Submitted on 14 January 2005 for the GIAC Certification program
for Computer Forensics
(Track 8 Assignment Version 1.5)

by

Stephen Armstrong

The two parts selected for completion:

In scenario analysis of the Floppy Disk image
(obtained from GIAC Web site).

&

The Analysis of a Hard Disk recovered from an abandoned
Computer.

Table of Contents

Abstract

This document is submitted as the practical part of the GCIA Certified Forensic Analyst program (GCFA)[1].

This practical is in two parts, the first of which required an image of a floppy disk to be analysed and a report submitted based upon the contents. During this part of the practical, the investigator discovered traces of a steganographic program (Camouflage.exe). The conclusion being that the owner and holder of the disk had attempted to export company data via this hidden means.

The second part of the practical required the analysis of a system that had been compromised. Due to difficulties obtaining such a system, approval was given for the author to analyse an abandoned pc bought from a refuse disposal facility (thus the investigator had no knowledge as to the contents of the drive, its purpose or the intent of the user).

During the second phase of this practical the contents of the abandoned system's hard drive was examined to glean the user's role, their style and skill in operating the system. An examination of the drive for illegal or inappropriate data/content was conducted and a comment made as to the possible breaches of UK or International laws. Finally, the drive's owner is identified from the contents of the hard disk, and their recent activities and actions traced.

The conclusion draws the problems and complexities of the whole process together and identifies how a lack of user knowledge resulted in a system being brought to its knees with Spyware before, in an effort to protect it, the user rendered it inoperable by the installed of defensive software.

Report on the Forensic Analysis of a recovered Floppy Disk

Background

On 27 April 2004, the forensic investigator was tasked by Mr Keen to conduct an analysis of a floppy disk recovered from a Robert John Leszczynski, Jr., who was employed by Ballard Industries, as the lead process control engineer for the project to design a new fuel cell battery.

The floppy disk was recovered by a security guard who seized it from the above RJ Leszczynski at 1645 on 24 April 2004. The disk had been in Leszczynski's briefcase, but this was in breach of the Company Security Policy and therefore the guard impounded the disk, forwarding it to Mr Keen to Security Administrator.

The Security Administrator was mindful for the ongoing investigation into customer drift and information leakage and request a full analysis of the disks contents.

The only item of evidence submitted or analysis was a single Floppy Disk. The disk received was identified and described as:

Item 1 – Identification details for recovered Floppy Disk

Description	3.5 inch TDK floppy disk
Serial Number of item:	Tag# fl-260404-RJL1
MD5 Hash of Disk	d7641eb4da871d980adbe4d371eda2ad

The Forensic Workstation

The forensic workstation image was re-ghosted to the laptop and all respective security and reliability patches applied. The workstation used was a Dell [Dell] Inspiron 5100 with removable hard disk caddies containing:

> 1 x 30 gb Linux Fedora Core 2 OS[2], complete (ie the everything option checked during the installation process) and Autopsy[3] v1.7 and The Sleuth Kit[4] v 1.72 installed.
>
> 1 x 30 gb Windows XP Pro[5] (complete build) with Norton AntiVirus 2003[6] (fully patched and up-to-date), Adobe PDF Reader.

All products were updated remotely via removable media and therefore, had never been connected to the internet; thus they can be judged to be forensically and operationally sound in that they will represent accurately all data they process and display. The image of the laptop has been retained for future use and reference should it be required.
Autopsy (v1.70) and The Sleuth Kit were then loaded to perform various analyses on

the image and files within. Due to some compiling issues with The Sleuth Kit v1.72 (TSK), the newer version (v2.03) of Autopsy could not be loaded onto the Forensics System (lib failure with Fedora Core 2 (FC2)). TSK is a collection of command line tools that have been adapted and modified from their original release in the form of 'The Coroner's Toolkit[7] (TCT). Autopsy is a graphical front end to TSK that uses perl to interprets the user's actions and builds the TSK commands in the background. The user interface is via a standard web browser but output is graphical with logs, recovered files, md5 hashes, timeline output etc being stored in a user definable mounted file structure. All these tools are available from <www.sleuthkit.org>.

These programs (Autopsy and The Sleuth Kit) are reputable open source Forensics tools, that themselves have both been subjected to Forensics Analysis to ensure they do not alter or corrupt data being analysed. The output from the Autopsy is in the form of test files that are stored in a folder designated by the initial investigator. These test files are created and md5 hashes performed on each as they are written to the HDD. The md5 hash is stored with the output and then the output is displayed for the investigator. All output listed in this report will be using the text saved by Autopsy (unless otherwise stated). Screen shots included will be of the web interface used by the investigator. Additionally, were command line interface (CLI) instructions, programs or commands are used their output will be reproduced in this report with information on the platform and OS the command was issued from or to.

Backing up the disk

A copy of the recovered floppy disk image was made and an MD5 Sum performed on the image. This MD5 sum was compared with the original and found to be an exact match, indicating the image was a bit for bit reproduction of the original disk. The original disk was then placed in an envelope marked with the details above and the md5 sum of the disk at the time of sealing. The envelope was then sealed and all joints signed by the investigator and the Security Administrator, with all signed parts then covered with anti-tamper tape. The disk was then placed in the fire proof a humidity controlled safe. The investigator has had no access to the disk, envelope or safe since they were secured. The working image of the disk was labelled:

Item 2 – Label details for the Master Working Disk (image)

Description	Image of floppy disk tagged Tag# fl-260404-RJL1
File name of image	V1_5.gz
MD5 Hash of image v1_5.gz	D7641eb4da871d980adbe4d371eda2ad

The `file` (Linux), `md5` (Linux) and `fsum`[8] (Windows) commands were run on the image to confirm it had retained its floppy disk properties despite being imaged.

Item 3 – file (Linux) Command Output of v1_5.gz

Command	`file v1_5.gz`

Output	/root/v1_5.gz: x86 boot sector, code offset 0x3c, OEM-ID " mkdosfs", root entries 224, sectors 2872 (volumes <=32 MB) , sectors/FAT 9, serial number 0x408bed14, label: "RJL ", FAT (12 bit)

Item 4 – md5 (Linux) Command Output of v1_5.gz

Command	Md5 v1_5.gz
Output	d7641eb4da871d980adbe4d371eda2ad /root/v1_5.gz

To prove the md5 software was correct and functioning correctly the same file was hashed on the windows system.

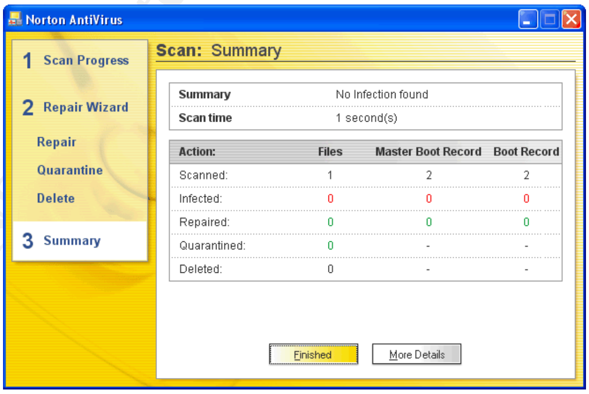
Item 5 – fsum (Windows) Command Output of v1_5.gz

Command	fsum -md5 v1_5.gz
Output	; SlavaSoft Optimizing Checksum Utility fsum 2.0 <www.slavasoft.com> ; ; Generated on 11/09/04 at 21:09:08 ; d7641eb4da871d980adbe4d371eda2ad *v1_5.gz

AntiVirus Scan of the disk image

The disk was subject to an AntiVirus Scan using Norton AV, which was updated moments before the scan being run. It was therefore considered that the image did not contain any viruses known at the time of the scan (that were detectable).

Item 6 – Screenshot of Norton AV (Windows) Completing Scan of v1_5.gz



Summary	No Infection found
Scan time	1 second(s)

Action:	Files	Master Boot Record	Boot Record
Scanned:	1	2	2
Infected:	0	0	0
Repaired:	0	0	0
Quarantined:	0	-	-
Deleted:	0	-	-

Creation of the Working Copy

A copy was then taken of the image file and the “Master Working” image placed in a separate folder. All activities were conducted on the “Working Copy”. If the working copy had become corrupt at any point new version could be made form the Master Working. At every stage MD5 Sums were taken and compared to the sum on the original label. All hashes for the Master Working, Working Copy and the documented floppy disk, were exactly the same.

The Initial Analysis

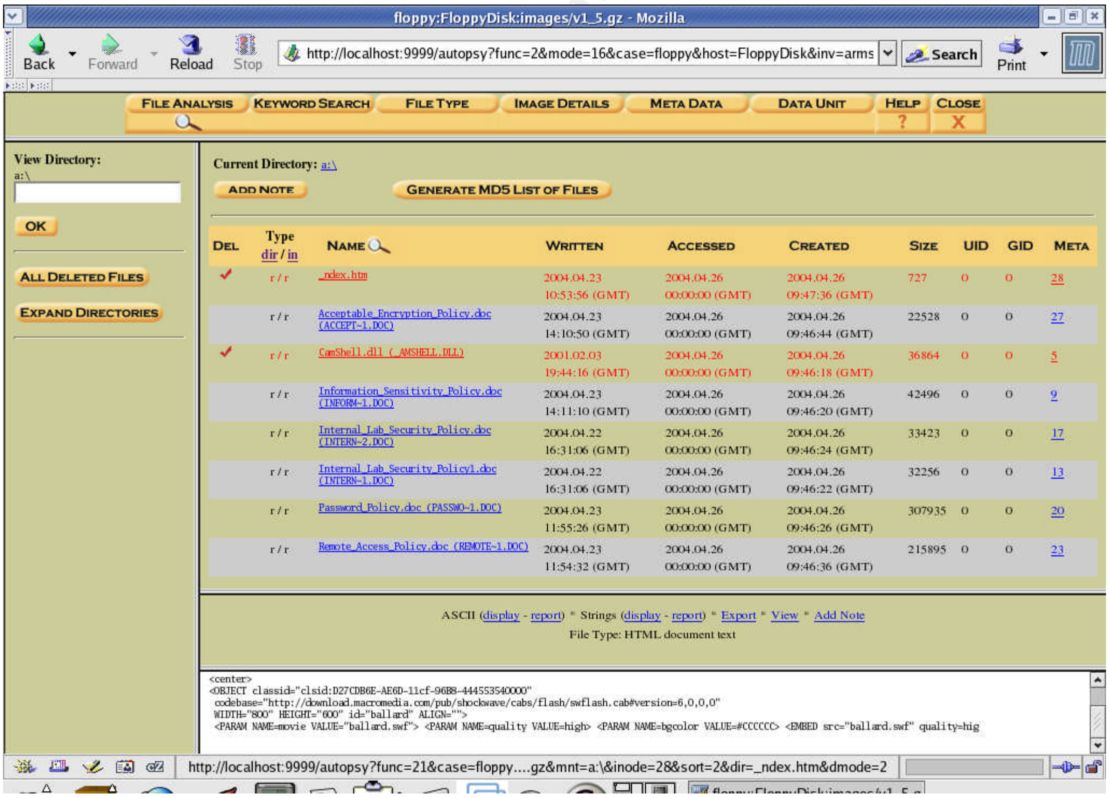
The disk image was made read only in the Linux OS [`chmod 444 v1_5.gz`] and thus any activity and investigation conducted by the investigator could not have affected the disk image. As a precaution once the investigation was complete a final md5 hash was conducted and it confirmed that the image had not been altered during the analysis.

Working with Autopsy

Viewing the file structure and disk contents

Having started Autopsy, the image was mounted and the file contents were checked and listed. The screenshot below shows the file index of the floppy disk. Of note are the two deleted files on the disk namely: "`_ndex.htm`" and "`_AMSHELL.DLL`". Md5 hashes were taken of the live files and this was saved as "`md5_of_std_files_on_RJL.txt`" (listed below).

Item 7 – Initial file browsing with Autopsy



http://localhost:9999/autopsy?func=2&mode=16&case=floppy&host=FloppyDisk&inv=arms

View Directory:
a:\

Current Directory: a:\

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
✓	r / r	_ndex.htm	2004.04.23 10:53:56 (GMT)	2004.04.26 00:00:00 (GMT)	2004.04.26 09:47:36 (GMT)	727	0	0	28
	r / r	Acceptable_Encryption_Policy.doc (ACCEPT~1.DOC)	2004.04.23 14:10:50 (GMT)	2004.04.26 00:00:00 (GMT)	2004.04.26 09:46:44 (GMT)	22528	0	0	27
✓	r / r	CamShell.dll (_AMSHELL.DLL)	2001.02.03 19:44:16 (GMT)	2004.04.26 00:00:00 (GMT)	2004.04.26 09:46:18 (GMT)	36864	0	0	5
	r / r	Information_Sensitivity_Policy.doc (INFORM~1.DOC)	2004.04.23 14:11:10 (GMT)	2004.04.26 00:00:00 (GMT)	2004.04.26 09:46:20 (GMT)	42496	0	0	9
	r / r	Internal_Lab_Security_Policy.doc (INTERN~2.DOC)	2004.04.22 16:31:06 (GMT)	2004.04.26 00:00:00 (GMT)	2004.04.26 09:46:24 (GMT)	33423	0	0	17
	r / r	Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)	2004.04.22 16:31:06 (GMT)	2004.04.26 00:00:00 (GMT)	2004.04.26 09:46:22 (GMT)	32256	0	0	13
	r / r	Password_Policy.doc (PASSWO~1.DOC)	2004.04.23 11:55:26 (GMT)	2004.04.26 00:00:00 (GMT)	2004.04.26 09:46:26 (GMT)	307935	0	0	20
	r / r	Remote_Access_Policy.doc (REMOTE~1.DOC)	2004.04.23 11:54:32 (GMT)	2004.04.26 00:00:00 (GMT)	2004.04.26 09:46:36 (GMT)	215895	0	0	23

ASCII (display - report) * Strings (display - report) * Export * View * Add Note
File Type: HTML document text

```
<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=movie VALUE="ballard.swf"> <PARAM NAME=quality VALUE=high> <PARAM NAME=bgcolor VALUE=#CCCCCC> <EMBED src="ballard.swf" quality=hig
```

http://localhost:9999/autopsy?func=21&case=floppy....gz&mnt=a:\&inode=28&sort=2&dir=_ndex.htm&dmode=2

Item 8 – Autopsy output of visible file on target disk

Command	Autopsy output of md5 request on visible files

Output	`MD5 Values for files in v1_5.gz`
	
	`99c5dec518b142bd945e8d7d2fad2004      Information_Sensitivity_Policy.doc (INFORM~1.DOC)`
	`e0c43ef38884662f5f27d93098e1c607      Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)`
	`b9387272b11aea86b60a487fbdc1b336      Internal_Lab_Security_Policy.doc (INTERN~2.DOC)`
	`ac34c6177ebdcaf4adc41f0e181be1bc      Password_Policy.doc (PASSWO~1.DOC)`
	`5b38d1ac1f94285db2d2246d28fd07e8      Remote_Access_Policy.doc (REMOTE~1.DOC)`
	`f785ba1d99888e68f45dabeddb0b4541      Acceptable_Encryption_Policy.doc (ACCEPT~1.DOC)`

Creating a File Activity Timeline

Next a file timeline was created from all Allocated and Unallocated space on the drive including the Unallocated Meta Data structures. This would show the order in which files were created, modified and deleted. The file was created by Autopsy and as the 'output/body' file was created an md5 hash of the file was also written to the working folder `(/forensics/floppy/FloppyDisk/)`. The final step for this item was to create the time-line file from the body with a start and end point. As Floppy disk contained small amounts of data a complete timeline was requested and this was saved as `'output/total-timeline'`.

The timeline would be later analysed and referred to as a key reference document, indicating file activity and user actions. As the timeline related to a floppy disk the activity recorded would primarily be that of the user as systems are rarely able to page or record system activity to the media (limited volume size, slow read and write speed coupled with a lack of system pre-notification as to its removal)

Item 9 – Timeline for Floppy Disk

```
Sat Feb 03 2001 19:44:16    36864 m..   -rwxrwxrwx 0        0        5        <v1_5.gz-_AMSHELL.DLL-dead-5>
                            36864 m.. -/-rwxrwxrwx 0        0        5        a:\/CamShell.dll (_AMSHELL.DLL) (deleted)
Thu Apr 22 2004 16:31:06    33423 m.. -/-rwxrwxrwx 0        0        17       a:\/Internal_Lab_Security_Policy.doc (INTERN~2.DOC)
                            32256 m.. -/-rwxrwxrwx 0        0        13       a:\/Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)
Fri Apr 23 2004 10:53:56      727 m.. -/-rwxrwxrwx 0        0        28       a:\/_ndex.htm (deleted)
                              727 m..   -rwxrwxrwx 0        0        28       <v1_5.gz-_ndex.htm-dead-28>
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   215895 .a. -/-rwxrwxrwx 0        0        23       a:\/Remote_Access_Policy.doc (REMOTE~1.DOC)
                              727 .a. -/-rwxrwxrwx 0        0        28       a:\/_ndex.htm (deleted)
                           307935 .a. -/-rwxrwxrwx 0        0        20       a:\/Password_Policy.doc (PASSWO~1.DOC)
                            33423 .a. -/-rwxrwxrwx 0        0        17       a:\/Internal_Lab_Security_Policy.doc (INTERN~2.DOC)
                            42496 .a. -/-rwxrwxrwx 0        0        9        a:\/Information_Sensitivity_Policy.doc (INFORM~1.DOC)
                            36864 .a.   -rwxrwxrwx 0        0        5        <v1_5.gz-_AMSHELL.DLL-dead-5>
                            32256 .a. -/-rwxrwxrwx 0        0        13       a:\/Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)
                            22528 .a. -/-rwxrwxrwx 0        0        27       a:\/Acceptable_Encryption_Policy.doc (ACCEPT~1.DOC)
                              727 .a.   -rwxrwxrwx 0        0        28       <v1_5.gz-_ndex.htm-dead-28>
                            36864 .a. -/-rwxrwxrwx 0        0        5        a:\/CamShell.dll (_AMSHELL.DLL) (deleted)
Mon Apr 26 2004 09:46:18    36864 ..c   -rwxrwxrwx 0        0        5        <v1_5.gz-_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       a:\/_ndex.htm (deleted)
                              727 ..c   -rwxrwxrwx 0        0        28       <v1_5.gz-_ndex.htm-dead-28>
```

Creating a String File

A ‘String File’ is the output of a search of any string of 4 or more characters in row. In other words it is a file of all the groups of characters that may be words. This Strings File can then be examined to gain insight into the contents of the originally searched file or disk structure. This file can be searched using the likes of `grep` or any text string search utility (even find in notepad).

Having obtained a file list, string file and file activity timeline, initial analysis could occur. This resulted in list of the files on the floppy disk being made and an examination of their size, contents and potential use being listed. The following is a list if the files observed as being ‘live’ on the disk:

Item 10 – List of 'live' files on the floppy disk

File Name	Notes
Password_Policy.doc	A large file that outlined the password policy
Remote_Access_Policy.doc	A large file that outlined the remote access policy
Internal_Lab_Security_Policy.doc	A small file that outlined the internal lab policy
Information_Sensitivity_Policy.doc	A small file on the policy on Information sensitivity
Acceptable_Encryption_Policy.doc	A small file that outlined the Encryption policy

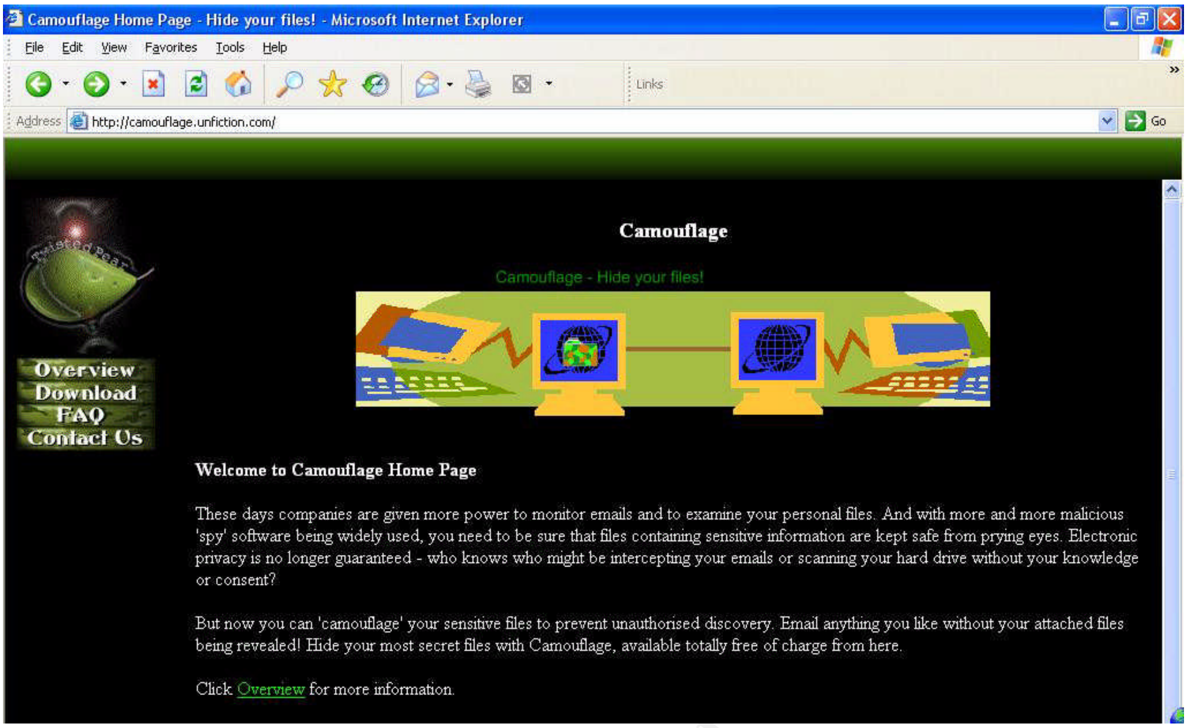
Item 11 – File ownership details

<table>
<tr><td>Command</td><td>ls –sl &gt; /root/fileownershipdetails.txt</td></tr>
<tr><td>Output</td><td><pre>
total 640
 22 -rwxr-xr-x 1 root root 22528 Apr 23 2004 Acceptable_Encryption_Policy.doc
 42 -rwxr-xr-x 1 root root 42496 Apr 23 2004 Information_Sensitivity_Policy.doc
 32 -rwxr-xr-x 1 root root 32256 Apr 22 2004 Internal_Lab_Security_Policy1.doc
 33 -rwxr-xr-x 1 root root 33423 Apr 22 2004 Internal_Lab_Security_Policy.doc
301 -rwxr-xr-x 1 root root 307935 Apr 23 2004 Password_Policy.doc
211 -rwxr-xr-x 1 root root 215895 Apr 23 2004 Remote_Access_Policy.doc
</pre></td></tr>
</table>

While the accuracy of the documents in relation to the current company policies is not something that the investigator would comment upon, the first 2 files listed above were deemed larger that expected given their limited textual content. These files were recorded as being ‘of interest’ and would be subjected to closer examination later.

An examination was then made of the files that had been marked as deleted, this included a `CamShell.dll` (probably a part of a program) and `_ndex.htm` (probably an ‘Index.htm’ page from a website). The time-line shows a file was deleted on 3rd Feb 2001 and that file was the `CamShell.dll`. A search of the internet revealed a handful of newsgroups that referred to an old and now unsupported program called Camouflage. Further searches led the investigator to this web site located at the URL: <http://camouflage.unfiction.com>[9] (pictured below).

Item 12 – Screenshot of the Camouflage Website


Camouflage Home Page - Hide your files! - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Links
Address
http://camouflage.unfiction.com/
Go
Twisted Pear
Overview
Download
FAQ
Contact Us

Camouflage

Camouflage - Hide your files!

Welcome to Camouflage Home Page

These days companies are given more power to monitor emails and to examine your personal files. And with more and more malicious 'spy' software being widely used, you need to be sure that files containing sensitive information are kept safe from prying eyes. Electronic privacy is no longer guaranteed - who knows who might be intercepting your emails or scanning your hard drive without your knowledge or consent?

But now you can 'camouflage' your sensitive files to prevent unauthorised discovery. Email anything you like without your attached files being revealed! Hide your most secret files with Camouflage, available totally free of charge from here.

Click Overview for more information.

The download link was followed and the self-expanding-executable-zipped file Camou121.exe was obtained and hashed.

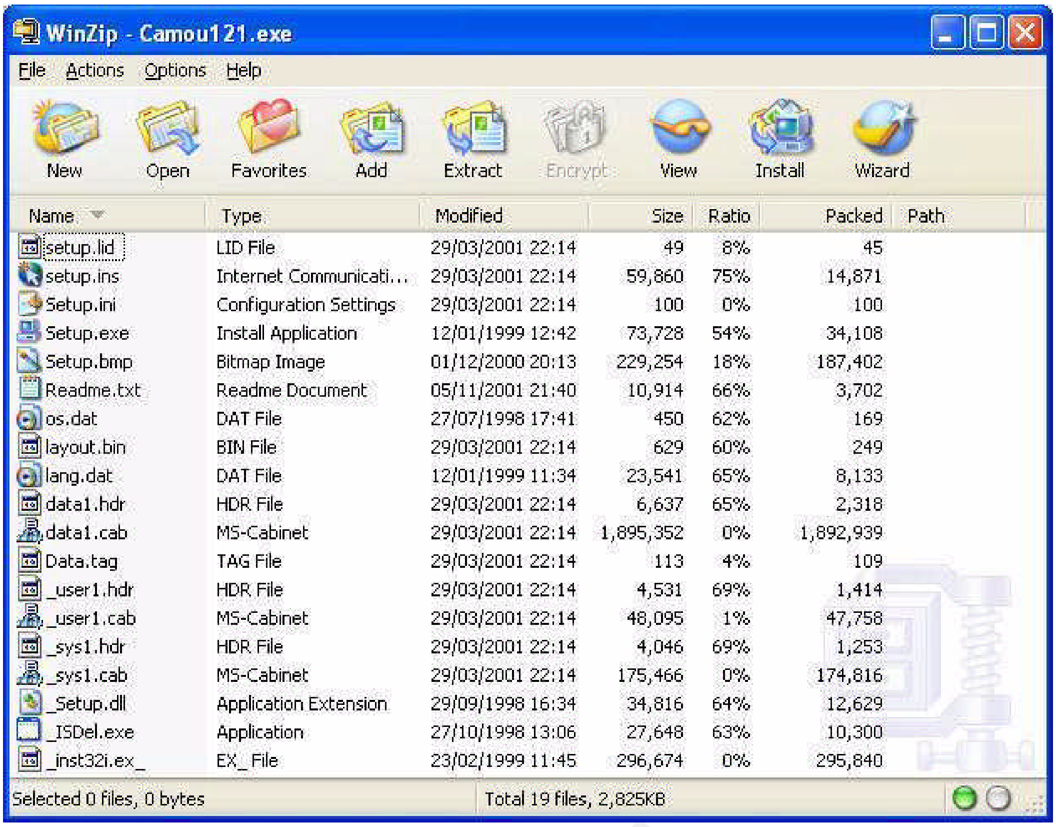
Item 13 – fsum (Windows) Command output of Camou121.exe

Command	`fsum -md5 Camou121.exe`

Output	`; SlavaSoft Optimizing Checksum Utility fsum 2.0 <www.slavasoft.com>`
	`;`
	`; Generated on 11/28/04 at 22:00:14`
	`;`
	`c62b050117c2cba3518e5a734fedef1f *Camou121.exe`

The zipped file was expanded on a control system and the contents examined. The following image shows the file contained in the self executing zip file. It is worth remembering that the zip folder also contains the installation software that will build the application and create the uninstall file to facilitate its ‘safe’ removal. Once the setup.exe file is execute the application is built with the majority of the application being installed in the user defined folder (by default this is ‘`C:\Program Files\Camouflage`’).

Item 14 – WinZip[10] (Windows) contents of Camou121.exe selfextracting zip file



Name	Type	Modified	Size	Ratio	Packed	Path
setup.lid	LID File	29/03/2001 22:14	49	8%	45	
setup.ins	Internet Communicati...	29/03/2001 22:14	59,860	75%	14,871	
Setup.ini	Configuration Settings	29/03/2001 22:14	100	0%	100	
Setup.exe	Install Application	12/01/1999 12:42	73,728	54%	34,108	
Setup.bmp	Bitmap Image	01/12/2000 20:13	229,254	18%	187,402	
Readme.txt	Readme Document	05/11/2001 21:40	10,914	66%	3,702	
os.dat	DAT File	27/07/1998 17:41	450	62%	169	
layout.bin	BIN File	29/03/2001 22:14	629	60%	249	
lang.dat	DAT File	12/01/1999 11:34	23,541	65%	8,133	
data1.hdr	HDR File	29/03/2001 22:14	6,637	65%	2,318	
data1.cab	MS-Cabinet	29/03/2001 22:14	1,895,352	0%	1,892,939	
Data.tag	TAG File	29/03/2001 22:14	113	4%	109	
_user1.hdr	HDR File	29/03/2001 22:14	4,531	69%	1,414	
_user1.cab	MS-Cabinet	29/03/2001 22:14	48,095	1%	47,758	
_sys1.hdr	HDR File	29/03/2001 22:14	4,046	69%	1,253	
_sys1.cab	MS-Cabinet	29/03/2001 22:14	175,466	0%	174,816	
_Setup.dll	Application Extension	29/09/1998 16:34	34,816	64%	12,629	
_ISDel.exe	Application	27/10/1998 13:06	27,648	63%	10,300	
inst32i.ex	EX_ File	23/02/1999 11:45	296,674	0%	295,840	

Selected 0 files, 0 bytes   Total 19 files, 2,825KB

The installation process was allowed to continue and the built application is detailed below:

Item 15 – dir (Windows) Command output of Camouflage folder post install

Command	`dir camouflage > dir_list_camouflage_folder.txt`
Output	Volume in drive F is STEVE_ARMS Volume Serial Number is 70A1-3272 Directory of F:\GIAC\Camouflage 16/11/2004 20:46 <DIR> . 16/11/2004 20:46 <DIR> .. 29/03/2001 22:13 217,088 Camouflage.exe 03/02/2001 19:44 36,864 CamShell.dll 28/03/2001 19:50 11,649 Readme.txt 08/11/2004 19:23 19,774 Uninst.isu 4 File(s) 285,375 bytes 2 Dir(s) 343,220,224 bytes free

Instantly the file called CamShell.dll jumped out as being of the same name, capitalization and size as one of the deleted files on the floppy disk. At this point it was decided to perform some detailed analysis on the following aspects of the floppy disk:

The use of `CamShell.dll` file the associated executable

`Camouflage.exe`.

The contents of the `Password_Policy.doc` and `Remote_Access_Policy.doc` files that were unusually large and whose size was not proportionate to their contents.

Detailed Analysis

Camouflage

The Camouflage program installed the `CamShell.dll` file into the installation directory specified (in this case we accepted the default):

```
C:/Program Files/Camouflage
```

And this also includes the executable and a Readme.txt and an Uninstall data file. The md5sums are:

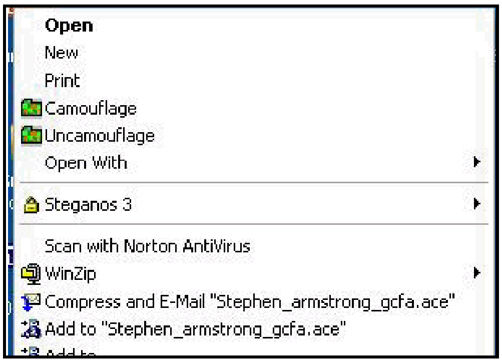
Item 16 – fsum (Windows) for files created by the Camouflage install process

Command	`fsum camouflage > dir_list_camouflage_folder.txt`

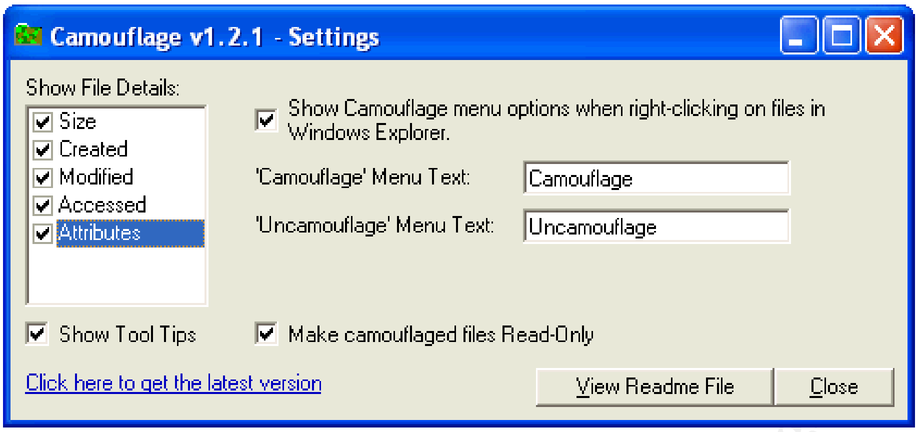
Output	`; SlavaSoft Optimizing Checksum Utility fsum 2.0 <www.slavasoft.com>`
	`;`
	`; Generated on 12/07/04 at 13:30:39`
	`;`
	`9f08258a80d578a0f1cc38fe4c2aebb5 *Camouflage.exe`
	`4e986ab0909d2946bed868b5f896906f *CamShell.dll`
	`0c25ad7792d555b6c8c37c77ceb9e224 *Readme.txt`
	`2902261874a65a2581f0a260fad6a9df *Uninst.isu`

Running the Camouflage program revealed a Settings GUI and initially this appeared to be the only impact of the installation:

Item 17 – Camouflage right click menu


Open
New
Print
Camouflage
Uncamouflage
Open With
Steganos 3
Scan with Norton AntiVirus
WinZip
Compress and E-Mail "Stephen_armstrong_gcfa.ace"
Add to "Stephen_armstrong_gcfa.ace"

Item 18 – Settings GUI window for the Camouflage program



Camouflage v1.2.1 - Settings

Show File Details:

- ☑ Size
- ☑ Created
- ☑ Modified
- ☑ Accessed
- ☑ Attributes

☑ Show Camouflage menu options when right-clicking on files in Windows Explorer.

'Camouflage' Menu Text: Camouflage

'Uncamouflage' Menu Text: Uncamouflage

☑ Show Tool Tips

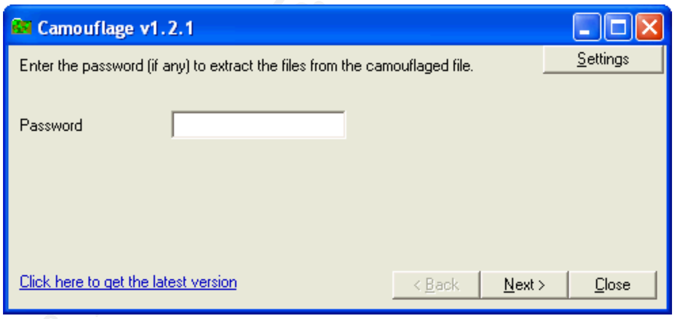
☑ Make camouflaged files Read-Only

A quick read of the Readme.txt file gleaned the advisory that the use of notepad.exe could compromise the presence of the encrypted data as it would display all data.

This opening with notepad was performed on all live files on the floppy disk and as thought the `Password_Policy.doc` and `Remote_Access_Policy.doc` did seem to have encrypted within their file sectors.

To test theory the Camouflage program was run for against the Password_Policy.doc file. To do this the file was selected and the right click or alternate menu brought up. Selecting the "Uncamouflage" option the following window appeared:

Item 19 – Password request GUI



Camouflage v1.2.1

Enter the password (if any) to extract the files from the camouflaged file.

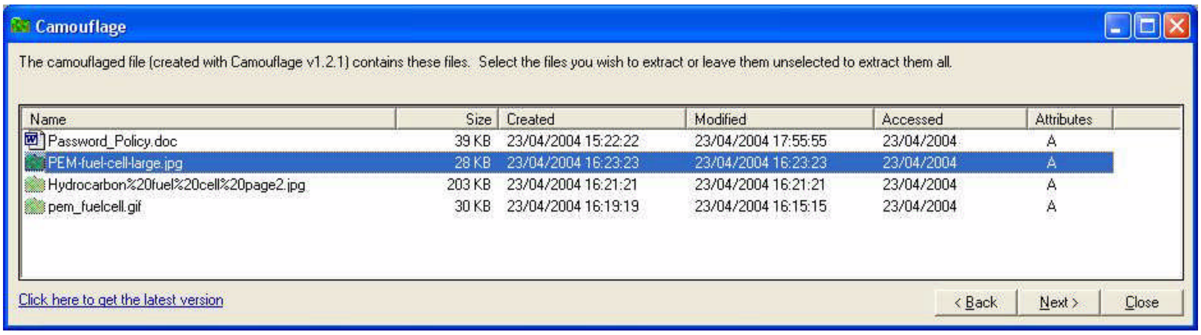
Password

This did present a problem as to this point no passwords had been recovered, either in text files on in the form of an obvious file or text in a file on the disk.

Passwords

The investigator then tried a few default passwords, starting with "`password`" which was rejected. The next one tried was "`Password`" this was the correct password as the image below shows the contents of the Camouflaged file.

Item 20 – Camouflage Window - contents of Password_Policy.doc carrier file



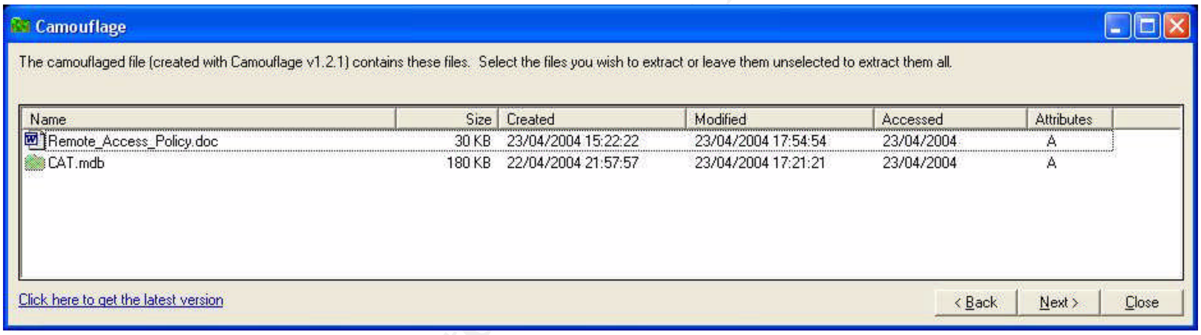
The camouflaged file (created with Camouflage v1.2.1) contains these files. Select the files you wish to extract or leave them unselected to extract them all.

Name	Size	Created	Modified	Accessed	Attributes
Password_Policy.doc	39 KB	23/04/2004 15:22:22	23/04/2004 17:55:55	23/04/2004	A
PEM-fuel-cell-large.jpg	28 KB	23/04/2004 16:23:23	23/04/2004 16:23:23	23/04/2004	A
Hydrocarbon%20fuel%20cell%20page2.jpg	203 KB	23/04/2004 16:21:21	23/04/2004 16:21:21	23/04/2004	A
pem_fuelcell.gif	30 KB	23/04/2004 16:19:19	23/04/2004 16:15:15	23/04/2004	A

Note how the 1st line of text on both screen shots shows the carrier files on the floppy disk were created by v1.2.1 of the program (or so the program believes).

The "`Password`" was then tried on the other potential carrier file but it was not accepted. At this point the investigator was slightly stumped and began to examine the strings file for the FD to glean any possible password. After some time and after trying several dozen passwords gold was struck. It closer examination indicated that the password for the `Password_Policy.doc` file was the first part of the file name, thus "`Remote`" was tried on `the Remote_Access_Policy.doc` file and the following files were revealed to inside the carrier.

Item 21 – Camouflage Window - contents of Remort_Access_Policy.doc



The camouflaged file (created with Camouflage v1.2.1) contains these files. Select the files you wish to extract or leave them unselected to extract them all.

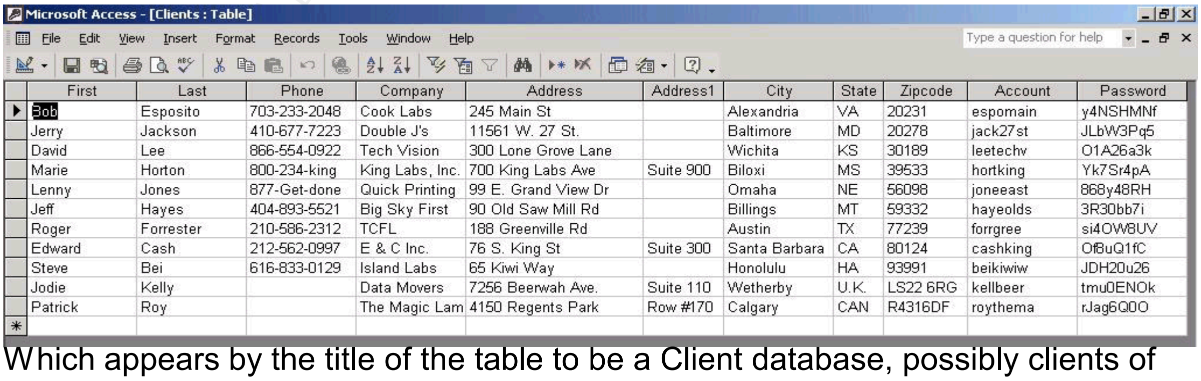
Name	Size	Created	Modified	Accessed	Attributes
Remote_Access_Policy.doc	30 KB	23/04/2004 15:22:22	23/04/2004 17:54:54	23/04/2004	A
CAT.mdb	180 KB	22/04/2004 21:57:57	23/04/2004 17:21:21	23/04/2004	A

The having opened the CAT.mdb file in notepad.exe the string:

"`M S y s A c c e s s O b j e c t s LTD`"

Indicated the file was a MS Access[11] file and opening it in MS Access revealed the following:

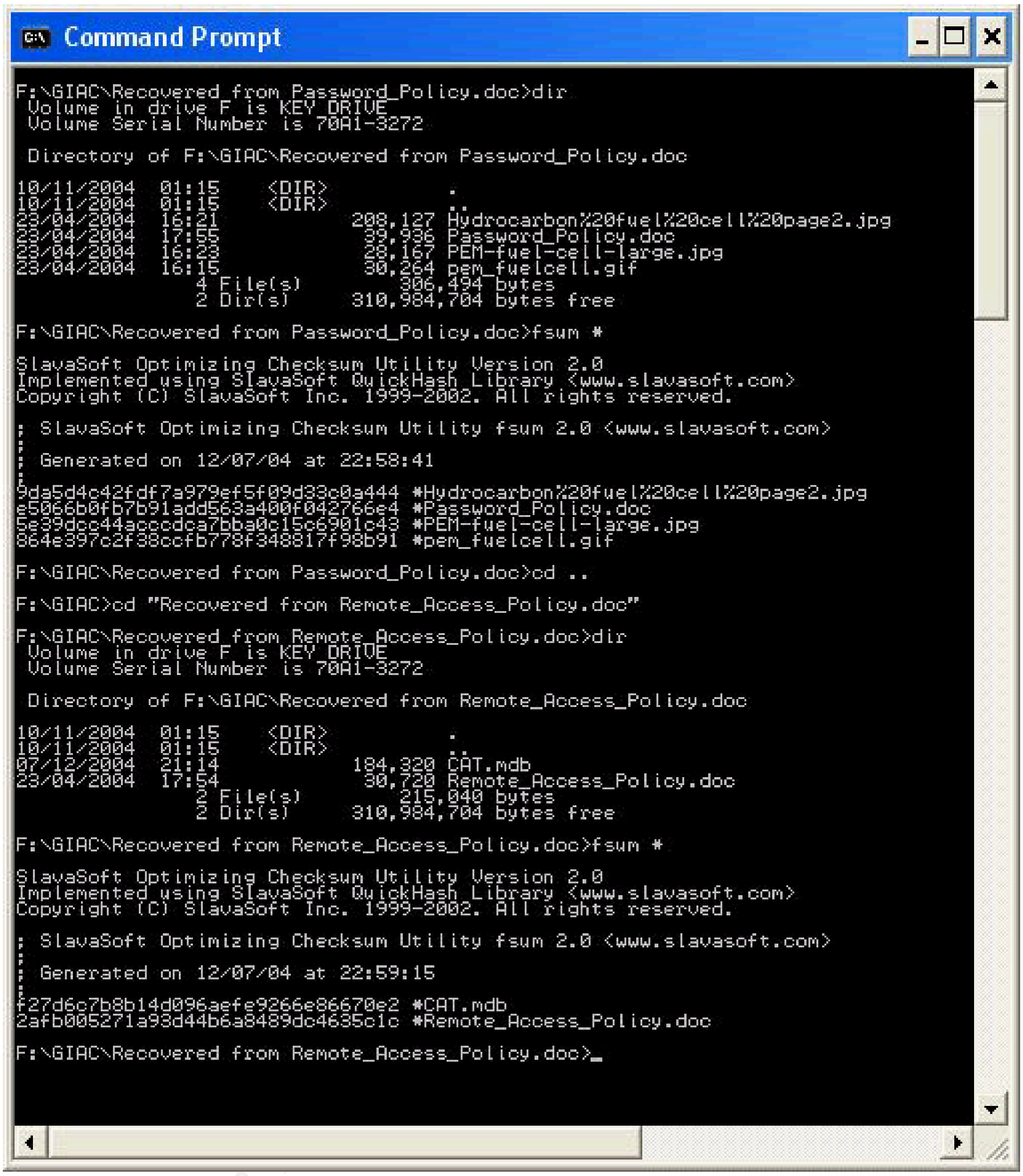
Item 22 – Table of CAB.mdb extracted from Remote_Access_Policy.doc



First	Last	Phone	Company	Address	Address1	City	State	Zipcode	Account	Password
Bob	Esposito	703-233-2048	Cook Labs	245 Main St		Alexandria	VA	20231	espomain	y4NSHMNf
Jerry	Jackson	410-677-7223	Double J's	11561 W. 27 St.		Baltimore	MD	20278	jack27st	JLbW3Pq5
David	Lee	866-554-0922	Tech Vision	300 Lone Grove Lane		Wichita	KS	30189	leetechv	O1A26a3k
Marie	Horton	800-234-king	King Labs, Inc.	700 King Labs Ave	Suite 900	Biloxi	MS	39533	hortking	Yk7Sr4pA
Lenny	Jones	877-Get-done	Quick Printing	99 E. Grand View Dr		Omaha	NE	56098	joneeast	868y48RH
Jeff	Hayes	404-893-5521	Big Sky First	90 Old Saw Mill Rd		Billings	MT	59332	hayeolds	3R30bb7i
Roger	Forrester	210-586-2312	TCFL	188 Greenville Rd		Austin	TX	77239	forrgree	si4OW8UV
Edward	Cash	212-562-0997	E & C Inc.	76 S. King St	Suite 300	Santa Barbara	CA	80124	cashking	Of8uQ1fC
Steve	Bei	616-833-0129	Island Labs	65 Kiwi Way		Honolulu	HA	93991	beikiwiw	JDH20u26
Jodie	Kelly		Data Movers	7256 Beerwah Ave.	Suite 110	Wetherby	U.K.	LS22 6RG	kellbeer	tmu0ENOk
Patrick	Roy		The Magic Lam	4150 Regents Park	Row #170	Calgary	CAN	R4316DF	roythema	rJag6Q0O

Which appears by the title of the table to be a Client database, possibly clients of the Ballard Inc?

Item 23 – fsum (windows) of all files recovered from Camouflage carrier files



```
F:\GIAC\Recovered from Password_Policy.doc>dir
 Volume in drive F is KEY DRIVE
 Volume Serial Number is 70A1-3272

 Directory of F:\GIAC\Recovered from Password_Policy.doc

10/11/2004  01:15    <DIR>          .
10/11/2004  01:15    <DIR>          ..
23/04/2004  16:21           208,127 Hydrocarbon%20fuel%20cell%20page2.jpg
23/04/2004  17:55            39,936 Password_Policy.doc
23/04/2004  16:23            28,167 PEM-fuel-cell-large.jpg
23/04/2004  16:15            30,264 pem_fuelcell.gif
               4 File(s)        306,494 bytes
               2 Dir(s)     310,984,704 bytes free

F:\GIAC\Recovered from Password_Policy.doc>fsum *

SlavaSoft Optimizing Checksum Utility Version 2.0
Implemented using SlavaSoft QuickHash Library <www.slavasoft.com>
Copyright (C) SlavaSoft Inc. 1999-2002. All rights reserved.

; SlavaSoft Optimizing Checksum Utility fsum 2.0 <www.slavasoft.com>
;
; Generated on 12/07/04 at 22:58:41
;
9da5d4c42fdf7a979ef5f09d33c0a444 *Hydrocarbon%20fuel%20cell%20page2.jpg
e5066b0fb7b91add563a400f042766e4 *Password_Policy.doc
5e39dcc44acccdca7bba0c15c6901c43 *PEM-fuel-cell-large.jpg
864e397c2f38ccfb778f348817f98b91 *pem_fuelcell.gif

F:\GIAC\Recovered from Password_Policy.doc>cd ..

F:\GIAC>cd "Recovered from Remote_Access_Policy.doc"

F:\GIAC\Recovered from Remote_Access_Policy.doc>dir
 Volume in drive F is KEY DRIVE
 Volume Serial Number is 70A1-3272

 Directory of F:\GIAC\Recovered from Remote_Access_Policy.doc

10/11/2004  01:15    <DIR>          .
10/11/2004  01:15    <DIR>          ..
07/12/2004  21:14           184,320 CAT.mdb
23/04/2004  17:54            30,720 Remote_Access_Policy.doc
               2 File(s)        215,040 bytes
               2 Dir(s)     310,984,704 bytes free

F:\GIAC\Recovered from Remote_Access_Policy.doc>fsum *

SlavaSoft Optimizing Checksum Utility Version 2.0
Implemented using SlavaSoft QuickHash Library <www.slavasoft.com>
Copyright (C) SlavaSoft Inc. 1999-2002. All rights reserved.

; SlavaSoft Optimizing Checksum Utility fsum 2.0 <www.slavasoft.com>
;
; Generated on 12/07/04 at 22:59:15
;
f27d6c7b8b14d096aefe9266e86670e2 *CAT.mdb
2afb005271a93d44b6a8489dc4635c1c *Remote_Access_Policy.doc

F:\GIAC\Recovered from Remote_Access_Policy.doc>_
```

File Timings Explained

Before explaining what the investigator believes occurred, it is worth explaining the somewhat unusual timings that are often connected to files that have been copied to new media (as happened in this case).

> Operating Systems. Operating Systems that are `POSIX` and E2 complaint record time stamps on files when they are Modified, Accessed or Created (called MAC times). Some like many UNIX flavours (inc Linux) apply stamps time stamps on all activity (unless prohibited by the tool accessing the file). Microsoft Windows however, will stamp full time and date information on

creation and modification but only date information on file access occurrences (the access time being stored else where).

File copying. File copying can create some strange timings as only the files creation time and date are updated. Therefore, it is possible to make a new file on 1st Nov, access it on the 2nd Nov, modify it on the 3rd Nov and copy it onto separate media on the 4th; when the MACs are viewed on the 5th however, it will appear to have been accessed and modified before it was created.

As will be explained in the next section, when a carrier file was modified to include a different file, the modification time was set; when the carrier file was copied to the floppy drive, it was given a creation time that was after the modification time. To confuse matters more the carrier file was made using a program that retained the MAC times of the original carried files. Thus when the carried files are exported from the carrier file a new instance is written to the new media and although this will have a different creation time again, it will retain the original accessed and modification times.

What Happened (Investigators Opinion)

Having examined the data obtained from various sources and parts of the disk, the following is offered as a possible explanation of what has been found:

Before 23 April 2004, a Mr Robert John Leszczynski, Jr., who was employed by Ballard Industries as the lead process control engineer for the project to design a new fuel cell battery. Mr RJ Leszczynski, it is believed, brought a Steganographic program (`Camouflage`) into Ballard Industries for reasons unknown.

This program may have been brought in file by file to prevent detection, as the `CamShell.dll` file had deleted been on floppy disk until it was deleted. The program was probably installed on a Ballard Ind. PC and this could be confirmed by scanning all systems to which Leszczynski would have had access, looking for the CamShell.dll file or remnants of it having been there.

The `Camouflage` program was used to hide 4 files for transportation out of the company grounds. The files being 2 graphical pictures and 1 an image of a report, the 4th file was a MS database of what appears to be clients' details. Fortunately the Camouflage program stores the original MAC times from the files as can be seen in items 20 and 21.

Once the Camouflage program had been used to make carrier files out of the `Password_Policy.doc` and `Remote_Assess_Policy.doc` files [believed to be 23 Apr 2004 @ 1155 & 1154 hours respectively].

These carrier files and four other word documents (policy documents from Ballard Ind.) were copied onto the Floppy disk [believed to be 26 Apr 2004 @

0946 hours]. These files accessed at some point on 26 Apr 2004, but as Microsoft does note record access times, only dates, specific data is not available.

As Mr RJ Leszczynski, went to leave the building at the end of the day he was stopped and the disk impounded. As the disk is logically labelled with his initials and he was in possession of it when stopped, it is suggested that Mr RJ Leszczynski was exporting information that he had access to, to outside the boundary of Ballard Ind. However, analysis of his work pc would reveal more information about his activities, and it is recommended that this is undertaken before it is used/switched on again.

Item 24 – List of all files (inc those hidden) found of the floppy disk

Serial	File name / description	Clear or hidden and by what
1	Acceptable_Encryption_Policy.doc	Clear
2	Internal_Lab_Security_Policy1.doc	Clear
3	Internal_Lab_Security_Policy.doc	Clear
4	Information_Sensitivity_Policy.doc	Clear
5	Password_Policy.doc	Clear
5a	*Hydrocarbon%20fuel%20cell%20page2.jpg*	*Hidden – Camouflage*
5b	*pem_fuelcell.gif*	*Hidden – Camouflage*
5c	*PEM-fuel-cell-large.jpg*	*Hidden – Camouflage*
5d	*Password_Policy.doc*	*Hidden – Camouflage*
6	Remote_Access_Policy.doc	Clear
6a	*CAT.mdb*	*Hidden – Camouflage*
6b	*Remote_Access_Policy.doc*	*Hidden – Camouflage*
Note the MAC times can be viewed in items 20 and 21 and have not been re-reproduced		

It is not possible to state if Mr RJ Leszczynski had transferred data out of the organisation on occasions or if this was the first attempt, however, examination of his work host PC may reveal details of the date and time the Camouflage software was installed.

The Software found and possibly used by Leszczynski

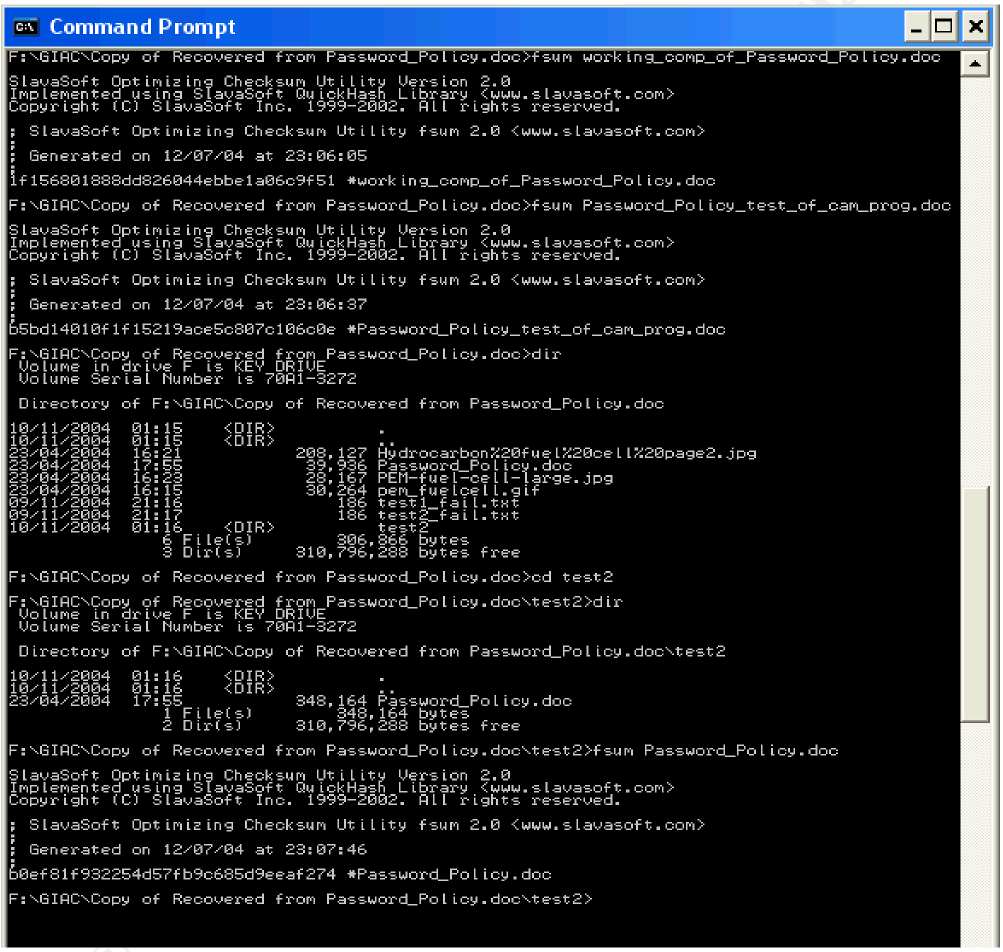
The program found on the disk went by the name of Camouflage. It is a Steganographic Program that hides user selected data inside carrier files. The following is a quote from a mirror of the old Camouflage web site[12]:

> ***"What is Camouflage?***
>
> *Camouflage allows you to hide files by scrambling them and then attaching them to the file of your choice. This camouflaged file then looks and behaves like a normal file, and can be stored, used or emailed without attracting attention. For example, you could create a picture file that looks and*

> *behaves exactly like any other picture file but contains hidden encrypted files, or you could hide a file inside a Word document that would not attract attention if discovered. Such files can later be safely extracted. For additional security you can password your camouflaged file. This password will be required when extracting the files within. You can even camouflage files within camouflaged files. Camouflage was written for use with Windows 95, Windows 98, Windows ME, Windows NT and Windows 2000, and is simple to install and use."*

An attempt to recreate the image made by Mr R J Leszczynski failed in that the md5 hashes of the output file are not the same. That said it is unlikely that they would as the files would be different given the different MAC times that would accompany the files that are inserted, see below:

Item 25 – Screenshot of hashes not matching



```
F:\GIAC\Copy of Recovered from Password_Policy.doc>fsum working_comp_of_Password_Policy.doc

SlavaSoft Optimizing Checksum Utility Version 2.0
Implemented using SlavaSoft QuickHash Library <www.slavasoft.com>
Copyright (C) SlavaSoft Inc. 1999-2002. All rights reserved.

; SlavaSoft Optimizing Checksum Utility fsum 2.0 <www.slavasoft.com>
;
; Generated on 12/07/04 at 23:06:05
;
1f156801888dd826044ebbe1a06c9f51 *working_comp_of_Password_Policy.doc

F:\GIAC\Copy of Recovered from Password_Policy.doc>fsum Password_Policy_test_of_cam_prog.doc

SlavaSoft Optimizing Checksum Utility Version 2.0
Implemented using SlavaSoft QuickHash Library <www.slavasoft.com>
Copyright (C) SlavaSoft Inc. 1999-2002. All rights reserved.

; SlavaSoft Optimizing Checksum Utility fsum 2.0 <www.slavasoft.com>
;
; Generated on 12/07/04 at 23:06:37
;
b5bd14010f1f15219ace5c807c106c0e *Password_Policy_test_of_cam_prog.doc

F:\GIAC\Copy of Recovered from Password_Policy.doc>dir
 Volume in drive F is KEY_DRIVE
 Volume Serial Number is 70A1-3272

 Directory of F:\GIAC\Copy of Recovered from Password_Policy.doc

10/11/2004  01:15    <DIR>          .
10/11/2004  01:15    <DIR>          ..
23/04/2004  16:21           208,127 Hydrocarbon%20fuel%20cell%20page2.jpg
23/04/2004  17:55            39,936 Password_Policy.doc
23/04/2004  16:23            28,167 PEM-fuel-cell-large.jpg
23/04/2004  16:15            30,264 pem_fuelcell.gif
09/11/2004  21:16               186 test1_fail.txt
09/11/2004  21:17               186 test2_fail.txt
10/11/2004  01:16    <DIR>          test2
               6 File(s)        306,866 bytes
               3 Dir(s)     310,796,288 bytes free

F:\GIAC\Copy of Recovered from Password_Policy.doc>cd test2

F:\GIAC\Copy of Recovered from Password_Policy.doc\test2>dir
 Volume in drive F is KEY_DRIVE
 Volume Serial Number is 70A1-3272

 Directory of F:\GIAC\Copy of Recovered from Password_Policy.doc\test2

10/11/2004  01:16    <DIR>          .
10/11/2004  01:16    <DIR>          ..
23/04/2004  17:55           348,164 Password_Policy.doc
               1 File(s)        348,164 bytes
               2 Dir(s)     310,796,288 bytes free

F:\GIAC\Copy of Recovered from Password_Policy.doc\test2>fsum Password_Policy.doc

SlavaSoft Optimizing Checksum Utility Version 2.0
Implemented using SlavaSoft QuickHash Library <www.slavasoft.com>
Copyright (C) SlavaSoft Inc. 1999-2002. All rights reserved.

; SlavaSoft Optimizing Checksum Utility fsum 2.0 <www.slavasoft.com>
;
; Generated on 12/07/04 at 23:07:46
;
b0ef81f932254d57fb9c685d9eeaf274 *Password_Policy.doc

F:\GIAC\Copy of Recovered from Password_Policy.doc\test2>
```

Post Incident Activities

Given the severity of the incident the following activities are recommended to by undertaken in priority order:

1. Impound Mr R J Leszczynski's PC and any other system on which he had unfettered access (without powering it on) and have it Forensically

Analysed. The hashes from items 13, 16 and 23 should be searched for on the imaged drives (having performed a deep or recursive hash of all files on his HDD; this will confirm or otherwise the presence of pre or post camouflaged files.

2. Prevent Mr R J Leszczynski from having any access to his or any Company system, all of his accounts should be frozen immediately and any current sessions terminated immediately; in case he tries to destroy evidence.

3. Obtain legal advice (from the Company's lawyers) on the possibilities of seeking legal recompense for Mr R J Leszczynski's actions.

4. Perform a sweep of the network for the Camshell.dll file and impound any system reporting its presence.

5. Seek an Search Order under Section 7 of the Civil Procedure Act 1997[13] (formerly an 'Anton Piller Order' after the case of the same name), and search and sieze his home pc and any media that may contain the exported data. Depending on the outcome of the search and subsequent forensic analysis of the media, sue the individual for theft of Intellectual Property and breach of IRP.

6. Perform a re-education programme on the IT and Security policies affecting the use of corporate and personal IT for the processing of Ballard Ind. data.

7. Write to the manager of the security guard whose excellent actions resulted in this leakage of data being stopped.

Legal position

As suggested above, although there has been no Criminal Law breach, the Corporate Espionage that appears to have been conducted can be addressed through the UK civil courts. Furthermore, this procedure carries less risk for the Company and achieves results considerably quicker. Having consulted with several UK IT Security lawyers it was confirmed that a Criminal case can take upto 18 months from the incident to appear in court. Additionally, the incident is turned over to the UK Police, who conduct the investigation as best they can with shifting priorities and reducing resources.

The civil court route places the responsibility in the Company's hands as they choose their investigators and legal team. The lawyers consulted spoke of cases taking less then 4 months from incident to the court case and the aware of damages.

Furthermore, the weight of argument required in a civilian court is less as 'the Balance or probabilities' as apposed to 'Beyond all reasonable doubt' in a criminal court.

As to breaching Ballard’s own Policies, the position is not clear cut there either:

Acceptable Encryption Policy

The Camouflage program is Steganographic and therefore only hides the data it does not encrypt it, therefore the Acceptable Encryption Policy has not been breached.

Information Sensitivity Policy

Here the subject could claim they were not aware of the sensitivity of the data he exported; however, this is unlikely to stand up to the balance of probabilities (remembering he had probably worked there for some time as he was the lead engineer) and there was no accident to the hiding and passwording of these files.

Therefore it is suggested that Mr R J Leszczynski is in breach of paragraph 3.3 on this policy:

Item 26 – Quote from Ballard Ind InformationSensivity Policy

> **3.3 Most Sensitive:** Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company
>
> Marking guidelines for information in hardcopy or electronic form.
>
> *Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that Ballard Industries Confidential information is very sensitive, you may should label the information "Ballard Industries Internal: Registered and Restricted", "Ballard Industries Eyes Only", "Ballard Industries Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of Ballard Industries Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.*
>
> **Access:** Only those individuals (Ballard Industries employees and non-employees) designated with approved access and signed non-disclosure agreements.
> **Distribution within Bright Industries:** Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.
> **Distribution outside of Ballard Industries internal mail:** Delivered direct; signature required; approved private carriers.
> **Electronic distribution:** No restrictions to approved recipients within Bright Industries, but it is highly recommended that all information be strongly encrypted.
> **Storage:** Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.
> **Disposal/Destruction:** Strongly Encouraged: In specially marked disposal bins on Ballard Industries premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
> **Penalty for deliberate or inadvertent disclosure:** Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

The Password, Remote Access and Lab Internal Security policies have no bearing on this matter.

In summary Mr R J Leszczynski has beached the company policy on Information Sensitivity, and given it was on the disk with which he caused the breach, he cannot argue that he was not aware of it either (double whammy!). It would be for the civilian court process to decide on the level of damages that could be awarded following a successful case, but before that is undertaken the search and seizure of the media at Mr R J Leszczynski's private address should be undertaken to ensure that data is returned to the data owner and that the full extent of his activities are declared to the courts.

Item 27 – Tools Used Matrix

Tools	Operating System	Notes
File	Linux	Describes the type and composition of a file
Md5sum	Linux	Performs an MD5 sum hash of a file
Fsum	Windows	Performs an MD5 sum hash of a file
Norton AntiVirus	Windows	For virus sweeping of found files
Autopsy (version #1.70)	Linux	For analysis of the recovered disk
The Sleuth Kit	Linux	Autopsy uses Perl scripts to run the various Sleuth Kit commands
Mozilla (version # 1.6)	Linux	Used to view and control Autopsy
Dir	Windows	Lists files
WinZip (version #8.1)	Windows	Examine zip files without executing
Camouflage (version #1.2.1)	Windows	The steganographic program examined and believed to have been used by subject disk's owner

End of Part One

IT Forensic Analysis of an abandoned computer and its Hard Disk

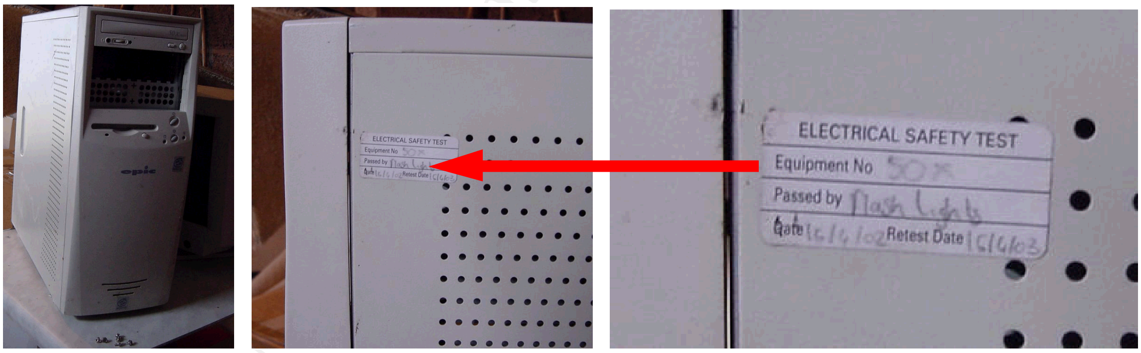
Background

On the 31st of August 2004, while depositing some refuse at the local tip a computer was found discarded. Inquiries with the local operative revealed that the system had been left there the previous day. Without opening the system up, a payment of £3 (approx ~$5) was requested from the site manage, as contribution to their 'tea fund'. Later investigations revealed the system to be an excellent purchase as can be seen:

Intel Pentium III operating at 600Mhz.but no memory (RAM)
1 x 50 speed CD ROM
Onboard sound card
Network card
1 x 6.4 Gb Integrated Disk Electronics (IDE) Hard Disk Drive (HDD)

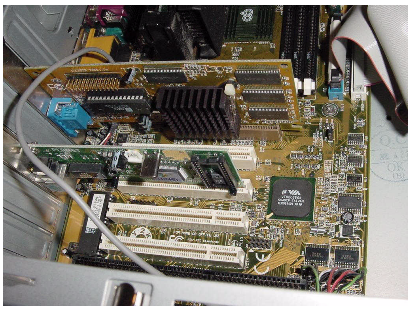
The system was the removed from the facility and returned to an examination area (investigators garage)where it was catalogued and photographed. Notice the electrical safety check record (dated 16 April 02 to expire 16 April 03) hinting to a production system as apposed to a home use one ; additionally the tower case from this manufacturer 'Epic PCs'[14] also suggests the use was not a personal one.

Item 28 – Pictures of the outside of the system



The side, HDD and Floppy drive removed the system was again photographed to show age, serial numbers and general condition (notice the almost total lack of dusk on all parts displayed).

Item 29 – Pictures of the inside of the system



The HDD removed it was catalogued as:

Investigation Serial number : **REC/SJA/01Aug04/HDD1**
Description **:** Fujitsu ATA Hard Disk Model No MPE3064AT Serial No 01334622

The system as discovered minus the HDD was described and catalogued as:

Investigation Serial number : **REC/SJA/01Aug04/BaseUnit_1**
Description: Epic tower system with CDROM, graphics card, FDD, PSU and NIC. With the 2nd 5½ Drive bay empty and both its and the 3rd bays front missing.

Case and Motherboard testing

The rest of the system was inspected for water or damage and with the drive removed, the system was powered to inspect the BIOS for clues as to the systems use. The two main points of note when booting the system were:

It worked, indicating that the HDD may too be functional.

The BOIS time was incorrect and was approx 62 minutes fast (see the picture below)

The BIOS date on the system was incorrect as motherboard date was the 3 Aug 2004 when in actual fact the picture below was taken on Tuesday 31st August 2004 ie the date is out by 28 days!.

The time and date discrepancy observed was not expected and was contrary to the general condition of the system and this hinted of either:

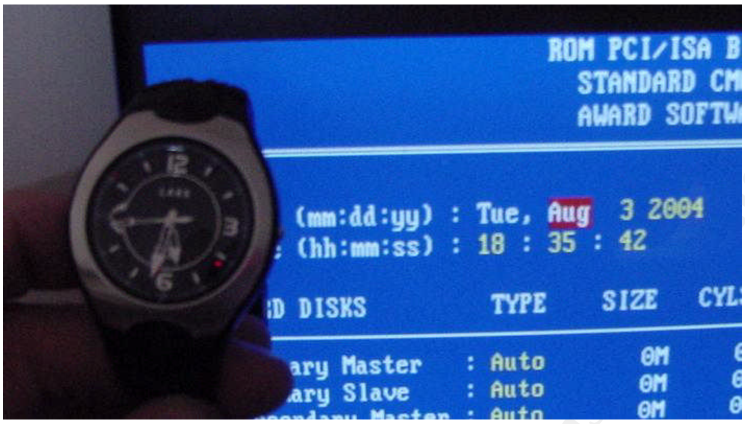
A lack of use (or synchronisation with an internet clock)

BIOS Battery failure – but as the right month and year were still held this was discounted.

The user must not have noticed or has deliberately changed the time and date for a particular reason.

BIOS battery was low or the system had been stored in a cold environment) failure as most mother boards alert the user to this fact, and a check with a exhausted confirmed this motherboard to do so.

Item 30 – BIOS Timings taken at 1733 hours on 31 August 2004

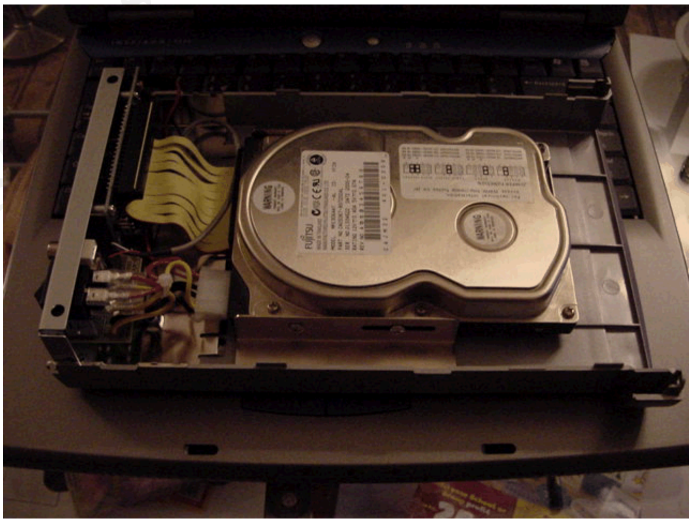


```
                              ROM PCI/ISA B
                               STANDARD CM
                               AWARD SOFTW

 (mm:dd:yy) : Tue, Aug  3 2004
: (hh:mm:ss) : 18 : 35 : 42

D DISKS              TYPE     SIZE    CYL

ary Master         : Auto      0M      0
ary Slave          : Auto      0M      0
```

Furthermore, any time error expected would have been in the other direction ie that the British Summer Time (BST) clock adjustment had not been applied (BST calls for the clock to advance 1 hour in Spring and retard 1 hour in October). The date error perplexed the investigator but he hoped that information gathered later would shed light on this matter, in the mean time, all dates and times would be treated with suspicion.

The function test of the remaining system complete it was sealed and stored in the locker of the garage. Meanwhile the HDD was prepared for imaging. The photograph below shows the hard disk installed in an external caddie ready to be connected to the Forensic Laptop (under it).

Item 31 – The external IDE caddie with the abandoned drive fitted



Forensic Laptop Specification

The forensic Laptop used for this examination was a Dell Inspiron 5100. The specification of the laptop being; Intel Pentium 4 2800 MHz with 768Mb RAM, a CDR/RW and 3com on board network card. The graphics processor was a 64 mb Mobile ATI card with a 1024x768 TFT screen. It boasts a IEEE 1394 port as well as 2 x USB 2 ports. This laptop has more than proven itself in the past and the performance of each of the components has been well above standard without the need for specialist drivers. It will accept over 15 different distributions of Linux and has run Windows from 95 – 2003 Enterprise Server. As the caddie cost in the region of £30 (~$55), the Main Forensic OS was a free distribution(FC2) and the laptop (inc 2 extra HDD and internal caddie drives) cost £550 (~$1030) the whole forensic outfit was comparatively cheep £580 ($1085).

The only glitch that was presented was with the use of the external caddie which connects IDE devices to either IEEE 1394 or USB2. While MS Windows was able to address the device, Fedora Core 2 did not have any support for it in the kernel. That said some research on the internet did reveal a patch had been submitted (see below) which when applied allowed the external caddie to be mounted in the Fedora Core 2 (FC2) OS in read only mode.

Item 32 – External Caddie OS Patch [15]

```
<alexander@all-2.com>
   [PATCH] USB storage: patch for unusual_devs.h

   I send a patch and copy of /proc/bus/usb/devices for my 5`25 external
   USB enclosure. I don't know exactly manufacturer of this device, but
   model is CD-509.
   It will be nice if it helps somebody else.
                     http://www.linuxhq.com/kernel/changelog/v2.6/1/
```

Note Write support for NTFS is very limited see cutting below from the Linux-NTFS sourceforge.net web site[16].

Item 33 – Quote on NFTS write support

> **3.2 Can the Driver write to an NTFS volume, too?**
>
> Not really, but if you only need to copy files from Linux to Windows on a dual-boot machine, see "How to write to NTFS" below for a possible way to work around the lack of write support. For write support in Linux, read on.
>
> There are two drivers, currently. The original driver, in 2.4 has some write code in it, but it is **extremely dangerous** to use it. The possibility of destroying your filesystem is very high.

Legal Implications of using the abandoned computer

Given the circumstances under which the system was acquired, it is worth recounting the legal position the author is in regarding the ownership of the system. Section 5(1) of the Theft Act 1968 provides a legal defence to the finder of items of property that the owner has abandoned:

Item 34 – Legal defence for Theft

> **5. Belonging to another**
> (1) Property shall be regarded as belonging to any person having possession or control of it, or having in it any proprietary right or interest (not being an equitable interest arising only from an agreement to transfer or grant an interest).
> Section 5 of the 1968 Theft Act[17]

Further clarification was listed as being:

> If property is genuinely and honestly abandoned then it cannot be theft because it belongs to no one.

However, as the item was effectively given to the site for disposal it is their property and thus the £3 payment can be considered sufficient given that the condition of the system was not known and that it had been left outside in the rain overnight.

The fact that the system had been left at a refuse tip led the author to believe that the owner had abandoned his rights of ownership of the hardware. This is a legal position under Section 2 of the Theft Act 1968, which allow anyone to claim ownership of the property if they believe the owner has given up the ownership of the property.

Content that the system had been legitimately acquired, analysis could commence.

Basic Analysis

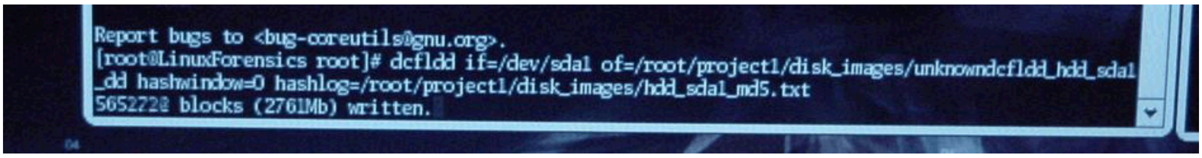
The Hard disk was installed into the external caddie and connected to the USB port of the investigators patched laptop. The Linux `dd` command was used to copy portions of the `/dev` directory in an attempt to identify which directory the drive had been mounted to. This had proved in the investigators experience to be the best method as the /dev directory used by the kernel varied between devices and USB ports. The procedure involved using dd with the syntax below:

```
#/ dd if=/dev/sda of=/tmp/mount_test1
```

This was executed and allowed to run for several seconds before being interrupted and the output file being examined with `vi`. If the output file was blank a different `/dev/` folder would b selected. Success was often being achieved within 2 guesses.

Once the correct directory was identified a `dcfldd`[18] command was executed to image the whole drive.

Item 35 – Imaging in progress



```
Report bugs to <bug-coreutils@gnu.org>.
[root@LinuxForensics root]# dcfldd if=/dev/sda1 of=/root/project1/disk_images/unknowndcfldd_hdd_sda1
_dd hashwindow=0 hashlog=/root/project1/disk_images/hdd_sda1_md5.txt
5652228 blocks (2761Mb) written.
```

The dcfldd command (written by the Defence Computer Forensics Laboratory as indicated by the 'dcfl' bit inform of the dd) was used image process as it is an improvement over the native dd command. The labs basically modified the native dd command so it performs an MD5 hash of the HDD as it images it (in the above screenshot it is the 'hashlog') and it also displays the counters showing the progress of the execution.

Once the whole disk image had been performed an md5 hash was taken of the source drive and this was compared with dcfldd hashlog. As these were found to be exactly the same the investigator has assumed the image file to be a bit-for-bit copy of the /dev/sda drive. The image of the drive that then obtained file was made read only (using the chmod 444 <image_file> command). To prevent any file handling errors from disrupting the investigation, the image file was copied to a different folder /root/datavault to allow copies to be made should a working copy be corrupted in any way. Once copied to the second location, an md5 hash was taken and stored in a separate file in the /root/datavault. This hash matched the original image file and the source drive itself and would serve as a reference should any one wish to confirm the authenticity of any file used or obtained during this investigation.

The file command was used in an effort to identify the contents of the file. The file command examines the contents of an object, its structure and the text within it, in an effort to classify what this object is. The output of the file upon the drive image was:

```
    Unknown_hdd_dfcldd_sda: x 86 boot sector
```

Next the process is repeated for the first partition on the drive which was mounted in the /dev/sda1 directory. The md5 hash, copying to the /root/datavault, chmod and file process was again repeated and the file command was used to examine the contents. This time the output was:

Item 36 – Output from the file command

```
Unknowndcfldd_hdd_sda1_dd: x86 boot sector, code
offset0x58, OEM-ID "MSWIN4.1", sectors/cluster 8, Media
descriptor 0xf8, heads 255, hidden sectors 63, sectors
12659157 (volumes > 32 MB) , FAT (32 bit), sectors/FAT
12342, reserved3 0x800000, serial number 0x1c12160a,
unlabeled
```

A look at the Microsoft web site[19] decoded the MSWIN4.1 as:

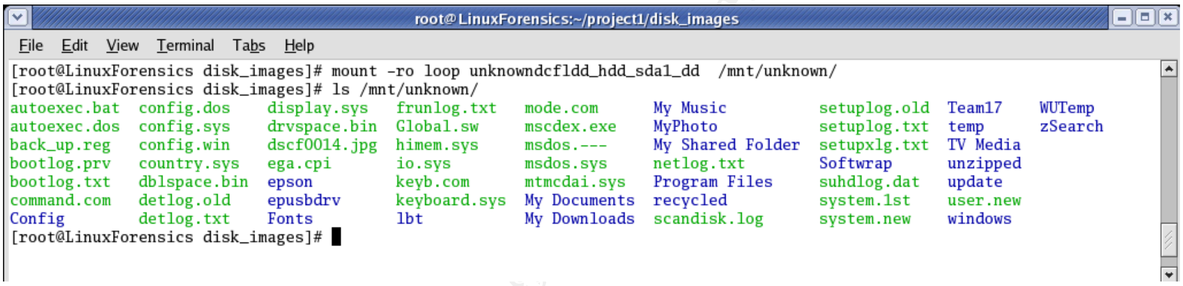
Item 37 – Quote from Microsoft explaining the HDD ID Tag

> You might also see the OEM ID "MSWIN4.0" on disks formatted by Windows 95 and "MSWIN4.1" on disks formatted by Windows 95 OEM Service Release 2 (OSR2), Windows 98, and Windows Me. Windows XP Professional does not use the OEM ID field in the boot sector except for verifying NTFS volumes.

Therefore, it is assumed that the hard disk was formatted with either Windows 95 (OSR2), Windows 98 or Windows ME. Whilst it is not impossible for this to be a production system, this latest fact would more than hint to a personal user.

With the image marked as read-only in the Linux file permissions, the image was mounted as a loop-back read only device in the `/mnt/unknown` directory. This was to allow the investigator see for the first time the directory structure. Additionally, as both the mount command and the Linux file permissions were set to read-only, browsing could be undertaken without fear of altering the data.

Item 38 – First look at the imaged file structure



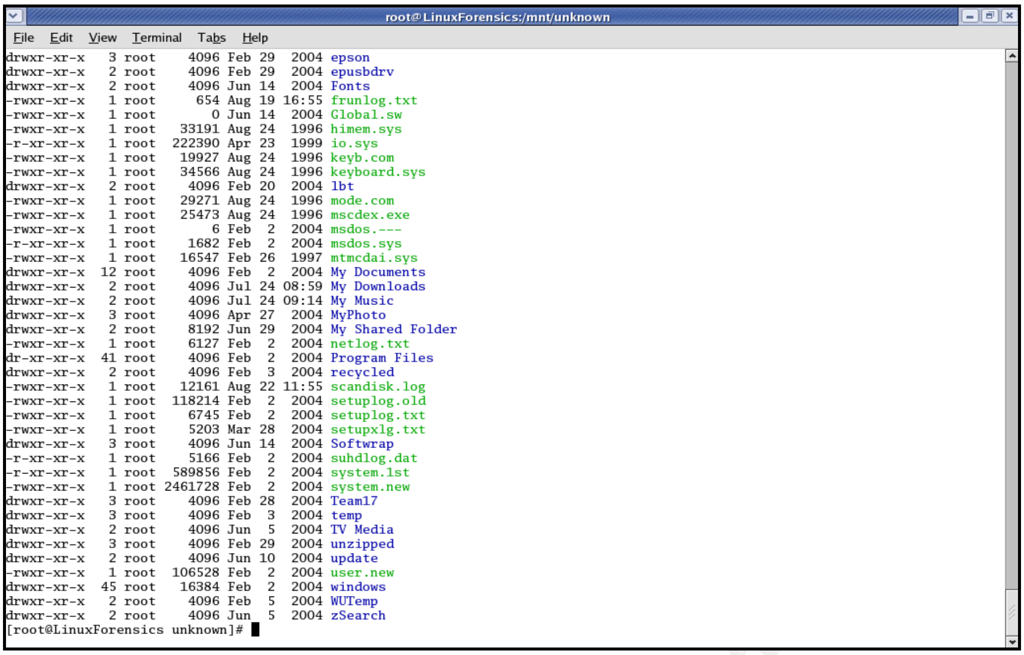
```
[root@LinuxForensics disk_images]# mount -ro loop unknowndcfldd_hdd_sda1_dd  /mnt/unknown/
[root@LinuxForensics disk_images]# ls /mnt/unknown/
autoexec.bat  config.dos    display.sys   frunlog.txt   mode.com      My Music          setuplog.old  Team17    WUTemp
autoexec.dos  config.sys    drvspace.bin  Global.sw     mscdex.exe    MyPhoto           setuplog.txt  temp      zSearch
back_up.reg   config.win    dscf0014.jpg  himem.sys     msdos.---     My Shared Folder  setupxlg.txt  TV Media
bootlog.prv   country.sys   ega.cpi       io.sys        msdos.sys     netlog.txt        Softwrap      unzipped
bootlog.txt   dblspace.bin  epson         keyb.com      mtmcdai.sys   Program Files     suhdlog.dat   update
command.com   detlog.old    epusbdrv      keyboard.sys  My Documents  recycled          system.1st    user.new
Config        detlog.txt    Fonts         lbt           My Downloads  scandisk.log      system.new    windows
[root@LinuxForensics disk_images]# 
```

A cursory examination of this the root of the system, would confirm the `file` identification of the early personal edition of Windows. Files like the `autoexec.bat` and `config.sys` are not used on windows NT (any version) and the FAT32 file structure was not readable by NT. In order that we might learn the install date of the operating system the `ls` command was executed with the ‘ `-abo` ’ switches. These have the effect of displaying (taken from the ls manual):

```
      -a    -     do not hide entries starting with .
      -b    -     print octal escapes for non graphic characters
      -o    -     use a long list format but do not list group
information
```

This produced the following output:

Item 39 – Initial look at file ownership and their associated creation times/dates



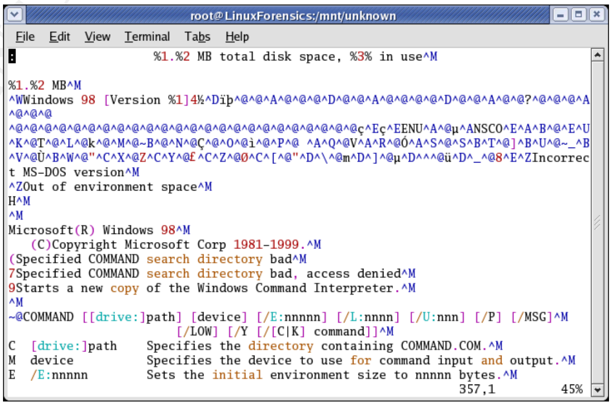
root@LinuxForensics:/mnt/unknown
File Edit View Terminal Tabs Help

```
drwxr-xr-x   3 root    4096 Feb 29  2004 epson
drwxr-xr-x   2 root    4096 Feb 29  2004 epusbdrv
drwxr-xr-x   2 root    4096 Jun 14  2004 Fonts
-rwxr-xr-x   1 root     654 Aug 19 16:55 frunlog.txt
-rwxr-xr-x   1 root       0 Jun 14  2004 Global.sw
-rwxr-xr-x   1 root   33191 Aug 24  1996 himem.sys
-r-xr-xr-x   1 root  222390 Apr 23  1999 io.sys
-rwxr-xr-x   1 root   19927 Aug 24  1996 keyb.com
-rwxr-xr-x   1 root   34566 Aug 24  1996 keyboard.sys
drwxr-xr-x   2 root    4096 Feb 20  2004 lbt
-rwxr-xr-x   1 root   29271 Aug 24  1996 mode.com
-rwxr-xr-x   1 root   25473 Aug 24  1996 mscdex.exe
-rwxr-xr-x   1 root       6 Feb  2  2004 msdos.---
-r-xr-xr-x   1 root    1682 Feb  2  2004 msdos.sys
-rwxr-xr-x   1 root   16547 Feb 26  1997 mtmcdai.sys
drwxr-xr-x  12 root    4096 Feb  2  2004 My Documents
drwxr-xr-x   2 root    4096 Jul 24 08:59 My Downloads
drwxr-xr-x   2 root    4096 Jul 24 09:14 My Music
drwxr-xr-x   3 root    4096 Apr 27  2004 MyPhoto
drwxr-xr-x   2 root    8192 Jun 29  2004 My Shared Folder
-rwxr-xr-x   1 root    6127 Feb  2  2004 netlog.txt
dr-xr-xr-x  41 root    4096 Feb  2  2004 Program Files
drwxr-xr-x   2 root    4096 Feb  3  2004 recycled
-rwxr-xr-x   1 root   12161 Aug 22 11:55 scandisk.log
-rwxr-xr-x   1 root  118214 Feb  2  2004 setuplog.old
-rwxr-xr-x   1 root    6745 Feb  2  2004 setuplog.txt
-rwxr-xr-x   1 root    5203 Mar 28  2004 setupxlg.txt
drwxr-xr-x   3 root    4096 Jun 14  2004 Softwrap
-r-xr-xr-x   1 root    5166 Feb  2  2004 suhdlog.dat
-r-xr-xr-x   1 root  589856 Feb  2  2004 system.1st
-rwxr-xr-x   1 root 2461728 Feb  2  2004 system.new
drwxr-xr-x   3 root    4096 Feb 28  2004 Team17
drwxr-xr-x   3 root    4096 Feb  3  2004 temp
drwxr-xr-x   2 root    4096 Jun  5  2004 TV Media
drwxr-xr-x   3 root    4096 Feb 29  2004 unzipped
drwxr-xr-x   2 root    4096 Jun 10  2004 update
-rwxr-xr-x   1 root  106528 Feb  2  2004 user.new
drwxr-xr-x  45 root   16384 Feb  2  2004 windows
drwxr-xr-x   2 root    4096 Feb  5  2004 WUTemp
drwxr-xr-x   2 root    4096 Jun  5  2004 zSearch
[root@LinuxForensics unknown]#
```

It is a known fact that Windows 9x and ME used fixed dates for the creation times and dates for its system files, directories and applications installed from the CDROM. However, as the OS is installed on the disk the new directories created as a result of the OS operation will be given the local, natural, real time and date settings (assuming the end user set the time and time zone correctly). Therefore, is can be assumed that the OS was installed on 2nd February 2004 given the data associated with the '`Windows`', '`My Documents`', '`Program Files`' directories and the stamps on the `setuplogs.old`, `setup.txt` and `system.1st` files. While some time and date errors have been found, the windows process of requesting the user to set the correct date, time and time zone are at this point assumed to have been done and that the information entered is accurate.

Finally, `vi` is used to display the contents of the command.com file as this would be used to start a command shell and MS Windows OS always reports the host OS at the top of any new shell. The screenshot below confirms the presence of a Windows 98[20] installation.

Item 40 – Windows version extracted from the shell



root@LinuxForensics:/mnt/unknown
File Edit View Terminal Tabs Help

```
:                  %1.%2 MB total disk space, %3% in use^M

%1.%2 MB^M
^WWindows 98 [Version %1]4½^Dïþ^@^@^A^@^@^@^D^@^@^A^@^@^@^@^D^@^@^A^@^@?^@^@^@^A
^@^@^@
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@ç^Eç^EENU^A^@µ^ANSCO^E^A^B^@^E^U
^K^@T^@^L^@k^@^M^@~B^@^N^@Ç^@^O^@ì^@^P^@ ^A^Q^@V^A^R^@Ó^A^S^@^S^B^T^@]^B^U^@~_^B
^V^@Ù^B^W^@"^C^X^@Z^C^Y^@£^C^Z^@Ø^C^[^@"^D^\^@m^D^]^@µ^D^^^@ü^D^_^@8^E^ZIncorrec
t MS-DOS version^M
^ZOut of environment space^M
H^M
^M
Microsoft(R) Windows 98^M
   (C)Copyright Microsoft Corp 1981-1999.^M
(Specified COMMAND search directory bad^M
7Specified COMMAND search directory bad, access denied^M
9Starts a new copy of the Windows Command Interpreter.^M
^M
~@COMMAND [[drive:]path] [device] [/E:nnnnn] [/L:nnnn] [/U:nnn] [/P] [/MSG]^M
                       [/LOW] [/Y [/[C|K] command]]^M
C  [drive:]path    Specifies the directory containing COMMAND.COM.^M
M  device          Specifies the device to use for command input and output.^M
E  /E:nnnnn        Sets the initial environment size to nnnnn bytes.^M
                                                                 357,1         45%
```

Before concluding the basic analysis, an assessment of the role the system operated under before disposal was conducted. The key factors in this are the files and directory structure, the OS, the systems hardware and the manner and style of disposal. The assessment is split into factors for the business use and factors for the private use.

Business Use:

1. Business type case (ie tower).
2. Electrical Safety Check sticker on the case, would indicate a Health and Safety requirement for the system owner to ensure the user's system is safe to use. The investigator had never heard of any one having such tests performed on home electrical appliances (due to cost).
3. The case was very clean inside indicating either regular and thorough cleaning or the fact the system was in an air conditioned environment.

Personal Use:

1. Operating System use is a classic home user one.
2. The age of the operating system (6 years) would indicate it was a outright purchase and not on contract for regular or frequent updating.
3. The system was a reasonable specification and in business would most likely have been reused for some other task as it met the min spec for Windows 2000 Professional, Windows 2003 Server and XP Pro (or home). However, given the current specification of home systems is would be considered dated and limited.
4. The Team17 folder would indicate the presence of a game (as Team17 install their games to these folders eg Worms), unlikely (but not impossible) for it to be used on a business system.

Conclusion

1. The system appears to be both and it is therefore believed it was indeed used for business purposes up to some time after 16 April 2002 when the electrical safety check was performed.
2. It was then possibly transferred to a home user where most recently on the 2nd February 2004 Windows 98 was installed.

Key areas and direction for Detailed Analysis

It is important when performing any detailed task to have both objectives and direction otherwise time and effort can be wasted proving points that are not relevant or of value to the investigation. The following will be used to direct investigation and data recovery during the next stage. The success and performance of the forensic examination and analysis will be gauged against these objectives.

Investigation Objectives

Number	System Objectives – (Identify)	Comments
S1	Operating System	
S2	Current OS	
S3	Previous OS	if identifiable
S4	Last booted / shutdown (date and time)	
Number	**User Objectives – (Identify)**	**Comments**
U1	The common and or last user	
U2	Owner (physical and email addresses)	Not for print in this report
U3	IP Address of the last user	Static IP not inc in this report
U4	General User activity	
Number	**Hidden software Objectives**	**Comments**
H1	Locate and identify any Viruses	
H2	Locate and identify any Spyware	
H3	Locate and identify any Malware	
H4	Locate and identify any Trojans	
Number	**Legal Objectives**	**Comments**
L1	Identify any illegal activity	
L2	Identify any illegal software	

Detailed Analysis

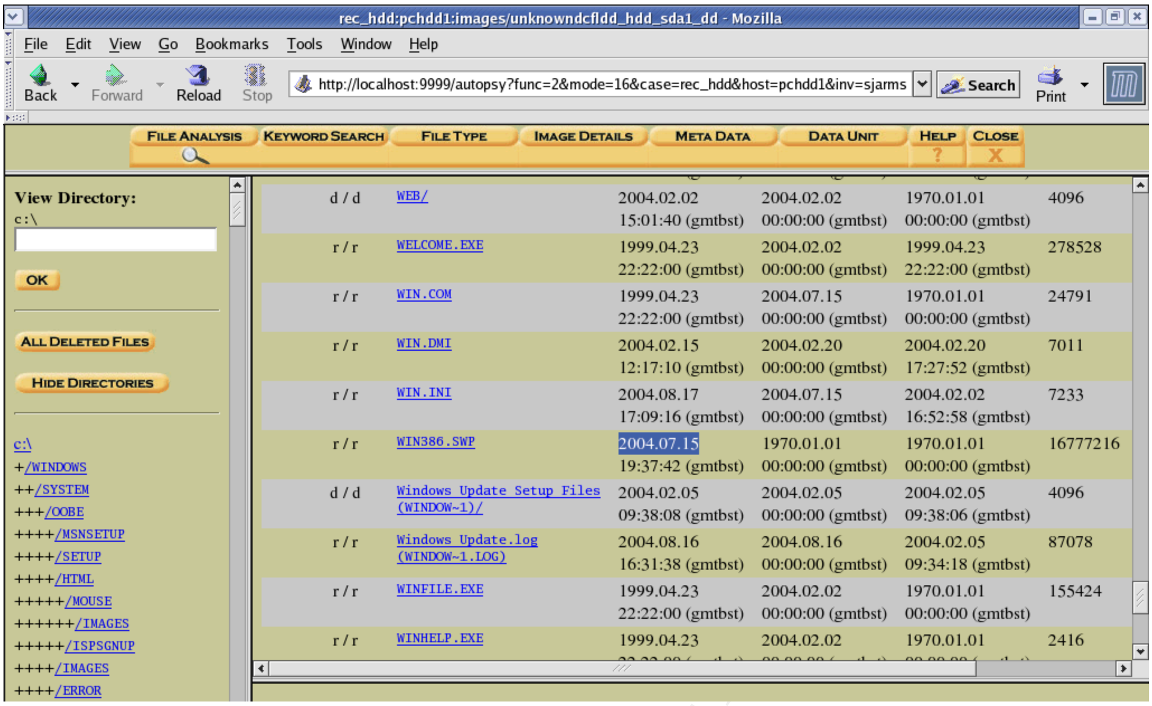
The detailed analysis commenced with the starting of the `Autopsy` (v1.70) and mounting of the disk images to the software. `Autopsy` given the investigator the option to adjust the time zone and mount time of the files to reflect minor discrepancies in the clock of the system. This would mainly be used when several systems are being compared and all times need to be accurate to an external reference. As this was the only system being analysed, it was not necessary and the time zone was set only to Greenwich Mean Time and British Summer Time (GMTBST).

Once mounted the system was subject to an md5 hash and this was compared to that of the original `dcfldd hashoutput`. Next the file browser window was opened and a general examination of the contents of the drive was conducted. The date and time that the `%systemroot%/win386.swp` held should have indicated the last point at which the OS conducted any swap operations. Swap operations are where data in memory is 'paged' or 'swapped' to the hard disk. This is used to allow the multitasking of the OS to be undertaken when it has insufficient RAM to host itself, the drivers and the applications.

In a typical Windows system the OS consumed up to 60% of the available RAM so the swap file was in regular use. When shut down, the swap file is one of the last files accessed and closed and as a result it is usually a good indication of the last time the system was used ie 15th July 2004 @ 1937 hours (GMTBST). However, the file picture directly above the `win386.swp` is the `win.ini` file, which is used store the configuration of the OS (only Win 9x and ME used this feature as the registry is used by NT, 2000, XP and 2003), and this file has a date of 17th August

2004! So a full time line analysis will be conducted on the information extracted via `Autopsy`.

Item 41 – Possibly the last use of the system



http://localhost:9999/autopsy?func=2&mode=16&case=rec_hdd&host=pchdd1&inv=sjarms

View Directory:
c:\

c:\
+/WINDOWS
++/SYSTEM
+++/OOBE
++++/MSNSETUP
++++/SETUP
++++/HTML
+++++/MOUSE
++++++/IMAGES
+++++/ISPSGNUP
++++/IMAGES
++++/ERROR

d / d	WEB/	2004.02.02 15:01:40 (gmtbst)	2004.02.02 00:00:00 (gmtbst)	1970.01.01 00:00:00 (gmtbst)	4096
r / r	WELCOME.EXE	1999.04.23 22:22:00 (gmtbst)	2004.02.02 00:00:00 (gmtbst)	1999.04.23 22:22:00 (gmtbst)	278528
r / r	WIN.COM	1999.04.23 22:22:00 (gmtbst)	2004.07.15 00:00:00 (gmtbst)	1970.01.01 00:00:00 (gmtbst)	24791
r / r	WIN.DMI	2004.02.15 12:17:10 (gmtbst)	2004.02.20 00:00:00 (gmtbst)	2004.02.20 17:27:52 (gmtbst)	7011
r / r	WIN.INI	2004.08.17 17:09:16 (gmtbst)	2004.07.15 00:00:00 (gmtbst)	2004.02.02 16:52:58 (gmtbst)	7233
r / r	WIN386.SWP	2004.07.15 19:37:42 (gmtbst)	1970.01.01 00:00:00 (gmtbst)	1970.01.01 00:00:00 (gmtbst)	16777216
d / d	Windows Update Setup Files (WINDOW~1)/	2004.02.05 09:38:08 (gmtbst)	2004.02.05 00:00:00 (gmtbst)	2004.02.05 09:38:06 (gmtbst)	4096
r / r	Windows Update.log (WINDOW~1.LOG)	2004.08.16 16:31:38 (gmtbst)	2004.08.16 00:00:00 (gmtbst)	2004.02.05 09:34:18 (gmtbst)	87078
r / r	WINFILE.EXE	1999.04.23 22:22:00 (gmtbst)	2004.02.02 00:00:00 (gmtbst)	1970.01.01 00:00:00 (gmtbst)	155424
r / r	WINHELP.EXE	1999.04.23	2004.02.02	1970.01.01	2416

The creation of the time line was the next objective. This would show the creation, modification and access times (MAC) for all current files. It would also obtain from the meta data the MACs for the files that have been deleted, this is less accurate as the meta data deteriorates when parts of the disk are reused. However, as we believe the system was a home PC that may have been used by a business, some remnants of the old data or data structures may remain. The `Autopsy` tool interface was directed to create the time line and the output analysed in a text reader (as the web browser is not ideal and cannot handle long documents very well).

Item 42 – Cutting from System Time Line

```
Thu Aug 19 2004 15:55:34        0 ..c -rwxrwxrwx 0        0        1188829  <unknowndcfldd_hdd_sda1_dd-_SL7235.TMP-dead-1188829>
                              654 m.. -/-rwxrwxrwx 0        0        6        c:\/FRUNLOG.TXT
                                0 ..c -/-rwxrwxrwx 0        0        1188829  c:\/WINDOWS/TEMP/_SL7235.TMP (deleted)
Thu Aug 19 2004 15:55:36        0 m.. -/-rwxrwxrwx 0        0        1188829  c:\/WINDOWS/TEMP/_SL7235.TMP (deleted)
                                0 m.. -rwxrwxrwx 0        0        1188829  <unknowndcfldd_hdd_sda1_dd-_SL7235.TMP-dead-1188829>
Sun Aug 22 2004 00:00:00     7329 .a. -/-rwxrwxrwx 0        0        1740848  c:\/WINDOWS/COMMAND/SCANDISK.INI
                           143818 .a. -/-rwxrwxrwx 0        0        1740816  c:\/WINDOWS/COMMAND/SCANDISK.EXE
                            12161 .a. -/-rwxrwxrwx 0        0        27       c:\/SCANDISK.LOG
Sun Aug 22 2004 10:55:16    12161 m.. -/-rwxrwxrwx 0        0        27       c:\/SCANDISK.LOG
Mon Oct 13 1930 09:02:20   606252 ..c -rwxrwxrwx 0        0        94135322 <unknowndcfldd_hdd_sda1_dd-_TA95930-dead-94135322>
                           552960 ..c -rwxrwxrwx 0        0        94135323 <unknowndcfldd_hdd_sda1_dd-_TB95930-dead-94135323>
                           552960 ..c -rwxrwxrwx 0        0        94135312 <unknowndcfldd_hdd_sda1_dd-_ISTRENU.DLL-dead-94135312>
                           606252 ..c -rwxrwxrwx 0        0        94135310 <unknowndcfldd_hdd_sda1_dd-_EOTRACE.EXE-dead-94135310>
Fri Nov 21 1930 08:44:30      660 ..c -rwxrwxrwx 0        0        94135947 <unknowndcfldd_hdd_sda1_dd-_TXCON~1.HTM-dead-94135947>
Thu Nov 27 1930 17:31:44   606252 .a. -rwxrwxrwx 0        0        94135322 <unknowndcfldd_hdd_sda1_dd-_TA95930-dead-94135322>
                           552960 .a. -rwxrwxrwx 0        0        94135323 <unknowndcfldd_hdd_sda1_dd-_TB95930-dead-94135323>
Mon Jan 19 1931 08:41:58   159744 ..c -rwxrwxrwx 0        0        94134854 <unknowndcfldd_hdd_sda1_dd-_TJ74961-dead-94134854>
                           258100 ..c -rwxrwxrwx 0        0        94134796 <unknowndcfldd_hdd_sda1_dd-_WHOME.DLL-dead-94134796>
                           159744 ..c -rwxrwxrwx 0        0        94134794 <unknowndcfldd_hdd_sda1_dd-_WPLUGIN.DLL-dead-94134794>
                           258100 ..c -rwxrwxrwx 0        0        94134849 <unknowndcfldd_hdd_sda1_dd-_TE74961-dead-94134849>
                           319543 ..c -rwxrwxrwx 0        0        94134850 <unknowndcfldd_hdd_sda1_dd-_TF74961-dead-94134850>
                           319543 ..c -rwxrwxrwx 0        0        94134798 <unknowndcfldd_hdd_sda1_dd-_WHOME~1.DLL-dead-94134798>
Mon Jan 19 1931 08:42:00   299008 ..c -rwxrwxrwx 0        0        94134848 <unknowndcfldd_hdd_sda1_dd-_TD74961-dead-94134848>
                           299008 ..c -rwxrwxrwx 0        0        94134811 <unknowndcfldd_hdd_sda1_dd-_WCORE.DLL-dead-94134811>
Mon Jan 19 1931 08:42:02   184320 ..c -rwxrwxrwx 0        0        94134855 <unknowndcfldd_hdd_sda1_dd-_TK74961-dead-94134855>
                           184320 ..c -rwxrwxrwx 0        0        94134819 <unknowndcfldd_hdd_sda1_dd-_WRULE~1.DLL-dead-94134819>
Mon Jan 19 1931 08:42:08    77824 ..c -rwxrwxrwx 0        0        94134846 <unknowndcfldd_hdd_sda1_dd-_TB74961-dead-94134846>
                           586860 ..c -rwxrwxrwx 0        0        94134860 <unknowndcfldd_hdd_sda1_dd-_TP74961-dead-94134860>
                           106496 ..c -rwxrwxrwx 0        0        94134847 <unknowndcfldd_hdd_sda1_dd-_TC74961-dead-94134847>
                           106496 ..c -rwxrwxrwx 0        0        94134823 <unknowndcfldd_hdd_sda1_dd-_WCHECK.DLL-dead-94134823>
                           143360 ..c -rwxrwxrwx 0        0        94134821 <unknowndcfldd_hdd_sda1_dd-_WSETUP.DLL-dead-94134821>
                            58368 ..c -rwxrwxrwx 0        0        94134827 <unknowndcfldd_hdd_sda1_dd-_CRTL32.DLL-dead-94134827>
                            58368 ..c -rwxrwxrwx 0        0        94134858 <unknowndcfldd_hdd_sda1_dd-_TN74961-dead-94134858>
                           143360 ..c -rwxrwxrwx 0        0        94134856 <unknowndcfldd_hdd_sda1_dd-_TL74961-dead-94134856>
                           586860 ..c -rwxrwxrwx 0        0        94134831 <unknowndcfldd_hdd_sda1_dd-_FW.CHM-dead-94134831>
                             5120 ..c -rwxrwxrwx 0        0        94134829 <unknowndcfldd_hdd_sda1_dd-_LSXPAND.DLL-dead-94134829>
                             5120 ..c -rwxrwxrwx 0        0        94134859 <unknowndcfldd_hdd_sda1_dd-_TO74961-dead-94134859>
                            77824 ..c -rwxrwxrwx 0        0        94134825 <unknowndcfldd_hdd_sda1_dd-_PD.EXE-dead-94134825>
Mon Jan 19 1931 08:42:12  2235610 ..c -rwxrwxrwx 0        0        94134833 <unknowndcfldd_hdd_sda1_dd-_ICENSE.PDF-dead-94134833>
                          2235610 ..c -rwxrwxrwx 0        0        94134864 <unknowndcfldd_hdd_sda1_dd-_TR74961-dead-94134864>
Mon Feb 16 1931 17:31:44     5120 .a. -rwxrwxrwx 0        0        94134859 <unknowndcfldd_hdd_sda1_dd-_TO74961-dead-94134859>
                           159744 .a. -rwxrwxrwx 0        0        94134854 <unknowndcfldd_hdd_sda1_dd-_TJ74961-dead-94134854>
                           106496 .a. -rwxrwxrwx 0        0        94134853 <unknowndcfldd_hdd_sda1_dd-_TI74961-dead-94134853>
                            58368 .a. -rwxrwxrwx 0        0        94134858 <unknowndcfldd_hdd_sda1_dd-_TN74961-dead-94134858>
                           258100 .a. -rwxrwxrwx 0        0        94134849 <unknowndcfldd_hdd_sda1_dd-_TE74961-dead-94134849>
                           208896 .a. -rwxrwxrwx 0        0        94134839 <unknowndcfldd_hdd_sda1_dd-_TA74961-dead-94134839>
                            42634 .a. -rwxrwxrwx 0        0        94134863 <unknowndcfldd_hdd_sda1_dd-_TQ74961-dead-94134863>
```

As can be seen above the time line revealed some very confusing data, especially given the assumption that the system was not used after 15 Jul 2004 when the windows swap file was last accessed. Although, the clock was believed to be inaccurate (being out by approximately 27 days and 62 minutes), some MACs claimed creating and access dates in the 1930s! This may be attributable to meta data being corrupt as few computers will allow their clock to be set so far in the past.

Ignoring the 1930s data, the last entry is `the c:\scandisk.log` which has a time stamp of 22nd August 2004 11:55 and 16 seconds. An examination of the log itself reveals the entry which matches the timestamp. Interestingly though, the `scandisk.log` file was created on 2nd Feb 2004 – the believed built date for the OS., however, the first scan recorded is on 11th Aug 2004 (and this was cancelled) only indicating a developing problem that required more and more attention from the user. Below is a summary of the `scandisk.log` file that has had the extra carriage returns removed and where a scan revealed no problem the text was removed.

Item 43 – Summary of the scandisk.log for the system

```
******************
Microsoft ScanDisk for Windows
NOTE: If you use an MS-DOS program to view this file, some of the characters
may appear incorrectly. Use a Windows program such as Notepad instead.
Log file generated at 09:50 on 8/11/2004.
ScanDisk used the following options:
  Thorough test
  Automatically fix errors
Drive  (C:) contained the following errors:
ScanDisk was canceled.

------------------
Log file generated at 05:12PM on Tuesday, August 17, 2004.
ScanDisk checked drive C for problems, with the following results: Directory structure & File
system
Log file generated at 05:15PM on Tuesday, August 17, 2004.
ScanDisk checked drive C for problems, with the following results: File system
Log file generated at 05:44PM on Tuesday, August 17, 2004.
ScanDisk checked drive C for problems, with the following results:
Log file generated at 05:55PM on Tuesday, August 17, 2004.
ScanDisk checked drive C for problems, with the following results: File system
Log file generated at 08:23PM on Tuesday, August 17, 2004.
ScanDisk checked drive C for problems, with the following results: File system
Log file generated at 03:57PM on Thursday, August 19, 2004.
ScanDisk checked drive C for problems, with the following results: File system
Log file generated at 03:58PM on Thursday, August 19, 2004.
ScanDisk checked drive C for problems, with the following results:
Log file generated at 04:00PM on Thursday, August 19, 2004.
ScanDisk checked drive C for problems, with the following results:
Log file generated at 04:03PM on Thursday, August 19, 2004.
ScanDisk checked drive C for problems, with the following results:
Log file generated at 05:27PM on Thursday, August 19, 2004.
ScanDisk checked drive C for problems, with the following results: File system
Log file generated at 05:37PM on Thursday, August 19, 2004.
ScanDisk checked drive C for problems, with the following results:
Log file generated at 05:42PM on Thursday, August 19, 2004.
ScanDisk checked drive C for problems, with the following results: File system
Log file generated at 06:10PM on Thursday, August 19, 2004.
ScanDisk checked drive C for problems, with the following results:
Log file generated at 09:57PM on Thursday, August 19, 2004.
ScanDisk checked drive C for problems, with the following results:
Log file generated at 10:22PM on Thursday, August 19, 2004.
ScanDisk checked drive C for problems, with the following results: File system
Log file generated at 01:46PM on Friday, August 20, 2004.
ScanDisk checked drive C for problems, with the following results:
Log file generated at 01:48PM on Friday, August 20, 2004.
ScanDisk checked drive C for problems, with the following results: File system
Log file generated at 01:52PM on Friday, August 20, 2004.
ScanDisk checked drive C for problems, with the following results:
Log file generated at 01:58PM on Friday, August 20, 2004.
ScanDisk checked drive C for problems, with the following results:
Log file generated at 03:48PM on Friday, August 20, 2004.
ScanDisk checked drive C for problems, with the following results:
Log file generated at 05:08PM on Friday, August 20, 2004.
ScanDisk checked drive C for problems, with the following results: File system
Log file generated at 06:37AM on Saturday, August 21, 2004.
ScanDisk checked drive C for problems, with the following results:
Log file generated at 08:25AM on Sunday, August 22, 2004.
ScanDisk checked drive C for problems, with the following results: File system
Log file generated at 10:55AM on Sunday, August 22, 2004.
ScanDisk checked drive C for problems, with the following results:
```

What is apparent is that the first check was requested/required by either the user of the system (upon boot), on 11 Aug 2004 then over the next 11 days a further 23 scans were imitated. This would indicate a failing of either the physical disk, the operating system or the presence of some software that was causing the system to crash, whereupon reboot a scandisk would automatically be invoked (and conducted unless cancelled by the user).

Furthermore a look at the MAC of the `boot.log` reveals a stamp of 17 Aug 2004:

Item 44 – MAC for the boot.log

```
Tue Aug 17 2004 17:26:30    55277 m.. -/-r-xr-xr-x 0         0        5         c:\/BOOTLOG.TXT
```

This hints strongly of a system that is failing and was operational for the last time on 17 Aug 2004. This with the `scandisk.log` file (above) suggests the user would attempt to booth the system (generally in the evening) and allowing it to conduct several scans in an effort to correct whatever problem prevents normal system operation. The scans do not appear to correct the problem and user gives up after 3-5 attempts.

It is the assumption of the investigator that the user gives up on 22 August 2004, believing the disk to be corrupt elects to scrap the system some time over the next week.

Why did the system fail?

Given the fact that the investigator was able to image the hard disk without any problems, it is surmised that the errors on the disk were software related. With this in mind the investigator looked for recent software installations that may have corrupted the logical integrity of the operating system on the hard disk.

Large numbers of files downloaded with a peer-2-peer software; there are traces of 4 such programs:

a. `Kazaa Lite`[21] <http://www.kazaalite.nl/en> (`c:\Program` Files)

b. `Kazaa Lite K++`[22] <http://www.kl-kpp.net/> (`c:\Program Files`)

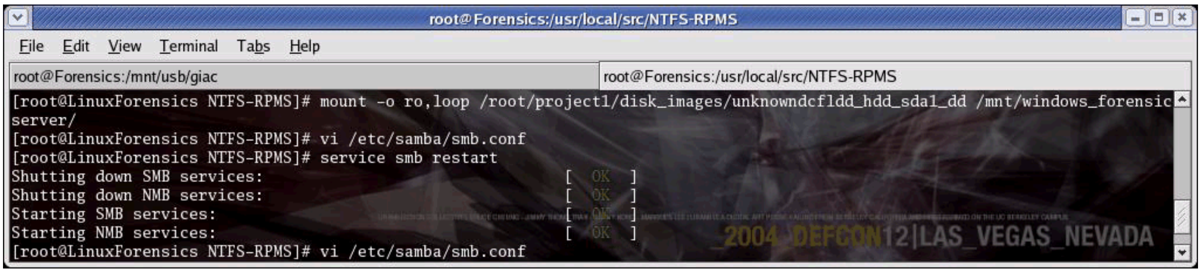
c. `Grokster`[23] <http://www.grokster.com> (`c:\Program` Files)

d. `MorpheusUltra`[24] <http://www.morpheusultra.com> (`c:\softwrap`)

Peer-2-peer software is a classic method of catching viruses, downloading Trojans and other Malware or Spyware.

In order that a Windows Spyware and Antivirus program could be loaded and run against the image, it was necessary to mount the `dd` image on a `samba` shared folder and to sweep the files remotely. First the `mount` command was used to mount the image onto the `/mnt/windows_forensic_server` directory which `samba` had been configured serve via Windows SMB file sharing protocol. Access was restricted to a the sole Windows system to be used to conduct further analysis. Although the image file itself is read only, the mount point is also defined as being read only.

Item 45 – Mounting the Image in Read Only mode[25]

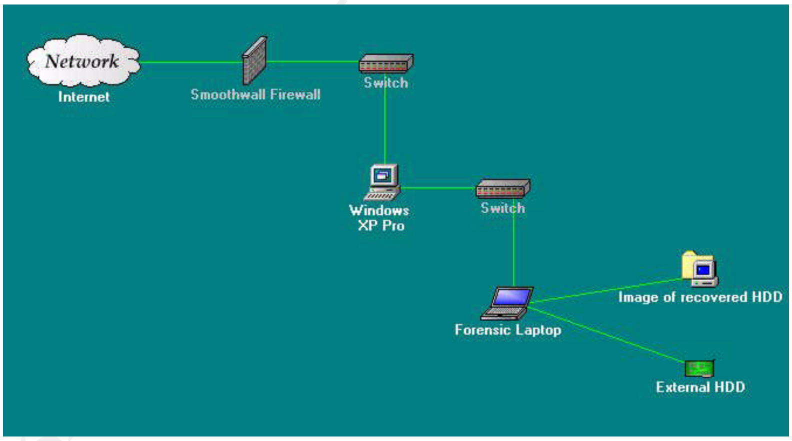

root@Forensics:/usr/local/src/NTFS-RPMS
File Edit View Terminal Tabs Help
root@Forensics:/mnt/usb/giac
root@Forensics:/usr/local/src/NTFS-RPMS

```
[root@LinuxForensics NTFS-RPMS]# mount -o ro,loop /root/project1/disk_images/unknowndcfldd_hdd_sda1_dd /mnt/windows_forensic
server/
[root@LinuxForensics NTFS-RPMS]# vi /etc/samba/smb.conf
[root@LinuxForensics NTFS-RPMS]# service smb restart
Shutting down SMB services:                                [  OK  ]
Shutting down NMB services:                                [  OK  ]
Starting SMB services:                                     [  OK  ]
Starting NMB services:                                     [  OK  ]
[root@LinuxForensics NTFS-RPMS]# vi /etc/samba/smb.conf
```

The set up was as follows:

The Laptop applied `samba` share level permissions to the Administrator of the Windows XP desktop. This intern was connected via a separate network card with a different address to a switch. The switch allowed access to the Green Interface on the `Smoothwall`[26] <www.smoothwall.org> Internet Firewall. The internet connection was enabled on the XP Pro system when an item required researching on the Internet, otherwise it was disabled. To reach the image from the internet, an attacker would be required to defeat the `Smoothwall` Firewall, identify the internal NATed address range, defeat the Norton Personal Firewall installed on the XP Pro system, enable IP Forwarding or install Windows Internet Connection Sharing (ICS), identify the IP Address of the Linux system and defeat the OS firewall installed. Therefore the investigator considered the read only samba shared data to reasonably safe – although as mentioned the connection to the Internet was limited and tightly controlled.

Item 46 – Diagram of the Network used[27]



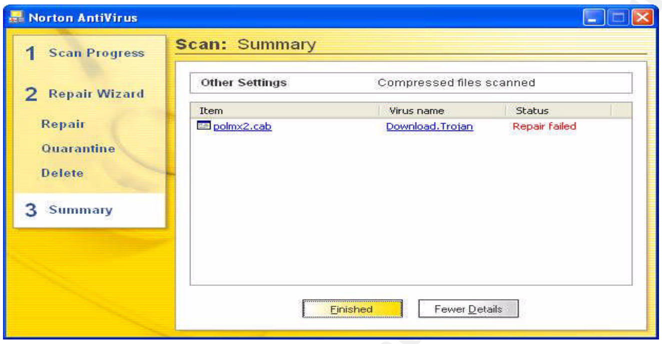
The purpose of the samba share was to allow the use of windows based tools (with which the investigator was more familiar). Upon connecting to the read only network share, a complete copy of the contents was taken to a temporary directory `E:\GIAC SANS TEMP\`. This was in case any of the Trojan hunting software tried to remove or alter the data. Although the data was safe, AntiVirus and Anti Malware software have a bad habit of freezing when they attempted to delete data that was prohibited by more than the system's own file permissions. Note as standard practice, all products were updated moments before being used on the target image.

AntiVirus, Trojan and Malware Scans

The investigator recognised that the fact that only complete files were visible and that any viruses etc held in slack or unused space would not be found by searching through samba shared data, he believed there would be sufficient to be going on, furthermore, a full slack and deleted file search would be conducted on the host Linux system.

The first a Virus Scan was performed using Norton Anti Virus a good produce that the investigator is familiar with, it is configurable and it will detect Trojans, Viruses, Worms and {as we will see only some} Malware. On this occasion it revealed one virus called '`polmx2.cab`' which it classed as a Trojan.

Item 47 – Norton Anti Virus Discovered Trojan



Scan: Summary

Other Settings Compressed files scanned

Item	Virus name	Status
polmx2.cab	Download.Trojan	Repair failed

A check of the complete timeline revealed the Trojan was created on the disk and modified on the times shown below:

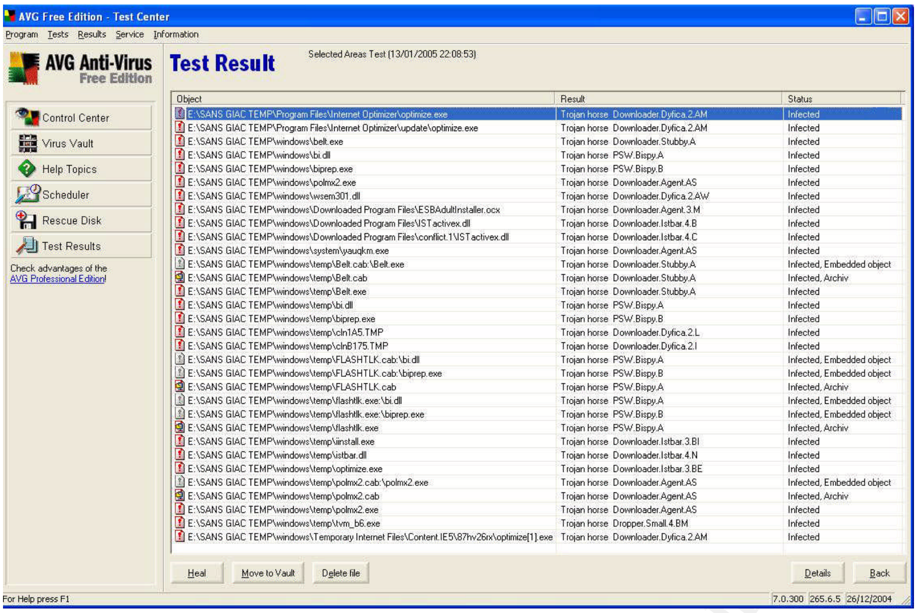
Item 48 – Creation and modification MACs for 'POLMX2.CAB' Trojan

```
Fri Jun 18 2004 16:09:22  42036 ..c -/-rwxrwxrwx 0  0    1188717  c:\/WINDOWS/TEMP/polmx2.cab (POLMX2.CAB)
Fri Jun 18 2004 16:09:26    357 ..c -/-rwxrwxrwx 0  0    1188723  c:\/WINDOWS/TEMP/polmx2.inf (POLMX2.INF)
                          37888 ..c -/-rwxrwxrwx 0  0    1188729  c:\/WINDOWS/TEMP/polmx2.exe (POLMX2.EXE)
```

```
Tue Jun 22 2004 00:00:00  42036 .a. -/-rwxrwxrwx 0  0    1188717  c:\/WINDOWS/TEMP/polmx2.cab (POLMX2.CAB)
                            357 .a. -/-rwxrwxrwx 0  0    1903505  c:\/WINDOWS/INF/POLMX2.INF
                           4096 .a. d/drwxrwxrwx 0  0    26855989 c:\/MYDOCU~1/2003_0~1/New Folder
(NEWFOL~1)
                            357 .a. -/-rwxrwxrwx 0  0    1188723  c:\/WINDOWS/TEMP/polmx2.inf (POLMX2.INF)
                          37888 .a. -/-rwxrwxrwx 0  0    3223257  c:\/WINDOWS/POLMX2.EXE
                           4096 .a. d/drwxrwxrwx 0  0   26855991 c:\/MYDOCU~1/2003_0~1/New
Folder(1)(NEWFOL~2)
                          37888 .a. -/-rwxrwxrwx 0  0    1188729  c:\/WINDOWS/TEMP/polmx2.exe (POLMX2.EXE)
```

The second Virus scan (its always a good idea to do at least two), was performed by the Free AVG Antivirus[28] tool <http://www.grisoft.com> this revealed a significantly larger number, 32! Although this may be because of the overlap in what AVG, Norton and Spyware Doctor[29] all scan for.

Item 49 – AVG Scan Results



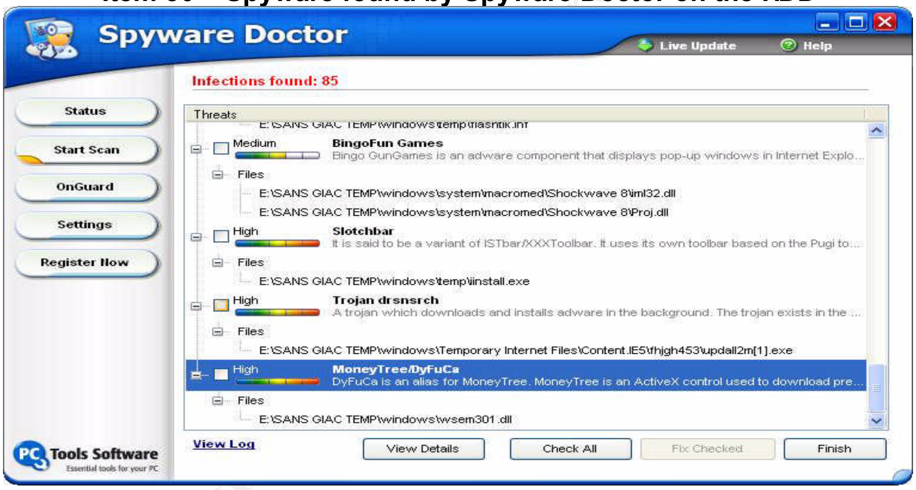
Test Result

Selected Areas Test (13/01/2005 22:08:53)

Object	Result	Status
E:\SANS GIAC TEMP\Program Files\Internet Optimizer\optimize.exe	Trojan horse Downloader.Dyfica.2.AM	Infected
E:\SANS GIAC TEMP\Program Files\Internet Optimizer\update\optimize.exe	Trojan horse Downloader.Dyfica.2.AM	Infected
E:\SANS GIAC TEMP\windows\belt.exe	Trojan horse Downloader.Stubby.A	Infected
E:\SANS GIAC TEMP\windows\bi.dll	Trojan horse PSW.Bispy.A	Infected
E:\SANS GIAC TEMP\windows\biprep.exe	Trojan horse PSW.Bispy.B	Infected
E:\SANS GIAC TEMP\windows\polmx2.exe	Trojan horse Downloader.Agent.AS	Infected
E:\SANS GIAC TEMP\windows\wsem301.dll	Trojan horse Downloader.Dyfica.2.AW	Infected
E:\SANS GIAC TEMP\windows\Downloaded Program Files\ESBAdultInstaller.ocx	Trojan horse Downloader.Agent.3.M	Infected
E:\SANS GIAC TEMP\windows\Downloaded Program Files\ISTactivex.dll	Trojan horse Downloader.Istbar.4.B	Infected
E:\SANS GIAC TEMP\windows\Downloaded Program Files\conflict.1\ISTactivex.dll	Trojan horse Downloader.Istbar.4.C	Infected
E:\SANS GIAC TEMP\windows\system\yauqkm.exe	Trojan horse Downloader.Agent.AS	Infected
E:\SANS GIAC TEMP\windows\temp\Belt.cab:\Belt.exe	Trojan horse Downloader.Stubby.A	Infected, Embedded object
E:\SANS GIAC TEMP\windows\temp\Belt.cab	Trojan horse Downloader.Stubby.A	Infected, Archiv
E:\SANS GIAC TEMP\windows\temp\Belt.exe	Trojan horse Downloader.Stubby.A	Infected
E:\SANS GIAC TEMP\windows\temp\bi.dll	Trojan horse PSW.Bispy.A	Infected
E:\SANS GIAC TEMP\windows\temp\biprep.exe	Trojan horse PSW.Bispy.B	Infected
E:\SANS GIAC TEMP\windows\temp\cln1A5.TMP	Trojan horse Downloader.Dyfica.2.L	Infected
E:\SANS GIAC TEMP\windows\temp\clnB175.TMP	Trojan horse Downloader.Dyfica.2.I	Infected
E:\SANS GIAC TEMP\windows\temp\FLASHTLK.cab:\bi.dll	Trojan horse PSW.Bispy.A	Infected, Embedded object
E:\SANS GIAC TEMP\windows\temp\FLASHTLK.cab:\biprep.exe	Trojan horse PSW.Bispy.B	Infected, Embedded object
E:\SANS GIAC TEMP\windows\temp\FLASHTLK.cab	Trojan horse PSW.Bispy.A	Infected, Archiv
E:\SANS GIAC TEMP\windows\temp\flashtlk.exe:\bi.dll	Trojan horse PSW.Bispy.A	Infected, Embedded object
E:\SANS GIAC TEMP\windows\temp\flashtlk.exe:\biprep.exe	Trojan horse PSW.Bispy.B	Infected, Embedded object
E:\SANS GIAC TEMP\windows\temp\flashtlk.exe	Trojan horse PSW.Bispy.A	Infected, Archiv
E:\SANS GIAC TEMP\windows\temp\iinstall.exe	Trojan horse Downloader.Istbar.3.BI	Infected
E:\SANS GIAC TEMP\windows\temp\istbar.dll	Trojan horse Downloader.Istbar.4.N	Infected
E:\SANS GIAC TEMP\windows\temp\optimize.exe	Trojan horse Downloader.Istbar.3.BE	Infected
E:\SANS GIAC TEMP\windows\temp\polmx2.cab:\polmx2.exe	Trojan horse Downloader.Agent.AS	Infected, Embedded object
E:\SANS GIAC TEMP\windows\temp\polmx2.cab	Trojan horse Downloader.Agent.AS	Infected, Archiv
E:\SANS GIAC TEMP\windows\temp\polmx2.exe	Trojan horse Downloader.Agent.AS	Infected
E:\SANS GIAC TEMP\windows\temp\tvm_b6.exe	Trojan horse Dropper.Small.4.BM	Infected
E:\SANS GIAC TEMP\windows\Temporary Internet Files\Content.IE5\87hv26rx\optimize[1].exe	Trojan horse Downloader.Dyfica.2.AM	Infected

Next up was a scan for Spyware, this was conducted using the PCtools Spyware Doctor (www.pctools.com/spyware-doctor). If the Norton result was bad, the Spyware doctor result was horrendous, as it discovered 85 instances of Spyware or Trojans.

Item 50 – Spyware found by Spyware Doctor on the HDD



Infections found: 85

Threats

```
E:\SANS GIAC TEMP\windows\temp\flashtlk.inf
□ Medium    BingoFun Games
            Bingo GunGames is an adware component that displays pop-up windows in Internet Explo...
  Files
    E:\SANS GIAC TEMP\windows\system\macromed\Shockwave 8\iml32.dll
    E:\SANS GIAC TEMP\windows\system\macromed\Shockwave 8\Proj.dll
□ High      Slotchbar
            It is said to be a variant of ISTbar/XXXToolbar. It uses its own toolbar based on the Pugi to...
  Files
    E:\SANS GIAC TEMP\windows\temp\iinstall.exe
□ High      Trojan drsnsrch
            A trojan which downloads and installs adware in the background. The trojan exists in the ...
  Files
    E:\SANS GIAC TEMP\windows\Temporary Internet Files\Content.IE5\fhjgh453\updall2m[1].exe
□ High      MoneyTree/DyFuCa
            DyFuCa is an alias for MoneyTree. MoneyTree is an ActiveX control used to download pre...
  Files
    E:\SANS GIAC TEMP\windows\wsem301.dll
```

Given the number of items discovered, it is the believed that either:

The user became aware of the number of item of Spyware to the point where they took action and removed something critical.

Or

The system simply failed under then number of malicious item of software running.

Or both, in that the system caused so many problems that the user took action and the software used caused the system to fail by either removing an infected file that was critical to the OS or by failing to install itself properly and corrupting the system partition in the process.

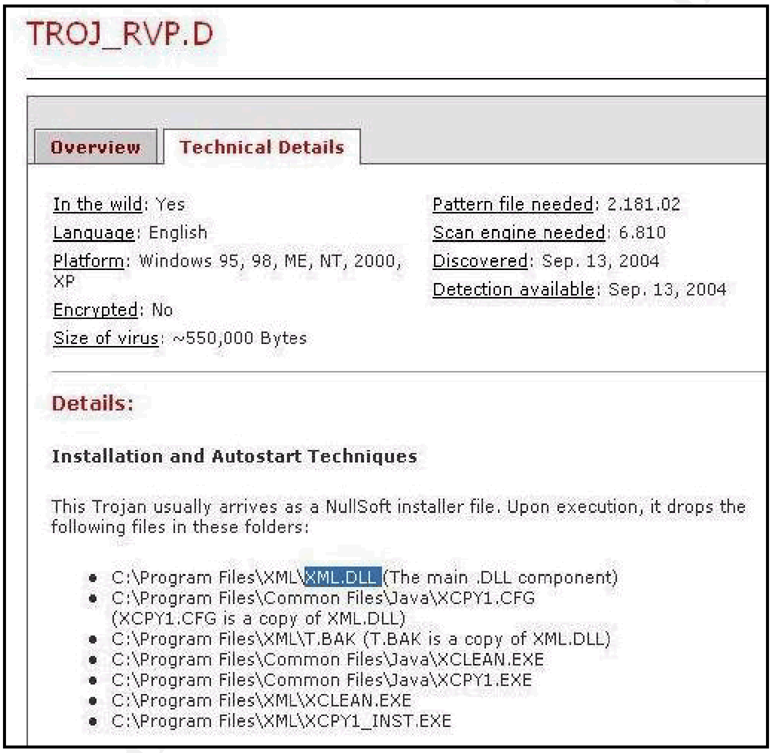
An examination of the time line in the last few days gives some hint as which it these is the case. Some items have been highlighted in the next portion of the time line:

The red indicate the presence of a malicious file or Trojan.

The blue indicate the presence of a defensive tool.

The Trojan installed is call (by Trendmicro.com) `TROJ_RVP.d` and the screen shot shows the files it installs, all of which can be seen in the time line.

Item 51 – TrendMicro details on TROJ_RVP.D Trojan[30]



TROJ_RVP.D

Overview | Technical Details

In the wild: Yes

Language: English

Platform: Windows 95, 98, ME, NT, 2000, XP

Encrypted: No

Size of virus: ~550,000 Bytes

Pattern file needed: 2.181.02

Scan engine needed: 6.810

Discovered: Sep. 13, 2004

Detection available: Sep. 13, 2004

Details:

Installation and Autostart Techniques

This Trojan usually arrives as a NullSoft installer file. Upon execution, it drops the following files in these folders:

- C:\Program Files\XML\XML.DLL (The main .DLL component)
- C:\Program Files\Common Files\Java\XCPY1.CFG (XCPY1.CFG is a copy of XML.DLL)
- C:\Program Files\XML\T.BAK (T.BAK is a copy of XML.DLL)
- C:\Program Files\Common Files\Java\XCLEAN.EXE
- C:\Program Files\Common Files\Java\XCPY1.EXE
- C:\Program Files\XML\XCLEAN.EXE
- C:\Program Files\XML\XCPY1_INST.EXE

The time line shows that just 5 minutes later the user attempted to install a defensive piece of software in the form of 'Spyblocker' from <www.spyblocker-software.com> , this can be seen from the time line entries coloured blue, that relate to the installation and modification of 6 files, as referred to in the installation report on the company's web site[31]:

Item 52 – Installation report for Sypblocker

```
http://www.spyblocker-software.com/spyblocker/instrpt.htm

Installation Report: GP-Install
Generated by InCtrl5, version 1.0.0.0
Install program: C:\trysb\spyblock.exe
3/22/2002 12:34 AM

<cut for brevity>

Files changed: 6
c:\dialer\PACKET.DAT
Old date: 3/22/2002 12:26 AM
New date: 3/22/2002 12:33 AM
Old size: 111 bytes
New size: 117 bytes
c:\WINDOWS\GPInstall.exe
Old date: 1/1/2002 12:39 PM
New date: 3/22/2002 12:27 AM
Old size: 796,672 bytes
New size: 796,672 bytes
c:\WINDOWS\POWERPNT.INI
Old date: 3/19/2002 12:02 PM
New date: 3/22/2002 12:28 AM
Old size: 60 bytes
New size: 60 bytes
c:\WINDOWS\SYSTEM.INI
Old date: 3/19/2002 5:14 PM
New date: 3/22/2002 12:28 AM
Old size: 2,206 bytes
New size: 2,206 bytes
c:\WINDOWS\WAVEMIX.INI
Old date: 3/19/2002 12:02 PM
New date: 3/22/2002 12:28 AM
Old size: 54 bytes
New size: 54 bytes
c:\WINDOWS\APPLOG\APPLOG.ind
Old date: 3/22/2002 12:20 AM
New date: 3/22/2002 12:27 AM
Old size: 10,151 bytes
New size: 10,215 bytes
```

However, the install does not go well and the installation process is not completed, as the next files modified are boot process ones suggesting that the install crashes the system, possible through conflict with any one of a number of Trojans.

```
Tue Aug 17 2004 17:10:40   634912 m.. -/---x--x--x 0        0        3223244   c:\/WINDOWS/USER.DAT
Tue Aug 17 2004 17:16:08       54 ..c -/-rwxrwxrwx 0        0        3222895   c:\/WINDOWS/WAVEMIX.INI
                             2151 ..c -/-rwxrwxrwx 0        0        3222851   c:\/WINDOWS/SYSTEM.INI
                               60 ..c -/-rwxrwxrwx 0        0        3222898   c:\/WINDOWS/POWERPNT.INI
Tue Aug 17 2004 17:16:10       54 m.. -/-rwxrwxrwx 0        0        3222895   c:\/WINDOWS/WAVEMIX.INI
                               60 m.. -/-rwxrwxrwx 0        0        3222898   c:\/WINDOWS/POWERPNT.INI
Tue Aug 17 2004 17:16:38    56886 m.. -/-r-xr-xr-x 0        0        28        c:\/BOOTLOG.PRV
                              108 m.. -/-r-xr-xr-x 0        0        3223082   c:\/WINDOWS/ttfCache
(TTFCACHE)
Tue Aug 17 2004 17:26:30    55277 m.. -/-r-xr-xr-x 0        0        5         c:\/BOOTLOG.TXT
```

From this point on the time line becomes corrupt and few entries are clear or logical. As seen from the `scandisk.log` file earlier the system now starts the sequence of what will become 23 scandisk checks that will fail to fix the problem and the system appears to never boot correctly again.

The reb dotted line indicates a point after which the disk records become so garbled that they fail to make any sense. The investigator believes the exhaustive number of scandisk operations conducted sequentially; on 2 occasions there are four scans running back to back as one sequence for four takes 12 minutes and the other 6 minutes! And as to how the system created the 1930's entries remain a mystery to this day, but is currently put down to hard disk corruption.

Item 53 – Last few days activity

```
Tue Aug 17 2004 17:08:26        6 m.. -/-r-xr-xr-x 0        0        3636869  c:\/WINDOWS/TASKS/SA.DAT
                            32711 m.. -/-rwxrwxrwx 0        0        3223057  c:\/WINDOWS/SchedLog.Txt (SCHEDLOG.TXT)
Tue Aug 17 2004 17:08:32  1429974 ..c -/-rwxrwxrwx 0        0        2630625  c:\/WINDOWS/SYSBCKUP/rb005.cab (RB005.CAB)
                          1429974 ..c -/-rwxrwxrwx 0        0        2630553  c:\/WINDOWS/SYSBCKUP/rbtemp.cab (_BTEMP.CAB) (deleted)
                          1429974 ..c   -rwxrwxrwx 0        0        2630553  <unknowndcfldd_hdd_sda1_dd-_BTEMP.CAB-dead-2630553>
Tue Aug 17 2004 17:08:40  1429974 m..   -rwxrwxrwx 0        0        2630553  <unknowndcfldd_hdd_sda1_dd-_BTEMP.CAB-dead-2630553>
                          1429974 m.. -/-rwxrwxrwx 0        0        2630625  c:\/WINDOWS/SYSBCKUP/rb005.cab (RB005.CAB)
                          1429974 m.. -/-rwxrwxrwx 0        0        2630553  c:\/WINDOWS/SYSBCKUP/rbtemp.cab (_BTEMP.CAB) (deleted)
Tue Aug 17 2004 17:08:42      474 ..c -/-rwxrwxrwx 0        0        3636880  c:\/WINDOWS/TASKS/Windows Critical Update Notification.job
(WINDOW~1.JOB)
Tue Aug 17 2004 17:08:44      474 m.. -/-rwxrwxrwx 0        0        3636880  c:\/WINDOWS/TASKS/Windows Critical Update Notification.job
(WINDOW~1.JOB)
Tue Aug 17 2004 17:08:46  5799936 m.. -/-rwxrwxrwx 0        0        4107654  c:\/WINDOWS/TEMPOR~1/CONTENT.IE5/index.dat (INDEX.DAT)
                            81920 m.. -/-rwxrwxrwx 0        0        1387398  c:\/WINDOWS/COOKIES/index.dat (INDEX.DAT)
                           491520 m.. -/-rwxrwxrwx 0        0        25391366 c:\/WINDOWS/HISTORY/HISTORY.IE5/index.dat (INDEX.DAT)
Tue Aug 17 2004 17:08:56        2 ..c -/-rwxrwxrwx 0        0        49381539 c:\/WINDOWS/TEMPOR~1/CONTENT.IE5/KPQTU5GV/xaupdate[1].htm
(XAUPDA~1.HTM)
Tue Aug 17 2004 17:08:58    46472 m.. -/-rwxrwxrwx 0        0        26286982 c:\/PROGRA~1/INTERN~2/UPDATE/optimize.exe (OPTIMIZE.EXE)
                            46472 m.. -/-rwxrwxrwx 0        0        25421702 c:\/PROGRA~1/INTERN~2/optimize.exe (OPTIMIZE.EXE)
                            46472 ..c -/-rwxrwxrwx 0        0        30378801 c:\/WINDOWS/TEMPOR~1/CONTENT.IE5/87HV26RX/optimize[1].exe
(OPTIMI~1.EXE)
                               10 ..c -/-rwxrwxrwx 0        0        28408224 c:\/WINDOWS/TEMPOR~1/CONTENT.IE5/Y90FEDM5/xaupdate[1].htm
(XAUPDA~1.HTM)
                                2 m.. -/-rwxrwxrwx 0        0        49381539 c:\/WINDOWS/TEMPOR~1/CONTENT.IE5/KPQTU5GV/xaupdate[1].htm
(XAUPDA~1.HTM)
Tue Aug 17 2004 17:09:00    46472 m.. -/-rwxrwxrwx 0        0        30378801 c:\/WINDOWS/TEMPOR~1/CONTENT.IE5/87HV26RX/optimize[1].exe
(OPTIMI~1.EXE)
                               10 m.. -/-rwxrwxrwx 0        0        28408224 c:\/WINDOWS/TEMPOR~1/CONTENT.IE5/Y90FEDM5/xaupdate[1].htm
(XAUPDA~1.HTM)
Tue Aug 17 2004 17:09:04  4845004 ..c -/-rwxrwxrwx 0        0        30360210 c:\/PROGRA~1/ZANGO/zango_kyf.dat.tmp (_ANGO_~1.TMP) (deleted)
                          4845004 ..c   -rwxrwxrwx 0        0        30360210 <unknowndcfldd_hdd_sda1_dd-_ANGO_~1.TMP-dead-30360210>
                               61 ..c -/-rwxrwxrwx 0        0        3223262  c:\/WINDOWS/wininit.ini (WININIT.BAK)
                           259198 ..c -/-rwxrwxrwx 0        0        1188827  c:\/WINDOWS/TEMP/ft22s.exe (FT22S.EXE)
                          4845004 ..c -/-rwxrwxrwx 0        0        30360207 c:\/PROGRA~1/ZANGO/zango_kyf.dat (ZANGO_~1.DAT)
Tue Aug 17 2004 17:09:06       61 m.. -/-rwxrwxrwx 0        0        3223262  c:\/WINDOWS/wininit.ini (WININIT.BAK)
Tue Aug 17 2004 17:09:08  4845004 m.. -/-rwxrwxrwx 0        0        30360210 c:\/PROGRA~1/ZANGO/zango_kyf.dat.tmp (_ANGO_~1.TMP) (deleted)
                          4845004 m..   -rwxrwxrwx 0        0        30360210 <unknowndcfldd_hdd_sda1_dd-_ANGO_~1.TMP-dead-30360210>
                          4845004 m.. -/-rwxrwxrwx 0        0        30360207 c:\/PROGRA~1/ZANGO/zango_kyf.dat (ZANGO_~1.DAT)
Tue Aug 17 2004 17:09:14   259198 m.. -/-rwxrwxrwx 0        0        1188827  c:\/WINDOWS/TEMP/ft22s.exe (FT22S.EXE)
                           307200 ..c -/-rwxrwxrwx 0        0        25422734 c:\/PROGRA~1/COMMON~1/JAVA/Xcpy1.cfg (XCPY1.CFG)
                             4096 ..c d/drwxrwxrwx 0        0        3147613  c:\/PROGRA~1/XML
Tue Aug 17 2004 17:09:16   307200 ..c -/-rwxrwxrwx 0        0        49471629 c:\/PROGRA~1/XML/XML.dll (XML.DLL)
                             4096 m.. d/drwxrwxrwx 0        0        3147613  c:\/PROGRA~1/XML
                             7233 m.. -/-rwxrwxrwx 0        0        3222792  c:\/WINDOWS/WIN.INI
Tue Aug 17 2004 17:09:44    70144 ..c -/-rwxrwxrwx 0        0        44392170 c:\/WINDOWS/TEMPOR~1/CONTENT.IE5/FHJGH453/updall2m[1].exe
(UPDALL~1.EXE)
Tue Aug 17 2004 17:09:46     7904 m.. -/-rwxrwxrwx 0        0        2704134  c:\/WINDOWS/APPLOG/APPLOG.ind (APPLOG.IND)
                            70144 m.. -/-rwxrwxrwx 0        0        44392170 c:\/WINDOWS/TEMPOR~1/CONTENT.IE5/FHJGH453/updall2m[1].exe
(UPDALL~1.EXE)
Tue Aug 17 2004 17:09:48        0 ..c -/-rwxrwxrwx 0        0        1188846  c:\/WINDOWS/TEMP/t9312.TMP (_9312.TMP) (deleted)
                                0 ..c   -rwxrwxrwx 0        0        1188831  <unknowndcfldd_hdd_sda1_dd-_9311.TMP-dead-1188831>
                                0 ..c   -rwxrwxrwx 0        0        1188846  <unknowndcfldd_hdd_sda1_dd-_9312.TMP-dead-1188846>
                                0 ..c -/-rwxrwxrwx 0        0        1188831  c:\/WINDOWS/TEMP/t9311.TMP (_9311.TMP) (deleted)
Tue Aug 17 2004 17:09:50        0 m..   -rwxrwxrwx 0        0        1188831  <unknowndcfldd_hdd_sda1_dd-_9311.TMP-dead-1188831>
                                0 m..   -rwxrwxrwx 0        0        1188846  <unknowndcfldd_hdd_sda1_dd-_9312.TMP-dead-1188846>
```

System ownership and why this happened

Having identified why the system was abandoned, the investigator turned his attention to the other information that could be obtained from the system as to its usage, the owner and the type of use the system was put to. Note this aspect of the report is heavily sanitised.

The first and main point of call when examining a windows system is the registry. The registry in Windows 98 was quit embryonic when compared to the likes of Windows XP, with its separate user logons, separate data storage area and even separate software installs and permissions. When Microsoft was designing Windows 98 they assumed the person sat in front of the system was authorised to see and access all data. In modern IT Security terms it was a dedicated operating system. As a result there is no ability to discern the particular users at any set time other than by their actual activity and behaviour. There is no logon security on Windows 98, the login process it simply for network shares and to prevent other users seeing each others desktops (laughable as there was no file security from preventing them from navigating to the files and desktop directory once 'logged on'.

User activity on this system is split into several areas:

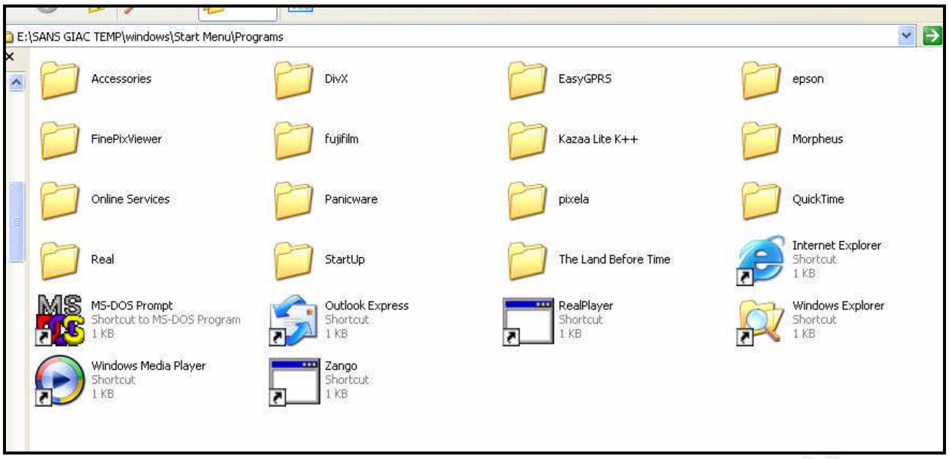
a. General Family type stuff – saving and printing digital pictures.
b. Playing computer games – 'Worms', 'The Land before time' and 'Totally Spies' (free from UK McDonalds during summer 2004)
c. Using an instant messenger (zango)
d. Watching films/DVDs (generally using the bundled bespoke software).
e. Downloading files from peer-to-peer networks (pornography in the form of avi and mpg files – the peek being 186mb on one day)

The user was relatively new to computing and did not really understand much of what was going on. For example:

a. Many of the default and unnecessary icons were still on the desktop.
b. Many of the Spyware programs conducted a social engineering attack and the user seems to have been duped into installing them. A classic example being the Internet Optimizer itself a browser hijacker[32] (see <http://www.2-spyware.com/browser-hijackers-removal>
c. The fact that they were connected to the internet via broadband and using peer-to-peer software without either a personal firewall or AntiVirus protection.

By the 8th August 2004 they appear to have become annoyed with the popups their Spyware was generating and they installed popup stopper. But given the number of items of Spyware and the fact that many had been legitimately installed (having duped the user), this had little chance of stopping the problem, furthermore, they were only treating the symptoms and not the cause.

Item 54 – The common user menu



Machine identification

Looking at the `[HKEY_Local_MACHINE]` keys can reveal numerous parts of the machines history, although on this occasion, the IP address is not recorded as it is allocated on boot and Windows 98 had a notoriously flaky TCP/IP stack.

Item 55 – IP Information from the Registry

```
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\NetTrans\000
0]
"DriverDesc"="TCP/IP"
"InfSection"="MSTCP.ndi"
"IPAddress"="0.0.0.0"
"IPMask"="0.0.0.0"
"DeviceVxDs"="vtdi.386,vip.386,vtcp.386,vdhcp.386,vnbt.386"
"InstallVnbt"="0"
"InfPath"="NETTRANS.INF"
"ProviderName"="Microsoft"
"DriverDate"=" 4-23-1999"
"DevLoader"="*ndis"
"NodeType"="1"
```

As was outlined earlier, the fact that the OS does not distinguish between users means the likes of a types url list has little value, to the assessment but again does shed light on the user's activities:

Item 56 – URLs Typed into Internet Explorer

```
[HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\TypedURLs]
"url1"="Dial-Up Networking"
"url2"="http://www.hotmail.com/"
"url3"="http://www.udate.com/"
"url4"="http://www.bbc.co.uk"
"url5"="www.udate.com"
"url6"="http://www.nyrrc.org/"
"url7"="http://www.thetrainline.com/"
"url8"="http://www.trainline.com/"
"url9"="www.hotmail.com"
"url10"="http://www.bbc.co.uk/"
"url11"="http://www.cokemusic.com/"
"url12"="http://www.spele.nl"
"url13"="www.cokeumsic.com"
"url14"="http://www.ziplip.com/"
"url15"="http://www.lloydstsb.com/"
"url16"="http://www.mg-rover.co.uk/"
"url17"="http://www.yahoo.co.uk/"
"url18"="http://www.mgrover.co.uk/"
"url19"="http://www.amazon.co.uk/"
"url20"="http://www.play.com/"
"url21"=http://www.zonelabs.com/”
```

The only points that jump out from the above list are that the investigator hopes the user didn’t use this system for online banking with Lloydstsb as several of the Spyware and Trojans installed were capable of keystroke logging. And it is a shame they didn’t stop longer at the Zonelabs site, even the free personal firewall would have been useful.

The last command execute key in the registry can be useful if the user has actually ruin some commands, but in this point and click age, few do. In this the key only points to the ‘Worms Blast’ game that used to be installed.

Item 57 – Last Command Executed

```
[HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
]
"a"="\"C:\\WINDOWS\\Desktop\\Worms Blast.lnk\"\\1"
"MRUList"="a"
```

The Windows Media Player was the default player for wma and avi files, there was a separate player installed for DivX files. The XXXX is where a pornographic file name was removed by the investigator. Notice where these files came from, their source directory would indicate they were downloaded via the peer-to-peer file sharing program Grokster (http://www.grokster.com/).

Item 58 – Windows Media Player recent file list

```
[HKEY_USERS\.DEFAULT\Software\Microsoft\MediaPlayer\Player\RecentFileList]
"File0"="C:\\Program Files\\Grokster\\My Shared Folder\\Sam Cooke - Stand By Me
(Original).mp3"
"File1"="C:\\Program Files\\Grokster\\My Shared Folder\\Elvis Presley - I Did It My Way.mp3"
"File2"="C:\\Program Files\\Grokster\\My Shared Folder\\XXXX.mpg"
"File3"="C:\\Program Files\\Grokster\\My Shared Folder\\XXXX.wmv"
"File4"="C:\\Program Files\\Grokster\\My Shared Folder\\XXXX.wmv"
"File5"="C:\\Program Files\\Grokster\\My Shared Folder\\XXXX.asf"
"File6"="C:\\Program Files\\Grokster\\My Shared Folder\\XXXX.mpg"
"File7"="C:\\Program Files\\Grokster\\My Shared Folder\\XXXX.wmv"
"File8"="C:\\Program Files\\Grokster\\My Shared Folder\\XXXX.wmv"
```

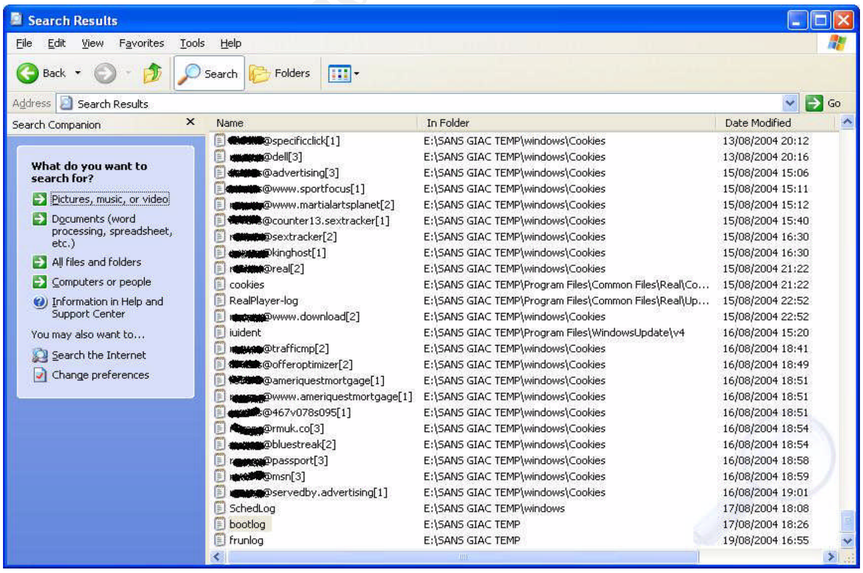
The username was initially hard to identify as the user did not use the bundled Microsoft email client – outlook express. Instead they used the instant messenger software installed. However, the registry came up trumps as the user completed a registration process. (The exact name has been removed under the GIAC conditions).

Item 59 – Identifying the Username

```
[HKEY_USERS\.DEFAULT\Software\Ahead\Nero - Burning ROM\Info]
"Company"=""
"Serial5"="1502-4240-1125-0482-1088-9784"
"User"="GIAC-REMOVED"

[HKEY_LOCAL_MACHINE\Network\Logon]
"username"=" GIAC-REMOVED "
"PrimaryProvider"="Microsoft Family Logon"

[HKEY_USERS\.DEFAULT\Software\Macromedia\Shockwave\registration\lastname
]
@=" GIAC-REMOVED "
```

If that hadn't worked the cookies were the next stop. Oh and notice the dell cookie on the 13 August 2004, it connects (time wise) to some images in the Internet Explorer History directory they show Dell 2400 desktop system[33] – wonder if the user was getting frustrated with their slow and dated operating system that was creaking under all the additional program running. These were drawn together in a search for all text files, as the investigator looked for logs etc, notice again how the numbers of log files and other text files modified and created comes to a grinding halt in 2 days.

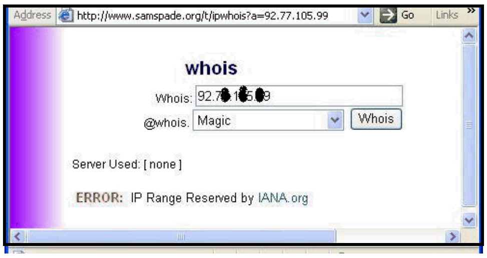
Item 60 – Text files and Cookies found


Search Results
File Edit View Favorites Tools Help
Back
Search
Folders
Address Search Results
Go
Search Companion
What do you want to search for?
Pictures, music, or video
Documents (word processing, spreadsheet, etc.)
All files and folders
Computers or people
Information in Help and Support Center
You may also want to...
Search the Internet
Change preferences

Name	In Folder	Date Modified
[redacted]@specificclick[1]	E:\SANS GIAC TEMP\windows\Cookies	13/08/2004 20:12
[redacted]@dell[3]	E:\SANS GIAC TEMP\windows\Cookies	13/08/2004 20:16
[redacted]@advertising[3]	E:\SANS GIAC TEMP\windows\Cookies	15/08/2004 15:06
[redacted]@www.sportfocus[1]	E:\SANS GIAC TEMP\windows\Cookies	15/08/2004 15:11
[redacted]@www.martialartsplanet[2]	E:\SANS GIAC TEMP\windows\Cookies	15/08/2004 15:12
[redacted]@counter13.sextracker[1]	E:\SANS GIAC TEMP\windows\Cookies	15/08/2004 15:40
[redacted]@sextracker[2]	E:\SANS GIAC TEMP\windows\Cookies	15/08/2004 16:30
[redacted]@kinghost[1]	E:\SANS GIAC TEMP\windows\Cookies	15/08/2004 16:30
[redacted]@real[2]	E:\SANS GIAC TEMP\windows\Cookies	15/08/2004 21:22
cookies	E:\SANS GIAC TEMP\Program Files\Common Files\Real\Co...	15/08/2004 21:22
RealPlayer-log	E:\SANS GIAC TEMP\Program Files\Common Files\Real\Up...	15/08/2004 22:52
[redacted]@www.download[2]	E:\SANS GIAC TEMP\windows\Cookies	15/08/2004 22:52
iuident	E:\SANS GIAC TEMP\Program Files\WindowsUpdate\v4	16/08/2004 15:20
[redacted]@trafficmp[2]	E:\SANS GIAC TEMP\windows\Cookies	16/08/2004 18:41
[redacted]@offeroptimizer[2]	E:\SANS GIAC TEMP\windows\Cookies	16/08/2004 18:49
[redacted]@ameriquestmortgage[1]	E:\SANS GIAC TEMP\windows\Cookies	16/08/2004 18:51
[redacted]@www.ameriquestmortgage[1]	E:\SANS GIAC TEMP\windows\Cookies	16/08/2004 18:51
[redacted]@467v078s095[1]	E:\SANS GIAC TEMP\windows\Cookies	16/08/2004 18:51
[redacted]@rmuk.co[3]	E:\SANS GIAC TEMP\windows\Cookies	16/08/2004 18:54
[redacted]@bluestreak[2]	E:\SANS GIAC TEMP\windows\Cookies	16/08/2004 18:54
[redacted]@passport[3]	E:\SANS GIAC TEMP\windows\Cookies	16/08/2004 18:58
[redacted]@msn[3]	E:\SANS GIAC TEMP\windows\Cookies	16/08/2004 18:59
[redacted]@servedby.advertising[1]	E:\SANS GIAC TEMP\windows\Cookies	16/08/2004 19:01
SchedLog	E:\SANS GIAC TEMP\windows	17/08/2004 18:08
bootlog	E:\SANS GIAC TEMP	17/08/2004 18:26
frunlog	E:\SANS GIAC TEMP	19/08/2004 16:55

There was only one IP address found in on the system in the live area, that of (the X's are for GIAC rules compliance) IP: 92.7X.1X5.X9, and this was drawn from a GPRS software log. However, research on the internet revealed it to have been a restricted range indicating it to have been internal to the provider. It is been partially removed as internal addresses of this kind are generally unique to the user and/or provider.

Item 61 – Attempting to locate the IP Address[34]



http://www.samspade.org/t/ipwhois?a=92.77.105.99

whois

Whois: 92.7[redacted]1[redacted]5[redacted]9

@whois. Magic

Server Used: [none]

ERROR: IP Range Reserved by IANA.org

Legal issues

The question as to whether the use conducted any illegal activity can be a difficult one to answer as it can depend on many things. The pornography for example is explicit but as to its breach of the Obscene Publications Act 1959 & 64 (OPA) the investigator turned to the Internet Watch Foundation <www.ifw.org.uk> for advice. On their site the OPA is defined as:

Item 62 – Quote from the Internet Watch Foundation[35]

> **<u>Obscene Publications Act 1959 & 1964</u>**
>
> The law on obscene publications is difficult to define in everyday terms.
> As a guide it could include images featuring acts of extreme sexual activity such as bestiality, necrophilia, rape or torture.
>
> This act makes it an offence to publish, whether for gain or not, any article whose effect, taken as a whole, is such, in the view of the court, to tend to "deprave and corrupt" those likely to read, see or hear the matter contained or embodied in it.
>
> <http://www.iwf.org.uk/police/page.22.38.htm>

Although the names of the pornography video files did include on several occasions the words rape, the belief is that many are either 'staged' or simply advertising tricks to increase hits. Note – this was professional advice obtained by the investigator from persons employed in these types of investigations. Apparently, this is a common renaming trick used by site owners to increase the size of their libraries and to maintain customer interest. Detailed analysis of these files was **not** performed.

There were also 30 music files and music videos, mainly of Elvis. They type and quality of these indicates they were originally released by one of the major recording labels. Their presence on the hard disk itself in not sufficient to prove they were illegally obtained however, they are in two locations:

```
C:\My Shared
```

```
C:\Program Files\Grokster\My Shared Folder
```

With online music purchasing increasing exponentially in the UK, the user may have an external device or other system where they legally acquire the files. However, it is the belief of the investigator that given the other files in these folders (ie pornography) which are unlikely to be 'purchased' these music videos were also downloaded via the peer-to-peer software especially as there were 4 different types of peer-to-peer applications.

Therefore, a breach of the recording labels licence's and IPR has occurred. However, this is currently a topical subject both in the USA and Europe with USA based companies using USA legislation against non US citizens outside the US and as such, the acceptable levels and applicability of these laws and procedures have yet to be determined.

Unused, slack and unallocated space searches

By searching the unallocated parts of the disk, the following information was obtained (the process is described but all detail is excluded under GIAC rules :

Telephone number: By searching for the area code of the city where the refuse facility is located a 1337 entries were found, these piped into `more` were scanned visually in 30 seconds and the partial number was then used as the basis for another search, this time revealing the complete number.

House Number, postal address and post code: Right next to one of the telephone numbers cashed from a web form.

Main user's name: Nero Registration and confirmed by the 1300+ other instances in cookies, text files, logs and web cache.

Email address: Easy when you have a name, search for the it near an '`@`'.

Other contacts know by main user: Several in Outlook Express identity files (`C;\windows\Application Data\Identities\{7D345F00-5592-11D8-B270-90928CAF6A4C}\Microsoft\Outlook Express`)

Summary of events and supposition by the investigator

The following is the summary of the events; the system was built in February 2004, with Windows 98 OSR2. It was used mainly by one individual, probably male who occasionally allowed others to access games or the internet. The user was not security orientated or particularly computer literate as much of the problem stemmed from the lack of basic internet security devices ie a Firewall and AntiVirus (although from this investigation not even Norton could have helped him). The user elected to install several 'free' internet accelerators and dubious software touting to be popup stoppers etc.

The installation of several peer-to-peer program facilitated the increase in downloaded software of dubious sources and the volume of pornography installed on the system hints to broadband being installed – there is a reference to NTL broadband medic in the unallocated space but much of this data is corrupt. The user seems to have become aware of the Spyware as a popup blocker is installed and a few weeks later the installation of Spyware-blocker is seemingly started, however possibly due to so many files being infected and corrupted or hardware failure, the system crashed during the install and despite attempts over several days the system is never again operational.

It was noted that the user had considered purchasing a new machine as several references to Dell <www.dell.co.uk> were seen in the cache and the Internet Explorer history points to the commencement or at least pricing of a Dell Dimension 2400.

When the system finally fails to boot on 22 August 2004 the user makes the decision to dispose of it. They remove the memory and, judging by the software and media players installed (one from X-Men2 and Nero Burning ROM), a DVDR/CDRW 51/2" device (see the images at the start). Then either believing that no data can be recovered or not knowing about data forensics, the case is then dumped at the local refuse facility, where the investigator spots it the next day.

Conclusions and points learnt

The failure of the hard disk – either its hardware or its logical structure did present significant problems for the forensic investigator. Furthermore, using a system obtained in this manner was a risk, as the disk may have been completely clean, well maintained ie with little meat for the report or loaded with child pornography or images of that nature. The last of these could have resulted in both the loss of not only the subject material but also the seizure of all equipment used by the investigator to the point where the content was discovered.

As it was, the system proved to be a even more of a challenge than originally expected as the numerous items of Malware, the failing structure and 23 scandisk executions all added to the tangled web of corrupt data and misleading facts. The fact that the BIOS clock was significantly out of sync with GMT also didn't help.

This system was an easy target for Malware and viruses as it had everything going for it; no antivirus software, no firewall, numerous peer-to-peer applications and several browser hijacking programs (and an uneducated user). The system lasted just under 9 months but given the sites and user activity it did well to last that long, especially as much of the problem was user installed under a social engineering attack aimed to trick them to thinking they would fit their problems.

Personal Statement:

I was honestly saddened by the death of this system, a strange but true comment. I believe that over the course of the investigation I have gotten to know this system well, as I discovered its habits and foibles. The process of investigating the reason for its disposal was an interesting journey that had me slowly piece the gruesome facts about the demise of this operating system. I was horrified when I approached the time line entries for 17 August 2004 as they pointed to the scandisk logs that in simple black and white showed how the system had not managed to reboot and correct itself despite numerous attempts – like watching someone drowning I suppose. Ironically, the fatal blow seems to have come from a piece of software designed to remove and protect the system from the numerous items of Spyware and Trojans that it housed.

Review of Investigation Objectives

Number	System Objectives – (Identify)	Comments	Completed
S1	Operating System		Yes
S2	Current OS		Yes
S3	Previous OS	HDD Errors prevented any meaningful data being extracted	No
S4	Last booted / shutdown (date and time)	Several versions obtained, almost depends on what is called a boot and what makes a shutdown	Yes
Number	**User Objectives – (Identify)**	**Comments**	**Completed**
U1	The common and or last user	Not printed in this report	Yes
U2	Owner (physical and email addresses)	Not printed in this report	Yes (not included in this report)
U3	IP Address of the last user	Static IP not printed in clear in this report	Yes
U4	General User activity		Yes
Number	**Hidden software Objectives**	**Comments**	**Completed**
H1	Locate and identify any Viruses	Numerous identified with several scans using different products	Yes
H2	Locate and identify any Spyware		Yes
H3	Locate and identify any Malware		Yes
H4	Locate and identify any Trojans		Yes
Number	**Legal Objectives**	**Comments**	**Completed**
L1	Identify any illegal activity	Some pornography of dubious subjects. None (thankfully) child orientated	Yes
L2	Identify any illegal software	Some pirated wma and avi files	Yes

End of Part 2

Table of Items (tables, command outputs and screen captures)

References

(In the order in which they appear in the document)

[1] "GIAC Certified Forensics Analyst (GCFA)" GIAC Web Site – Individual Subject Certifications SANS 12 Jan 2005 <http://www.giac.org/subject_certs.php#gcfa>

[2] "Fedora Core 2" Open Source Operating System. Operating System used for the forensics workstation. 12 Jan 05 <http://fedora.redhat.com/>

[3] "Autopsy Forensic Browser Overview" Sleuth Kit Web Site. 12 Jan 2005 <http://www.sleuthkit.org/autopsy/>

[4] "The Sleuth Kit Overview" The Sleuth Kit Web Site. 12 Jan 2005 <http://www.sleuthkit.org/sleuthkit/index.php>

[5] "Microsoft XP Professional" Windows XP Operating System. Microsoft 12 Jan 2005 <http://www.microsoft.com/windowsxp/pro/evaluation/default.mspx>

[6] "Norton AntiVirus" Norton Anti Virus Software 12 Jan 2005 <http://www.symantec.com/nav/nav_9xnt/>

[7] "The Coroners Tool Kit" The Coroners Tool Kit Web Site. Forensic software written by Dan Farmer and Wietse Venema 12 Jan 2005 <http://www.porcupine.org/forensics/tct.html>

[8] "Overview of Fsum" Fast Data Integrity Checker. SlavaSoft Inc Web site. 12 Jan 2005 <http://www.slavasoft.com/fsum/overview.htm >

[9] "Camouflage Home Page" Hide Your Files. 12 Jan 2005 <http://camouflage.unfiction.com/>

[10] “WinZip” The Zip file utility for Windows. WinZip Computing 12 Jan 2005 <http://www.winzip.com>

[11] “Microsoft Access” A Powerful Database Solution. Microsoft 12 Jan 2005 <http://office.microsoft.com/en-gb/FX010857911033.aspx>

[12] “Overview of Camouflage” Camouflage – Hide Your Files. 12 Jan 2005 <http://camouflage.unfiction.com/Overview.html>

[13] “Search Orders” Power of Officials to Enter Your Home – The Liberty guide to]Human Rights. 12 Jan 2005 <http://www.yourrights.org.uk/your-rights/chapters/the-right-to-privacy/power-of-officials-to-enter-your-home/search_orders.shtml>

[14] Home Page for EPICPC. The main Web site of the company that trade under the name ‘EPIC Computers’ . 12 Jan 2005 < www.epicpc.co.uk>

[15] “[PATCH] USB storage: patch for unusual_devs.h” Summary of changes from v2.6.0 to v2.6.1. Author <Alexander<at>all-2.com> published by LinuxHQ.com 5 Jul 2004 / 12 Jan 2005 <http://www.linuxhq.com/kernel/changelog/v2.6/1/>

[16] “NTFS Documentation – Chapter 3 Linux and NTFS” NTFS FAQ. The Linux-NTFS Project Team 12 Jan 2005 <http://linux-ntfs.sourceforge.net/info/ntfs.html#3.0>

[17] “Sections 1 – 6 of Theft Act 1968 Explained” Theft Act 1968. A production of the UK Theft Act 1968 (online version not available from HM Government source) Poole: The Bournemouth and Poole College. 12 Jan 2005 <http://www.sixthform.info/law/01_modules/mod5/14_1_theft.htm>.

[18] “The Linux command ‘dfcldd’” Written by the Defense Computer Forensics Lab 12 Jan 2005 <http://www.dcfl.gov/dcfl/dcfl.htm> available from <http://sourceforge.net/project/showfiles.php?group_id=46038>

[19] “Boot Sectors on MBR Disks” XP Resource Kit – Troubleshooting. Microsoft. 12 Jan 2005 <http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/Default.asp?url=/resources/documentation/Windows/XP/all/reskit/en-us/prkd_tro_ilxl.asp>.

[20] “Windows 98” Windows 98 Operating System. Microsoft 12 Jan 2005 <http://www.microsoft.com/windows98/default.asp>

[21] “Kazaa Lite” Music and Movis Download Site. Parent Company: MP3 Diamond/IPC Solution 12 Jan 2005 <http://www.kazaalite.nl/en/>

[22] “Kazaa Lite K++” Music and Movis Download Site. Parent Company: K-Litetk/IPC Solution 12 Jan 2005 <http://www.kl-kpp.net/>

[23] "Grokster" Next Generation File Sharing. Grokster Web Site. 12 Jan 2005 <http://www.grokster.com/>

[24] "MorpheusUltra" Peer to Peer file Sharing. MorpheusUltra Web site. 12 Jan 2005 <http://www.morpheusultra.com>

[25] "dc-12-buranii dinvid-1-lg.jpg" by [uranii]invid. Submitted Artwork for Defcon 12. Seen as the desktop background in Item 35 and 45. Published by Defcon.org 12 Jan 2005 <http://www.defcon.org/html/defcon-12/dc-12-art/dc-12-art-8.html>

[26] "Smoothwall Firewall" The Smoothwall Open Source Project. The Smoothwall Project Team 12 Jan 2005 <http://www.smoothwall.org>

[27] "Friendly Net Viewer General Info" Friendly Net Viewer Product Information. A.Kilevich & Co 12 Jan 2005 <http://www.kilievich.com/fviewer/>
(used to make the image)

[28] "Free AVG Virus Scanner" The AVG Free Edition. 12 Jan 2005 < http://free.grisoft.com/freeweb.php/doc/2/>

[29] "Spyware Doctor" PC Tools Software Web Site PC Tools 12 Jan 2005 <http://www.pctools.com/spyware-doctor>

[30] "Technical Details for TROJ_RVP.D" Virus Encyclopaedia. TrendMicro 12 Jan 2005 <http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_RVP.D>

[31] "Installation Report" Product Information. Spyblocker-software 12 Jan 2005 < http://www.spyblocker-software.com/spyblocker/instrpt.htm>

[32] "Browser Hijacker Description" How to remove Browser Hijackers parasites from computer? 12 Jan 2005 <http://www.2-spyware.com/browser-hijackers-removal>.

[33] Dell Computer Corporation Web Site. Dell Computer Corporation 12 Jan 2005 <http://www1.euro.dell.com/content/products/features .aspx/dimen_2400?c=uk&cs=ukdhs1&l=en&s=dhs>

[34] "The Online Sam Spade Tools" Sam Spade Web Site. 12 Jan 2005 <http://www.samspade.org> (tool used to obtain information and pictured)

[35] "Obscene Publications Act 1959 & 1964" The Laws. Internet Watch Foundation. 12
Jan 2005 <http://www.iwf.org.uk/police/page.22.38.htm>