Fight crime. Unravel incidents... one byte at a time.

Interested in learning more?
Check out the list of upcoming events offering "Advanced Incident Response, Threat Hunting, and Digital Forensics (FOR508) at http://digital-forensics.sans.orghttp://digital-forensics.sans.org/events/
Table of Contents

Stephen_Armstrong_GCFA.doc
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**

**Report on the Forensic Analysis of a recovered Floppy Disk**

- Background
- The Forensic Workstation
- Backing up the disk
- AntiVirus Scan of the disk image
- Creation of the Working Copy
- The Initial Analysis
- Working with Autopsy
- Creating a File Activity Timeline

**Detailed Analysis**

- Camouflage
- Passwords
- File Timings Explained

**What Happened (Investigators Opinion)**

- The Software found and possibly used by Leszczynski

**Post Incident Activities**

**Legal position**

**IT Forensic Analysis of an abandoned computer and its Hard Disk**

- Background
- Legal Implications of using the abandoned computer
- Basic Analysis
- Investigation Objectives

**Detailed Analysis**

- Why did the system fail?
- AntiVirus, Trojan and Malware Scans
- System ownership and why this happened
- Legal issues
- Summary of events and supposition by the investigator

**Conclusions and points learnt**
Abstract

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

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:

<table>
<thead>
<tr>
<th>Item 1 – Identification details for recovered Floppy Disk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Serial Number of item:</td>
</tr>
<tr>
<td>MD5 Hash of Disk</td>
</tr>
</tbody>
</table>

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 OS³, complete (ie the everything option checked during the installation process) and Autopsy³ v1.7 and The Sleuth Kit⁴ v 1.72 installed.

1 x 30 gb Windows XP Pro⁵ (complete build) with Norton AntiVirus 2003⁶ (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’ (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:

<table>
<thead>
<tr>
<th>Item 2 – Label details for the Master Working Disk (image)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>File name of image</strong></td>
</tr>
<tr>
<td><strong>MD5 Hash of image v1_5.gz</strong></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Item 3 – file (Linux) Command Output of v1_5.gz</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command</strong></td>
</tr>
</tbody>
</table>

5 of 57
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Md5 v1_5.gz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output</td>
<td>d7641eb4da871d980adbe4d371eda2ad</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>fsum -md5 v1_5.gz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output</td>
<td>; SlavaSoft Optimizing Checksum Utility fsum 2.0 &lt;www.slavasoft.com&gt; ; ; Generated on 11/09/04 at 21:09:08 ; d7641eb4da871d980adbe4d371eda2ad *v1_5.gz</td>
</tr>
</tbody>
</table>

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

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 from the Master Working. At every stage MD5 Sums were taken and compared to the sum

6 of 57
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 \([\text{chmod} \ 444 \ v1\_5\_gz]\) 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: “\_index.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**

![Screenshot of Autopsy output](image)

**Item 8 – Autopsy output of visible file on target disk**

![Autopsy output screenshot](image)
<table>
<thead>
<tr>
<th>Command</th>
<th>Autopsy output of md5 request on visible files</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output</td>
<td>MD5 Values for files in v1_5.gz</td>
</tr>
<tr>
<td></td>
<td>99c5dec518b142bd945e8d7d2fad2004 Information_Sensitivity_Policy.doc (INFORM~1.DOC)</td>
</tr>
<tr>
<td></td>
<td>e0c43ef38884662f5f27d93098c6c607 Internal_LaB_Security_Policy1.doc (INTERN~1.DOC)</td>
</tr>
<tr>
<td></td>
<td>b938727211ae846b60487fbc01b336 Internal_LaB_Security_Policy.doc (INTERN~2.DOC)</td>
</tr>
<tr>
<td></td>
<td>ac34c617?ebca4d41f0e181be1bc Password_Policy.doc (PASSWO~1.DOC)</td>
</tr>
<tr>
<td></td>
<td>Sb38d1ac1f94285db2d224d28fd07e8 Remote_Access_Policy.doc (REMOTE~1.DOC)</td>
</tr>
<tr>
<td></td>
<td>f785bald99888e68f45dabedd8b4541 Acceptable_Encryption_Policy.doc (ACCEPT~1.DOC)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Size</th>
<th>Permissions</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sat Feb 03 2001 19:44:16</td>
<td>36864 m. -rwxrwxrwx 0 0 5</td>
<td>&lt;v1.5.gz-_AMSHELL.DLL-dead-5&gt;</td>
<td>deleted</td>
<td></td>
</tr>
<tr>
<td>Thu Apr 22 2004 16:31:06</td>
<td>33423 m. -rwxrwxrwx 0 0 17</td>
<td>a:/Internal_Lab_Security_Policy.doc (INTERN~2.DOC)</td>
<td>deleted</td>
<td></td>
</tr>
<tr>
<td>Fri Apr 23 2004 10:53:56</td>
<td>727 m. -rwxrwxrwx 0 0 28</td>
<td>a:/_ndex.htm (deleted)</td>
<td>deleted</td>
<td></td>
</tr>
<tr>
<td>Fri Apr 23 2004 11:54:32</td>
<td>215895 m. -rwxrwxrwx 0 0 23</td>
<td>a:/Remote_Access_Policy.doc (REMOTE~1.DOC)</td>
<td>deleted</td>
<td></td>
</tr>
<tr>
<td>Fri Apr 23 2004 11:55:26</td>
<td>307935 m. -rwxrwxrwx 0 0 20</td>
<td>a:/Password_Policy.doc (PASSWO~1.DOC)</td>
<td>deleted</td>
<td></td>
</tr>
<tr>
<td>Fri Apr 23 2004 14:10:50</td>
<td>22528 m. -rwxrwxrwx 0 0 27</td>
<td>a:/Acceptable_Encryption_Policy.doc (ACCEPT~1.DOC)</td>
<td>deleted</td>
<td></td>
</tr>
<tr>
<td>Fri Apr 23 2004 14:11:10</td>
<td>42496 m. -rwxrwxrwx 0 0 9</td>
<td>a:/Information_Sensitivity_Policy.doc (INFORM~1.DOC)</td>
<td>deleted</td>
<td></td>
</tr>
<tr>
<td>Mon Apr 26 2004 00:00:00</td>
<td>215895 .a. -rwxrwxrwx 0 0 23</td>
<td>a:/Remote_Access_Policy.doc (REMOTE~1.DOC)</td>
<td>deleted</td>
<td></td>
</tr>
<tr>
<td>Mon Apr 26 2004 09:46:18</td>
<td>36864 .c -rwxrwxrwx 0 0 5</td>
<td>&lt;v1.5.gz-_AMSHELL.DLL-dead-5&gt;</td>
<td>deleted</td>
<td></td>
</tr>
<tr>
<td>Mon Apr 26 2004 09:46:20</td>
<td>36864 .c -rwxrwxrwx 0 0 5</td>
<td>&lt;v1.5.gz-_AMSHELL.DLL-dead-5&gt;</td>
<td>deleted</td>
<td></td>
</tr>
<tr>
<td>Mon Apr 26 2004 09:46:22</td>
<td>32256 .c -rwxrwxrwx 0 0 9</td>
<td>a:/_ndex.htm (deleted)</td>
<td>deleted</td>
<td></td>
</tr>
<tr>
<td>Mon Apr 26 2004 09:46:24</td>
<td>32256 .c -rwxrwxrwx 0 0 13</td>
<td>a:/Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)</td>
<td>deleted</td>
<td></td>
</tr>
<tr>
<td>Mon Apr 26 2004 09:46:26</td>
<td>307935 .c -rwxrwxrwx 0 0 20</td>
<td>a:/Password_Policy.doc (PASSWO~1.DOC)</td>
<td>deleted</td>
<td></td>
</tr>
<tr>
<td>Mon Apr 26 2004 09:46:36</td>
<td>215895 .c -rwxrwxrwx 0 0 23</td>
<td>a:/Remote_Access_Policy.doc (REMOTE~1.DOC)</td>
<td>deleted</td>
<td></td>
</tr>
<tr>
<td>Mon Apr 26 2004 09:46:44</td>
<td>22528 .c -rwxrwxrwx 0 0 27</td>
<td>a:/Acceptable_Encryption_Policy.doc (ACCEPT~1.DOC)</td>
<td>deleted</td>
<td></td>
</tr>
<tr>
<td>Mon Apr 26 2004 09:47:36</td>
<td>727 .c -rwxrwxrwx 0 0 28</td>
<td>a:/_ndex.htm (deleted)</td>
<td>deleted</td>
<td></td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>File Name</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password_Policy.doc</td>
<td>A large file that outlined the password policy</td>
</tr>
<tr>
<td>Remote_Access_Policy.doc</td>
<td>A large file that outlined the remote access policy</td>
</tr>
<tr>
<td>Internal_Lab_Security_Policy.doc</td>
<td>A small file that outlined the internal lab policy</td>
</tr>
<tr>
<td>Information_Sensitivity_Policy.doc</td>
<td>A small file on the policy on Information sensitivity</td>
</tr>
<tr>
<td>Acceptable_Encryption_Policy.doc</td>
<td>A small file that outlined the Encryption policy</td>
</tr>
</tbody>
</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 _index.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> (pictured below).
Item 12 – Screenshot of the Camouflage Website

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

<table>
<thead>
<tr>
<th>Command</th>
<th>fsum -md5 Camou121.exe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output</td>
<td>; SlavaSoft Optimizing Checksum Utility fsum 2.0 &lt;www.slavasoft.com&gt; ; ; Generated on 11/28/04 at 22:00:14 ; c62b050117c2cba3518e5a734fedef1f *Camou121.exe</td>
</tr>
</tbody>
</table>

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 – WinZip10 (Windows) contents of Camou121.exe selfextracting zip file

11 of 57
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>dir camouflage &gt; dir_list_camouflage_folder.txt</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Output</strong></td>
<td><strong>Volume in drive F is STEVE_ARMS</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Volume Serial Number is 70A1-3272</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Directory of F:\GIAC\Camouflage</strong></td>
</tr>
<tr>
<td></td>
<td>16/11/2004 20:46 &lt;DIR&gt;</td>
</tr>
<tr>
<td></td>
<td>16/01/2004 20:46 &lt;DIR&gt;</td>
</tr>
<tr>
<td>29/03/2001 22:13</td>
<td>217,088 Camouflage.exe</td>
</tr>
<tr>
<td>03/02/2001 19:44</td>
<td>36,864 CamShell.dll</td>
</tr>
<tr>
<td>28/03/2001 19:50</td>
<td>11,649 Readme.text</td>
</tr>
<tr>
<td>08/11/2004 19:23</td>
<td>19,774 Uninst.isu</td>
</tr>
<tr>
<td></td>
<td>4 File(s) 285,375 bytes</td>
</tr>
<tr>
<td></td>
<td>2 Dir(s) 343,220,224 bytes free</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>fsum camouflage &gt; dir list camouflage folder.txt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output</td>
<td>; SlavaSoft Optimizing Checksum Utility fsum 2.0 &lt;www.slavasoft.com&gt; ; Generated on 12/07/04 at 13:30:39 ; 9f08258a80d578a0f1cc38fe4c2aebb5 *Camouflage.exe 4e986ab0909d2946bed868b5f896906f *CamShell.dll 0c25ad7792d555b6c8c37c77ce9e224 *Readme.txt 2902261874a65a2581f0a260fad6a9df *Uninst.isu</td>
</tr>
</tbody>
</table>

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

![Camouflage right click menu](image-url)
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:

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.
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 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

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

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 1\textsuperscript{st} Nov, access it on the 2\textsuperscript{nd} Nov, modify it on the 3\textsuperscript{rd} Nov and copy it onto separate media on the 4\textsuperscript{th}; when the MACs are viewed on the 5\textsuperscript{th} 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 4\textsuperscript{th} 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 not 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.

<p>| Item 24 – List of all files (inc those hidden) found of the floppy disk |</p>
<table>
<thead>
<tr>
<th>Serial</th>
<th>File name / description</th>
<th>Clear or hidden and by what</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Acceptable_Encryption_Policy.doc</td>
<td>Clear</td>
</tr>
<tr>
<td>2</td>
<td>Internal_Lab_Security_Policy1.doc</td>
<td>Clear</td>
</tr>
<tr>
<td>3</td>
<td>Internal_Lab_Security_Policy.doc</td>
<td>Clear</td>
</tr>
<tr>
<td>4</td>
<td>Information_Sensitivity_Policy.doc</td>
<td>Clear</td>
</tr>
<tr>
<td>5</td>
<td>Password_Policy.doc</td>
<td>Clear</td>
</tr>
<tr>
<td>5a</td>
<td>Hydrocarbon%20fuel%20cell%20page2.jpg</td>
<td>Hidden – Camouflage</td>
</tr>
<tr>
<td>5b</td>
<td>pem_fuelcell.gif</td>
<td>Hidden – Camouflage</td>
</tr>
<tr>
<td>5c</td>
<td>PEM-fuel-cell-large.jpg</td>
<td>Hidden – Camouflage</td>
</tr>
<tr>
<td>5d</td>
<td>Password_Policy.doc</td>
<td>Hidden – Camouflage</td>
</tr>
<tr>
<td>6</td>
<td>Remote_Access_Policy.doc</td>
<td>Clear</td>
</tr>
<tr>
<td>6a</td>
<td>CAT.mdb</td>
<td>Hidden – Camouflage</td>
</tr>
<tr>
<td>6b</td>
<td>Remote_Access_Policy.doc</td>
<td>Hidden – Camouflage</td>
</tr>
</tbody>
</table>

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:

"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**

![Screenshot of hashes not matching](image.png)

**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\(^\text{13}\) (formerly an ‘Anton Piller Order’ after the case of the same name), and search and seize 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 up to 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 than 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**

<table>
<thead>
<tr>
<th>3.3 Most Sensitive:</th>
<th>Trade secrets &amp; marketing, operational, personnel, financial, source code, &amp; technical information integral to the success of our company</th>
</tr>
</thead>
</table>

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 breached 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**

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

**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’ 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 dust 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

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 cheap £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

<table>
<thead>
<tr>
<th><a href="mailto:alexander@all-2.com">alexander@all-2.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>[PATCH] USB storage: patch for unusual_devs.h</td>
</tr>
</tbody>
</table>

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/](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.

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**

<table>
<thead>
<tr>
<th>Belonging to another</th>
</tr>
</thead>
<tbody>
<tr>
<td>(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).</td>
</tr>
</tbody>
</table>

Section 5 of the 1968 Theft Act

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:

```bash
#/ 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 be selected. Success was often being achieved within 2 guesses.

Once the correct directory was identified a *dcfldd* command was executed to image the whole drive.
Item 35 – Imaging in progress

The `dcfl-dd` command (written by the Defence Computer Forensics Laboratory as indicated by the 'dcfl' bit in the `dd` command) was used image processing 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 `dcfl-dd` 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:

```
Unknowndcfl-dd_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\(^9\) decoded the MSWIN4.1 as:

```
```

28 of 57

© SANS Institute 2005

© SANS Institute 2005
Author retains all rights.
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

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
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, it can be assumed that the OS was installed on 2\textsuperscript{nd} 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, \texttt{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\textsuperscript{20} installation.

**Item 40 – Windows version extracted from the shell**

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

<table>
<thead>
<tr>
<th>Number</th>
<th>System Objectives – (Identify)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>Operating System</td>
<td></td>
</tr>
<tr>
<td>S2</td>
<td>Current OS</td>
<td></td>
</tr>
<tr>
<td>S3</td>
<td>Previous OS if identifiable</td>
<td></td>
</tr>
<tr>
<td>S4</td>
<td>Last booted / shutdown (date and time)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number</th>
<th>User Objectives – (Identify)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>U1</td>
<td>The common and or last user</td>
<td></td>
</tr>
<tr>
<td>U2</td>
<td>Owner (physical and email addresses)</td>
<td>Not for print in this report</td>
</tr>
<tr>
<td>U3</td>
<td>IP Address of the last user</td>
<td>Static IP not inc in this report</td>
</tr>
<tr>
<td>U4</td>
<td>General User activity</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number</th>
<th>Hidden software Objectives</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1</td>
<td>Locate and identify any Viruses</td>
<td></td>
</tr>
<tr>
<td>H2</td>
<td>Locate and identify any Spyware</td>
<td></td>
</tr>
<tr>
<td>H3</td>
<td>Locate and identify any Malware</td>
<td></td>
</tr>
<tr>
<td>H4</td>
<td>Locate and identify any Trojans</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number</th>
<th>Legal Objectives</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>L1</td>
<td>Identify any illegal activity</td>
<td></td>
</tr>
<tr>
<td>L2</td>
<td>Identify any illegal software</td>
<td></td>
</tr>
</tbody>
</table>

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 dcfdiff hash output. 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**

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
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 metadata 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 timestamp of 22\textsuperscript{nd} 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 2\textsuperscript{nd} Feb 2004 – the believed built date for the OS, however, the first scan recorded is on 11\textsuperscript{th} 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.

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 03:57PM on Thursday, August 19, 2004.
ScanDisk checked drive C for problems, with the following results:
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:
ScanDisk checked drive C for problems, with the following results: File system
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:

<table>
<thead>
<tr>
<th>Item 44 – MAC for the boot.log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tue Aug 17 2004 17:26:30 55277 m.. -/-xr-xr-x 0 0 5 c:\BOOTLOG.TXT</td>
</tr>
</tbody>
</table>

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<sup>21</sup> <http://www.kazaalite.nl/en> (c:\Program Files)

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

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

d. MorpheusUltra<sup>24</sup> <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

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\textsuperscript{24} <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\textsuperscript{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

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>MAC</th>
<th>File Name</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fri Jun 18</td>
<td>16:09:22</td>
<td>42326</td>
<td>-rw-rw-rw-</td>
<td>0 1188717  c:\WINDOWS\TEMP\polmx2.cab (POLMX2.CAB)</td>
</tr>
<tr>
<td>Fri Jun 18</td>
<td>16:09:26</td>
<td>357</td>
<td>-rw-rw-rw-</td>
<td>0 1188723  c:\WINDOWS\TEMP\polmx2.inf (POLMX2.INF)</td>
</tr>
<tr>
<td>Tue Jun 22</td>
<td>00:00</td>
<td>37888</td>
<td>-rw-rw-rw-</td>
<td>0 1188729  c:\WINDOWS\TEMP\polmx2.exe (POLMX2.EXE)</td>
</tr>
</tbody>
</table>

The second Virus scan (its always a good idea to do at least two), was performed by the Free AVG Antivirus 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 all scan for.

Item 49 – AVG Scan Results
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

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**

![TROJ_RVP.D](image)

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:

**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

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.

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>User</th>
<th>Mode</th>
<th>Size</th>
<th>Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tue Aug 17 2004</td>
<td>17:10:40</td>
<td>m</td>
<td>x-x-x-x</td>
<td>3223244</td>
<td>c:\WINDOWS\USER.DAT</td>
</tr>
<tr>
<td>Tue Aug 17 2004</td>
<td>17:16:08</td>
<td>54</td>
<td>x-x-x-x</td>
<td>322295</td>
<td>c:\WINDOWS\WAVEMIX.INI</td>
</tr>
<tr>
<td>Tue Aug 17 2004</td>
<td>17:16:10</td>
<td>54</td>
<td>x-x-x-x</td>
<td>322295</td>
<td>c:\WINDOWS\WAVEMIX.INI</td>
</tr>
<tr>
<td>Tue Aug 17 2004</td>
<td>17:16:38</td>
<td>56886</td>
<td>x-x-x-x</td>
<td>28</td>
<td>c:\WINDOWS\POWERPNT.INI</td>
</tr>
<tr>
<td>(TTFCACHE)</td>
<td></td>
<td>55277</td>
<td>x-x-x-x</td>
<td>5</td>
<td>c:\WINDOWS\ttfCache</td>
</tr>
<tr>
<td>Tue Aug 17 2004</td>
<td>17:26:30</td>
<td>55277</td>
<td>x-x-x-x</td>
<td>323082</td>
<td>c:\WINDOWS\ttfCache</td>
</tr>
<tr>
<td>Tue Aug 17 2004</td>
<td>17:26:30</td>
<td>55277</td>
<td>x-x-x-x</td>
<td>5</td>
<td>c:\WINDOWS\ttfCache</td>
</tr>
</tbody>
</table>

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
<table>
<thead>
<tr>
<th>Time</th>
<th>Type</th>
<th>Permissions</th>
<th>Owner</th>
<th>Size</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tue Aug 17 2004 17:08:26</td>
<td>6 m..</td>
<td>-r-xr-xr-x</td>
<td>0</td>
<td>3636869</td>
<td>c:\WINDOWS\TASKS\SA.DAT</td>
</tr>
<tr>
<td>Tue Aug 17 2004 17:08:32</td>
<td>32711 m..</td>
<td>-rwxrwxrwx</td>
<td>0</td>
<td>3223057</td>
<td>c:\WINDOWS\SchedLog.Txt (SCHEDLOG.TXT)</td>
</tr>
<tr>
<td>Tue Aug 17 2004 17:08:40</td>
<td>1429974 c..</td>
<td>-rwxrwxrwx</td>
<td>0</td>
<td>2630625</td>
<td>c:\WINDOWS\SYSBCKUP\rb005.cab (RB005.CAB)</td>
</tr>
<tr>
<td>Tue Aug 17 2004 17:08:42</td>
<td>1429974 m..</td>
<td>-rwxrwxrwx</td>
<td>0</td>
<td>2630553</td>
<td>c:\WINDOWS\SYSBCKUP\rbtemp.cab (_BTEMP.CAB) (deleted)</td>
</tr>
<tr>
<td>Tue Aug 17 2004 17:08:44</td>
<td>1429974 c..</td>
<td>-rwxrwxrwx</td>
<td>0</td>
<td>2630553</td>
<td>&lt;unknown&gt; (deleted)</td>
</tr>
<tr>
<td>Tue Aug 17 2004 17:08:46</td>
<td>1429974 m..</td>
<td>-rwxrwxrwx</td>
<td>0</td>
<td>2630553</td>
<td>c:\WINDOWS\SYSBCKUP\rb005.cab (RB005.CAB)</td>
</tr>
<tr>
<td>Tue Aug 17 2004 17:08:48</td>
<td>1429974 c..</td>
<td>-rwxrwxrwx</td>
<td>0</td>
<td>2630553</td>
<td>&lt;unknown&gt; (deleted)</td>
</tr>
<tr>
<td>Tue Aug 17 2004 17:08:50</td>
<td>1429974 m..</td>
<td>-rwxrwxrwx</td>
<td>0</td>
<td>2630553</td>
<td>c:\WINDOWS\SYSBCKUP\rbtemp.cab (_BTEMP.CAB) (deleted)</td>
</tr>
<tr>
<td>Tue Aug 17 2004 17:17:03</td>
<td>1429974 c..</td>
<td>-rwxrwxrwx</td>
<td>0</td>
<td>2630553</td>
<td>&lt;unknown&gt; (deleted)</td>
</tr>
</tbody>
</table>

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46
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.
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 8\(^{th}\) 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]
"DriverDesc"="TCP/IP"
"InfSection"="MSTCP.ndi"
"IPAddress"="0.0.0.0"
"IPMask"="0.0.0.0"
"DeviceVxDs"="vtdi.386,vip.386,vtcp.386,vtcp.386,vtcp.386,vtcp.386,vtcp.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
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"
"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\Elvis Presley - I Did It My Way.mp3"
"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.wmv"
"File6"="C:\Program Files\Grokster\My Shared Folder\XXXX.wmv"
"File7"="C:\Program Files\Grokster\My Shared Folder\XXXX.wmv"
"File8"="C:\Program Files\Grokster\My Shared Folder\XXXX.wmv"
```

51 of 57
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 – 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**

There was only one IP address found 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**

![Image of command prompt]

**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**

<table>
<thead>
<tr>
<th>Obscene Publications Act 1959 &amp; 1964</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 &quot;deprave and corrupt&quot; those likely to read, see or hear the matter contained or embodied in it.</td>
</tr>
</tbody>
</table>

<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
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 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 DVDVR/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

<table>
<thead>
<tr>
<th>Number</th>
<th>System Objectives – (Identify)</th>
<th>Comments</th>
<th>Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>Operating System</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>S2</td>
<td>Current OS</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>S3</td>
<td>Previous OS</td>
<td>HDD Errors prevented any meaningful data being extracted</td>
<td>No</td>
</tr>
<tr>
<td>S4</td>
<td>Last booted / shutdown (date and time)</td>
<td>Several versions obtained, almost depends on what is called a boot and what makes a shutdown</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number</th>
<th>User Objectives – (Identify)</th>
<th>Comments</th>
<th>Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>U1</td>
<td>The common and or last user</td>
<td>Not printed in this report</td>
<td>Yes</td>
</tr>
<tr>
<td>U2</td>
<td>Owner (physical and email addresses)</td>
<td>Not printed in this report</td>
<td>Yes (not included in this report)</td>
</tr>
<tr>
<td>U3</td>
<td>IP Address of the last user</td>
<td>Static IP not printed in clear in this report</td>
<td>Yes</td>
</tr>
<tr>
<td>U4</td>
<td>General User activity</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number</th>
<th>Hidden software Objectives</th>
<th>Comments</th>
<th>Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1</td>
<td>Locate and identify any Viruses</td>
<td>Numerous identified with several scans using different products</td>
<td>Yes</td>
</tr>
<tr>
<td>H2</td>
<td>Locate and identify any Spyware</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>H3</td>
<td>Locate and identify any Malware</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>H4</td>
<td>Locate and identify any Trojans</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number</th>
<th>Legal Objectives</th>
<th>Comments</th>
<th>Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>L1</td>
<td>Identify any illegal activity</td>
<td>Some pornography of dubious subjects. None (thankfully) child orientated</td>
<td>Yes</td>
</tr>
<tr>
<td>L2</td>
<td>Identify any illegal software</td>
<td>Some pirated wma and avi files</td>
<td>Yes</td>
</tr>
</tbody>
</table>

End of Part 2
**Table of Items (tables, command outputs and screen captures)**

| Item 1 | Identification details for recovered Floppy Disk |
| Item 2 | Label details for the Master Working Disk (image) |
| Item 3 | file (Linux) Command Output of v1_5.gz |
| Item 4 | md5 (Linux) Command Output of v1_5.gz |
| Item 5 | fsum (Windows) Command Output of v1_5.gz |
| Item 6 | Screenshot of Norton AV (Windows) Completing Scan of v1_5.gz |
| Item 7 | Initial file browsing with Autopsy |
| Item 8 | Autopsy output of visible file on target disk |
| Item 9 | Timeline for Floppy Disk |
| Item 10 | List of 'live' files on the floppy disk |
| Item 11 | File ownership details |
| Item 12 | Screenshot of the Camouflage Website |
| Item 13 | fsum (Windows) Command output of Camou121.exe |
| Item 14 | WinZip (Windows) contents of Camou121.exe selfextracting zip file |
| Item 15 | dir (Windows) Command output of Camouflage folder post install |
| Item 16 | fsum (Windows) for files created by the Camouflage install process |
| Item 17 | Camouflage right click menu |
| Item 18 | Settings GUI window for the Camouflage program |
| Item 19 | Password request GUI |
| Item 20 | Camouflage Window - contents of Password_Policy.doc carrier file |
| Item 21 | Camouflage Window - contents of Remort_Access_Policy.doc |
| Item 22 | Table of CAB.mdb extracted from Remote_Access_Policy.doc |
| Item 23 | fsum (windows) of all files recovered from Camouflage carrier files |
| Item 24 | List of all files (inc those hidden) found of the floppy disk |
| Item 25 | Screenshot of hashes not matching |
| Item 26 | Quote from Ballard Ind InformationSensivity Policy |
| Item 27 | Tools Used Matrix |
| Item 28 | Pictures of the outside of the system |
| Item 29 | Pictures of the inside of the system |
| Item 30 | BIOS Timings taken at 1733 hours on 31 August 2004 |
| Item 31 | The external IDE caddie with the abandoned drive fitted |
| Item 32 | External Caddie OS Patch |
| Item 33 | Quote on NFTS write support |
| Item 34 | Legal defence for Theft |
| Item 35 | Imaging in progress |
| Item 36 | Output from the file command |
| Item 37 | Quote from Microsoft explaining the HDD ID Tag |
| Item 38 | First look at the imaged file structure |
| Item 39 | Initial look at file ownership and their associated creation times/dates |
| Item 40 | Windows version extracted from the shell |
| Item 41 | Possibly the last use of the system |
| Item 42 | Cutting from System Time Line |
| Item 43 | Summary of the scandisk.log for the system |
| Item 44 | MAC for the boot.log |
| Item 45 | Mounting the Image in Read Only mode |
| Item 46 | Diagram of the Network used |
Item 47 – Norton Anti Virus Discovered Trojan
Item 48 – Creation and modification MACs for ‘POLMX2.CAB’ Trojan
Item 49 – AVG Scan Results
Item 50 – Spyware found by Spyware Doctor on the HDD
Item 51 – TrendMicro details on TROJ_RVP.D Trojan
Item 52 – Installation report for Sypblocker
Item 53 – Last few days activity
Item 54 – The common user menu
Item 55 – IP Information from the Registry
Item 56 – URLs Typed into Internet Explorer
Item 57 – Last Command Executed
Item 58 – Windows Media Player recent file list
Item 59 – Identifying the Username
Item 60 – Text files and Cookies found
Item 61 – Attempting to locate the IP Address
Item 62 – Quote from the Internet Watch Foundation

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/>


9 “Camouflage Home Page” Hide Your Files. 12 Jan 2005 <http://camouflage.unfiction.com>


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>


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


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)


60 of 57
# Upcoming SANS Forensics Training

<table>
<thead>
<tr>
<th>Course Name</th>
<th>City, Country</th>
<th>Dates</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Norfolk 2020</td>
<td>Norfolk, VA</td>
<td>Mar 16, 2020 - Mar 21, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS San Francisco Spring 2020</td>
<td>San Francisco, CA</td>
<td>Mar 16, 2020 - Mar 27, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Secure Singapore 2020</td>
<td>Singapore, Singapore</td>
<td>Mar 16, 2020 - Mar 28, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Oslo March 2020</td>
<td>Oslo, Norway</td>
<td>Mar 23, 2020 - Mar 28, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Seattle March 2020</td>
<td>Seattle, WA</td>
<td>Mar 23, 2020 - Mar 28, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Frankfurt March 2020</td>
<td>Frankfurt, Germany</td>
<td>Mar 30, 2020 - Apr 04, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS vLive - FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics</td>
<td>FOR508 - 202003,</td>
<td>Mar 31, 2020 - May 07, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>SANS 2020</td>
<td>Orlando, FL</td>
<td>Apr 03, 2020 - Apr 10, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Bethesda 2020</td>
<td>Bethesda, MD</td>
<td>Apr 14, 2020 - Apr 19, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Minneapolis 2020</td>
<td>Minneapolis, MN</td>
<td>Apr 14, 2020 - Apr 19, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Brussels April 2020</td>
<td>Brussels, Belgium</td>
<td>Apr 20, 2020 - Apr 25, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London April 2020</td>
<td>London, United Kingdom</td>
<td>Apr 20, 2020 - Apr 25, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Baltimore Spring 2020</td>
<td>Baltimore, MD</td>
<td>Apr 27, 2020 - May 02, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Bucharest May 2020</td>
<td>Bucharest, Romania</td>
<td>May 04, 2020 - May 09, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security West 2020</td>
<td>San Diego, CA</td>
<td>May 06, 2020 - May 13, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Amsterdam May 2020</td>
<td>Amsterdam, Netherlands</td>
<td>May 11, 2020 - May 18, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Hong Kong 2020</td>
<td>Hong Kong, Hong Kong</td>
<td>May 11, 2020 - May 16, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Northern Virginia- Alexandria 2020</td>
<td>Alexandria, VA</td>
<td>May 17, 2020 - May 22, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS San Antonio 2020</td>
<td>San Antonio, TX</td>
<td>May 17, 2020 - May 22, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Autumn Sydney 2020</td>
<td>Sydney, Australia</td>
<td>May 18, 2020 - May 23, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Nashville Spring 2020</td>
<td>Nashville, TN</td>
<td>May 26, 2020 - May 31, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Atlanta Spring 2020</td>
<td>Atlanta, GA</td>
<td>May 26, 2020 - May 31, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS London June 2020</td>
<td>London, United Kingdom</td>
<td>Jun 01, 2020 - Jun 06, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Chicago Spring 2020</td>
<td>Chicago, IL</td>
<td>Jun 01, 2020 - Jun 06, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Las Vegas Summer 2020</td>
<td>Las Vegas, NV</td>
<td>Jun 08, 2020 - Jun 13, 2020</td>
<td>Live Event</td>
</tr>
</tbody>
</table>