.EXE)(deleted)
Apr212002 00:00:00 0 .a. 65460872 <H_PSO_1_290402_1.dd-_216309.EXE-dead-65460872>
Apr212002 00:00:00 475 .a. 65463621 <H_PSO_1_290402_1.dd-_UTLOOK.LNK-dead-65463621>
Apr212002 00:00:00 0 .a. 65590918
/PROGRA~1/NORTON~1/NORTON~1/QUARAN~1/INCOMING/AP0.exe(_P0.EXE)(deleted)
Apr212002 00:00:00 0 .a. 65590918 <H_PSO_1_290402_1.dd-_P0.EXE-dead-65590918>
Apr212002 00:00:00 4096 .a. 65709329
/WINDOWS/HISTORY/HISTORY.IE5/MSHist012002042120020422(MSHIST~3)
Apr212002 00:00:00 0 .a. 65590920 <H_PSO_1_290402_1.dd-_P1.EXE-dead-65590920>
Apr212002 00:00:00 475 .a. 65463621 /WINDOWS/RECENT/OUTLOOK.lnk(_UTLOOK.LNK)(deleted)
Apr212002 21:43:48 2590 ..c 65464860 /RECYCLED/NPROTECT/_0007995.HTT(deleted)
Apr212002 21:43:48 2590 ..c 65464860 <H_PSO_1_290402_1.dd-_0007995.HTT-dead-65464860>
Apr212002 21:43:50 2590 m.. 65464860 <H_PSO_1_290402_1.dd-_0007995.HTT-dead-65464860>
Apr212002 21:43:50 2590 m.. 65464860 /RECYCLED/NPROTECT/_0007995.HTT(deleted)
Apr212002 21:43:52 32768 m.. 3449222
/WINDOWS/HISTORY/HISTORY.IE5/MSHIST~3/index.dat(INDEX.DAT)
Apr212002 21:44:00 2194297 ..c 65466515 /WINDOWS/SYSBCKUP/rb000.cab(RB000.CAB)
Apr212002 21:44:18 2194297 m.. 65466515 /WINDOWS/SYSBCKUP/rb000.cab(RB000.CAB)
Apr212002 21:44:34 64 ..c 65464857 /RECYCLED/NPROTECT/_0007992.LDB(deleted)
Apr212002 21:44:34 64 ..c 65464857 <H_PSO_1_290402_1.dd-_0007992.LDB-dead-65464857>
Apr212002 21:44:40 64 m.. 65464857 /RECYCLED/NPROTECT/_0007992.LDB(deleted)
Apr212002 21:44:40 64 m.. 65464857 <H_PSO_1_290402_1.dd-_0007992.LDB-dead-65464857>
Apr212002 21:46:02 74720 ..c 65465017 <H_PSO_1_290402_1.dd-_0008161.DBX-dead-65465017>
Apr212002 21:46:02 74720 ..c 65465017 /RECYCLED/NPROTECT/_0008161.DBX(deleted)
Apr212002 21:46:04 74720 m.. 65464858 <H_PSO_1_290402_1.dd-_0007993.DBX-dead-65464858>
Apr212002 21:46:04 74720 m.. 65464858 /RECYCLED/NPROTECT/_0007993.DBX(deleted)
Apr212002 21:46:56 64 ..c 65464859 <H_PSO_1_290402_1.dd-_0007994.LDB-dead-65464859>
Apr212002 21:46:56 64 ..c 65464859 /RECYCLED/NPROTECT/_0007994.LDB(deleted)
Apr212002 21:46:58 64 m.. 65464859 <H_PSO_1_290402_1.dd-_0007994.LDB-dead-65464859>
Apr212002 21:46:58 64 m.. 65464859 /RECYCLED/NPROTECT/_0007994.LDB(deleted)
Apr212002 21:47:18 2884 ..c 109883805
/WINDOWS/TEMPOR~1/CONTENT.IE5/W12FWT6B/ChichesterFestivalTheatre-SpringSeason
Apr212002 21:47:18 0 ..c 105919221 /WINDOWS/TEMPOR~1/CONTENT.IE5/W12FWT6B/[65](_65_~1)
Apr212002 21:47:20 2884 m.. 109883805
/WINDOWS/TEMPOR~1/CONTENT.IE5/W12FWT6B/ChichesterFestivalTheatre-SpringSeason
Apr212002 21:47:20 0 m.. 105919221 /WINDOWS/TEMPOR~1/CONTENT.IE5/W12FWT6B/[65](_65_~1)
Apr212002 21:47:30 0 ..c 105919223 /WINDOWS/TEMPOR~1/CONTENT.IE5/W12FWT6B/[66](_66_~1)
Apr212002 21:47:30 864 ..c 105919228
/WINDOWS/TEMPOR~1/CONTENT.IE5/W12FWT6B/Orienteering.dat(ORIENT~1.DAT)
Apr212002 21:47:30 0 ..c 109883782 /WINDOWS/TEMPOR~1/CONTENT.IE5/W12FWT6B/[67](_67_~1)
Apr212002 21:47:30 864 ..c 109883791
/WINDOWS/TEMPOR~1/CONTENT.IE5/W12FWT6B/Orienteering(1).dat(ORIENT~2.DAT)
Apr212002 21:47:32 0 m.. 105919223 /WINDOWS/TEMPOR~1/CONTENT.IE5/W12FWT6B/[66](_66_~1)
Apr212002 21:47:32 864 m.. 109883791
/WINDOWS/TEMPOR~1/CONTENT.IE5/W12FWT6B/Orienteering(1).dat(ORIENT~2.DAT)
Apr212002 21:47:32 864 m.. 105919228
/WINDOWS/TEMPOR~1/CONTENT.IE5/W12FWT6B/Orienteering.dat(ORIENT~1.DAT)
Apr212002 21:47:32 0 m.. 109883782 /WINDOWS/TEMPOR~1/CONTENT.IE5/W12FWT6B/[67](_67_~1)
Apr212002 21:49:42 3034 ..c 109883829
/WINDOWS/TEMPOR~1/CONTENT.IE5/W12FWT6B/InternetSecurityUpdate.dat(INTERN~1.DAT)
Apr212002 21:49:42 3034 ..c 109883833
/WINDOWS/TEMPOR~1/CONTENT.IE5/W12FWT6B/InternetSecurityUpdate(1).dat(INTERN~2.DAT)
Apr212002 21:49:42 0 ..c 109883786 /WINDOWS/TEMPOR~1/CONTENT.IE5/W12FWT6B/[68](_68_~1)
Apr212002 21:49:42 0 ..c 109883795 /WINDOWS/TEMPOR~1/CONTENT.IE5/W12FWT6B/[69](_69_~1)
Apr212002 21:49:44 0 m.. 109883786 /WINDOWS/TEMPOR~1/CONTENT.IE5/W12FWT6B/[68](_68_~1)
Apr212002 21:49:44 3034 m.. 109883833
/WINDOWS/TEMPOR~1/CONTENT.IE5/W12FWT6B/InternetSecurityUpdate(1).dat(INTERN~2.DAT)
Apr212002 21:49:44 3034 m.. 109883829
/WINDOWS/TEMPOR~1/CONTENT.IE5/W12FWT6B/InternetSecurityUpdate.dat(INTERN~1.DAT)
Apr212002 21:49:44 0 m.. 109883795 /WINDOWS/TEMPOR~1/CONTENT.IE5/W12FWT6B/[69](_69_~1)
Apr212002 21:50:02 10 m.. 65711110
/WINDOWS/ALLUSE~1/APPLIC~1/SYMANTEC/LIVEUP~1/DOWNLO~1/autoupdt.trg(AUTOUPDT.TRG)
Apr212002 21:51:38 2590 ..c 65464959 /RECYCLED/NPROTECT/_0008094.HTT(deleted)
Apr212002 21:51:38 2590 ..c 65464959 <H_PSO_1_290402_1.dd-_0008094.HTT-dead-65464959>
Apr212002 21:51:40 2590 m.. 65464959 <H_PSO_1_290402_1.dd-_0008094.HTT-dead-65464959>
Apr212002 21:51:40 2590 m.. 65464959 /RECYCLED/NPROTECT/_0008094.HTT(deleted)
Apr212002 21:51:42 4096 ..c 65532317 <H_PSO_1_290402_1.dd-_MP32B4.TMP-dead-65532317>
Apr212002 21:51:42 4096 ..c 65532317
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/tmp32B4.TMP(_MP32B4.TMP)(deleted)
Apr212002 21:51:44 4096 m.. 65532317 <H_PSO_1_290402_1.dd-_MP32B4.TMP-dead-65532317>
Apr212002 21:51:44 4096 m.. 65532317
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/tmp32B4.TMP(_MP32B4.TMP)(deleted)
Apr212002 21:52:12 774217 ..c 65464895 /RECYCLED/NPROTECT/_0008030.VXD(deleted)
Apr212002 21:52:12 308122 ..c 65464907 /RECYCLED/NPROTECT/_0008042.DAT(deleted)
```

```
Apr212002 21:52:12 57344 ..c 65464918 /RECYCLED/NPROTECT/_0008053.DAT(deleted)
Apr212002 21:52:12 354244 ..c 65464909 /RECYCLED/NPROTECT/_0008044.DAT(deleted)
Apr212002 21:52:12 586816 ..c 65464894 /RECYCLED/NPROTECT/_0008029.SYS(deleted)
Apr212002 21:52:12 774217 ..c 65464895 <H_PSO_1_290402_1.dd-_0008030.VXD-dead-65464895>
Apr212002 21:52:12 224 ..c 65464917 /RECYCLED/NPROTECT/_0008052.DAT(deleted)
Apr212002 21:52:12 453 ..c 65464919 /RECYCLED/NPROTECT/_0008054.DAT(deleted)
Apr212002 21:52:12 453 ..c 65464919 <H_PSO_1_290402_1.dd-_0008054.DAT-dead-65464919>
Apr212002 21:52:12 741888 ..c 65464896 /RECYCLED/NPROTECT/_0008031.DLL(deleted)
Apr212002 21:52:12 804736 ..c 65464893 /RECYCLED/NPROTECT/_0008028.EXP(deleted)
Apr212002 21:52:12 7485 ..c 65464902 /RECYCLED/NPROTECT/_0008037.CAT(deleted)
Apr212002 21:52:12 1957 ..c 65464921 /RECYCLED/NPROTECT/_0008056.DAT(deleted)
Apr212002 21:52:12 804736 ..c 65464893 <H_PSO_1_290402_1.dd-_0008028.EXP-dead-65464893>
Apr212002 21:52:12 32 ..c 80683551
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/VIRSCANT.DAT
Apr212002 21:52:12 140800 ..c 65464900 /RECYCLED/NPROTECT/_0008035.DLL(deleted)
Apr212002 21:52:12 32 ..c 65533190
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/TEXTHUB/virscant.dat(VIRSCANT.DAT)
Apr212002 21:52:12 1179 ..c 65464923 /RECYCLED/NPROTECT/_0008058.DAT(deleted)
Apr212002 21:52:12 455976 ..c 65464905 /RECYCLED/NPROTECT/_0008040.DAT(deleted)
Apr212002 21:52:12 7485 ..c 65464902 <H_PSO_1_290402_1.dd-_0008037.CAT-dead-65464902>
Apr212002 21:52:12 4096 ..c 65532318 /PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005
Apr212002 21:52:12 140800 ..c 65464900 <H_PSO_1_290402_1.dd-_0008035.DLL-dead-65464900>
Apr212002 21:52:12 308122 ..c 65464907 <H_PSO_1_290402_1.dd-_0008042.DAT-dead-65464907>
Apr212002 21:52:12 98048 ..c 65464898 /RECYCLED/NPROTECT/_0008033.EXP(deleted)
Apr212002 21:52:12 224 ..c 65464917 <H_PSO_1_290402_1.dd-_0008052.DAT-dead-65464917>
Apr212002 21:52:12 1957 ..c 65464921 <H_PSO_1_290402_1.dd-_0008056.DAT-dead-65464921>
Apr212002 21:52:12 531452 ..c 65464911 <H_PSO_1_290402_1.dd-_0008046.DAT-dead-65464911>
Apr212002 21:52:12 586816 ..c 65464894 <H_PSO_1_290402_1.dd-_0008029.SYS-dead-65464894>
Apr212002 21:52:12 741888 ..c 65464896 <H_PSO_1_290402_1.dd-_0008031.DLL-dead-65464896>
Apr212002 21:52:12 531452 ..c 65464911 /RECYCLED/NPROTECT/_0008046.DAT(deleted)
Apr212002 21:52:12 57344 ..c 65464918 <H_PSO_1_290402_1.dd-_0008053.DAT-dead-65464918>
Apr212002 21:52:12 455976 ..c 65464905 <H_PSO_1_290402_1.dd-_0008040.DAT-dead-65464905>
Apr212002 21:52:12 354244 ..c 65464909 <H_PSO_1_290402_1.dd-_0008044.DAT-dead-65464909>
Apr212002 21:52:12 1179 ..c 65464923 <H_PSO_1_290402_1.dd-_0008058.DAT-dead-65464923>
Apr212002 21:52:12 98048 ..c 65464898 <H_PSO_1_290402_1.dd-_0008033.EXP-dead-65464898>
Apr212002 21:52:14 70482 ..c 65464908 /RECYCLED/NPROTECT/_0008043.DAT(deleted)
Apr212002 21:52:14 65920 ..c 65464897 /RECYCLED/NPROTECT/_0008032.SYS(deleted)
Apr212002 21:52:14 31400 ..c 65464914 /RECYCLED/NPROTECT/_0008049.TXT(deleted)
Apr212002 21:52:14 65920 ..c 65464897 <H_PSO_1_290402_1.dd-_0008032.SYS-dead-65464897>
Apr212002 21:52:14 1253 ..c 65464903 <H_PSO_1_290402_1.dd-_0008038.DAT-dead-65464903>
Apr212002 21:52:14 140196 ..c 65464906 <H_PSO_1_290402_1.dd-_0008041.DAT-dead-65464906>
Apr212002 21:52:14 455827 ..c 65464910 <H_PSO_1_290402_1.dd-_0008045.DAT-dead-65464910>
Apr212002 21:52:14 403731 ..c 65464912 /RECYCLED/NPROTECT/_0008047.DAT(deleted)
Apr212002 21:52:14 5232 ..c 65464916 <H_PSO_1_290402_1.dd-_0008051.TXT-dead-65464916>
Apr212002 21:52:14 925 ..c 65464901 /RECYCLED/NPROTECT/_0008036.INF(deleted)
Apr212002 21:52:14 9380 ..c 65464922 <H_PSO_1_290402_1.dd-_0008057.DAT-dead-65464922>
Apr212002 21:52:14 70482 ..c 65464908 <H_PSO_1_290402_1.dd-_0008043.DAT-dead-65464908>
Apr212002 21:52:14 31400 ..c 65464914 <H_PSO_1_290402_1.dd-_0008049.TXT-dead-65464914>
Apr212002 21:52:14 118865 ..c 65464899 /RECYCLED/NPROTECT/_0008034.VXD(deleted)
Apr212002 21:52:14 6479 ..c 65464915 /RECYCLED/NPROTECT/_0008050.TXT(deleted)
Apr212002 21:52:14 106236 ..c 65464913 /RECYCLED/NPROTECT/_0008048.INF(deleted)
Apr212002 21:52:14 9380 ..c 65464922 /RECYCLED/NPROTECT/_0008057.DAT(deleted)
Apr212002 21:52:14 106236 ..c 65464913 <H_PSO_1_290402_1.dd-_0008048.INF-dead-65464913>
Apr212002 21:52:14 6479 ..c 65464915 <H_PSO_1_290402_1.dd-_0008050.TXT-dead-65464915>
Apr212002 21:52:14 5232 ..c 65464916 /RECYCLED/NPROTECT/_0008051.TXT(deleted)
Apr212002 21:52:14 403731 ..c 65464912 <H_PSO_1_290402_1.dd-_0008047.DAT-dead-65464912>
Apr212002 21:52:14 1253 ..c 65464903 /RECYCLED/NPROTECT/_0008038.DAT(deleted)
Apr212002 21:52:14 148 ..c 65464920 /RECYCLED/NPROTECT/_0008055.DAT(deleted)
Apr212002 21:52:14 804736 ..c 80683555
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/navex15.exp(NAVEX15.EXP)
Apr212002 21:52:14 925 ..c 65464901 <H_PSO_1_290402_1.dd-_0008036.INF-dead-65464901>
Apr212002 21:52:14 118865 ..c 65464899 <H_PSO_1_290402_1.dd-_0008034.VXD-dead-65464899>
Apr212002 21:52:14 140196 ..c 65464906 /RECYCLED/NPROTECT/_0008041.DAT(deleted)
Apr212002 21:52:14 148 ..c 65464920 <H_PSO_1_290402_1.dd-_0008055.DAT-dead-65464920>
Apr212002 21:52:14 699257 ..c 65464904 /RECYCLED/NPROTECT/_0008039.DAT(deleted)
Apr212002 21:52:14 699257 ..c 65464904 <H_PSO_1_290402_1.dd-_0008039.DAT-dead-65464904>
Apr212002 21:52:14 455827 ..c 65464910 /RECYCLED/NPROTECT/_0008045.DAT(deleted)
Apr212002 21:52:14 4096 m.. 65532318 /PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005
Apr212002 21:52:16 586816 ..c 80683530
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/navex15.sys(NAVEX15.SYS)
Apr212002 21:52:16 65920 ..c 80683559
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/naveng.sys(NAVENG.SYS)
Apr212002 21:52:16 98048 ..c 80683526
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/naveng.exp(NAVENG.EXP)
```

```
Apr212002 21:52:16 774217 ..c 80683557
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/navex15.vxd(NAVEX15.VXD)
Apr212002 21:52:16 118865 ..c 80683561
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/naveng.vxd(NAVENG.VXD)
Apr212002 21:52:16 741888 ..c 80683532
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/navex32a.dll(NAVEX32A.DLL)
Apr212002 21:52:18 925 ..c 80683563
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/symaveng.inf(SYMAVENG.INF)
Apr212002 21:52:18 7485 ..c 80683536
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/symaveng.cat(SYMAVENG.CAT)
Apr212002 21:52:18 140268 ..c 80683569
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/virscan3.dat(VIRSCAN3.DAT)
Apr212002 21:52:18 308550 ..c 80683546
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/virscan4.dat(VIRSCAN4.DAT)
Apr212002 21:52:18 70482 ..c 80683571
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/virscan5.dat(VIRSCAN5.DAT)
Apr212002 21:52:18 466368 ..c 80683544
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/virscan2.dat(VIRSCAN2.DAT)
Apr212002 21:52:18 140800 ..c 80683528
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/naveng32.dll(NAVENG32.DLL)
Apr212002 21:52:18 702493 ..c 80683567
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/virscan1.dat(VIRSCAN1.DAT)
Apr212002 21:52:18 1253 ..c 80683565
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/catalog.dat(CATALOG.DAT)
Apr212002 21:52:20 1957 ..c 80683540
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/tinfl.dat(TINFL.DAT)
Apr212002 21:52:20 1179 ..c 80683542
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/tscan1hd.dat(TSCAN1HD.DAT)
Apr212002 21:52:20 459787 ..c 80683573
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/virscan7.dat(VIRSCAN7.DAT)
Apr212002 21:52:20 57488 ..c 80683534
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/scrauth.dat(SCRAUTH.DAT)
Apr212002 21:52:20 354132 ..c 80683548
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/virscan6.dat(VIRSCAN6.DAT)
Apr212002 21:52:20 536010 ..c 80683550
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/virscan8.dat(VIRSCAN8.DAT)
Apr212002 21:52:20 453 ..c 80683538
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/tinf.dat(TINF.DAT)
Apr212002 21:52:20 5232 ..c 80683583
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/technote.txt(TECHNOTE.TXT)
Apr212002 21:52:20 148 ..c 80683585
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/tinfidx.dat(TINFIDX.DAT)
Apr212002 21:52:20 9380 ..c 80683587
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/tscan1.dat(TSCAN1.DAT)
Apr212002 21:52:20 224 ..c 80683553
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/zdone.dat(ZDONE.DAT)
Apr212002 21:52:20 406284 ..c 80683575
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/virscan9.dat(VIRSCAN9.DAT)
Apr212002 21:52:20 28279 ..c 80683579
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/whatsnew.TXT(WHATSNEW.TXT)
Apr212002 21:52:20 106236 ..c 80683577
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/virscan.inf(VIRSCAN.INF)
Apr212002 21:52:20 6479 ..c 80683581
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/20020419.005/ncsacert.txt(NCSACERT.TXT)
Apr212002 21:52:22 57 m.. 65532307
/PROGRA~1/COMMON~1/SYMANT~1/VIRUSD~1/definfo.dat(DEFINFO.DAT)
Apr212002 21:52:28 5272 m.. 65710765
/WINDOWS/ALLUSE~1/APPLIC~1/SYMANTEC/LIVEUP~1/3.Log.LiveUpdate(3LOG~1.LIV)
Apr212002 21:52:28 2545 m.. 65710758
/WINDOWS/ALLUSE~1/APPLIC~1/SYMANTEC/LIVEUP~1/3.Settings.LiveUpdate(3SETTI~1.LIV)
Apr212002 21:52:28 5014 m.. 65710762
/WINDOWS/ALLUSE~1/APPLIC~1/SYMANTEC/LIVEUP~1/3.Product.Catalog.LiveUpdate(3PRODU~1.LIV)
Apr212002 21:53:40 130880 ..c 65464956 /RECYCLED/NPROTECT/_0008091.EXE(deleted)
Apr212002 21:53:40 130880 ..c 65464956 <H_PSO_1_290402_1.dd-_0008091.EXE-dead-65464956>
Apr212002 21:53:40 130880 ..c 65464957 <H_PSO_1_290402_1.dd-_0008092.EXE-dead-65464957>
Apr212002 21:53:40 0 ..c 65591046 <H_PSO_1_290402_1.dd-_4760DFB.EXE-dead-65591046>
Apr212002 21:53:40 0 ..c 65460872 <H_PSO_1_290402_1.dd-_216309.EXE-dead-65460872>
Apr212002 21:53:40 130880 ..c 65464957 /RECYCLED/NPROTECT/_0008092.EXE(deleted)
Apr212002 21:53:40 0 ..c 65460872 /MYDOCU~1/q216309.exe(_216309.EXE)(deleted)
Apr212002 21:53:40 0 ..c 65591046
/PROGRA~1/NORTON~1/NORTON~1/QUARAN~1/PORTAL/14760DFB.exe(_4760DFB.EXE)(deleted)
Apr212002 21:53:42 130880 m.. 65464957 /RECYCLED/NPROTECT/_0008092.EXE(deleted)
Apr212002 21:53:42 130880 m.. 65464956 /RECYCLED/NPROTECT/_0008091.EXE(deleted)
Apr212002 21:53:42 130880 m.. 65464956 <H_PSO_1_290402_1.dd-_0008091.EXE-dead-65464956>
```

```
Apr212002 21:53:42 130880 m.. 65464957 <H_PSO_1_290402_1.dd-_0008092.EXE-dead-65464957>
Apr212002 21:55:02 0 m.. 65460872 /MYDOCU~1/q216309.exe(_216309.EXE)(deleted)
Apr212002 21:55:02 0 m.. 65460872 <H_PSO_1_290402_1.dd-_216309.EXE-dead-65460872>
Apr212002 21:55:02 0 ..c 65590918
/PROGRA~1/NORTON~1/NORTON~1/QUARAN~1/INCOMING/AP0.exe(_P0.EXE)(deleted)
Apr212002 21:55:02 0 ..c 65590918 <H_PSO_1_290402_1.dd-_P0.EXE-dead-65590918>
Apr212002 21:55:20 0 ..c 65590920
/PROGRA~1/NORTON~1/NORTON~1/QUARAN~1/INCOMING/AP1.exe(_P1.EXE)(deleted)
Apr212002 21:55:20 0 ..c 65590920 <H_PSO_1_290402_1.dd-_P1.EXE-dead-65590920>
Apr212002 21:55:22 0 m.. 65590920 <H_PSO_1_290402_1.dd-_P1.EXE-dead-65590920>
Apr212002 21:55:22 0 m.. 65590920
/PROGRA~1/NORTON~1/NORTON~1/QUARAN~1/INCOMING/AP1.exe(_P1.EXE)(deleted)
Apr212002 21:55:44 388 m.. 65587858 /PROGRA~1/NORTON~1/NORTON~1/excludel.dat(EXCLUDEL.DAT)
Apr212002 21:55:44 676 m.. 65587856 /PROGRA~1/NORTON~1/NORTON~1/exclude.dat(EXCLUDE.DAT)
Apr212002 21:56:02 307 ..c 65463909 <H_PSO_1_290402_1.dd-_216309.LNK-dead-65463909>
Apr212002 21:56:02 307 ..c 65463909 /WINDOWS/RECENT/q216309.lnk(_216309.LNK)(deleted)
Apr212002 21:56:04 307 m.. 65463909 <H_PSO_1_290402_1.dd-_216309.LNK-dead-65463909>
Apr212002 21:56:04 307 m.. 65463909 /WINDOWS/RECENT/q216309.lnk(_216309.LNK)(deleted)
Apr262002 16:10:46 50 m.. 65460279 /WINDOWS/wiaservc.log(WIASERVC.LOG)
```

Appendix C: Boot sector of disk as reported by Diskedit

```
 Disk Editor
                            Symantec Core Component
                             June 27, 2002 3:20pm

                                  ***********
                                  Boot Record
                                  ***********


Sector 0
                                OEM ID: MSWIN4.1
                      Bytes per sector: 512
                   Sectors per cluster: 8
           Reserved sectors at beginning: 32
                           FAT Copies: 2
                             Reserved: 0
                             Reserved: (Unused)
                  Media descriptor byte: F8 Hex
                        Sectors per FAT: 0
                     Sectors per track: 63
                                 Sides: 240
                Special hidden sectors: 63
             Big total number of sectors: 15618897
                    Big Sectors Per Fat: 15224
                Number of active Fats:   0
                             Reserved: (Unused)
                             Mirrored: Yes
                             Reserved: (Unused)
               File System Ver (major): 0
               File System Ver (minor): 0
                 First Cluster of Root: 2
                      FS Sector number: 1
           (hotlink)  Backup Boot Sector: 6
                             Reserved: (Unused)
                Physical drive number: 128
                             Reserved: (Unused)
          Extended Boot Record Signature: 29 Hex
                    Volume Serial Number: 11F33136 Hex
                            Volume Label: ...........
                          File System ID: FAT32
                               Signature: AA550000 Hex

Sector 1
                 Extended Boot Signature: 41615252 Hex
                             Reserved: (Unused)
                       FSINFO Signature: 61417272 Hex
                    Free Cluster Count: 1316217
                     Next Free Cluster: 2
                             Reserved: (Unused)
                FSINFO Ending Signature: AA550000 Hex

Sector 2
                             Reserved: (Unused)
                            Signature: AA550000 Hex

Sector 3
                                OEM ID: ........
                      Bytes per sector: 0
                   Sectors per cluster: 0
           Reserved sectors at beginning: 0
                           FAT Copies: 0
                             Reserved: 0
                             Reserved: (Unused)
                  Media descriptor byte: 00 Hex
                        Sectors per FAT: 0
                     Sectors per track: 0
                                 Sides: 0
                Special hidden sectors: 0
             Big total number of sectors: 0
```

Appendix D: Message containing W32.Gibe virus attachment.

```
Received: from mk-smarthost-1.mail.uk.tiscali.com ([212.74.112.71])
             by uranium.btinternet.com with esmtp (Exim 3.22 #8)
             id 16zCSf-0005Xe-00; Sun, 21 Apr 2002 09:12:41 +0100
Received: from [80.225.83.184] (helo=pfuckie)
             by mk-smarthost-1.mail.uk.tiscali.com with smtp (Exim 3.35 #1)
             id 16zCId-000LC7-00; Sun, 21 Apr 2002 09:02:20 +0100
From: "Microsoft Corporation Security Center" <rdquest12@microsoft.com>
To: "Microsoft Customer" <'customer@yourdomain.com'>
Subject: Internet Security Update
Reply-To: <rdquest12@microsoft.com>
MIME-Version: 1.0
Content-Type: multipart/mixed;
             boundary="NextPart_000235"
Message-Id: <E16zCId-000LC7-00@mk-smarthost-1.mail.uk.tiscali.com>
Date: Sun, 21 Apr 2002 09:02:20 +0100
Status:

This is a multi-part message in MIME format.
You should read this with client which
supported MIME standard.

--NextPart_000235
Content-Type: text/plain;
             charset="us-ascii"
Content-Transfer-Encoding: quoted-printable

Microsoft Customer,

     this is the latest version of security update, the
 "17 Apr 2002 Cumulative Patch" update which eliminates all
known security vulnerabilities affecting Internet Explorer and
MS Outlook/Express as well as six new vulnerabilities, and is
discussed in Microsoft Security Bulletin MS02-005. Install now to
protect your computer from these vulnerabilities, the most serious of which
could allow an attacker to run code on your computer.

Description of several well-know vulnerabilities:

- "Incorrect MIME Header Can Cause IE to Execute E-mail Attachment" vulnerability.
If a malicious user sends an affected HTML e-mail or hosts an affected
e-mail on a Web site, and a user opens the e-mail or visits the Web site,
Internet Explorer automatically runs the executable on the user's computer.

- A vulnerability that could allow an unauthorized user to learn the location
of cached content on your computer. This could enable the unauthorized
user to launch compiled HTML Help (.chm) files that contain shortcuts to
executables, thereby enabling the unauthorized user to run the executables
on your computer.

- A new variant of the "Frame Domain Verification" vulnerability could enable a
malicious Web site operator to open two browser windows, one in the Web site's
domain and the other on your local file system, and to pass information from
your computer to the Web site.

- CLSID extension vulnerability. Attachments which end with a CLSID file extension
do not show the actual full extension of the file when saved and viewed with
Windows Explorer. This allows dangerous file types to look as though they are simple,
harmless files - such as JPG or WAV files - that do not need to be blocked.

System requirements:
Versions of Windows no earlier than Windows 95.

This update applies to:
Versions of Internet Explorer no earlier than 4.01
Versions of MS Outlook no earlier than 8.00
Versions of MS Outlook Express no earlier than 4.01

How to install
Run attached file q216309.exe

How to use
```

```
You don't need to do anything after installing this item.

For more information about these issues, read Microsoft Security Bulletin MS02-005, or visit
link below.
http://www.microsoft.com/windows/ie/downloads/critical/default.asp
If you have some questions about this article contact us at rdquest12@microsoft.com

Thank you for using Microsoft products.

With friendly greetings,
MS Internet Security Center.
----------------------------------------
----------------------------------------
Microsoft is registered trademark of Microsoft Corporation.
Windows and Outlook are trademarks of Microsoft Corporation.

--NextPart_000235
Content-Type: application/x-msdownload;
              name="q216309.exe"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
              filename="q216309.exe"
```

Part 1 - Option 2: Analysis of unknown binary

4. Background Scenario

An unknown binary file has been obtained from a suspect computer. This report details the steps taken to analyse the program in order to determine the capabilities of the program, its purpose and what it may have been used for on the suspect computer. The binary was supplied within a zip archive along with an MD5 hash checksum. On receipt of this file the checksum was validated.

The binary has been analysed on a Systemax full tower PC running Red Hat Linux 7.2 (custom kernel based on 2.4.7-10). In order to support the heavy processing load required, this PC is equipped with 5000MB of RAM.

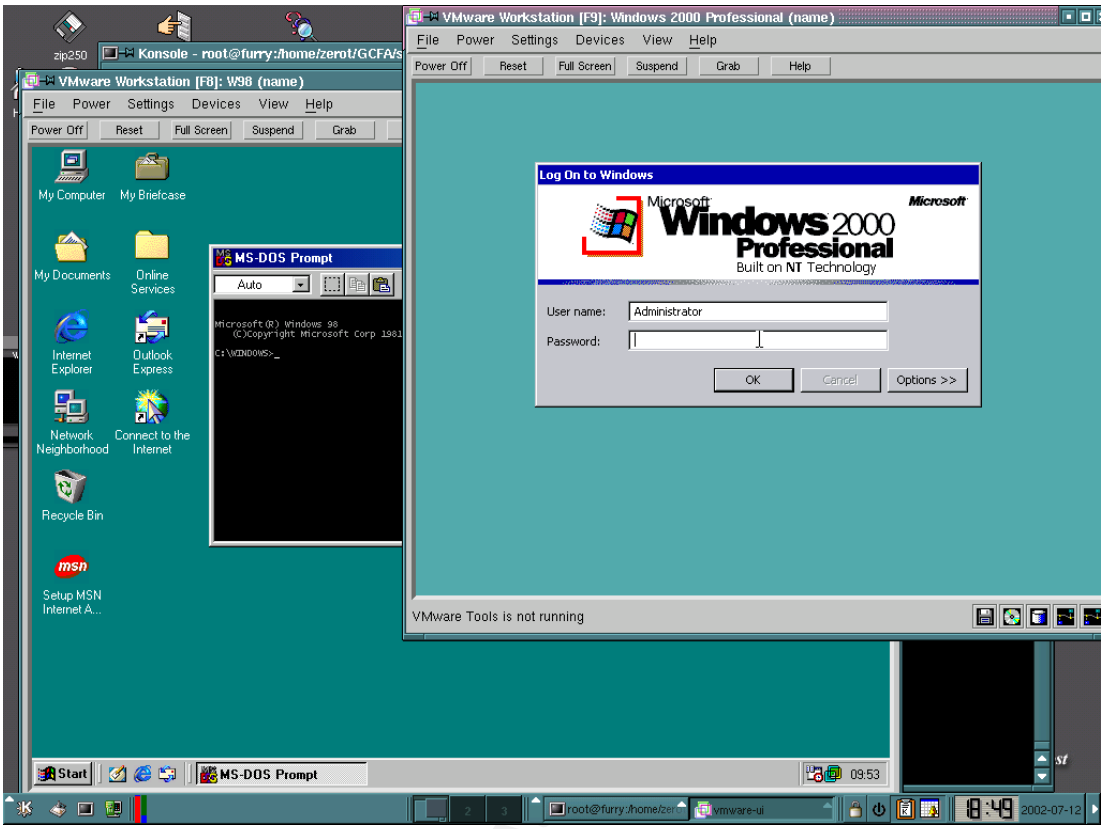


Illustration 4: Screenshot of Linux platform running W2K and W98 Vmware virtual machines.

A virtual networking environment has been created using Vmware[17] software. The virtual LAN consists of

4. Windows 98 virtual machine with IP address 192.168.192.10
5. Windows 2000 virtual machine with IP address 192.168.192.11
6. Red Hat Linux 7.2 virtual machine with IP address 192.168.192.16

All machines have been configured to permit bridged networking which enables them to communicate with the underlying (Linux) operating system which has the IP address 192.168.192.169.
In order to provide a transparent fishbowl environment for studying suspect executables, a number of protective/capture measures are in place:

xi) The platform Linux system runs the network sniffing software Snort to record any packets sent by executables.
xii) Tripwire is installed and configured on the virtual Linux system to record any changes to pre-determined (mostly system) directories by the executable.

This environment allows the analyst to study and manipulate suspect files without worrying about damaging production computers or having programs running amok on a live network. The Vmware virtual machine installations are, essentially flat files and

17 www.vmware.com

so can easily be backed up. In the event of a catastrophic failure it is trivial to restore a test operating system.

2. Binary Details

*(a)*Name: *sn.dat*

*(b)*File: *sn.dat: ELF 32-bit LSB executable, Intel 80386, version 1, statically linked, stripped*

(c) File details.

Permissions:	*-rwxr-xr-x*
File owner	*root*
File size	*399124*
Last modified[18] time,	*Fri Jul 12 12:13:12 2002*
Last change time	*Thu Apr 11 09:29:58 2002*

This date time is stored within the zip archive and is the same for the text file containing the MD5 hash. This may bear no relevance to the case and cannot be used in support of any conclusions about the use (or otherwise) of the binary on the seized system.

*(d)*MD5 hash: *0e954f43fd73f56e812a7285f32e41d3 sn.dat*

(e)Keywords: The following is a list of interesting keywords extracted:

```
/usr/share/zoneinfo
unknown physical layer type 0x%x
Cannot send after transport endpoint shutdown
Transport endpoint is not connected
Transport endpoint is already connected
Software caused connection abort
Network dropped connection on reset
Cannot assign requested address
Address family not supported by protocol
Protocol wrong type for socket
Socket operation on non-socket
Interrupted system call should be restarted

Invalid or incomplete multibyte or wide character
C/o Keld Simonsen, Skt. Jorgens Alle 8, DK-1615 Kobenhavn V
ISO/IEC JTC1/SC22/WG20 - internationalization
DST not allowed in SUID/SGID programs

priv 1.0
ADMsniff %s <device> [HEADERSIZE] [DEBUG]
ex   : admsniff le0
 ..ooOO The ADM Crew OOoo..
cant open pcap device :<
init_pcap : Unknown device type!
```

18Of file status information

```
ADMsniff %s  in libpcap we trust !
credits: ADM, mel , ^pretty^ for the mail she sent me
The_l0gz
@(#) $Header: pcap-linux.c,v 1.15 97/10/02 22:39:37 leres Exp $ (LBL)
@(#) $Header: pcap.c,v 1.29 98/07/12 13:15:39 leres Exp $ (LBL)
@(#) $Header: savefile.c,v 1.37 97/10/15 2 1:58:58 leres Exp $ (LBL)
@(#) $Header: bpf_filter.c,v 1.33 97/04/26 13:37:18 leres Exp $ (LBL)

linux socket: %s
linux SIOCSIFFLAGS: %s
GCC: (GNU) 2.96 20000731 (Red Hat Linux 7.1 2.96 -97)
```

5.Program Description

The file is a binary program which operates as a “network sniffer”. Sniffers are applications used to monitor and validate network traffic. They can read packets that travel the network at various levels of the OSI layer. Like most security tools they can be used for both good and malicious purposes. They are frequently installed by intruders in order to record usernames and passwords of other network users (they can capture passwords are often transmitted in clear text by remote applications such as telnet).

The first clue that this program is a sniffer are the references to “pcap” (Packet CAPture) in the file's strings. This library is a key ingredient in any packet sniffer (including Win32 software) and is vital to the operation of Snort.

The program is reported as an Intel 80386 class ELF binary which implies that the operating system is likely to be Linux or *BSD. From the appearance of the string `pcap-linux.c` the program appears to have been written in C for the Linux operating system, probably Red Hat 7.1.

The binary is statically linked. This means that the executable contains not only the compiled code written by the programmer, but also object code from the appropriate libraries.

The executable has also been stripped and therefore has no symbol table. It is possible to reveal more information about the file using objdump. For example it is possible to discover the compiler used to produce the program by examining the comment section of the binary. The listing of ELF sections can be easily extracted using the Readelf facility and the results of this action are included in Appendix A.

```
objdump -j -comment -s sn.dat | head

sn.dat:     file format elf32-i386

Contents of section .comment:
 0000 00474343 3a202847 4e552920 322e3936  .GCC: (GNU) 2.96
 0010 20323030 30303733 31202852 65642048   20000731 (Red H
 0020 6174204c 696e7578 20372e31 20322e39  at Linux 7.1 2.9
 0030 362d3937 29000047 43433a20 28474e55  6-97)..GCC: (GNU
```

```
0040 2920322e 39362032 30303030 37333120  ) 2.96 20000731
0050 28526564 20486174 204c696e 75782037  (Red Hat Linux 7
```

This reveals that the compiler gcc 2.96 was used, and also reveals more about the Red Hat kernel used.

Although it is possible to further disassemble the executable using objdump, this can be a prolonged, difficult process.

Therefore the next step was to run the program on the Vmware Linux machine with the monitoring procedures described earlier in operation.

Running any suspect program must be undertaken with care. This procedure should only be carried out once the initial analysis steps detailed below have been performed. Even then, only an isolated sacrificial system (such as the one outlined above) should be used.

When the program is activated from the command line (having first had appropriate execute permissions added), what appears to be a “usage” message is produced. This corresponds to some of the strings found within the file. This output is shown on the screenshot of illustration 2.

It appears that an network interface needs to be passed as a command line argument to the program. Using the primary (virtual) interface eth0 the following output is produced:

```
ADMsniff priv 1.0  in libpcap we trust !
credits: ADM, mel , ^pretty^ for the mail she sent me
```

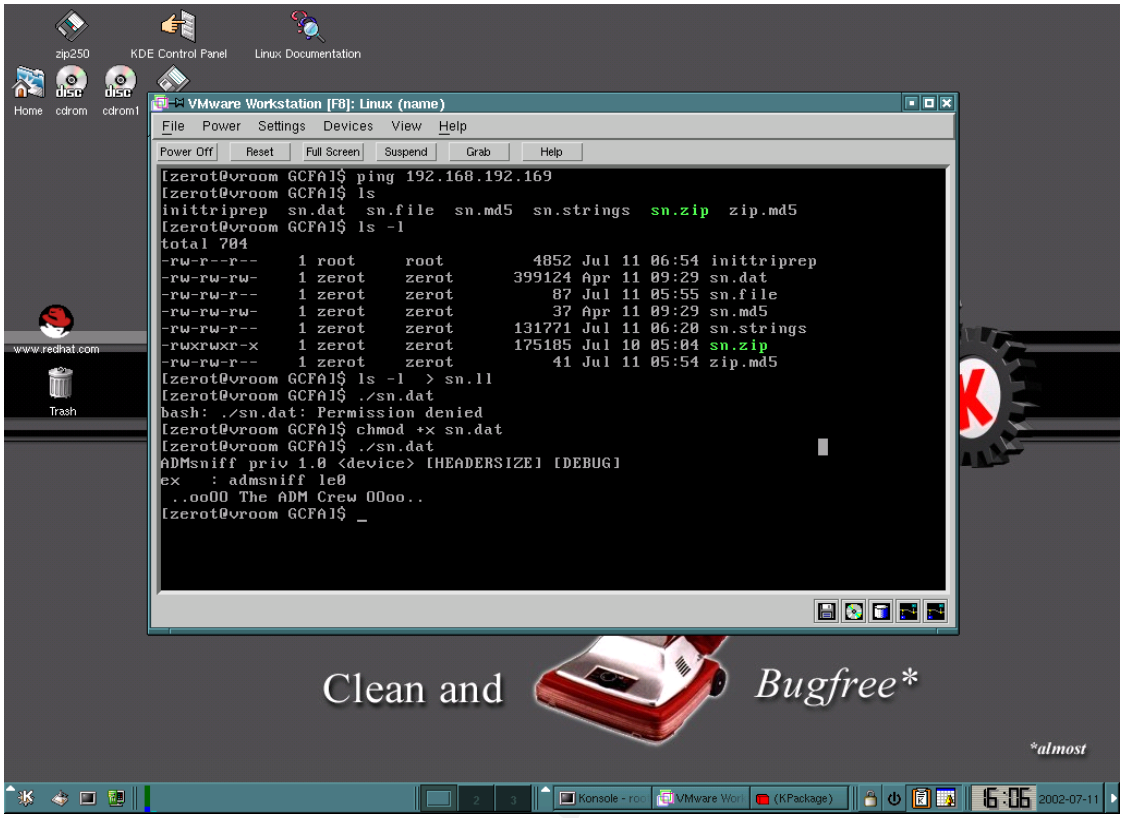


Illustration 5: Red Hat Linux 7.2 platform running an instance of the same operating system as a virtual machine. The suspect program has been run from within this virtual operating system.

The command prompt is not returned - it appears that the sniffer is now active. An entry in /var/log/messages file confirms this:

```
Jul 13 18:27:30 GnR kernel: device eth0 entered promiscuous
mode
```

Network cards must be switched into promiscuous mode. This means they receive and pass *all* packets they see up the stack, regardless of whether they are intended for that specific card as identified by its MAC address.

The suspect file itself is not altered during its execution. Therefore there is no way of establishing when it was last used from the binary file itself. Displaying the last modified time on the seized computer or examining the messages log file might provide this information.

These are the results obtained from the monitoring software:

v)No packets from the virtual machine were recorded by Snort.
vi)None of the files included in the Tripwire database were modified.

It appears that the program is reasonably covert and inoffensive. It does not try to make contact with any external entity when executed (it contains no spyware), nor does it alter any files of the computer on which it is installed. This fits the profile of a clandestine tool which would be popular with hackers or other users who do not wish to draw attention to themselves on the machine on which they wish to operate network sniffer.

By tracing the actions performed by the binary as it executes it is possible to build up a picture of how the sniffer works. These details are included in the next section.

6. Forensic Details

The statically compiled binary appears to operate adequately on the Linux analysis computer without the need for compilation or any other supporting files. Therefore the forensic footprints which will be visible to an examiner are limited. If the user did download and build the file from source code rather than just retrieving the binary alone, then a MACTime analysis of the seized computer's hard disk might show evidence of this process. TASK[19], coupled with the Autopsy forensic browser[20], would be ideal tools for performing this analysis.

The system calls and signals produced by the binary on execution can be trapped and recorded using the strace utility:

```
strace -ffo sn_strace ./sn.dat lo
```

In the example above the sniffer is run against the loopback interface from within strace. This utility is configured to record similar debug information for any child processes forked by the primary execution thread. The details are recorded in files whose names will begin with “sn_trace”. While the sniffer is operating, a telnet session is initiated against the localhost interface. A single strace output file is created, the output from which is listed below. Line numbers are added to aid the discussion.

```
2.execve("./sn.dat", ["./sn.dat", "lo"], [/* 24 vars */]) = 0
3.fcntl64(0, 0x1, 0, 0xbffffb54)          = 0
4.fcntl64(0x1, 0x1, 0, 0xbffffb54)        = 0
5.fcntl64(0x2, 0x1, 0, 0xbffffb 54)        = 0
6.uname({sys="Linux", node="GnR" , ...})   = 0
7.geteuid32()                             = 0
8.getuid32()                              = 0
9.getegid32()                             = 0
10.getgid32()                              = 0
11.brk(0)                                   = 0x80ab488
12.brk(0x80ab4a8)                          = 0x80ab4a8
13.brk(0x80ac000)                          = 0x80ac000
14.socket(PF_INET, SOCK_PACKET, 0x300 /* IPPROTO_??? */) = 3
15.bind(3, {sin_family=AF_INET, sin_port=htons(27759),
  sin_addr=inet_addr("0.0.0.0")}}, 16) = 0
16.ioctl(3, 0x8927, 0xbffff970)            = 0
17.ioctl(3, 0x8921, 0xbffff970)            = 0
```

19 Available from www.atstake.com/research/tools/task
20 Available from www.atstake.com/research/tools/autopsy

```
18.brk(0x80b1000)                          = 0x80b1000
19.fstat64(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 2), ...}) = 0
20.old_mmap(NULL, 40 96, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS,  -1, 0) =
  0x40000000
21.write(1, "ADMsniff priv 1.0  in libpcap we"..., 41) = 41
22.write(1, "credits: ADM, mel , ^pretty^ for"..., 54) = 54
23.open("The_10gz", O_WRONLY|O_CREAT|O_TRUNC, 0666) = 4
24.recvfrom(3, "\0\0\0\0\0\0\0\0\0\0\0\10\0E\20\0<k5@\0@\6\321t\177\0"...,
  16498, 0, {sin_family=0x304 /* AF_??? */, {sa_family=772,
  sa_data="lo\0\0\0\0\0\0\0\0\0\0\0\0\0"}, [18]) = 74
25.ioctl(3, 0x8906, 0xbffff960)            = 0
26.time(NULL)                              = 1026 639906
27.time(NULL)                              = 1026639906
28.time(NULL)                              = 1026639906
29.recvfrom(3, "\0\0\0\0\0\0\0\0\0\0\0\10\0E\20\0<k5@\0@\6\321t\177\0"...,
  16498, 0, {sin_family=0x304 /* AF_??? */, {sa_family=772,
  sa_data="lo\0\0\0\0\0\0\0\0\0\0\0\0\0"}, [18]) = 74
30.ioctl(3, 0x8906, 0xbffff960)            = 0
31.time(NULL)                              = 1026639906
32.time(NULL)                              = 1026639906
33.recvfrom(3, "\0\0\0\0\0\0\0\0\0\0\0\10\0E\20\0(\0\0@\0\377\6}\275"..., 16498,
  0, {sin_family=0x304 /* AF_??? */, {sa_family=772,
  sa_data="lo\0\0\0\0\0\0\0\0\0\0\0\0\0"}, [18]) = 54
34.ioctl(3, 0x8906, 0xbffff960)            = 0
35.brk(0x80b2000)                          = 0x80b2000
36.time(NULL)                              = 1026 639906
37.time(NULL)                              = 1026639906
38.fstat64(4, {st_mode=S_IFREG|0644, st_size=0, ...}) = 0
39.old_mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS,  -1, 0) =
  0x40001000
40.write(4, "\n--=[ 127.0.0.1:23  --> 127.0.0.1"..., 45 ) = 45
41.recvfrom(3, "\0\0\0\0\0\0\0\0\0\0\0\10\0E\20\0(\0\0@\0\377\6}\275"..., 16498,
  0, {sin_family=0x304 /* AF_??? */, {sa_family=772,
  sa_data="lo\0\0\0\0\0\0\0\0\0\0\0\0\0"}, [18]) = 54
42.ioctl(3, 0x8906, 0xbffff960)            = 0
43.time(NULL)                               = 1026639906
44.time(NULL)                              = 1026639906
45.write(4, "\n--=[ 127.0.0.1:23  --> 127.0.0.1"..., 45) = 45
46.recvfrom(3, 0x80ab8a2, 16498, 0, 0xbffff970, 0xbffff95c) = ? ERESTARTSYS (To be
  restarted)
47.--- SIGINT (Interrupt) ---
48.+++ killed by SIGINT +++
```

Line 5: The operating system and computer hostname are enumerated via calls to the uname facility.
Lines 6-9: The userids and execution privileges are enumerated. If the program is run with insufficient privilege it will be unable to bind to the network interface (line 14).
Lines 20-21: The greetings text is written to stdout.
Line 22: It can be seen that the program opens and writes to a file called The_10gz in the directory from which the program was executed. This could also be searched for on the seized computer's filesystem, possibly as part of a MACTime analysis. Lines 39 & 44: The strace output above shows the information related to the telnet to localhost being written to this file on the analysis machine.
Line 47: Execution is terminated by ctrl-c signal.

Another important clue to establishing whether the binary has been run on the seized machine is that the program switches the network interface on which it is listening into promiscuous mode. Unless the user has sufficient privilege on the system to alter logs, the messages file may reveal when the program was used.

From the strings obtained earlier from the file the name (and a possible address) Keld Simonsen was retrieved. An investigator should always resist the urge to immediately report an individual identified in this way to Law Enforcement. Much of the software available on the internet has evolved in an iterative way, building on the work of others. A binary file, especially one with statically linked libraries may contain compiled code originally produced by numerous people. The actual person who built and produced the final binary may be completely dissociated from these programmers. A search at Google reveals a number of hits for Keld Simonsen, typically on German web-sites.

At this stage of the investigation, we have a clear indication of the binary's intended use and the “real name” of the application. Given this information the next step is to try to locate the program on the internet.

7.Program Identification

When the program is run it identifies itself as ADMsniff v1.0. The seized executable appears to have been built on a Red Hat Linux 7.1 computer, so in order to exactly duplicate this binary it might have been necessary to install a Vmware virtual machine running this distribution and version of Linux. However as the current analysis machine used so far was Red Hat 7.2 with gcc compiler version 2.96-98, it seemed sensible to at least attempt the reconstruction on this machine and hope that minor differences between the two versions would not lead to significant variation in the final executable.

A search at Google provides a number of sites offering the ADMSniff program for download. Two versions - v0.8 and the v1.0 of interest - were available. The complete package is distributed as a compressed tar file.

ADMsniff.tgz was downloaded[21] and un-buttoned to produce:

```
-rw-r--r--    1 root     root        18815 Jul 12 10:24 adm.strings
-r--r--r--    1 root     root         8447 Jan 19  1999 bpf.h
-rw-r--r--    1 root     root          486 May  7  1999 ip.h
drwxr-xr-x    6 root     root         4096 Jul 12 17:42 libpcap -0.4
-rw-r--r--    1 root     root       487424 May  7  1999 libpcap -0.4.tar
-rw-r--r--    1 root     root        91142 Jul 12 17:4 2 libpcap.a
-rw-r--r--    1 root     root          770 Jul 12 17:42 Makefile
-rw-r--r--    1 root     root         4908 Jan 19  1999 pcap.h
-rw-r--r--    1 root     root         1072 May 30  1999 README
-rw-r--r--    1 root     root         1491 Jan 19  19 99 tcp.h
-rw-r--r--    1 root     root           92 Jul 12 14:17 The_l0gz
-rw-r--r--    1 root     root         8432 May 11  1999 thesniff.c
```

The makefile has two optional sections (for SUNoS libraries and log compression). Initially these were left out and the Makefile left unchanged. Running `make` for the first time produced an error pointing to the absence of the zlib libraries (the Readme

21From www.unixhq.org/june-1999-rs.shtml

makes reference to this, and indicates that the user should install this package if they wish to use compressed log files). The Zlib-1.1.3-24 rpm was installed onto the Linux virtual machine and the compilation process re-run. This time it completed with no errors. However the file created was a different size than the suspect program:

```
-rwxr-xr-x    1 root     root        37632 Jul 12 17:39
ADMsniff-1
```

It was already known that the suspect program is statically linked so the -static option is added to the gcc flags within the makefile. After subsequent recompilation the program which is now produced is much too large when compared with the original suspect version sn.dat:

```
-rwxr-xr-x    1 root     root      1719300 Jul 12 17:42
ADMsniff-1
```

Finally the object file must be stripped to discard symbols. Running the strip command produced a final program identical in size to the suspect file:

```
-rwxr-xr-x    1 root     root       399124 Jul 12 17:44
ADMsniff-1
```

Calculating an MD5 hash for the file produced an identical value to that of the suspect file.

```
0e954f43fd73f56e812a7285f32e41d3  ADMsniff-1
```

Further testing on the Linux virtual analysis machine demonstrated that ADMsniff-1 exhibited exactly the same executional behaviour as the seized sn.dat.

8.Legal Implications

This binary has been shown to be a network sniffer. Under UK law, the use of such a program would be categorised as the interception of a communication channel. Part Three of this assignment covers the relevant legislation which mediates in such cases. There are a number of situations in which the use of this program would be perfectly legal. Basically if the user of the program were a System Administrator, or another individual charged with ensuring that the computer(s) deliver a reasonable level of service, then its use would be justified if in support of this aim providing reasonable efforts were made to inform other users of the system that monitoring was carried out.

In this case there is insufficient evidence to prove that the binary had been run on any other system. As shown in Section 4, it is possible to produce an identical copy of the binary. Without access to the seized computer from which the file came (to perform MACTime analysis or view log files), there is no way to establish whether the program was just executed or merely downloaded to the computer's filesystem. A forensic image of the computer's hard disk, or at the very least, the partition on which

it was found, would be required to produce conclusive proof that this program had been operated. Ideally this image would have been taken as soon as possible after the discovery of the suspect binary. A list of active processes at that time might also be helpful: indication that the sniffer was running would offer irrefutable evidence that the program had been used!.

Under the UK Criminal Misuse Act (CMA) , if no authorisation for this act had been granted to the perpetrator, even installing this program , regardless of its intended use, may be an offense in its own right. Penalties under the CMA range from 6 months in prison for a small infringement to 5 years in prison on indictment of persistent hacking.

As is also detailed in Part Three of this assignment, The Human Rights Act (HRA) and The Regulation of Investigatory Powers Act (RIP) both contain recommendations on the need for an acceptable use policy. My organisation has such a policy and unauthorised use of a network sniffer or similar monitoring software would be a clear breach of this and the Security Operating procedures for our networks.

9.Interview Questions

If further investigation as described above proved that the binary had indeed been executed and a suspect was identified, the following questions might be helpful during the course of an interview. It is assumed that forensic studies have also revealed the user account which installed the package, and the date and time at which the program was executed. Ideally such an interview should be conducted with a third party present to provide corroboration at a later date if necessary.

Preamble: *We've asked you to come and see us because we are investigating some unusual behavior that has been detected on the JKL network. We are trying to understand what has been going on so that we can formally record the incident and get on with normal operation. We are speaking to some of the users of the network to try and find out what happened before the matter is escalated and senior management get involved.*

Are the registered user of account XYZ?

What are your normal duties as a user of computer ABC?

Are you aware of anyone else who has access to account XYZ?

Were you logged on to computer ABC on DAY of MONTH?

At what time do you remember being logged on?

Can you remember what work were you carrying out on ABC at this time?

Did you download any software during this session?

Did you build or compile any software during this session?

Did you create the file sn.dat?

Did you execute the file sn.dat?

Hopefully at this point the user will come clean and admit to running the sniffer. Typically the user may just be curious about network security, perhaps having purchased a “Hacking Exposed” book or even after having their interest heightened having attended a SANS conference!

If the user denies using the sniffer, it may be necessary to reveal more of our investigative work.

I can see from the firewall logs that you've been visiting some web-sites that deal with network security... you might have seen some papers on computer forensics... it is quite amazing the kind of things that can be discovered by analysing a computer hard disk... what sort of stuff might we find if we looked at your workstation using forensic software?

Concentrate on getting the user to first admit that they were logged in at the time the program was used:
Our organisation's acceptable use policy says that you must not divulge your password to anyone else, and the system forces the use of strong passwords. If you weren't logged-in, how did someone else gain access to your account?

Well, you admit that you were logged in at that specific time on the day. In fact the e-mail logs show that you sent some messages to PQR. You say that you didn't run this program... are you sure you don't remember compiling some software?

I think this kind of software is really great. You can use it to see exactly what's going on, on the network. It's pretty fascinating stuff. There's no problem with running it if you were just curious, we just need to assure senior management that nothing malicious has been going on. They don't really care about the details, they just want to know that our security is intact.

If the user still insists on denying the use of the tool it may be necessary to refer the matter to internal disciplinary procedures or even Law Enforcement. At this stage it is worth laying out all the evidence you have collected and giving the user one last chance to confess.

10. Additional Information

The UK Computer Misuse Act: www.lancs.ac.uk/users/iss/rules/cmisuse.htm

Excellent examples of reverse engineering from the results from HoneyNet Reverse Challenge: www.honeynet.org/reverse/results

Basic Packet-Sniffer Construction:
www.unixgeeks.org/security/newbie/security/sniffer/sniffer_construction.txt

Discussion about Sniffers including ADMSniff: www.cotse.com/tools/sniffers.htm

Help on using Binutils resources: www.gnu.org/software/binutils/binutils.html

Detailed discussion and explanation of ELF binaries:
www.cs.ucdavis.edu/~haungs/paper/node10.html

Appendix A: Output from Readelf for unknown binary.

```
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF32
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX  - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Intel 80386
  Version:                           0x1
  Entry point address:               0x80480e0
  Start of program headers:          52 (bytes into file)
  Start of section headers:          398364 (bytes into file)
  Flags:                             0x0
  Size of this header:               52 (bytes)
  Size of program headers:           32 (bytes)
  Number of program headers:         3
  Size of section headers:           40 (bytes)
  Number of section headers:         19
  Section header string table index: 18

Section Headers:
  [Nr] Name              Type            Addr     Off    Size   ES Flg Lk Inf Al
  [ 0]                   NULL            00000000 000000 000000 00      0   0    0
  [ 1] .init             PROGBITS        080480b4 0000b4 000018 00  AX  0   0  4
  [ 2] .text             PROGBITS        080480e0 0000e0 048080 00  AX  0   0 32
  [ 3] .fini             PROGBITS        08090160 048160 00001e 00  AX  0   0  4
  [ 4] .rodata           PROGBITS        08090180 048180 012be0 00   A  0   0 32
  [ 5] __libc_atexit     PROGBITS        080a2d60 05ad60 000004 00   A  0   0  4
  [ 6] __libc_subfreeres PROGBITS        080a2d64 05ad64 000040 00   A  0   0  4
  [ 7] __libc_subinit    PROGBITS        080a2da4 05ada4 000008 00   A  0   0  4
  [ 8] .data             PROGBITS        080a3dc0 05adc0 001260 00  WA  0   0 32
  [ 9] .eh_frame         PROGBITS        080a5020 05c020 000d64 00  WA  0   0  4
  [10] .ctors            PROGBITS        080a5d84 05cd84 000008 00  WA  0   0  4
  [11] .dtors            PROGBITS        080a5d8c 05cd8c 000008 00  WA  0   0  4
  [12] .got              PROGBITS        080a5d94 05cd94 000010 04  WA  0   0  4
  [13] .sbss             PROGBITS        080a5da4  05cdc0 000000 00   W  0   0  1
  [14] .bss              NOBITS          080a5dc0 05cdc0 0056c8 00  WA  0   0 32
  [15] .comment          PROGBITS        00000000 05cdc0 0032d6 00      0   0  1
  [16] .note.ABI-tag     NOTE            08048094 000094 00002 0 00   A  0   0  4
  [17] .note             NOTE            00000000 060096 0012d4 00      0   0  1
  [18] .shstrtab         STRTAB          00000000 06136a 0000af 00      0   0  1
Key to Flags:
  W (write), A (alloc), X (execute), M (merge), S (strings)
  I (info), L (link order), G (group), x (unknown)
  O (extra OS processing required) o (OS specific), p (processor specific)

Program Headers:
  Type           Offset   VirtAddr   PhysAddr   FileSiz MemSiz  Flg Align
  LOAD           0x000000 0x08048000 0x 08048000 0x5adac 0x5adac R E 0x1000
  LOAD           0x05adc0 0x080a3dc0 0x080a3dc0 0x01fe4 0x076c8 RW  0x1000
  NOTE           0x000094 0x08048094 0x08048094 0x00020 0x00020 R   0x4

 Section to Segment mapping:
  Segment Sections...
   00     .init .text  .fini .rodata __libc_atexit __libc_subfreeres __libc_subinit
.note.ABI-tag
   01     .data .eh_frame .ctors .dtors .got .bss
   02     .note.ABI-tag

There is no dynamic segment in this file.

There are no relocations in this file.
```

```
There are no unwind sections in this file.

No version information found in this file.
```

Part 3 - Legal Issues of Incident Handling: Wiretap Statute

Status as of 1st May 2002

1) Introduction

There are a number of laws and documents which affect the legality of network traces and other interceptions of communication channels by UK-based system administrators. The legal structure behind the various rules and rights that relate to legal monitoring are quite complex and often overlap. In essence, however, they all boil down to striking a balance between the right of an individual employee to privacy and the legitimate requirements of an employer to process information/data .

Relevant legislation:
11. The Human Rights Act
12. The Regulation of Investigatory Powers Act.
13. The Computer Misuse Act.
14. The Telecommunications (Lawful Business Practice) (Interception of communications) Regulations
15. The Data Protection Act.
16. The Code of Practice on the use of Personal Data in Employer/Employee Relationships
17. Employment Rights act 1996

7. The Laws: The Human Rights Act

Introduced on the 2nd October 2000, the United Kingdom's Human Rights Act (HRA) incorporated into UK law the main principles of the European Convention for the protection of Human Rights and Fundamental Freedoms.

Although the HRA itself only has effect upon the actions of "public bodies" , Courts and Tribunals are legally bound to take the provisions of the HRA into consideration when interpreting employment legislation under which an employee is making a claim. For example, a number of lawyers speculated that a sacked employee could allege constructive dismissal if their telephone calls or e-mails had been monitored. In this case the tribunal might throw out any evidence of wrong-doing obtained in this way because it breached the employee's right to privacy under the HRA.

These predictions were later proven in law. In the case of Halford v United kingdom 1997 IRLR 471, Alison Halford, a senior police officer alleged that her employer had tapped her private work telephone. She successfully claimed that this was a breach of her rights under The Convention. The European Court of Human Rights held that, as her employer had not given her any prior warning that her telephone calls were liable to interception, she would have had a reasonable expectation of privacy for such calls. The fact that the calls were made

from her workplace did not mean that they were not covered by her right to privacy under The Convention.

xiii)The Laws: The Regulation of Investigatory Powers Act

The previous arrangements for the interception of communications were established in the Interception of Communications Act 1985. The RIP Act repealed the 1985 act and provided a new regime incorporating changes proposed in the Interception of Communications in the United Kingdom (CM 4368) consultation paper published in June 1999.

The Regulation of Investigatory Powers Act 2000 (RIP) updated the legislation governing the interception and monitoring of communications and covers both civil and criminal liability. The main purpose of the act is to ensure that the relevant investigatory powers are applied in accordance with human rights. One of the difficulties encountered by the United Kingdom when defending the claim by Halford was that The Interception of Communications Act 1985 covered only telephone calls made on public lines and therefore did not extend to calls made on private networks. The new Act covers the interception of communications made via public postal systems, public telecommunications systems and private telecommunications systems. It applies to England, Wales, Scotland and Northern Ireland. The Act deals with the acquisition of communications data which includes traffic data such as billing information and other data associated with an individual's use of a system.

Two sections of The Act are applicable to wiretaps.

Section 1 of The Act states that it is unlawful to intentionally intercept communications over a public or private telecommunications system without lawful authority. Article 20 of this section seeks to distinguish between a communication and communication data (for an e-mail this might be the content and the transmission headers). The definition provided is somewhat vague in that communications data is said to include “any information which includes none of the contents of a communication”. Referring to an EU document ENFOPOL 98, this categorises IP addresses, account logon IDs, e-mail addresses and details such as who sent and received a message, as communications data.

Section 2 defines the meaning and location of interception. Specifically a private communications system is defined as “any telecommunication system which is not a public telecommunications system; but is attached to such a system. This means that an office network, linked to a public telecommunication system by a private exchange, is to be treated as a private system.” It is in this section that the notion of a system administrator is introduced: “interception of such a system other than by the system controller or with his consent is a criminal offense.” Interestingly an “entirely self-standing system... such as a secure intranet, does not fall within the definition”. On the specific topic of e-mail this section notes that there are times when a communication is not actually in transit and may reside on an intermediate Mail Transfer Agent (MTA). Accessing the data in this location still constitutes interception.

The RIP Act enables employees to sue their employer if the employer unlawfully intercepts or monitors telephone calls or e-mail messages on its networks.

Initially it would appear that the surreptitious monitoring of employees' communications is impossible. Fortunately the Secretary of State was granted powers under RIP to issue regulations authorising the interception and recording of communications where reasonably required for business purposes.

Specifically, section 3 of RIP deals with lawful interception without a formal warrant. For example it states that if *both* parties to the communication can reasonably be believed to have consented to the interception then section 1 need not apply. Similarly if such conduct is in relation to the provision or operation of services then no warrant is needed. Lawful interception and the issuing of warrants is covered in section 4 of the Act.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 subsequently came into force on 24th October 2000.

These regulations allow employers to perform monitoring even if the employee has not given explicit consent, as long as it is for one of the reasons listed below:

3. To establish the existence of facts (i.e. recording evidence of business transactions).
4. To ascertain compliance with regulatory or self-regulatory practices.
5. To maintain the effective operation of the employer's systems.
6. For quality control purposes (for example, monitoring standards of training and service).
7. To prevent or detect criminal activity.
8. To prevent or investigate the unauthorised use of the computer/telephone system (i.e. ensuring that an employee does not breach the company's e-mail or telephone policies.
9. If it is in the interests of National Security.

For example, system operators may monitor (but not record) system traffic to determine its source where this is necessary to ensure the effective performance of their mail servers, for example to eliminate unsolicited commercial email (UCE or `spam').

Thus interception is not a criminal offense where the person intercepting the communication is a person with a right to control the relevant *private* telecommunications network, or a person who has express or implied permission of such a person to intercept communications on that private network. In such circumstances, the interception may, if it is made "without lawful authority", instead give rise to a civil action on behalf of the sender or the recipient of the communication. In this way the use of any network/packet sniffer without the authority of the owner of the network is likely to be a criminal act under either the Computer Misuse Act 1990 or the Regulation of Investigatory Powers Act 2000.

vii)The Laws: The Computer Misuse Act 1990.

In the late 1980s there was considerable concern that United Kingdom law was inadequate to deal with computer hacking. Attempts to charge hackers with theft of electricity were not found to be viable. Moreover, laws such as the Telecommunications Act and Interception of Communications Act did not apply to private networks or to the common situation where a hacker instituted and received communications rather than intercepted them. Consequently a private member's bill became law as the Computer Misuse Act in 1990.

Despite the apparent exemptions which allow employers to intercept communications, the regulations still place the onus on the employer to take reasonable steps to inform employees that their communications might be intercepted. An e-mail/network usage policy is therefore a stringent requirement for any organisation. This should clearly establish the right to monitor communications. Informing users of the system may also take the form of clauses in employment contracts and/or regular reminders in the form of notices in offices and stickers on computers and login banners. As yet, however, the courts have not had the chance to decide exactly what constitutes `reasonable'. However, since the publication of the Computer Misuse Act 1990 it has been strongly recommended that computers display a banner before allowing users to log in. The Act stipulates that an offence of unauthorised access can only be committed if the offender knew at the time that the access he intended to obtain was unauthorised. Login banners have always been viewed as the best way to achieve this. Of course many computer intrusions are perpetrated without the attacker actually logging in by conventional means (for example by pressing ctrl-alt-del at an NT login window). However United Kingdom Courts will generally accept that, if established and intentional avenues of communication with the computer (login screen, remote access greetings, web-sites etc) carry suitable warnings, then the victim can be shown to have made all reasonable efforts to inform people of what they authorised to do on the system. The same approach is advised for organisations seeking to advice users of their rights with regard to monitoring.

49.The Laws: The Data Protection Act.

The DPA is generally accepted as being a difficult document to interpret. Under the terms of the Act, there are certain requirements placed upon any organisation (as a “data controller” within the meaning of the Act) in respect of “personal data” (i.e. Data relating to a living being that can be identified either from the data alone or from the data and some other information held by the data holders) that is processed. “Processing” was originally broadly defined as the holding of the automated data as well as obtaining and disseminating it. In October 2001 the Act was extended to manual records that form part of a relevant filing system. In terms of a wiretap, it is never known exactly what traffic may be intercepted - it may be a flirtatious e-mail or a member of staff's end-of-year appraisal - so it must assumed that personal data is being recorded. Therefore such recordings must comply with the appropriate data protection principles, which are that any personal data must be:

2.processed fairly and lawfully
3.processed for limited purposes
4.adequate, relevant and not excessive
5.accurate
6.not kept for longer than necessary
7.processed in accordance with an individual's rights
8.secure

This is mostly self-explanatory but the first item requires further elaboration. In order for processing to be lawful it must satisfy one of the following:

- the employee has given consent
- the processing is necessary to the performance of a contract
- the processing is necessary to pursue the legitimate interests of the employer

To establish fair processing, regard must be given to the method by which the data was obtained. Information must also be given to the employees about the purposes of which the processing will be conducted.

50.The laws: Employment Rights Act 1996

Typically, if an employer can obtain evidence of a misuse or abuse of their networks by legal means (as defined in the preceding sections), then it may be relatively easy to assess whether the abuse amounts to gross misconduct sufficient to terminate an employment contract. However the Data Protection Commissioner's proposed standards make it quite difficult to enable an employee to be dismissed purely as a result of viewing or downloading "unacceptable material".

Relevant Employment Tribunal cases:

Morse -v- Future Reality Limited (22.19.96 case No 54571/95)
Parr -v- Derwentside District Council (23.9.98, case No 2501507/98)
Gale -v- Parknotts (17.4.96, case No 72487/95)
Humphries -v- Joinson (10.7.98, Case No 2304001/97)

The consensus from these and other cases is that, if a dismissed employee is prepared to be candid about the web-sites they have visited using their employers internet service, any Employment Tribunal is likely to be sympathetic unless the employer can demonstrate some form of unequivocal instruction written in unambiguous language forbidding access to certain types of material.

51.The Laws: Conclusions

Contention between the HRA and the Telecommunications Regulations still remains. In fact shortly after the Regulations were implemented, the Data Protection Commissioner issued a draft Code of Practice entitled "The use of personal Data in Employer/employee Relationships" which is far more restrictive in its guidelines for monitoring by organisations. The code provides that when monitoring involves the interception of personal electronic communications such as e-mail, it will almost certainly be covered by the Data Protection principles. The employer will then have to consider whether the monitoring intrudes unnecessarily on the employee's privacy. A balance should be reached such that any intrusion should be in proportion to the benefits of the monitoring to the employer. In particular it states that the interceptor should " unless monitoring would be ineffective and the circumstances justify the additional intrusion:

2.Limit monitoring to traffic data rather than the contents of communications.
3.Undertake spot checks rather than continuous monitoring.
4.As far as possible, automate the monitoring so as to reduce the extent to which extraneous information is made available to any person other than the parties to a communications.
5.Target monitoring on areas of highest risk."

This draft code also notes that individuals have no control over the content of e-mails which

are sent to them. It accepts that there is "no obvious, practical way of giving advance warning to those sending personal e-mails to an employee at his/her address that they might be intercepted by others".

It also provides greater guidance on the level of monitoring which should take place. The actual content of messages (as opposed to just the headers and address information) should only be recorded if this header (or "traffic " record) is "not sufficient to achieve the business purpose use". Following from the previous point, an interceptor should take account of the privacy of those sending e-mails into their organistion. On the specific subject of anti-virus protection, the Code suggests that, in this case, content monitoring may take place if performed by a purely automatic procedure. It specifically states that "a need for virus protection does not warrant the reading of the content of incoming e-mails".

For general internet access (for example web-sites which are visited by staff) , there is a recommendation that any monitoring should be proportionate to the risk faced by the employer. Such measures should therefore be designed to prevent rather than detect misuse.

Because of the inter-relationship between the RIP Act, the Lawful Business Regulations, the Data Protection Act and any code issued under it, it is necessary not only to warn employees of interception as required by this legislation but also to obtain consent from employees to interception and to the processing of data. Since under the Data Protection Act if interception involves obtaining, recording or otherwise processing personal data by means of automated equipment e.g. recording calls or filtering e-mails, this will fall within the scope of the Data Protection Act and consent will be required.

Although there is a potential conflict here between the much wider power given by the Telecommunications Regulations, this may be explained by the fact that, at the time the code was drafted, the details and recommendations of the HRA and RIP were well publicised whereas the Telecommunications Regulations had not yet been published.

Both documents do agree on the need for an acceptable use policy. Collectively there are a number of recommendations as to what form such a policy should take:

2. It should be in writing.
3. It should be clearly communicated to all employees.
4. It must contain specific details of permissible uses of both e-mail and the Internet and set out acceptable online behaviour.
5. It must contain clear definitions of the form any monitoring will take.
6. It should set out privacy rules in relation to both the employer's right to monitor and other users.
7. Any disciplinary consequences of breaching the policy should be explained.
8. Any prohibited uses or unauthorised access areas should be stipulated.

In my organisation, following detailed research by our legal experts, we have determined that any monitoring carried out is legal and conforms to the requirements of all relevant legislature. We have warning banners which inform users that their use of the system may be monitored and that that have no expectation of privacy relating to this use. The message also states that, by continuing to logon, the user consents to these conditions. Additionally we have

in place acceptable use policies for our internal and externally-connected networks. All access avenues to our externally connected systems have suitable banners warning users that authorisation is required to use the computer facilities. An acceptable use policy is posted on our community internet web-site.

8) References

The Regulation of Investigatory Powers Act 2000
www.hmso.gov.uk/acts/acts2000/20000023.htm
www.homeoffice.gov.uk/ripa/ripact.htm

Data Protection Commissioner:
www.dataprotection.gov.uk/commissioner.htm

The use of personal Data in Employer/employee Relationships
www.dataprotection.gov.uk/dpr/dpdoc.nsf

Human Rights Act 1998 Chapter 42
www.hmso.gov.uk/acts/acts1998/19980042.htm

Computer Misuse Act 1990
www.legislation.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

The Telecommunications (Lawful Business Practice) (Interception of communications) Regulations
www.hmso.gov.uk/si/si2000/20002699.htm

ENFOPOL www.fipr.org/polarch/enfopol19.html