Global Information Assurance Certification Paper

GIAC Certified Forensics Analyst GCFA Practical

Assignment Version 1.5

Richard Bunnell

SANS Great Lakes Chicago
Rob Lee, Instructor
May 2004

Abstract: This paper, the Practical for GIAC Certified Forensics Analyst Certification, covers the following topics:

1. Analysis of an Unknown Image
2. Performance of a Forensic Analysis on a System

Table of Contents

List of Illustrative Materials

List of Tables

Description of Forensic Lab

Forensic machine 1. This is a Dell Latitude C610 laptop. The processor speed is 1.00 GHz and the memory size is 1024 MB. This machine has Red Hat 9.0 with VMWare Workstation 4 for Linux installed so that other operating systems can be run. The machine name is LinuxForensics. This machine has a 60 GB hard drive.

Forensic Machine 2. This is a Dell OptiPlex GX1 500BTbr+ desktop with 768 MB of memory. This is a dual boot machine between Red Hat Linux 9.0 and Windows 2000 Professional SP3. The Red Hat machine name is LinuxStorage and the Windows 2000 machine name is RB-PC001. This machine has a 20 GB and a 120 GB hard drive, a CD –R/RW drive, and a removable IDE drive bay.

Forensic machine 3 – This is a NEC desktop with a speed of 125 MHz and 196 MB memory. This machine has only a floppy drive and a removable hard drive.

Forensic machines 1 and 2 are connected by a 100 Mbps Ethernet connection through a Link-Max LM205 5-port switch.

Programs Used During Initial Acquisition of the Drive

Linux programs used during the initial discovery process were:

- fdisk - This program is a Linux partition table creator and manipulator. A partition is a logical division of a physical hard disk. Fdisk will recognize many different types of partitions and display information about their size and location. Many different types of operation system partitions are recognized including partitions from Windows 9x, DOS, and many types of Unix and Linux - from fdisk manual page from Linux 2.0 Programmers Manual, June 1998.

- dd - This program is used to copy a file with the ability to convert and format the file as it is being copied. Normal command line parameters are -if=<input file name> of=<output file name> - from dd manual page from coreutils 4.5.3, Feb. 2003.

- md5 / md5sum - These programs create message digests. To be more specific, a message digest is a unique 32-byte signature for any file, disk device, partition or image. This means that if even one bit in a file is changed the message digest will be different. This unique signature will show if electronic evidence has been changed or altered.

- chmod – Paragraphs could be written about this program, but for the purposes of this paper only permissions will be discussed. Every file has three sets of permissions, commonly known as user, group, and all. Each set of permissions has three levels of access that are mapped by bits turned on or off.

The following table (placeholders are noted by "**.**") illustrates:

Table 1 - Permission Bits Set for Groups and Security Levels

	Permission Groups		
	User	Group	All
Read	1..	... 1.. ...	... ... 1..
Write	.1.	... .1. ...	... ... .1.
Execute	..1	... ..1 ...	1

If the permission is turned on, it is indicated by a '1' and turned off by a '0'

Table 2 - Permission Representations and Security Levels

Permission	Binary Representation	Decimal Representation
No permissions	'000'	0
Execute only	'001'	1
Write only	'010'	2
Write and execute	'011'	3
Read only	'100'	4
Read and execute	'101'	5
Read and write	'110'	6
Read, write, and execute	'111'	7

If a file has permissions of 744 or 111 100 100 it means that the owner has all permissions, the group and everyone else has read only permission.

After an image has been extracted, the permissions can be changed to 444 which means that no one has write or execute privileges – essentially this becomes a read-only file.

- Autopsy – This toolkit, by Brian Carrier (http://www.sleuthkit.org/autopsy/) is a graphical tool that enables investigators to "perform system file analysis on UNIX and Windows images." This system allows report generation, investigator notes, and logging of activities performed during an investigation. This toolkit has proven invaluable to translate forensic concepts to analytic practice.

- file – This utility allows investigators to make an educated guess about what kind of file is being examined. From the manual page for file:

  > There are three sets of tests, performed in this order: filesystem tests, magic number tests, and language tests. The first test that succeeds causes the file type to be printed.

Part 1 - Analyzing an Unknown Image

Investigative Summary

Everything in this summary is explained in detail later in the report.

The floppy disk seized from RJL was found to have six documents on it. These documents are:

Information_Sensitivity_Policy.doc
Internal_Lab_Security_Policy1.doc
Internal_Lab_Security_Policy.doc
Password_Policy.doc
Remote_Access_Policy.doc
Acceptable_Encryption_Policy.doc

These documents are policy documents that relate to computer polices at Ballard Industries. All of these documents have meta-data within them that indicates someone originally wrote them from Cisco Systems.

Within three of these documents various files were hidden and encrypted. The documents that had hidden files and the names of the hidden files are listed below:

Table 3 - Extracted Files From Floppy Disk

File on Floppy Disk	File Hidden Within
Internal_Lab_Security_Policy.doc	Internal_Lab_Security_Policy.doc
Internal_Lab_Security_Policy.doc	Opportunity.txt
Password_Policy.doc	Pem_fuelcell.gif
Password_Policy.doc	Password_Policy.doc
Password_Policy.doc	PEM-fuel-cell-large.jpg
Password_Policy.doc	Hydrocarbon%20fuel%20cell%20page2.jpg
Remote_Access_Policy.doc	Remote_Access_Policy.doc
Remote_Access_Policy.doc	CAT.mdb

Three of these files were policy documents (appendices L, O, and S). Three more of these files were images depicting internal fuel cell processes (appendices N, P, and Q). One file was a note from RJL (appendix M) indicating that he could supply more information for $5 million dollars. The last one as an extract from the Client Authorized Table (CAT) database (appendix R).

Of all the evidence, the CAT database sample and the offer from RJL (appendices M and R) seems to be most pertinent to the investigation. Although there may be legal consequences for RJL, there needs to be a further investigation to gather more evidence on other PC's within Ballard and possibly outside of the company.

The intent of RJL was to remove these documents on the floppy disk, and the files hidden within them from Ballard premises. Beyond that, until the investigation is complete, there is no way to determine the identity of the recipients of these documents.

The program used was Camouflage, version 1.2. It is a program that is freely downloadable from several sites on the Internet. It works by encrypting files within other files. The encrypted files are added to the end of the original file. The original file looks unmodified to the program that uses it - in this case Mocrosoft ® Word. The password is stored toward the end of the encrypted file and can be discovered easily. The algorithm used is to change bits by using exclusive or (XOR) with each character of the password with a predefined pattern.

At the end of this report are descriptions of legal implications, challenges for Ballard system administrators, and Internet references.

Evidence Tag for Seized Floppy

A floppy disk was seized from an employee, RJL, as he was leaving the lab. The seizure occurred on April 26, 2004 at 4:45 MST. The security administrator has asked that it be analyzed prior to returning it to the employee. The evidence tag for the seized floppy is:

- Tag # fl-260404-RJL1
- 3.5 inch TDK floppy disk
- MD5: d7641eb4da871d980adbe4d371eda2ad
- fl-260404-RJL1.img.gz

Initial Image Verification and Discovery

Using the Red Hat Linux forensic machine, the floppy disk is imaged with dd. The program md5 is used to create a hash.

```
d7641eb4da871d980adbe4d371eda2ad        v1_5.gz
```

The two files, fl-260404-RJL1.img.gz and v1_5.gz have the same hash so they are identical. This verifies the first step in the chain of custody.

The rights of the file were changed so all users will only be able to read it. The details of the chmod command were explained in detail earlier.

```
chmod 444 v1_5.gz
-r--r--r--    1 root     root      1474560 Aug 22 12:13 v1_5.gz
```

The file command was run to discover what file type is being examined.

```
file v1_5.gz
v1_5.gz: x86 boot sector, system mkdosfs, FAT (12 bit)
```

Using Autopsy to Collect Information

Autopsy was run to collect as much information as possible from the image. The time zone was set to MST7MDT and the time skew was set to 0. Information was copied from Autopsy to show the steps completed.

```
Copying /mnt/hdb10/v1_5.gz to
/EvidenceLocker/GIAC_Part_1/host1/images/v1_5.gz
Calculating MD5 of images/v1_5.gz (this could take a while)
Current MD5: D7641EB4DA871D980ADBE4D371EDA2AD
```

The md5 hash shows that the image file had not been changed when it was imported to Autopsy.

Running fls -r -m on images/v1_5.gz - the command "fls" creates an intermediate image file with all the filename information.

Running ils -m on images/v1_5.gz - the command "ils" creates another intermediate image file with all the inode information. These two intermediate files are used to create the body file.

Body file saved to /EvidenceLocker/GIAC_Part_1/host1/output/body
Entry added to host config file
Calculating MD5 Value
MD5 Value: A6B3C1BF78A6226C8FA206792F0389AB

Creating Timeline using all dates (Time Zone: MST7MDT)
Timeline saved to /EvidenceLocker/GIAC_Part_1/host1/output/GIAC_1.timeline
Entry added to host config file
Calculating MD5 Value
MD5 Value: D9FD42FD695905280E2057E560ECA8D0

Extracting strings from images/v1_5.gz and saving to v1_5.gz.str
output/v1_5.gz.str added to host config file - this step creates a file containing all of the human readable strings of characters. This can be quite useful later in the investigation.
Calculating MD5 Value
MD5 Value: DCF7CC7B4BDF4E681DA25EE4E0618F1F

Extracting unallocated data from images/v1_5.gz and saving to output/v1_5.gz.dls - this step creates an image containing all of the unallocated data on the diskette.
output/v1_5.gz.dls added to host config file
Calculating MD5 Value
MD5 Value: 4388A93BA6F61181DA3E5FE4B6173DC2

Extracting strings from output/v1_5.gz.dls and saving to v1_5.gz.dls.str - the image with all the unallocated data is scanned for human readable strings.
output/v1_5.gz.dls.str added to host config file
Calculating MD5 Value
MD5 Value: 0B6106935755A33BEC6639262316235A

Executing: sorter -h -m 'a:\' -d '/EvidenceLocker/GIAC_Part_1/host1/output/sorter-v1_5.gz/' -f fat12 '/EvidenceLocker/GIAC_Part_1/host1/images/v1_5.gz' - sorter scans through the files in the image, identifies them through file header (and sometimes file trailer) information, and sends them to folders. This step also detects mismatches between the file extension and the file header information. The summary information is saved to an html file.

Analyzing /EvidenceLocker/GIAC_Part_1/host1/images/v1_5.gz
Loading Allocated File Listing
Processing 9 Allocated Files and Directories
100%

Loading Unallocated File Listing
Processing 5 Unallocated meta-data structures
100%

All files have been saved to: /EvidenceLocker/GIAC_Part_1/host1/output/sorter-v1_5.gz/
Output can be found by viewing:
/EvidenceLocker/GIAC_Part_1/host1/output/sorter-v1_5.gz//index.html

Results Summary
Images
/EvidenceLocker/GIAC_Part_1/host1/images/v1_5.gz

Files (14)
Allocated (9)
Unallocated (5)

Files Skipped (4)
Non-Files (4)
'ignore' category (0)

Extensions
Extension Mismatches (1)
Extension Mismatch
a:\CamShell.dll
HTML document text (Ext: dll)
Image: /EvidenceLocker/GIAC_Part_1/host1/images/v1_5.gz Inode: 5

Categories (10)
archive (0)
audio (0)
compress (0)
crypto (0)
data (0)
disk (0)
documents (6)

documents Category
a:\Information_Sensitivity_Policy.doc
Microsoft Office Document
Image: /EvidenceLocker/GIAC_Part_1/host1/images/v1_5.gz Inode: 9

a:\Internal_Lab_Security_Policy1.doc
Microsoft Office Document
Image: /EvidenceLocker/GIAC_Part_1/host1/images/v1_5.gz Inode: 13

a:\Internal_Lab_Security_Policy.doc
Microsoft Office Document
Image: /EvidenceLocker/GIAC_Part_1/host1/images/v1_5.gz Inode: 17

a:\Password_Policy.doc
Microsoft Office Document
Image: /EvidenceLocker/GIAC_Part_1/host1/images/v1_5.gz Inode: 20

a:\Remote_Access_Policy.doc
Microsoft Office Document
Image: /EvidenceLocker/GIAC_Part_1/host1/images/v1_5.gz Inode: 23

a:\Acceptable_Encryption_Policy.doc
Microsoft Office Document
Image: /EvidenceLocker/GIAC_Part_1/host1/images/v1_5.gz Inode: 27

exec (0)
images (0)
system (0)
text (4)

text Category
a:\CamShell.dll
HTML document text
--- Extension Mismatch! ---
Image: /EvidenceLocker/GIAC_Part_1/host1/images/v1_5.gz Inode: 5

a:_ndex.htm
HTML document text
Image: /EvidenceLocker/GIAC_Part_1/host1/images/v1_5.gz Inode: 28

a:\<v1_5.gz-_AMSHELL.DLL-dead-5>
HTML document text
Image: /EvidenceLocker/GIAC_Part_1/host1/images/v1_5.gz Inode: 5

a:\<v1_5.gz-_ndex.htm-dead-28>
HTML document text
Image: /EvidenceLocker/GIAC_Part_1/host1/images/v1_5.gz Inode: 28

unknown (0)
video (0)

After returning to Autopsy and going into the File Analysis section more information can be collected about the directory entries in the image. The table below summarizes what was found. Later versions of Windows support long file names. Long file names can include capital and small letters and don't have to conform to the 8.3 (filename(8).extension(3)) rule. There are two types of directory entries. The first type stores the long filename in reverse order. The second type stores the name in 8.3 format. For example, the 8.3 format (file name = 8 characters, a period, then the extension = 3 characters - INFORM~1.DOC - or Information_Sensitivity_Policy.doc).

The table below illustrates the following sequence:

1. CamShell.dll is written to the disk. The file name is considered to be a long filename because it has capital and small letters. Because of this Directory Entry 4 is written with the true name of the file - CamShell.dll.
2. Directory Entry 5 is written with the 8.3, upper case filename - CAMSHELL.DLL.
3. CAMSHELL.DLL is written to sectors 33-104.
4. The other document files are written to the diskette. They use up directory entries 6-27 and sectors 105-1384.
5. Sometime later CAMSHELL.DLL is deleted. This merely writes a hex 'E5' over the first character of the file name. The hex 'E5' tells the operating system that sectors 33-104 are available in which to write a file. All the other file information remains on the disk.
6. The next file to be written is index.htm. This uses directory entry 28 only and is not considered to be a long file name. It is written to sectors 33 and 34. This means that the remainder of CamShell.dll is still on the disk. At this point in the analysis, the purpose of CamShell.dll is unclear.

Table 4 - Directory Entry Information for Seized Floppy Disk

Directory Entry Number	Allocated / Not Allocated	Attribute	Size	Name	Sectors Used
4	Not Allocated	Long File Name	0	CamShell.dll	0
5	Not Allocated	File, Archive	36864	_AMCHELL.DLL	33-104
6	Allocated	Long File Name	0	licy.doc	0
7	Allocated	Long File Name	0	ensitivity_Po	0
8	Allocated	Long File Name	0	Information_S	0
9	Allocated	File, Archive	42496	INFORM~1.DOC	105-187
10	Allocated	Long File Name	0	cy1.doc	0
11	Allocated	Long File Name	0	Security_Poli	0
12	Allocated	Long File Name	0	Internal_Lab_	0
13	Allocated	File, Archive	32256	INTERN~1.DOC	105-187
14	Allocated	Long File Name	0	cy1.doc	0
15	Allocated	Long File Name	0	Security_Poli	0
16	Allocated	Long File Name	0	Internal_Lab_	0
17	Allocated	File, Attribute	33423	INTERN~2.DOC	251-316
18	Allocated	Long File Name	0	cy.doc	0
19	Allocated	Long File Name	0	Password_Poli	0
20	Allocated	File, Archive	307935	PASSWO~1.DOC	317-918

Directory Entry Number	Allocated / Not Allocated	Attribute	Size	Name	Sectors Used
21	Allocated	Long File Name	0	_Policy.doc	0
22	Allocated	Long File Name	0	Remote_Access	0
23	Allocated	File, Archive	215895	REMOTE_1.DOC	919-1340
24	Allocated	Long File Name	0	cy.doc	0
25	Allocated	Long File Name	0	cryption_Poli	0
26	Allocated	Long File Name	0	Acceptable_E	0
27	Allocated	File Archive	22528	ACCEPT_1.DOC	1341-1384
28	Allocated	File Archive	727	ndex.htm	33-34

Summary of Autopsy Results

Summary of Results:
Name: images/v1_5.gz
Mounting Point: a:\
File System Type: fat12
MD5: D7641EB4DA871D980ADBE4D371EDA2AD
Host Directory: /EvidenceLocker/GIAC_Part_1/host1/
Strings File: output/v1_5.gz.str
Unallocated Sectors (dls) File: output/v1_5.gz.dls
Strings of Unallocated Sectors File:output/v1_5.gz.dls.str

Extracting the Documents from the Image

The image is mounted so that it looks like a disk drive to the operating system.

```
mount -o ro,loop v1_5.gz /mnt/analysis
ls -l /mnt/analysis
total 640
-rwxr-xr-x    1 root     root        22528 Apr 23 14:10
Acceptable_Encryption_Policy.doc

-rwxr-xr-x    1 root     root        42496 Apr 23 14:11
Information_Sensitivity_Policy.doc

-rwxr-xr-x    1 root     root        33423 Apr 22 16:31
Internal_Lab_Security_Policy.doc

-rwxr-xr-x    1 root     root        32256 Apr 22 16:31
Internal_Lab_Security_Policy1.doc

-rwxr-xr-x    1 root     root       307935 Apr 23 11:55 Password_Policy.doc
```

```
-rwxr-xr-x    1 root     root       215895 Apr 23 11:54 Remote_Access_Policy.doc
```

The md5 hash for all the documents is collected:

```
md5 *.doc > md5_docs.txt
cat md5_docs.txt
f785ba1d99888e68f45dabeddb0b4541   Acceptable_Encryption_Policy.doc
99c5dec518b142bd945e8d7d2fad2004   Information_Sensitivity_Policy.doc
b9387272b11aea86b60a487fbdc1b336   Internal_Lab_Security_Policy.doc
e0c43ef38884662f5f27d93098e1c607    Internal_Lab_Security_Policy1.doc
ac34c6177ebdcaf4adc41f0e181be1bc    Password_Policy.doc
5b38d1ac1f94285db2d2246d28fd07e8   Remote_Access_Policy.doc
```

The documents are copied to a FAT drive that is shared between Linux and Windows 2000.

```
cp /mnt/analysis/*.doc /mnt/hdb10/GIAC\ Paper/Part_1_files/docs
-r--r--r--    1 root     root        22528 Aug 22 14:39
Acceptable_Encryption_Policy.doc

-r--r--r--    1 root     root        42496 Aug 22 14:39 Information_Sensitivity_Policy.doc

-r--r--r--    1 root     root        33423 Aug 22 14:39 Internal_Lab_Security_Policy.doc

-r--r--r--    1 root     root        32256 Aug 22 14:39
        Internal_Lab_Security_Policy1.doc

-r--r--r--    1 root     root       307935 Aug 22 14:39 Password_Policy.doc

-r--r--r--    1 root     root       215895 Aug 22 14:39 Remote_Access_Policy.doc
```

Additionally, there might be some other unicode or other metadata strings that might be recoverable. Using KhexEdit v. 0.8.5 by Espen Sand (http://home.sol.no/~espensa/khexedit/) the following strings were recovered:

Table 5 - Unicode and Text Strings Found in Documents

Document Name	Unicode and Text Strings Recovered / Offset into File (Decimal)
Acceptable Encryption Policy	“Cisco User” - unicode / 10,012 "Cisco Systems, Inc." - text / 15,128
Information Sensitivity Policy	“Cisco User” - unicode / 30,802 "Cisco Systems, Inc." - text / 35,496
Internal Lab Security Policy	“Cisco User” - unicode / 20,760 "Cisco Systems, Inc." - text / 25,256

Document Name	Unicode and Text Strings Recovered / Offset into File (Decimal)
Internal Lab Security Policy1	“Cisco User” - unicode / 20,760 "Cisco Systems, Inc." - text / 25,256
Password Policy	“Cisco User” - unicode / 28,183 "Cisco Systems, Inc." - text / 32,936
Remote Access Policy	“Cisco User” - unicode / 19,239 "Cisco Systems, Inc." - text / 23,720

This would seem to indicate that all the documents had a connection to Cisco Systems, Inc. - either originating there or going through there at some point in their existence.

The text of these six documents is in Appendices A - F.

Using Windows and Word to Continue Discovery

Under Windows Explorer, each document is right clicked, Properties selected, and then the Read-only attribute is checked and applied.

The md5 hashes are collected again from Windows 2000.

Acceptable_Encryption_Policy.doc
F785BA1D99888E68F45DABEDDB0B4541

Information_Sensitivity_Policy.doc
99C5DEC518B142BD945E8D7D2FAD2004

Internal_Lab_Security_Policy.doc
B9387272B11AEA86B60A487FBDC1B336

Internal_Lab_Security_Policy1.doc
E0C43EF38884662F5F27D93098E1C607

Password_Policy.doc
AC34C6177EBDCAF4ADC41F0E181BE1BC

Remote_Access_Policy.doc
5B38D1AC1F94285DB2D2246D28FD07E8

Since the hashes match, the documents have not been changed. To continue the discovery phase basic information is collected about the documents. Metadata - data stored in the documents by the application, here Microsoft ® Word - is noted in Appendix G. This was collected by locating each document in Windows Explorer, right clicking it,

selecting Properties, selecting the Summary tab and then noting what was found. The information collected included the document name, author, revision number, company name, creation date, and date last saved.

Other basic information was collected, such as word count, character count, and file length in bytes. This was obtained by opening each document in Windows Explorer, selecting Tools, then Word Count. This information is in Appendix H.

Appendix H has the first indication that something might be suspicious. After all the documents were examined, two new documents were created by using the text from "Acceptable_Use_Policy.doc" and "Remote_Access_Policy.doc". As can be seen, there is a big discrepancy between the size of the text in Remote_Access_Policy.doc (215,895 bytes) and Sample Document 2 (Remote Access Policy).doc (7,913 bytes). This indicates that there is be something worth investigating.

Checking the Output From the Strings Command

Searching the strings file, v1_5.gz.dls.str, from unallocated space for "camshell.dll" gives:

```
23120 CamShell.dll
```

Searching for "cam" from unallocated space gives:

```
5270   ll\SheCamouflageShell
5648   CamShell
5674   CamouflageShell
7528   CamouflageShell
11596 C:\My Documents\VB Programs\Camouflage\Shell\IctxMenu.tlb
23120 CamShell.dll
31919 1CamouflageShellW
```

From the path inside the dll it looks like there is a program called Camouflage that might be at work.

Discovery and Installation of Camouflage

Searching the Internet brings us here - http://camouflage.unfiction.com/Overview.html

From their description:

> 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.

They also have a disclaimer on their site:

> Camouflage is free, but make sure you have read and understood the license agreement before downloading it.
>
> We regret that Camouflage is no longer supported or developed. The decision to abandon the project came after much debate, but we can no longer spare the resources needed to continue to provide quality service and support.
>
> We hope that you will continue to use 'Camouflage', and although we will ensure that this site remains on-line for as long as possible, we encourage you to distribute Camouflage from your own 'unofficial' web site. Feel free to mirror these pages and to include the FAQ.
>
> Please be aware that Unfiction.com is in no way affiliated with Camouflage software or it's developers.
>
> The owners of the site have mirrored our site on their server, but any emails sent to them regarding Camouflage software will be deleted without being read.
> This zip file was downloaded from the site:

The executable (a self-extracting zip file) was downloaded - Camou121.exe (2,718,208 bytes). The md5 hash of this file was:

> Camou121.exe C62B050117C2CBA3518E5A734FEDEF1F

This file was scanned with Norton Anti-Virus (http://www.symantec.com/index.htm), v. 9.05.15, and found to be clean.

The software was loaded onto a clean install of Windows 2000. The default installation was into C:\Program Files\Camouflage.

The files that were installed were:

Table 6 - Files Installed by Camouflage

File Name	Creation Date	Length (Bytes)	Md5 Hash
Camouflage.exe	3/29/2001	217,088	9F08258A80D578A0F1CC38FE4C2AEBB5
CamShell.dll	2/3/2001	36,864	4E986AB0909D2946BED868B5F896906F
Readme.txt	3/28/2001	11,649	0C25AD7792D555B6C8C37C77CEB9E224
Uninst.isu	8/24/2004	19,758	31FDDD3C832ED63393A206F33D567A0D

After the installation process, the installer is asked to view the readme file. This was captured in Appendix I.

Testing Procedures for Camouflage

In order to discover how this program works, several files were created. The first file, "HiddenDocument.doc" has twenty repeating lines with the text "This document will be hidden." The second file, "originalEULA.doc" contains the Camouflage End User License Agreement text found in Appendix J. After the document "HiddenDocument.txt" is hidden within "originalEULA.doc" Camouflage asks for a new filename. The filename used is the same as the password - "ggggggggggggggggggg.doc." The process is repeated and a second file, "hhhhhhhhhhhhhhhhhhhh.doc" is created. The next document has no password and its name is space.doc. Examination of these documents will enable discovery of the changes done to a document by Camouflage.

By doing the DOS command fc (file compare) on any of the two of the files containing "HiddenDocument.doc" the only difference will be the password. The password location within the document will be discovered and if the password is encrypted, clues will be obtained for the password decryption. Screen shots of this process follow.

HiddenDocument.doc is right-clicked and there is now a Camouflage and UnCamouflage icon in the box. Clicking the Camouflage icon gives this screen.

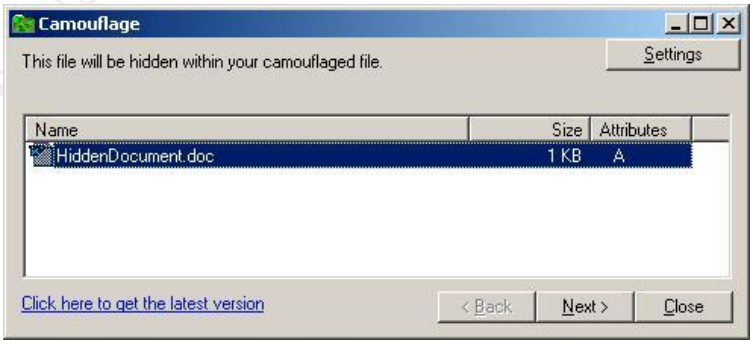


Figure 1 - Camouflage Select Hidden File Screen

Clicking Next gives this screen. The file "originalEULA" will be used.

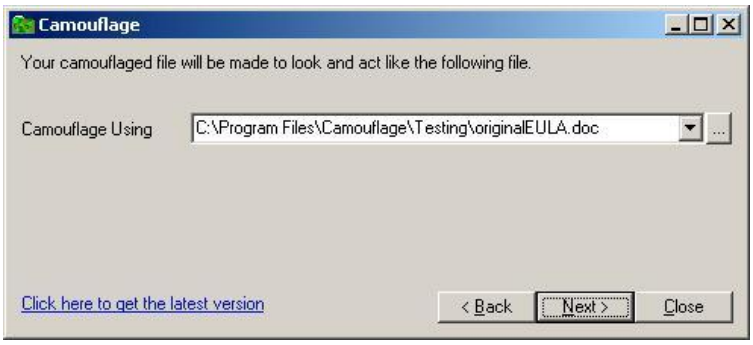


Figure 2 - Camouflage Select File to Contain Hidden File Screen

The file to be created will be "ggggggggggggggggggg.doc".

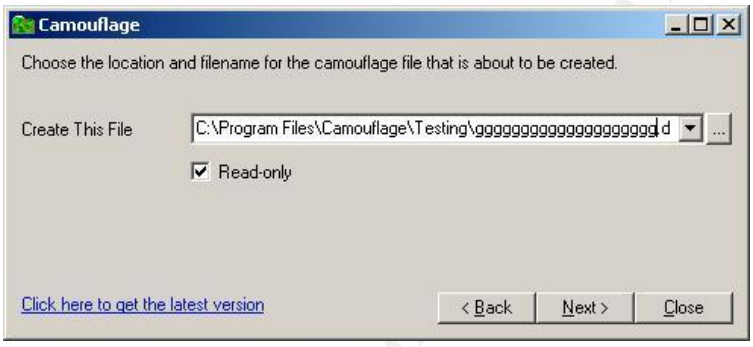


Figure 3 - Camouflage Select File to Create Screen

The password "ggggggggggggggggggg" is used.

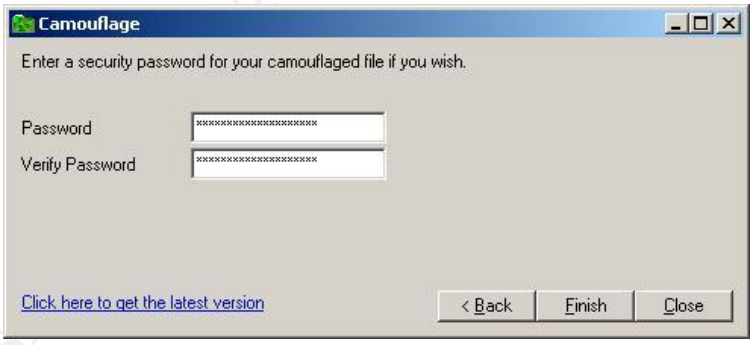


Figure 4 - Camouflage Select Password Screen

Another document, "hhhhhhhhhhhhhhhhhhhh.doc" is created the same way.

The next table contains documents:

Table 7 - Test Document Information

File Name	Length (bytes)	Md5 Hash
HiddenDocument.doc	620	F81DC33369E39514BA8E6F043DF290F0
OriginalEULA.doc	11,653	C563ED0AE952941B308100958920996C
space.doc (no password)	13,128	75F8E392DA78AE5C94A82E92833F0CDF
Gggggggggggggggggg.doc	13,128	68F8D6FA89F9EBDAFBEA14894CEBB473
Hhhhhhhhhhhhhhhhhhh.doc	13,128	7680216191F08DCFBEE4E08658365E32

Discovery of the Camouflage Password

Running the DOS command fc with the option to produce binary output (/B) on space.doc and ggggggggggggggggggg.doc gives these results.

The left column is the distance in bytes (hex) from the start of the file.
The center column is the byte value from space.doc.
The right column is the byte value in ggggggggggggggggggg.doc

Comparing files space.doc and ggggggggggggggggggg.DOC
00002D8F: 2D F0
00002D90: 8A 89
00002D94: BE AF
00002D95: E8 50
00002D96: E6 EC
0000301D: 2E 2D
00003021: F0 60
00003022: 0F 43
00003023: D7 BA
00003024: 29 C3
00003235: 20 **65**
00003236: 20 **F2**
00003237: 20 **1D**
00003238: 20 **45**
00003239: 20 **6B**
0000323A: 20 **C1**
0000323B: 20 **73**
0000323C: 20 **86**
0000323D: 20 **86**
0000323E: 20 **A8**
0000323F: 20 **D8**
00003240: 20 **02**
00003241: 20 **47**
00003242: 20 **08**

00003243: 20 **F9**
00003244: 20 **D4**
00003245: 20 **FE**
00003246: 20 **02**
00003247: 20 **2D**
00003248: 20 **34**

Running the DOS command fc with the option to produce binary output (/B) on space.doc and hhhhhhhhhhhhhhhhhhhh.doc gives these results.

The left column is the distance in bytes (hex) from the start of the file.
The center column is the byte value from space.doc.
The right column is the byte value in hhhhhhhhhhhhhhhhhhhh.doc

Comparing files space.doc and hhhhhhhhhhhhhhhhhhhh.DOC
00002D8F: 2D 2E
00002D93: 80 20
00002D94: BE 6C
00002D95: E8 44
00002D96: E6 38
00003021: F0 B0
00003022: 0F 4B
00003023: D7 9F
00003024: 29 39
00003235: 20 **6A**
00003236: 20 **FD**
00003237: 20 **12**
00003238: 20 **4A**
00003239: 20 **64**
0000323A: 20 **CE**
0000323B: 20 **7C**
0000323C: 20 **89**
0000323D: 20 **89**
0000323E: 20 **A7**
0000323F: 20 **D7**
00003240: 20 **0D**
00003241: 20 **48**
00003242: 20 **07**
00003243: 20 **F6**
00003244: 20 **DB**
00003245: 20 **F1**
00003246: 20 **0D**
00003247: 20 **22**
00003248: 20 **3B**

There is one area of twenty bytes in both files that is probably the password:

location 00003235 - 00003248 - 20 bytes (bold and underlined below)

Decoding the Camouflage Password Scheme

Since the password is twenty bytes, the twenty-byte area will be examined. Bit translations may be significant so the value of the password before and after translation will be compared.

The first chart contains the password translations from "ggggggggggggggggggg.doc" and the second chart contains the password translations from "hhhhhhhhhhhhhhhhhhh.doc". Each character in the file from locations 3235 to 3248 is compared with the known password and the bit differences are noted.

"-" will indicate unchanged bits
"x" will indicate changed bits

The hex value (column 3) for the next two tables comes from the hex conversion table in Appendix K.

Table 8 - Password Bit Differences for ggggggggggggggggggg.doc

ggggggggggggggggggg.doc						
Location (hex)	Password	Hex	Binary	Hex Value In File	Binary	Bit Difference = x
3235	g	67	0110 0111	65	0110 0101	---- --x-
3236	g	67	0110 0111	F2	1111 0010	x--x -x-x
3237	g	67	0110 0111	1D	0001 1101	-xxx x-x-
3238	g	67	0110 0111	45	0100 0101	--x- --x-
3239	g	67	0110 0111	6B	0110 1011	---- xx--
323A	g	67	0110 0111	C1	1100 0001	x-x- -xx-
323B	g	67	0110 0111	73	0111 0011	---x -x--
323C	g	67	0110 0111	86	1000 0110	xxx- ---x
323D	g	67	0110 0111	86	1000 0110	xxx- ---x
323E	g	67	0110 0111	A8	1010 1000	xx-- xxxx
323F	g	67	0110 0111	D8	1101 1000	x-xx xxxx
3240	g	67	0110 0111	02	0000 0010	-xx- -x-x
3241	g	67	0110 0111	47	0100 0111	--x- ----
3242	g	67	0110 0111	08	0000 1000	-xx- xxxx
3243	g	67	0110 0111	F9	1111 1001	x--x xxx-
3244	g	67	0110 0111	D4	1101 0100	x-xx --xx
3245	g	67	0110 0111	FE	1111 1110	x--x x--x
3246	g	67	0110 0111	02	0000 0010	-xx- -x-x
3247	g	67	0110 0111	2D	0010 1101	-x-- x-x-
3248	g	67	0110 0111	34	0011 0100	-x-x --xx

"-" will indicate unchanged bits
"x" will indicate changed bits

Table 9 - Password Bit Differences for hhhhhhhhhhhhhhhhhhhh.doc

hhhhhhhhhhhhhhhhhhhh.doc						
Location (hex)	Password	Hex	Binary	Hex Value In File	Binary	Bit Difference = x
3235	h	68	0110 1000	6A	0110 1010	---- --x-
3236	h	68	0110 1000	FD	1111 1101	x--x -x-x
3237	h	68	0110 1000	12	0001 0010	-xxx x-x-
3238	h	68	0110 1000	4A	0100 1010	--x- --x-
3239	h	68	0110 1000	64	0110 0100	---- xx--
323A	h	68	0110 1000	CE	1100 1110	x-x- -xx-
323B	h	68	0110 1000	7C	0111 1100	---x -x--
323C	h	68	0110 1000	89	1000 1001	xxx- ---x
323D	h	68	0110 1000	89	1000 1001	xxx- ---x
323E	h	68	0110 1000	A7	1010 0111	xx-- xxxx
323F	h	68	0110 1000	D7	1101 0111	x-xx xxxx
3240	h	68	0110 1000	0D	0000 1101	-xx- -x-x
3241	h	68	0110 1000	48	0100 1000	--x- ----
3242	h	68	0110 1000	07	0000 0111	-xx- xxxx
3243	h	68	0110 1000	F6	1111 0110	x--x xxx-
3244	h	68	0110 1000	DB	1101 1011	x-xx --xx
3245	h	68	0110 1000	F1	1111 0001	x--x x--x
3246	h	68	0110 1000	0D	0000 1101	-xx- -x-x
3247	h	68	0110 1000	22	0010 0010	-x-- x-x-
3248	h	68	0110 1000	3B	0011 1011	-x-x --xx

Upon examination, the column "Bit Difference = x" from both "ggggggggggggggggggg.doc" and "hhhhhhhhhhhhhhhhhhhh.doc" is the same. The bit pattern for the first twenty characters of any password has been discovered.

Since the operation seems to flip bits, it should be possible to use the same operation to flip them back. The one operation that flips bits back and forth is exclusive or (XOR). Here is the truth table for XOR (http://www.fact-index.com/t/tr/truth_table.html).

Table 10 - XOR Truth Table

Col. 1 - Original Password (binary)	Col. 2 - XOR Operation to be Done on Original Password	Col. 3 - Result of Col.1 XOR Col. 2	Col. 4 - XOR Operation to be Done on Col. 3	Col. 5 - Result of Col. 3 XOR Col. 4
1	1	0	1	1
1	0	1	0	1
0	1	1	1	0
0	0	0	0	0

Since Column 1 = column 5, the operation on the passwords can be reversed and the passwords decoded.

Before that can be done the XOR pattern must be determined. The Bit Pattern needs to be translated to hex characters. After this, it is tested against the password from "hhhhhhhhhhhhhhhhhhhh.doc".

Table 11 - Test of Hex Pattern on Password from hhhhhhhhhhhhhhhhhhh.doc

Bit Difference = x	Binary Pattern	Hex Pattern from hhhhhhhhhh hhhhhhhhhh. doc	Password from locations 3235 - 3248	Translated Password (Hex Pattern XOR Password)
---- --x-	0000 0010	02	6A	68 ('h' text)
x--x -x-x	1001 0101	95	FD	68
-xxx x-x-	0111 1010	7A	12	68
--x- --x-	0010 0010	22	4A	68
---- xx--	0000 1100	0C	64	68
x-x- -xx-	1010 0110	A6	CE	68
---x -x--	0001 0100	14	7C	68
xxx- ---x	1110 0001	E1	89	68
xxx- ---x	1110 0001	E1	89	68
xx-- xxxx	1100 1111	CF	A7	68
x-xx xxxx	1011 1111	BF	D7	68
-xx- -x-x	0110 0101	65	0D	68
--x- ----	0010 0000	20	48	68
-xx- xxxx	0110 1111	6F	07	68
x--x xxx-	1001 1110	9E	F6	68
x-xx --xx	1011 0011	B3	DB	68
x--x x--x	1001 1001	99	F1	68
-xx- -x-x	0110 0101	65	0D	68
-x-- x-x-	0100 1010	4A	22	68
-x-x --xx	0101 0011	53	3B	68

Location of the Password in Any "Camouflaged" File

The last piece of the puzzle is to determine where the password is in any file.

Looking at the file "hhhhhhhhhhhhhhhhhhhh.doc" through a hex editor (WinHex 10.9 SR-6 - http://www.winhex.com) there seems to be long runs of '20' hex at the end of this "camouflaged" file. Here is the image with the password highlighted.

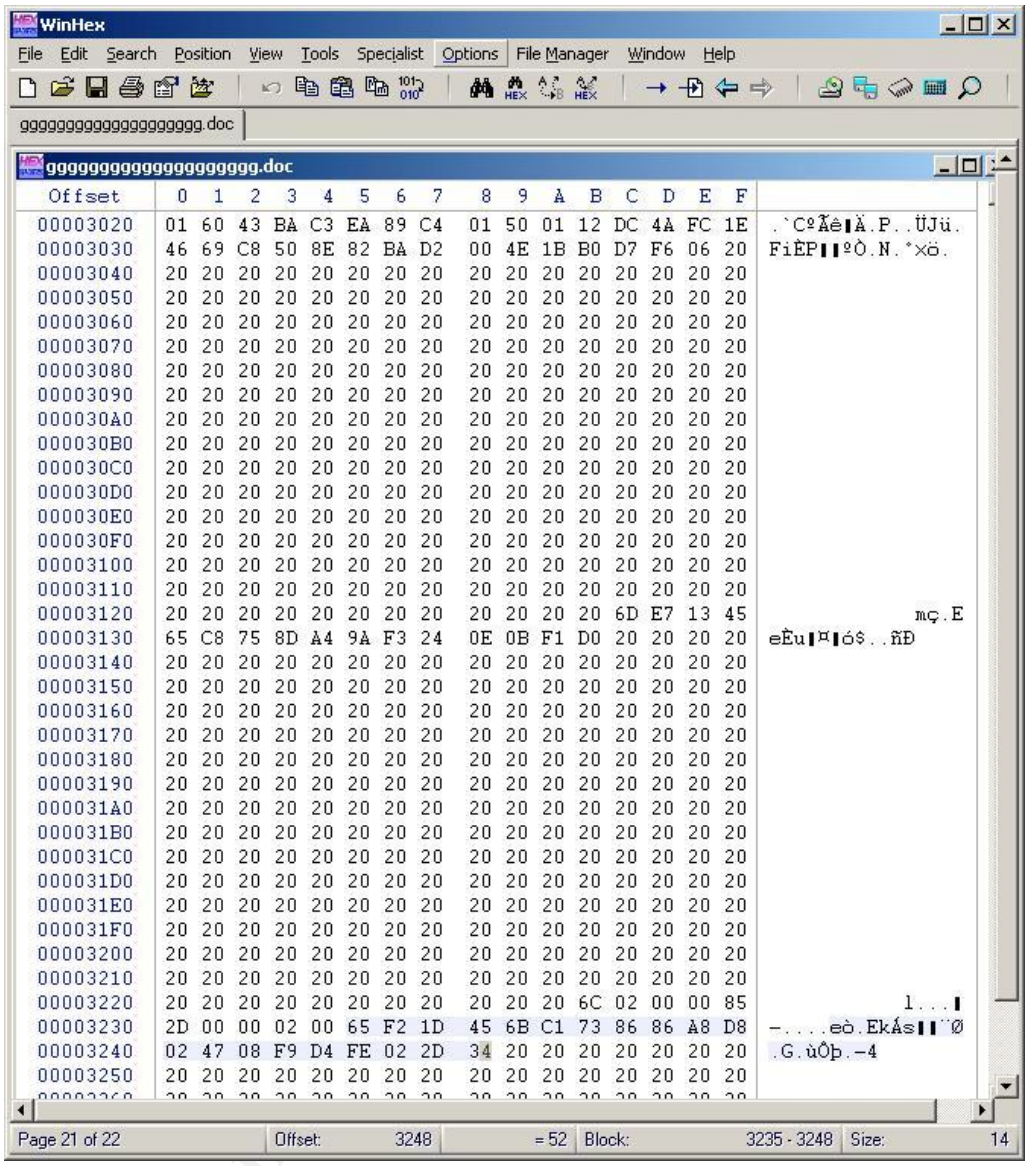


Figure 5 - Location of Password (highlighted) in gggggggggggggggggg.doc

By looking at the files recovered from the diskette through a hex editor it should be possible to recover the password and then recover whatever is "camouflaged" in the document.

Examination of the Recovered Documents

Examination of Acceptable_Encryption_Policy.doc

This file doe not have the strings of '20' hex at the end of the file and does not contain any "camouflaged" documents.

Examination of Information_Sensitivity_Policy.doc

This file doe not have the strings of '20' hex at the end of the file and does not contain any "camouflaged" documents.

Examination of Internal_Lab_Security_Policy.doc

This document has strings of '20' hex at the end of the document and probably has a something "camouflaged" within it. Further examination showed that this file had no password. All files recovered were checked to see if they had additional files "camouflaged" within them.

The following files were recovered from this document:

Table 12 - Files Recovered from Internal_Lab_Security_Policy.doc

File Name	Md5 Hash
Internal_Lab_Security_Policy.doc	E0C43EF38884662F5F27D93098E1C607
Opportunity.txt	3EBD8382A19C88C1D276645035E97CE9

These files are in Appendices L and M.

Examination of Internal_Lab_Security_Policy1.doc

This file does not have the strings of '20' hex at the end of the file and does not contain any "camouflaged" documents.

Examination of Password_Policy.doc

This document has strings of '20' hex at the end of the document and probably has a something "camouflaged" within it. The hex string containing the password starts at 4B1CC (hex). The password is decoded as follows. All files recovered were checked to see if they had additional files "camouflaged" within them. The password column was decoded by using the table in Appendix K.

Table 13 - Password Decode from Password_Policy.doc

Hex Character	Hex Decoder Pattern	Password (hex / text)
52	02	50 / P
F4	95	61 / a
09	7A	73 / s
51	22	73 / s
7B	0C	77 / w
C9	A6	6F / o
66	14	72 / r
85	E1	64 / d

The following files were recovered from this document:

Table 14 - Files Recovered from Password_Policy.doc

File Name	Md5 Hash
pem_fuelcell.gif	864E397C2F38CCFB778F348817F98B91
Password_Policy.doc	E5066B0FB7B91ADD563A400F042766E4
PEM-fuel-cell-large.jpg	5E39DCC44ACCCDCA7BBA0C15C6901C43
Hydrocarbon%20fuel%20cell%20page2.jpg	9DA5D4C42FDF7A979EF5F09D33C0A444

These files are in Appendices N - Q.

Examination of Remote_Access_Policy.doc

This document has strings of '20' hex at the end of the document and probably has a something "camouflaged" within it. All files recovered were checked to see if they had additional files "camouflaged" within them. The hex string containing the password starts at 34A44 (hex).

Table 15 - Password Decode from Remote_Access_Policy.doc

Hex Character	Hex Decoder Pattern	Password (hex / text)
50	02	52 / R
F0	95	65 / e
17	7A	6D / m
4D	22	6F / o
78	0C	74 / t
C3	A6	65 / e

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The following files were recovered from this document:

Table 16 - Files Recovered from Remote_Access_Policy.doc

File Name	Md5 Hash
Remote_Access_Policy.doc	2AFB005271A93D44B6A8489DC4635C1C
CAT.mdb	C3A869FF6B71C7BE3EB06B6635C864B1

These files are in Appendices R - S.

The Final Check - CamShell.dll

There are two copies of CamShell available. The first has been partially overwritten on the floppy disk image. The second is on the forensic machine from the installation. In order to make a reasonable determination that these are the same file, the remainder of CamShell.dll on the floppy disk image will be exported and a md5 hash calculated for the fragment. The CamShell.dll on the forensic machine will be exported and the first 1000 (hex) bytes (those overwritten by index.htm) will be removed. A md5 hash will be calculated for these remaining bytes. If these hashes match, this is the tool used by RJL.

Table 17 - md5 Comparison of CamShell.dll from Diskette and Installation

File Name	Start Location (hex)	End Location (hex)	Md5 Hash
Extract from v1_5.gz	5200	D1FF	B43FB827CC49F1511F73AC3F08FFFA5B
Extract from CamShell.dll	1000	8FFF	B43FB827CC49F1511F73AC3F08FFFA5B

The program used by RJL was Camouflage.

Analyzing the Timeline

The timeline ends at 4:45 p.m. when the diskette was seized by the security guard from RJL on 26 April 2004.

As the timeline is examined there are two things that stand out. The first is that the Access times are 00:00:00. The second is that the Create time is after the Modification time. Both can be explained.

Under Windows, it is possible to determine the various times that relate to a file. This can be done through opening a DOS command window or right-clicking the file and selecting properties. For this example the DOS command window will be used.

The DIR command has many options that can be displayed by typing "dir /?".

The options for this command are shown below. The options that will be focused on are highlighted.

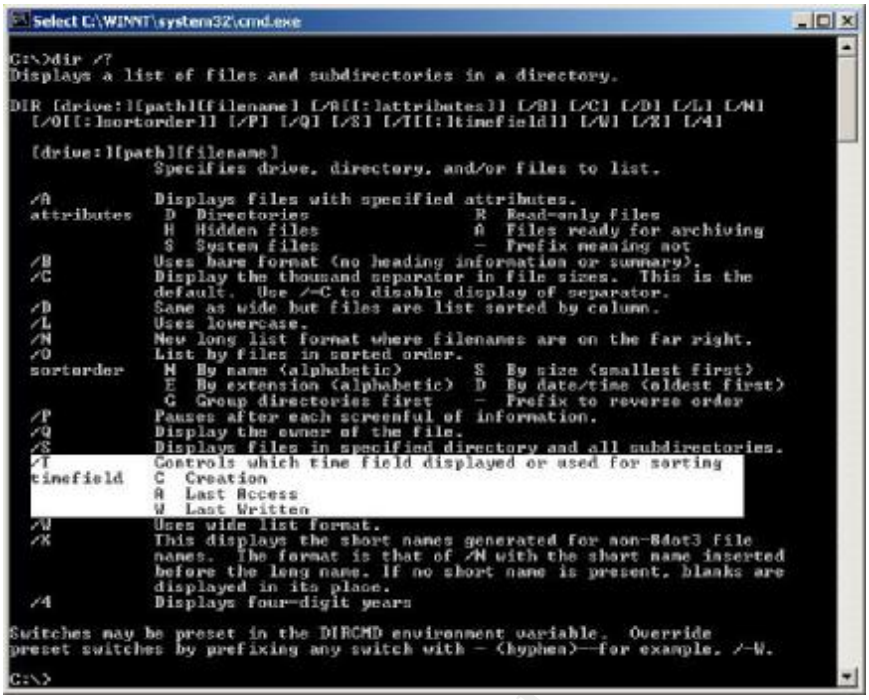


Figure 6 - DOS dir Command Options for Timefield Discovery

Instead of Modified, Accessed, and Created (MAC), Windows has Written, Accessed, and Created (WAC). To illustrate if a file is created on a hard disk, "test1.doc" the commands show the presence of all three of the WAC times.

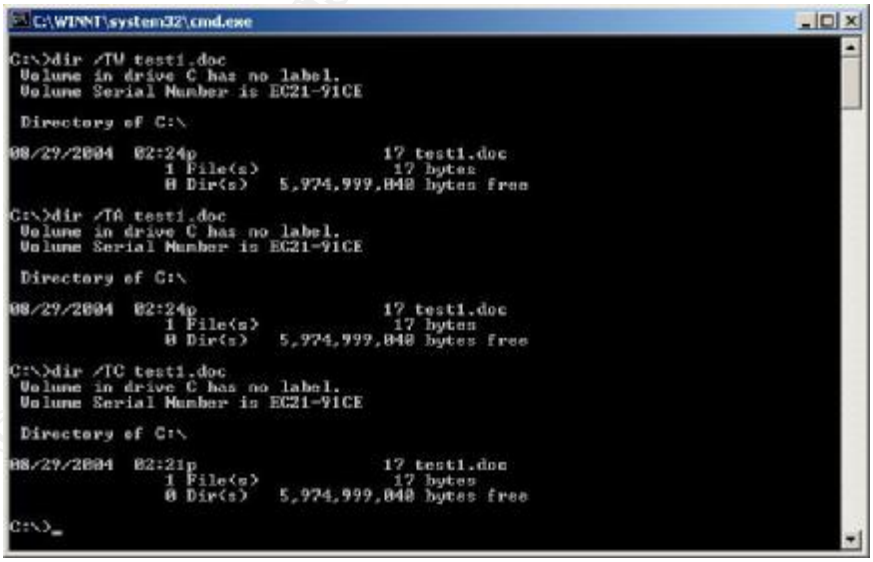


Figure 7 - Timefield Discovery on Test Document - test1.doc (1)

The document times are:

Written time - 2:24 p.m. - After modification, the last write time of this file.
Access time - 2:24 p.m.
Created Time - 2:21p.m. - The time the file was put onto the hard drive.

Note that the Created time is before the Written and Accessed time.

If test1.doc is copied to a floppy disk, here is a screen shot of the times:

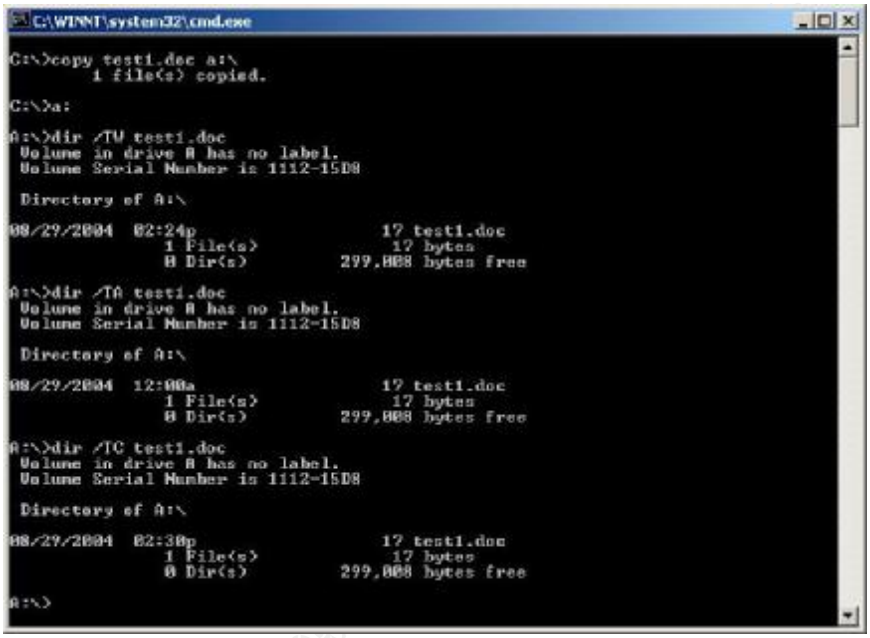


Figure 8 - Timefield Discovery on Test Document - test1.doc (2)

The times are:

Written time - 2:24 p.m. - The same time as the Written time above.
Access time - 12:00 a.m. (effectively 00:00:00)
Created Time - 2:30 p.m. - The time the file was copied onto the floppy disk.

Note that this is exactly the situation that is found on the floppy image. The Written (or Modification) time is earlier than the Creation time. Also the Access time is 00:00:00 because on floppy disks the Access time is not available.

Knowing this information here is the sequence of events.

1. Feb. 3, 2001 CamShell.dll was created - probably by the developers of Camouflage.
2. April 23, 2004 between 10:53 a.m. and 2:11 p.m. all the documents were modified. The three documents that had files within them were "camouflaged" also.
3. April 25, 2004 at 10:53:40 a.m. the floppy disk was formatted and the volume label added.

4. April 26, 2004 at 9:46:18 a.m. CamShell.dll was copied to the floppy diskette.
5. April 26, 2004 from 9:46:20 a.m. to 9:46:44 a.m. all the other files were copied to the floppy disk.

It is still an open question when the files CamShell.dll and index.htm were deleted. Using the test file, "test1.doc", the file was deleted. Since the file was deleted, it is no longer possible to use the DOS dir command. The forensic machine was rebooted to Linux and the floppy imaged using dd. The floppy image was brought into Autopsy and the file information for "_est1.doc" is shown below.

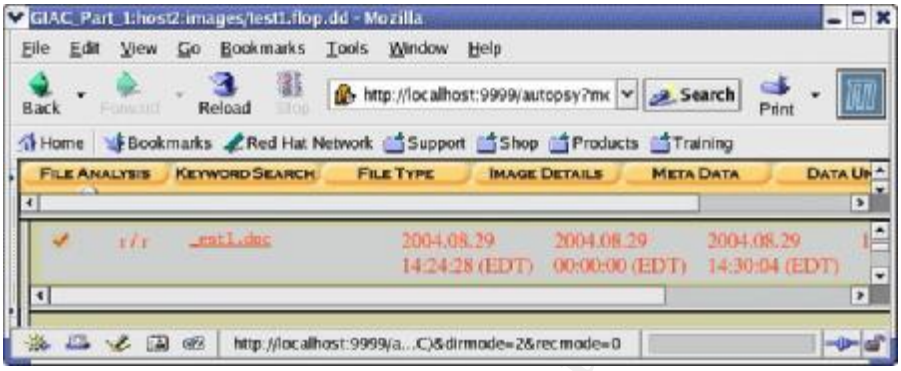


Figure 9 - Autopsy Screen Shot for Deleted test1.doc Showing Timefields

As can be seen the Write time is still 14:24 (2:24 p.m.), the Access time is still 00:00 (12:00 a.m.), and the Create time is still 14:30 (2:30 p.m.). It is impossible to determine the exact time of deletion - even though in the test it was deleted at 3:05 p.m.

The same holds true for CamShell.dll and index.htm. Although it is impossible to determine the exact time, it most likely occurs after the six documents have been copied to the floppy disk (April 26, 2004, 09:46:20 to 09:46:44) and before index.htm is copied to the floppy disk (April 26, 2004, 09:47:36).

Review and Significance of Evidence

It has already been shown that RJL used Camouflage to conceal files on a floppy disk so that they could be removed from the premises of Ballard Industries. All of the documents, including the ones that did not have files within them had metadata strings that indicated that their original author used a copy of Microsoft ® Word registered to Cisco Systems.

The next table summarizes the concealed document findings.

Table 18 - Summary of Recovered Documents and Where Hidden

File Name	Recovered From
Internal_Lab_Security_Policy.doc	Internal_Lab_Security_Policy.doc
Opportunity.txt	
pem_fuelcell.gif	Password_Policy.doc
Password_Policy.doc	
PEM-fuel-cell-large.jpg	
Hydrocarbon%20fuel%20cell%20page2.jpg	
Remote_Access_Policy.doc	Remote_Access_Policy.doc
CAT.mdb	

Putting the documents aside temporarily, the other files will be examined.

Opportunity.txt (Appendix M)

In this short note, with the name of RJL, he says that he has included previously unpublished schematics and a sample of the Client Authorized Table (CAT) database. He will also supply more information and asks for $5,000,000.

> Pro - this definitely seems to point the finger at RJL and if what he says is true, would be grounds for serious charges.
>
> Con - There are a few questions that would need to be answered. Is there a copy of this file (discoverable in allocated or unallocated space) on his PC at work or at home? What discovery has been done on his work PC or those PC's that he has access to that would point to previous information going out of the company? Have his emails been examined? Who are his possible contacts and by what companies are they employed?

pem_fuelcell.gif (Appendix N)

> Pro - This is a schematic, or diagram of the elements of a fuel cell showing inputs and outputs.
>
> Con - The diagram is very high level and does not show enough detail to create a duplicate. It does not show power or electrical requirements. This gif file is available on the Internet on a publicly accessible page. It can be found here: http://www.ballard.com/be_informed/fuel_cell_technology/abouttechnology/how_the_technology_works. It might be possible to determine when this file was placed on the web page - did RJL make this available before it was put on the web? This schematic, without further investigation, has very little value.

PEM-fuel-cell-large.jpg (Appendix P)

Pro - This is another schematic that shows high level details about a PEM fuel cell stack.

Con - Although research did not turn up this particular file, one very similar was found here:
http://www.ballard.com/be_informed/media_resources/image_gallery/full-info/expandedstack.gif

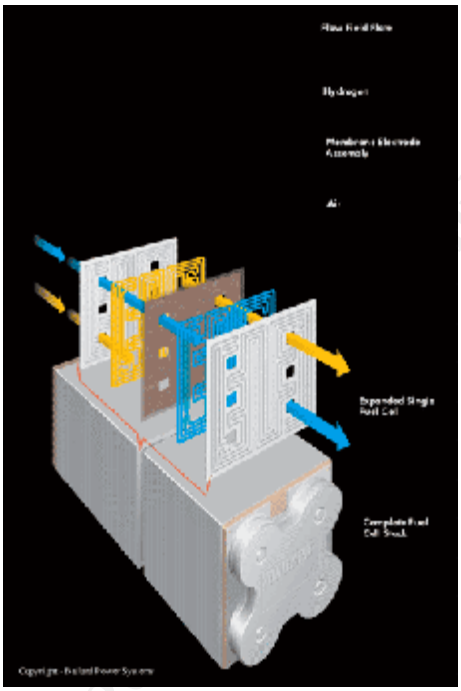


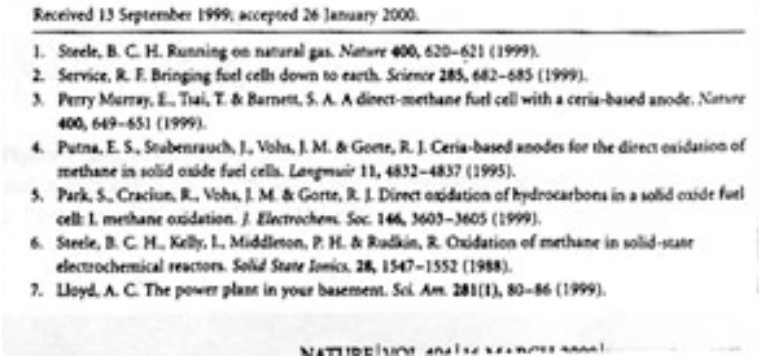
Figure 10 - Similar File to PEM-fuel-cell-large.jpg Found on Internet

The same could be said about this file as was said about the previous one. It does not show power or electrical requirements. This (similar) jpg file is available on the Internet on a publicly accessible page. It might be possible to determine when this file was placed on the web page - did RJL make this available before it was put on the web? This schematic, without further investigation, has very little value.

Hydrocarbon%20fuel%20cell%20page2.jpg (Appendix Q)

Pro - Upon first examination of this file it seems to supply some of the pieces not supplied by the other files. There are chemical specifications and formulae. There are also power density vs. time graphs that show that when certain chemicals are present there are great variations in output.

Con - This is just a scanned image of a published article - and an old one at that.



Received 13 September 1999; accepted 26 January 2000.

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

Figure 11 - Enlarged Portion (Lower Right Corner) of Hydrocarbon%20fuel%20cell%20page2.jpg

The dates on the sources range from 1988 (?) to 1999. The text above the sources says "Received 15 (?) September 1999, Accepted 26 January 2000". This does not seem to be proprietary or much value - especially since the complete text of the article is not included.

CAT.mdb (Appendix R)

Pro - Although the investigator does not have access to knowledge of the infrastructure of Ballard Industries this database sample seems to be a gateway into systems shared by Ballard and the companies in this database. This also seems to indicate that there are customers overseas as well as throughout the United States. By giving out this information, there could be a strong case for theft of proprietary information. An immediate, high priority effort should be made to discover what is at risk here, and what types of accesses are granted by passwords and ID's in the database. Again, examination of his previous email is warranted so that information leaks can be discovered.

Con - until further investigation is done, there is very little information to devalue this file.

All of these files should be located on PC's that RJL has had access to - as previously noted they were copied onto this floppy diskette. There is enough information to institute a complete forensic investigation of all of these PC's.

Policy Review and Implications

All the policies contain this statement which lays out the consequences for policy violations.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

The policies will be reviewed in alphabetical order and the relevant sections noted.

Acceptable Encryption Policy

The section, 1.0 Purpose, clearly gives guidance as to the types of encryption that can be used.

> The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively.

The Camouflage program does not meet these guidelines. The algorithm has not received public review and is easily broken.

The section, 3.0 Policy, gives examples of proven standard algorithms. Camouflage is not noted in the list.

> Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies.

Also in this section is a prohibition against proprietary encryption algorithms.

> The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by InfoSec.

Information Sensitivity Policy

The section, 1.0 Purpose, describes the information covered by this policy.

> The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

Note that electronic information is explicitly covered. This would include information on electronic media - including floppy disks.

The section, 2.0 Scope, discusses the levels of sensitivity. The information discovered would not be considered "Ballard Industries Public" and would fall into the "continuum" of "Ballard Industries Confidential". By possessing the account names and passwords of companies connecting to the Ballard network, the receiver would have access to "Ballard Industries Third Party Confidential" information. The sensitivity of this information is indicated in this excerpt.

> This is confidential information belonging or pertaining to another corporation which has been entrusted to Ballard Industries by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into Bright Industry's network to support our operations.

In sections 3.2 and 3.3, there are more specific guidelines. The information that might be discovered by the receiver of the encrypted document might be considered:

> More Sensitive: Business, financial, technical, and most personnel information

or

> Most Sensitive: Trade secrets & marketing, operational, personnel, financial, & technical information integral to the success of our company.

The penalties are also higher.

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

Internal Lab Security Policy

The section, 2.0 Scope, clearly states that RJL is covered by this policy.

> This policy applies to all internally connected labs, Ballard Industries employees and third parties who access Ballard Industries labs.

The lab manager, unidentified in the case description, is also responsible for security.

> Lab managers are responsible for the security of their labs and the lab's impact on the corporate production network and any other networks.

The section, 3.2 General Configuration Requirements, has several applicable parts. The expectation of privacy for network traffic is removed (3.2.5).

> InfoSec reserves the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls and network peripherals.

Restrictions on the kinds of data that can reside on lab machines are stated (3.2.8).

> Additionally, no Ballard Industries confidential information can reside on any computer equipment in these labs.

Password Policy

The sections, 1.0 Overview, and 2.0 Purpose, clearly state the importance of passwords and the security of those passwords.

> Passwords . . . are the front line of protection for user accounts.
>
> The purpose of this policy is to establish a standard for . . . the protection of those passwords . . .

The section, 4.1 General, covers password storage.

> All production system-level passwords must be part of the InfoSec administered global password management database.

The questions to ask are who has access to this password management database and if prior accesses can be discovered?

The section, 4.2.B Password Protection Standards, defines what should be done immediately if there is a compromise.

> If an account or password is suspected to have been compromised, report the incident to InfoSec and change all passwords.

Remote Access Policy

In order to minimize the impact of incidents on Ballard Industries standards are set for remote access. Damages might be the result of computer incidents.

> Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Ballard Industries internal systems, etc.

Passwords should be protected, even from family members (3.2.2).

> At no time should any Ballard Industries employee provide their login or email password to anyone, not even family members.

Policy Review Summary

It is clear the information discovered in the encrypted CAT database has the potential for serious damage. It is also clear that this incident should kick off a review of security procedures, an audit of the password database, and a forensic examination of the machines in the lab at a minimum.

The policies are well thought out. Specific types of incidents will fall into covered categories and remove ambiguity whether a policy has been violated or not.

Legal Review and Implications

18 U.S.C. §1030

There are several statutes that apply to the situation described earlier. Before these statutes are covered it is helpful to review definitions from these statutes. Non-applicable parts of these statutes will not be included here. From 18 U.S.C. §1030: (http://www.usdoj.gov/criminal/cybercrime/1030_new.html)

> the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device (18 U.S.C. §1030(e)(1))

There are many variations in the definition of a protected computer. This is definition (B).

> the term "protected computer" means a computer . . . which is used in interstate or foreign commerce or communications, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States (18 U.S.C. §1030(e)(2)(B))

In order for RJL to download Camouflage he had to access the Internet. In order for the receiver of the encrypted CAT database to be able to access the accounts and passwords contained in the database, they would have had to access the Internet. These accounts and passwords affect commerce between Ballard Industries and the other companies, domestic and foreign - this satisfies the "interstate or foreign commerce" requirement.

Since the requirements for a "protected computer" have been established, the statutes can be examined with this in mind.

> the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information (18 U.S.C. §1030(e)(8))
>
> the term 'loss' includes any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service (18 U.S.C. §1030(e)(11))

The victim, Ballard Industries, can aggregate the costs of recovery. If the losses are greater than $5,000 in one year the incident is considered a federal crime. (Salgado, R.P., (2004), Forensics Frameworks and Best Practices: Managerial and Legal Issues, 8.5, page 17)

> If the attacker acted intentionally and without permission, then the attacker may be charged with a felony.
> If the attacker "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer," the attacker has committed a felony violation of the law. 18 U.S.C. § (a)(5)(A)(i)
> The maximum penalty for first time offenses is a fine and 10 years imprisonment. The maximum rises to a fine and 20 years for subsequent offenses. 18 U.S.C. § 1030 (c)(4)(A) & (C) (Salgado, R.P., (2004), page 18)

Passwords are specifically covered in this statute. It is a criminal offense to

> knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization (18 U.S.C. §1030(a)(6))

Other statutes besides 18 U.S.C. §1030 can be used for prosecution.

18 U.S.C. §1831 - Economic Espionage

Although this investigation has just begun, one of the possibilities is that RJL is being paid by another company or even a foreign government. If this turns out to be true this statute will apply.

In summary, if this act

> will benefit any foreign government, foreign instrumentality, or foreign agent (http://www.usdoj.gov/criminal/cybercrime/18usc1831.htm)

and the person

(1) steals, or without authorization appropriates, takes, carries away, or conceals . . . a trade secret
(2) without authorization . . . downloads, uploads, . . . , transmits, delivers, sends, mails, communicates, or conveys a trade secret;
(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

shall, . . . be fined not more than $500,000 or imprisoned not more than 15 years, or both. (http://www.usdoj.gov/criminal/cybercrime/18usc1831.htm)

If an organization is the perpetrator the maximum fine will be $10,000,000.

18 U.S.C. §1832 - Theft of Trade Secrets

This statute deals with conversion of trade secrets to benefit anyone other than the owner of the trade secret. The language is similar to 1831. If a person

(1) steals, or without authorization appropriates, takes, carries away, or conceals . . . a trade secret
(2) without authorization . . . downloads, uploads, . . . , transmits, delivers, sends, mails, communicates, or conveys a trade secret;
(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

shall, . . . be fined under this title or imprisoned not more than 10 years, or both. (http://www.usdoj.gov/criminal/cybercrime/18usc1832.htm)

If an organization is the perpetrator the maximum fine will be $5,000,000.

Future Challenges for the System Administrators

Several steps can be taken by system administrators to decrease the possibilities of this happening again.

1. There should be an immediate access review of everyone who has access to Ballard's Client Authorized Table (CAT) database. Those with improper access should be removed and everyone else should change their password.
2. A review should also be done on all accesses to that database within the past six months. It is possible that someone with proper access supplied RJL the accounts and passwords.
3. A review of all system entry screens should be done to ensure they are properly bannered. The notice should be very clear so that anyone who enters the systems should be warned that it is illegal to continue it they are not authorized. The legal

department should review the text of these banners. It should be made clear there is no expectation of privacy on the use of these systems.

4. Some research should be done and the sites that allow download of hacker and encryption tools should be blocked.
5. If Ballard uses an automated software update program such as Microsoft's SMS, the capability of these systems to scan the network for specific executables should be used to find all instances of Camouflage.exe on the network. The users of these machines should be included in the investigation.
6. All documents on RJL's machines should be checked to see if any more use of Camouflage could be detected.

Internet Resources

Company Resources

http://www.ballard.com - site for Ballard Power Systems

Legal Resources

http://www.usdoj.gov/criminal/cybercrime/1030_new.html - text of the statute for Fraud and Related Activity in Connection With Computers, 18 U.S.C. 1030

http://www.usdoj.gov/criminal/cybercrime/18usc1831.htm - text of statute for Economic Espionage, 18 U.S.C. 1831

http://www.usdoj.gov/criminal/cybercrime/18usc1832.htm - text of the statute for Theft of Trade Secrets

Software Resources and Tools

http://camouflage.unfiction.com/Overview.html - site used to download Camouflage software for this investigation

http://home.sol.no/~espensa/khexedit - the source for the hex editor that was used with Red Hat version 9

http://www.fact-index.com/t/tr/truth_table.html - this site explained the bit changes that happened if various operations were performed on data

http://www.guillermito2.net/stegano/camouflage/index.html - article confirming this paper's method for breaking Camouflage software

http://www.symantec.com - anti-virus scanning software to ensure that the examination of evidence does not damage the examiner's workstation

http://www.winhex.com - a Windows hex editing software useful in forensic examinations

Part 2 - Option 1: Perform Forensic Analysis on a System

Starting the Project

Shortly after I returned from GIAC conference in Chicago, the article, portions included below, appeared on MSNBC. (http://msnbc.msn.com/id/5173972/)

> For sale by public auction -- juicy laptop secrets
> By Bernhard Warner
> http://www.reuters.com/
> Updated: 5:39 p.m. ET June 09, 2004
>
> LONDON - Laptops containing sensitive financial details and all manner of corporate secrets can be snapped up at auctions for a pittance, a security firm revealed on Wednesday.
>
> Stockholm-based Pointsec Mobile Technologies said it bought 100 laptop computers from a host of Internet and public auctions over the past two months.
>
> The exercise intended to demonstrate that the scores of lost or stolen laptops that wind up at auction every day have hard drives with little or no security, giving identity thieves and fraudsters easy access to lucrative data.
>
> What it did not expect to find was a cache of corporate laptops that were as easy to crack as grandma's PC.
>
> In all, the firm's technicians were able to pull sensitive details from 70 of the 100 machines it bought.
>
> In one case, it obtained a particularly vulnerable hard drive from online auction site eBay that apparently once belonged to one of Europe's largest insurance companies.
>
> On the hard drive were current details of customers' pension plans, payroll records, personnel details, login codes and administration passwords for the company's Intranet site. Home addresses, telephone numbers and dates of birth of customers were also listed in 77 Microsoft Excel files, the company said.
>
> . . .
>
> "Pointsec's research demonstrates just how easy it is to access information which is not adequately protected," said Tony Neate of Britain's National Hi-Tech Crime Squad.

Acquiring the Hard Drive to Be Examined

Because of this article, I thought it might be relatively easy to buy a hard drive or two on eBay. [1] So I looked at eBay for auctions with the following characteristics:

[1] www.eBay.com

- The seller shouldn't have a lot of similar auctions of computer equipment going on at the same time or in the recent past.
- There should be no indication in the description that the drive has been cleaned or sanitized.
- Multiple drives for sale are as good as single drives.
- The price should be reasonable.

After searching for a short while this auction caught my eye:

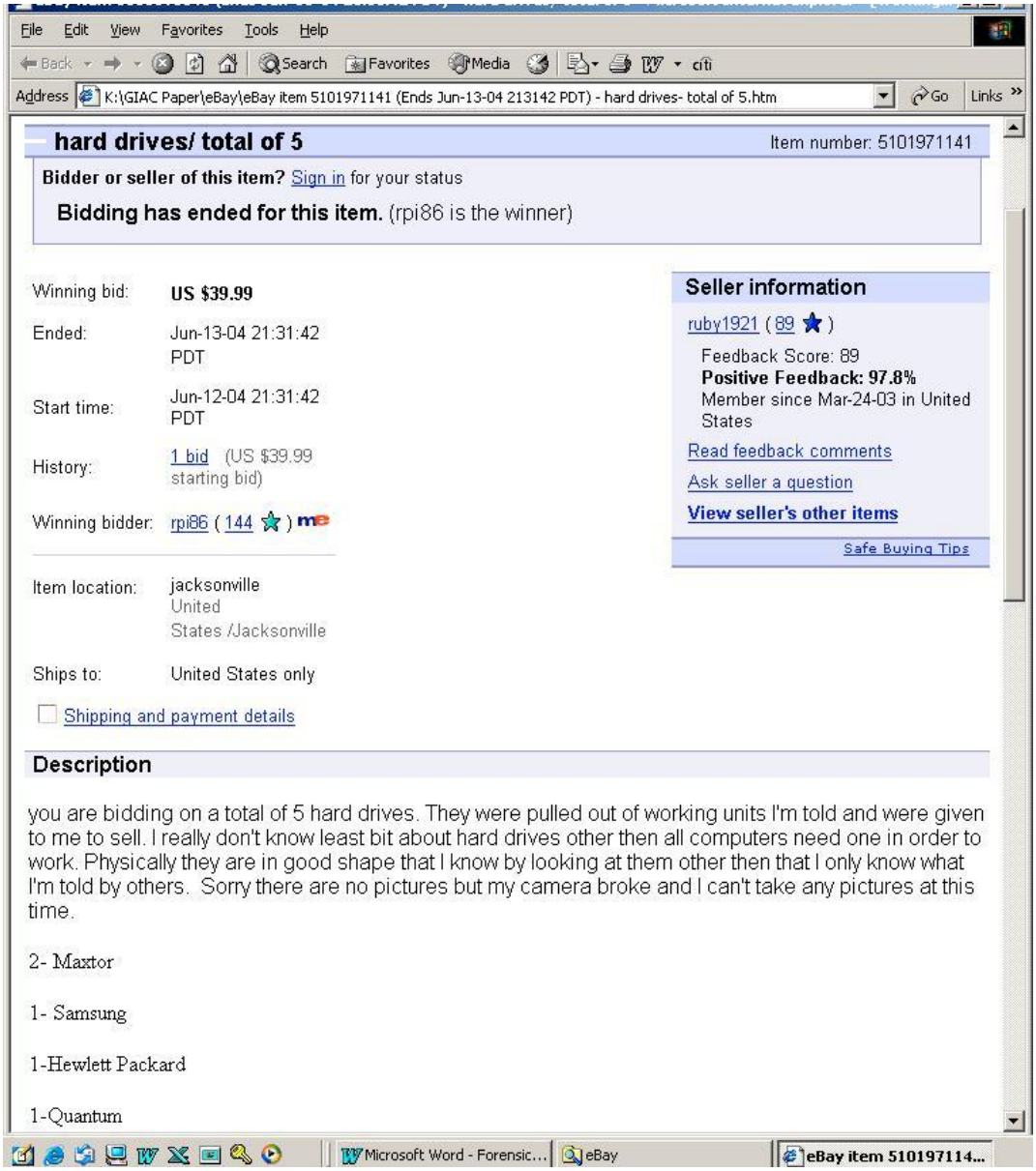


Figure 12 - eBay Auction results for Purchase of Hard Drives

A friend bought them for me and they arrived on June 18. Note that the bidding started June 12 and ended June 13. The last day I would expect to see any drive activity would

be several days before June 12. Of all the drives, the only one that was usable was one of the Maxtor drives. The drive turned out to be an LXT213A.

Starting the Physical Examination

In order to ensure that the jumper settings were correct I went to the Melron Electronics site [2] where I was able to find what was needed. Here is an excerpt from this page:

LXT213A CAP=213MB, CYL= 683, HDS=16, W/P=0, L/Z= 683, SPT=38, **T=3**

TABLE 3
JUMPER SETTINGS FOR J6
SINGLE DRIVE - NO JUMPERS INSTALLED
MASTER DRIVE - JUMPER PINS 7 & 8
SLAVE DRIVE - JUMPER PINS 1 & 2

Here is the bottom of the drive with J6 indicated by an arrow.

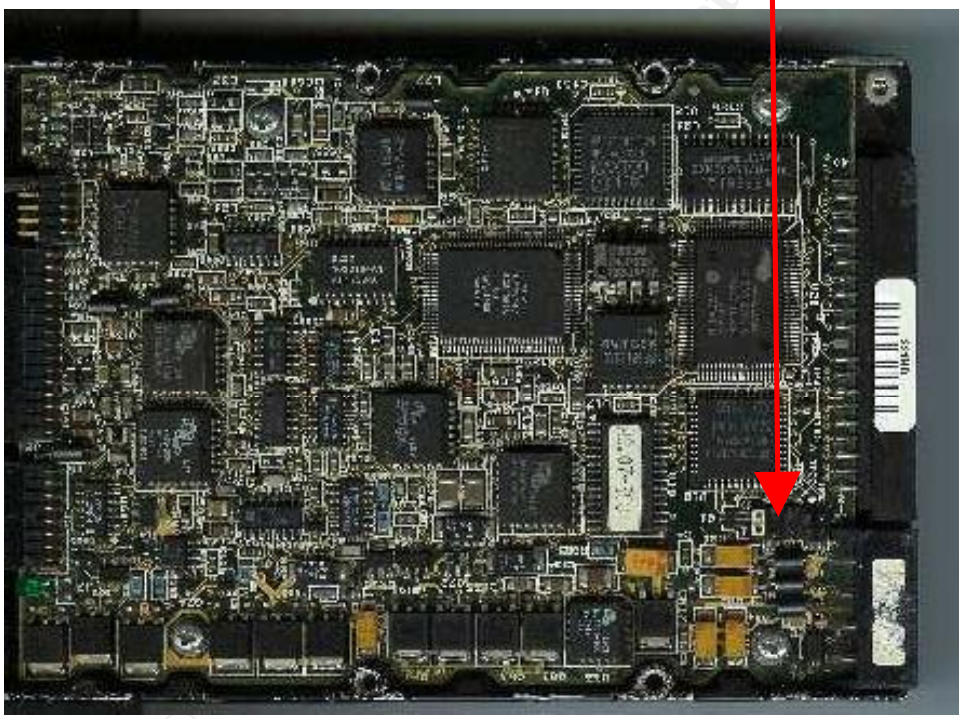


Figure 13 - Bottom of Hard drive Selected for Analysis Showing Jumper for Master / Slave

The jumper is in place indicating that this is configured as a slave.

Because this drive is about 1½ inches tall, it would not fit into my removable drive bay. In order to image the drive I had to remove the case and lay the computer on its side. The

[2] http://www.melron.com/Maxtor.html

power and IDE cable of the removable drive bay were removed and connected to the Maxtor drive. A protective sleeve was made of cardboard to avoid electrical shorts.

Figure 14 - Maxtor Drive in Protective Cardboard Sleeve

This drive was given an evidence tag and description as follows:

- Tag # 009
- Maxtor Hard Drive, Model LXT213A, Serial Number: 2D05009441. Size: 213 Mb

The Acquisition of the Drive

Mounting details for hard drive in Forensic machine 2 for imaging
- remove cover
- remove IDE cable and power from removable drive housing
- boot to Linux on LinuxStorage
- run fdisk to determine size and configuration of the hard drive (only the part of the output relating to the (to-be examined) hard disk is included).

fdisk -l /dev/hdd

Disk /dev/hdd: 212 MB, 212615168 bytes
16 heads, 38 sectors/track, 683 cylinders
Units = cylinders of 608 * 512 = 311296 bytes

Device	Boot	Start	End	Blocks	Id	System
/dev/hdd1	*	1	682	207309	6	FAT16

The program md5 is run to get a hash of the drive:

md5 /dev/hdd1
53ac7407e7cabd1db281884aa59474bf /dev/hdd1

Appendix A gives information about the partitions found on the drive.

The LinuxStorage machine is restarted and a File Allocation Table (FAT) partition is created to hold the image using PartitionMagic ® Version 8. When this is complete, the machine is restarted in Linux and fdisk is run to determine the drive partition information so that the drive to be examined can be mounted and imaged.

```
  fdisk -l /dev/hdb
Disk /dev/hdb: 120.0 GB, 120034123776 bytes
255 heads, 63 sectors/track, 14593 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

Device     Boot   Start     End     Blocks       Id  System
/dev/hdb1 *        2       14593  117210240    f   Win95 Ext'd (LBA)
/dev/hdb5          2        2551   20482843+   7    HPFS/NTFS
/dev/hdb6          2552     13317   86477863+  83 Linux
/dev/hdb7          13318    13573   2056288+   6    FAT16
/dev/hdb8          13574    13957   3084448+   b    Win95 FAT32
/dev/hdb9          13958    14467   4096543+   b    Win95 FAT32
/dev/hdb10         14468    14593   1012063+   b    Win95 FAT32
```

We see that the partition we want is /dev/hdb7.

The partition is mounted and checked with fdisk:

```
mount -t vfat /dev/hdb7 /mnt/image
fdisk -l /dev/hdb7

Disk /dev/hdb7: 2105 MB, 2105639424 bytes
255 heads, 63 sectors/track, 255 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
```

Before adding any data to the partition, it is cleansed by using dd to write zeros to the whole partition.

```
dd if=/dev/zero of=/dev/hdd1
```

Note that /dev/zero is a special Linux device, that when used as an input file, produces nulls.

A directory was created to hold the image in /mnt/storage named Drive_9.

```
Mkdir /mnt/storage/Drive_9
```

In order to capture the image and put it in the desired location dd is used:

```
dd if=/dev/hdd1 of=/mnt/storage/Drive_9/Drive_9.img
414618+0 records in
414618+0 records out
```

The program md5 is used to ensure that the image is a perfect copy of the hard drive.

```
md5 /mnt/storage/Drive_9/Drive_9.img
53ac7407e7cabd1db281884aa59474bf       /mnt/storage/Drive_9/Drive_9.img
```

And it since the md5 hashes match it is a perfect copy.

The next step is to ensure that the image cannot be written to by changing all of the permissions to read-only:

```
chmod 444 Drive_9.img
```

This command changes the file permissions so that the file may not be written to or changed in any way throughout the forensic process.

The file command was also used to discover more information about the image.

```
Drive_9.img: x86 boot sector, code offset 0x3e, OEM-ID "MSWIN4.0",
sectors/cluster 8, root entries 512, Media descriptor 0xf8, sectors/FAT
203, heads 16, hidden sectors 38, sectors 414618 (volumes > 32 MB) ,
serial number 0x31500fd5, label: "           ", FAT (16 bit)
```

The Original Equipment Manufacturer-ID (OEM-ID) is MSWIN4.0. Checking the Windows 95a Boot Sector page (http://home.att.net/~rayknights/pc_boot/w95aboot.htm) gives Windows 95 - the type of operating system that has this for an OEM-ID.

FAT stands for File Allocation Table, an early Microsoft file system. From the information above:

number of root entries = 512
number of sectors / drive = 414,618

Looking at the captured image:

length of Drive_9.img = 212,284,416

By doing a little math we can determine the cluster and sector size (sector is the smallest data unit):

bytes / sector = 212,284,416 (length of image) / 414,618 (number of sectors) = 512
sectors / cluster = 8
bytes / cluster (FAT) = 512 * 8 = 4096

Therefore we will have 414,618 'data units' or inodes on this drive.

Since a forensic image was obtained, one of the first tasks is to determine which operating system is on the hard drive. Since we know that the captured drive has a FAT partition

we know that it could be almost any Microsoft operating system. The question to be solved is which operating system version is it?

Before this question can be answered Autopsy was used to analyze the image and perform as much data collection as possible

Autopsy has log files that show what operations were performed. On my forensic computer, the logs can be found here:

/mnt/analysis/Drive9/Host_9/logs

The log from which extracts will be taken is:

rlb.exec.log

Extracts from these logs can be found in Appendix B along with explanations of what is being done.

Which Operating System Version?

Returning to the question of which Microsoft operating system is on this hard drive, I used Autopsy to look at the files in the root directory. Selecting the option for File Analysis the following files were listed:

AUTOEXEC.BAT
AUTOEXEC.DOS
BOOTLOG.TXT
COMMAND.COM
COMMAND.DOS
CONFIG.DOS
CONFIG.SYS
DBLSPACE.000
DBLSPACE.BIN
DBLSPACE.INI
DRVSPACE.BIN
FAILSAFE.DRV (dir)
IO.DOS
IO.SYS
MSDOS.DOS
MSDOS.SYS
RECYCLED (dir)

Two clues were apparent. This was a Win9x system (probably Windows 95 because of the dates on the files. COMMAND.COM had a create date of 1995.07.11). Since

DBLSPACE.000 was present, the drive was probably compressed. DBLSPACE.000 had a length of 196,843,926.

In order to verify the version of the O.S. I displayed the strings in COMMAND.COM and discovered this:

> Windows 95. [Version 4.00.950]

Here was the answer to the question about the version. I also verified that this was the original manufacturer's version by checking this site:

> http://users.iafrica.com/c/cq/cquirke/win95ver.htm

Now that the version was revealed the various files created by Autopsy were examined and a few discoveries were brought to light.

One of the things that can be done by Autopsy is to create a time line of events happening to the file system on a drive. This information is stored in:

> /mnt/analysis/Drive9/Host_9/output/Drive9.timeline

The file Drive9.timeline contained only 967 lines.

The first group of lines has the date Dec. 31 1969 and is the date when the files in the root directory were created. This date is impossible because PC's were not even invented until 1981 so possibly the clock was not set until sometime later.

In order to understand the timeline file it is helpful to look at three entries for a single file. The second file on the list is COMMAND.COM. Here are the entries for that file:

	Length		Permissions			
Timestamp / Filename		MAC Time		User	Group	Inode
Tue Jul 11 1995 09:50:00 C:/COMMAND.COM	92870	m..	-/-rwxrwxrwx	0	0	8
Wed Dec 23 1998 00:00:00 C:/COMMAND.COM	92870	.a.	-/-rwxrwxrwx	0	0	8
Wed Dec 31 1969 19:00:00 C:/COMMAND.COM	92870	..c	-/-rwxrwxrwx	0	0	8

The fields to be examined here are the MAC Times. These are called MAC times because MAC stands for Modification, Access, and Change times. The MAC Time definitions come from page167, Unix Forensics 8.2 8.3.

Modification Time (m..)- last time a file was written. This date is 7/11/95 and is the date assigned by Microsoft for files in this operating system.

Access Time (.a.) - last time a file was read. It might be thought that this is the date of the last bootup. But since there are dates before and after Dec. 23, 1998 this is not the case. Other events around that time will have to be checked to see what was happening.

Change Time (..c) - last time the contents were written. This date is the last time the file was changed. This is not the correct time because PC's were not invented until 1971.

By doing a little data mining on the timeline it becomes apparent that this machine might have had an earlier version of one of Microsoft's operating systems. Often when products are upgraded the old files are renamed rather than deleted so the user can return to the original system if there is a problem. There are two ways to see if this happened on this machine. The Windows operating systems typically allocate inodes for files sequentially. This means that if the time line is sorted by inode then if the file has not been deleted, and later files have higher inodes than earlier files. Let's to back to our earlier example of COMMAND.COM.

The inode for COMMAND COM is 8. If the timeline is brought into Microsoft ® Excel and sorted by inode number there is another file that stands out. Here are the MAC times for that file.

	Length		Permissions			
Timestamp / Filename		MAC Time	User	Group	Inode	
Wed Mar 10 1993 06:00:00 C:/COMMAND.DOS	52925	m..	-/--wx-wx-wx	0	0	6
Thu Dec 03 1998 00:00:00 C:/COMMAND.DOS	52925	.a.	-/--wx-wx-wx	0	0	6
Wed Dec 31 1969 19:00:00 C:/COMMAND.DOS	52925	..c	-/--wx-wx-wx	0	0	6

Modification Time (m..)- last time a file was written. This date is 3/10/93. Could this be the date assigned by Microsoft for files in this operating system?

Access Time (.a.) - last time a file was read. It might be thought that this is the date of the last bootup. But since there are dates before and after Dec. 3, 1998 this is not the case. Other events around that time will have to be checked to see what was happening.

Change Time (..c) - last time the inode contents were written. This date is the last time the file was written. This is not the correct time because PC's were not invented until 1981.

Looking at the strings within this file this is found:

> Microsoft(R) MS-DOS(R) Version 6
> (C)Copyright Microsoft Corp 1981-1993.

From this information it is possible to see that the drive started life running MS-DOS version 6 and was upgraded to Windows 95.

The versions of Command.Com are described here (http://home.earthlink.net/~rlively/MANUALS/VERSIONS/INDEX.HTM) and note that COMMAND.COM in the image is the OEM retail version of Windows 95. If the Year 2000 fix had been applied, the date would be 3/23/1998. This site also confirms that COMMAND.DOS (Renamed from COMMAND.COM) is from DOS v6.0.

Analyzing DBLSPACE.000

The largest file on the drive is DBLSPACE.000
General information on DBLSPACE.000 can be found here:

> http://www.geocities.com/politalk/dos/dbldos.htm

Two pieces of information are significant to understanding how the data is stored within DBLSPACE.000.

From Byte (http://www.byte.com/art/9402/sec6/art1.htm) magazine there is a description of how DoubleSpace compression works.

> Instead, DoubleSpace and other real-time disk compressors use a sliding dictionary form of LZ compression, no matter what kind of data the file contains. To shrink a file, the compressor looks for repeating patterns. It then replaces each pattern with a pointer that refers back to an earlier occurrence of the same pattern, as well as a token that specifies the length of the pattern. Later, when the file is decompressed, the pointers and tokens are replaced with the original patterns.
>
> Microsoft cites this example: "the rain in Spain falls mainly on the plain." Counting spaces and the period, this phrase normally requires 44 bytes. But it contains several repeating patterns, including ‘ain’ and ‘the’. DoubleSpace would encode the phrase as follows:
>
> > the rain [3,3]Sp[9,4]falls m[11,3]ly on [34,4]pl[15,3].

Bracketed numbers represent pointers and tokens, so [9,4] tells DoubleSpace to replace the pointer (9) and token (4) with the four-character pattern that begins nine characters before the pointer.

The result: The compressed version requires 37 bytes instead of 44. That's not an enormous saving, but the method works much better on database files, whose fields are padded with lots of spaces, and on graphics files that have large areas of solid color. (The algorithm does not care whether the patterns of bytes represent ASCII characters or any other kind of data.)

This method is known as sliding dictionary because the compressed data itself contains the "dictionary" of patterns that's later used to reconstruct the file and because the compressor works its way through the file using a fixed-size sliding window. In other words, the compressor will not scan backward through the entire file to locate a matching pattern; it searches only a window of bytes that slides through the file during compression. The size of that window usually ranges from 2 to 8 KB. (DoubleSpace's sliding window is about 4 KB.)

The second piece of information talks about how files are stored in dblspace.000.

This is from the DUX Computer Digest (http://www.duxcw.com/dcforum/DCForumID6/381.html).

Drive storage is build up in clusters.
One cluster can literally house ONLY ONE file, even if more files will physically fit in that cluster. (32Kb on FAT-16 means 31Kb lost when placed a 1Kb is file in it)
As you see, with small files, there is wasted space!
There comes DoubleSpace, and later on DriveSpace.
This is what happens when you use one of those:

1 A small piece of drive will be left intact, the rest will be used to house ONE gigantic file. (dblspace.000)
2 The label is renamed so the operator can determine the way the drive was used
3 Inside that large file, your complete contents of your hard drive is stored **head-to-tail**, so there is NO wasted space by almost empty clusters.
4 In the OS, in conjunction with the statements in Config.dos and Autoexec.dos there will be a conversion shell started who "Creates" a virtual disk and links the file "dblspace.000" to it.
5 The normal disk "C" will be moved to drive "D".
6 The virtual disk becomes the new "C".

Head-to-tail is highlighted because slack space is dramatically reduced by Double-Space. This prevents unallocated space from appearing in dblspace.000.

After searching for on the Internet about three weeks on ways to extract data from DBLSPACE.000 using forensically correct methods this link produced some ideas:

http://www.guidancesoftware.com/support/EnCaseForensic/version4/acquisition.shtm

Encase, from Guidance Software is not available but Guidance recommends using the native Windows 95 tools to make the data available. Here are the steps followed.

1. After DD was used to capture the original image and Autopsy was used to analyze the data, it is possible to export DBLSPACE.000 and verify the integrity by creating a md5 hash. The hash is:

   File: C:/DBLSPACE.000
   MD5 of file: efb213e3c4679d7c5fc39c6ee5f40cd0

2. The DBLSPACE 000 file was burned to a CD so that it could be moved between the Linux machine and the Windows 95 machine. Again the md5 hash was calculated using md5.exe from maresware.com to make sure the file had not changed.

   Done with md5 maresware,com
   Program started Wed Jul 21 02:40:08 2004 GMT, 18:40 PST (-8*) (timezone not set)
   DBLSPACE.000 EFB213E3C4679D7C5FC39C6EE5F40CD0

   In order to extract the files it was necessary to mount the compressed drive. A clean copy of Windows 95 was created using VMWare and these steps followed.

   Start Programs -> Accessories -> System Tools -> Drivespace

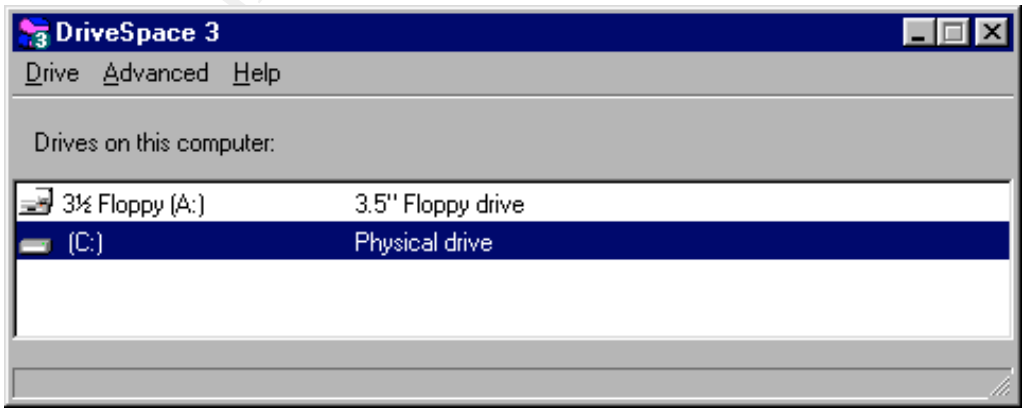


Figure 15 - Drivespace Initial Screen Showing Drives A: and C:

Only drives A: and C: are visible.

Click Advanced -> Mount and the file C:\dblspace.000 will be found.

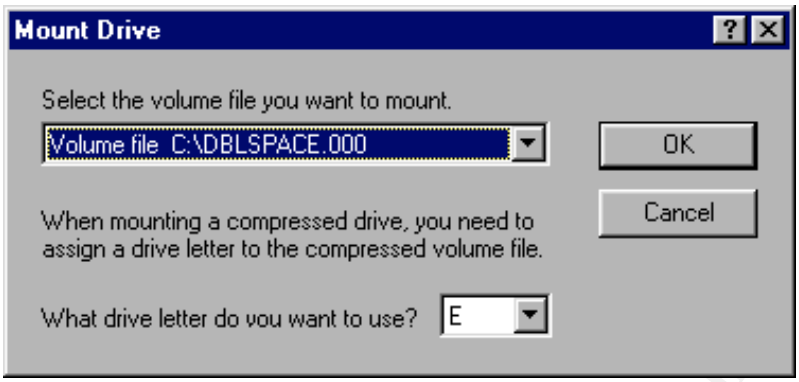


Figure 16 - Drivespace Mount Drive Screen

Click OK.

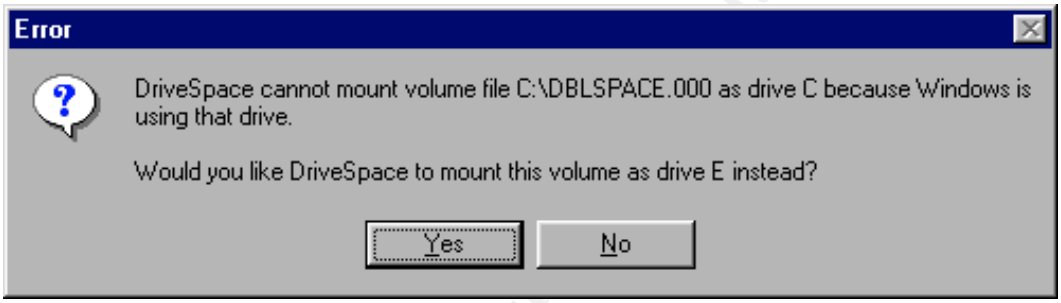


Figure 17 - Drivespace Error Screen

Click Yes

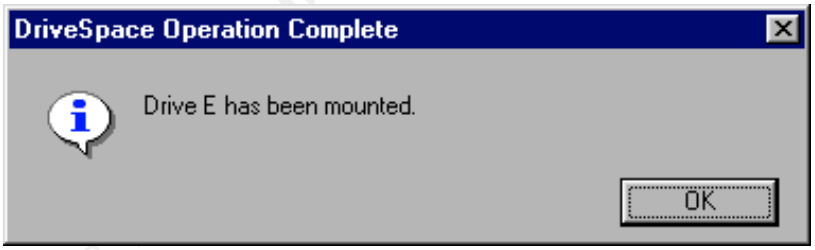


Figure 18 - Drivespace Mount Screen for Drive E:

Drive E: is now mounted.

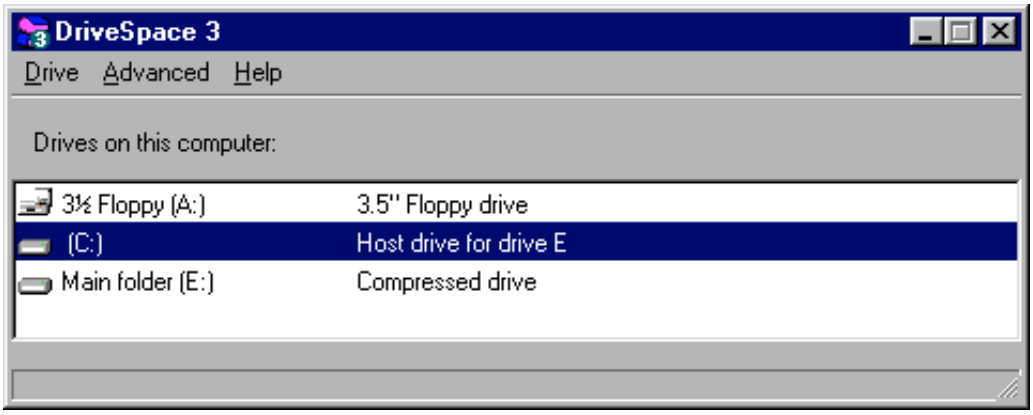


Figure 19 - Drivespace Showing Drives A:, C:, and E:

3. Net Watcher is started so that drives C: and E: can be shared. This is necessary so that they can be mounted under Linux.

Start Programs -> Accessories -> System Tools -> Net Watcher

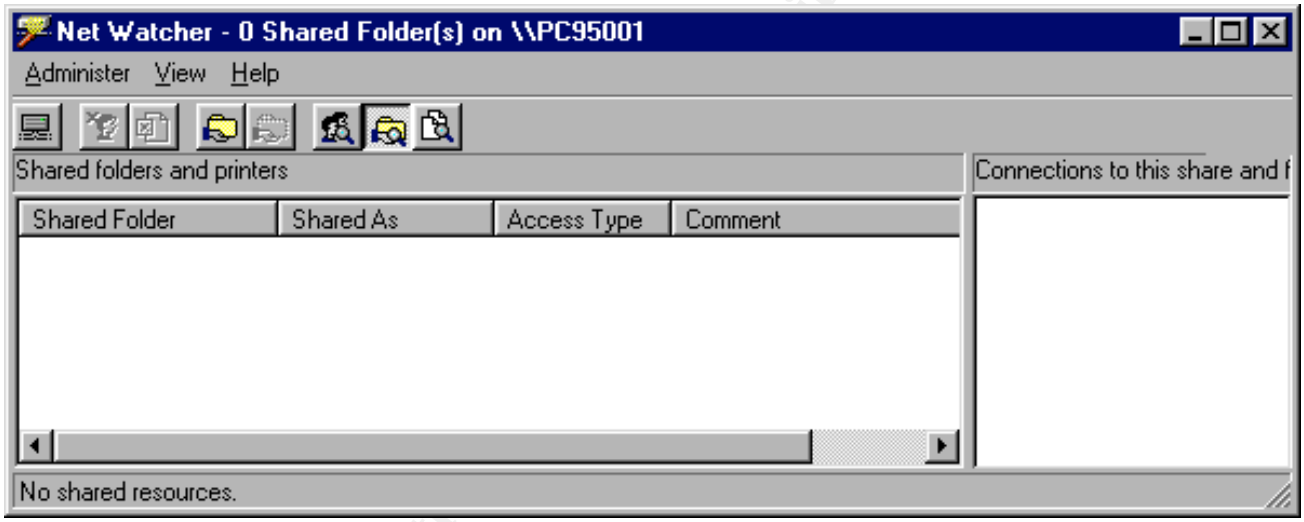


Figure 20 - Net Watcher Screen for Drive Sharing

Drive E: is shared. Drive C: is shared the same way.

Administer -> Add Shared Folder

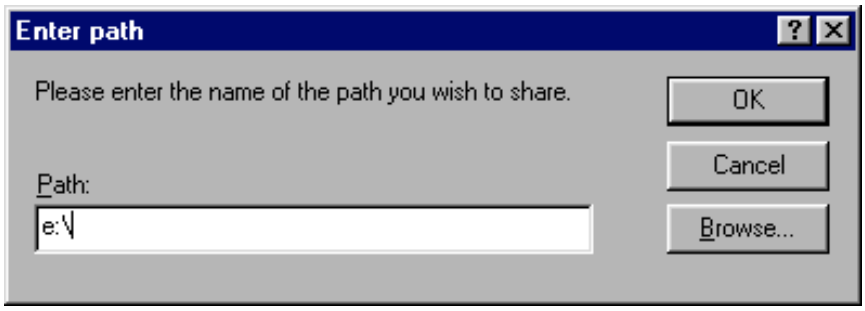


Figure 21 - Net Watcher Screen for Entering Path for Shared Drive

Click OK

The share name and a password are set.

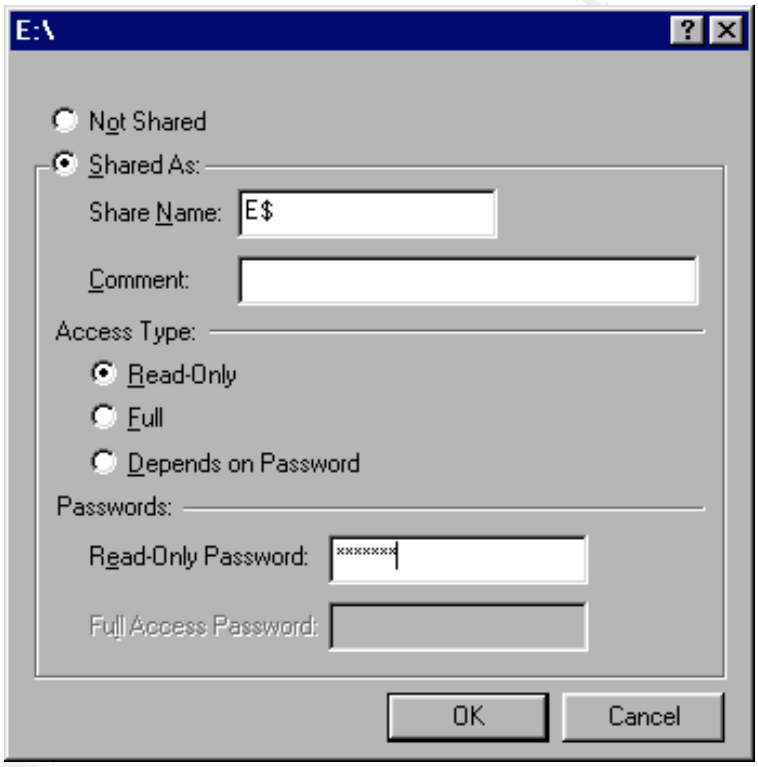


Figure 22 - Net Watcher Password and Share Name Screen

Click OK

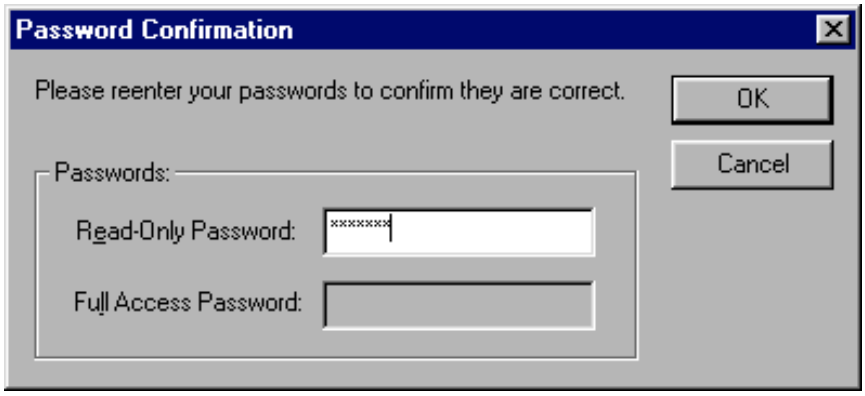


Figure 23 - Net Watcher Set Password Screen

Click OK

When this is complete for Drives C: and E: they are mounted on LinuxForensics using VMWare. These commands are used to mount them so that Linux could see these drives.

mount -t smbfs -o ro,noexec,username=RLB,password=xxxxx //PC95001/c$ /mnt/w95

mount -t smbfs -o ro,noexec,username=RLB,password=xxxxx //PC95001/e$ /mnt/w95_e

4. Using the Linux command mirrirdir, a mirror was created of the uncompressed drive on file system shared between LinuxForensics (as /mnt/analysis) and LinuxStorage (as /mnt/storage). Drive C: was done in the same way.

   mirrordir /mnt/w95_e /mnt/analysis/compressed_drive_e

5. On LinuxStorage a CD image of this directory, **e.cd**, was created with mkisofs.

   mkisofs -R -o /var/tmp/**e.cd** /mnt/storage/compressed_drive_e/

6. After the CD image was created, it was burned to a CD with cdrecord.

   cdrecord -v speed=2 dev=0,0,0 -data /var/tmp/**e.cd**

The CD can be used as a read-only copy of the now uncompressed drive E:.

After the uncompressed drive was unmounted and returned to its compressed state as a file, file name was now dblspace.001 and another md5 hash was done and found to be different (0E9D2DC413A990FF863488DDE2B242CE). The question that had to be answered was, what step in the process caused the change in the file so that the hash was different?

Was the change from the mount by DriveSpace, the sharing by Net Watcher, or by mounting from Linux?

Dblspace.001 was deleted and recopied from the CD. Another md5 hash was done and found to be the same as the original one (EFB213E3C4679D7C5FC39C6EE5F40CD0). Then Drive Space was used to mount the file and then unmount it. The md5 hash was different from the original but the same as the hash taken from dblspace.001 (0E9D2DC413A990FF863488DDE2B242CE).

Dblspace.001 was remounted and shared out using Net Watcher, and then mounted with Linux. The process was reversed and the md5 hash had not changed from the previous check (0E9D2DC413A990FF863488DDE2B242CE). That told me that it was the first Drive Space mount that effected the change.

Did this mount affect the contents of the expanded drive? The whole process was done again – the results follow.

The whole sequence of steps was redone and a second CD created. These steps were done:

1. Start Windows 95 and mount the compressed drive.
2. Open Net Watcher and make sure drive E: is shared.
3. Mount drive E: under Linux.
4. Use mirrordir to create a second copy of drive E: in /mnt/analysis/compressed_drive_e_2
5. Use mkisofs to create a second CD image for burning onto a second CD: mkisofs -R -o /var/tmp/**e.2.cd** /mnt/storage/compressed_drive_e_2/
6. Burn the image to a CD using cdrecord: cdrecord -v speed=2 dev=0,0,0 -data /var/tmp/**e.2.cd**
7. Do md5deep -r on both CD's and save the results to files md5.1.txt (first CD) and md5.2.txt (second CD).
8. Do md5 on the two files created in step 7:
   md5.1.txt
   62c7a001249fd87032c54c6cdf92530d md5.1.txt
   md5 md5.2.txt
   62c7a001249fd87032c54c6cdf92530d md5.2.txt

This means that the two files, each containing uncompressed copies of drive E are identical – md5.*.txt contains md5 hashes of every file in that directory.

Although this solves the problems of getting the files from the compressed directory, it does not solve the problem of getting the MACtimes of the files. Retrieving MACtimes require an image file, not a directory.

Several strategies were tried. The first was to see if a version of dd.exe was available that worked under Windows 95. None was found that worked under Windows 95.

The second was to try dd from within Linux. When the compressed drive is shared over a samba (SMB) connection, it is seen as a directory rather than as a file or volume and cannot be imaged.

The third attempt was successful. The compressed drive would be decompressed, and then the image of the machine would be burned to a CD. The Linux tools could be used to analyze the drive image. These steps followed on a spare 2-gigabyte hard drive. The original image was not modified in this procedure.

A 500-megabyte partition was created on the drive using PartitionMagic version 8 and formatted it as FAT. Then dd was used sanitize the drive by writing zeros to the partition.

This drive will be /dev/hdd - a drive in a removable drive bay.

```
fdisk -l /dev/hdd

Disk /dev/hdd: 2111 MB, 2111864832 bytes
64 heads, 63 sectors/track, 1023 cylinders
Units = cylinders of 4032 * 512 = 2064384 bytes

Device Boot    Start       End    Blocks   Id  System
/dev/hdd1          1       254    512032+   6  FAT16
```

The partition was sanitized by writing zero's to it.

```
dd if=/dev/zero of=/dev/hdd1
dd: writing to `/dev/hdd1': No space left on device
1024065+0 records in
1024064+0 records out
```

dd was used to put the image onto the new fat16 partition

```
dd if=Drive_9.img of=/dev/hdd1
414618+0 records in
414618+0 records out
```

Using the File command on the image gives this result:

```
file Drive_9.img
Drive_9.img: x86 boot sector
```

After putting the image on the drive, the drive was put into an old Dell 166. The machine was booted and a DOS box opened. The version of OS was verified to be the same as above. It should be noted that booting the drive does change files and file dates but since

all the files were already burned to two copies of a CD and the original image was captured in Autopsy it will not be a problem.

Since both DRVSPACE and DBLSPACE files were found on the machine it was necessary to understand what needed to be done to uncompress the drive. The hard drive used for this was put into the NEC desktop and booted. The following sequence was done.

After searching for dblspace.bat or drvspace.bat it was discovered that DRVSPACE.EXE needed to be run from within Windows. Shortly after the process started a message popped up stating that scandisk.exe needed to be run. After scandisk ran, DRVSPACE continued to run for a couple of hours until it finished. After this was complete dd was used to capture another image.

Now that the image has been uncompressed, a new image was captured from the formatted and reloaded hard disk:

```
fdisk -l /dev/hdd

Disk /dev/hdd: 2111 MB, 2111864832 bytes
64 heads, 63 sectors/track, 1023 cylinders
Units = cylinders of 4032 * 512 = 2064384 bytes

Device Boot    Start       End    Blocks   Id  System
/dev/hdd1   *        1       260    524128+   6  FAT16

dd if=/dev/hdd1 of=/mnt/storage/Drive_9/Drive_9_uncompressed.img
1048256+0 records in
1048256+0 records out
```

Checking the drive and the captured image shows that nothing has changed.

```
md5 /dev/hdd1
11ae9d098753557f0a1ff080c4b4f293        /dev/hdd1

md5 Drive_9_uncompressed.img
11ae9d098753557f0a1ff080c4b4f293        Drive_9_uncompressed.img
```

Autopsy was used to create a string file, and a timeline. Sorter was run to analyze the types of files found. These procedures were done just like the procedures used to analyze the first image described in Appendix V.

The next step is to create a CD of all the files so that they can be analyzed on a Windows platform. The expanded drive was mounted read-only under Linux.

```
mount -o ro -t vfat /dev/hdd1 /mnt/analysis
```

Then a CD image was created in /var/tmp.

```
mkisofs -R -o /var/tmp/expanded.cd /mnt/analysis
```

Here is the md5 of expanded.cd that was just created.

```
ef860abc9dc78064ebd60dc970e758dd        expanded.cd
```

Then cdrecord took the cd image and put in on a CD.

```
drecord -v speed=2 dev=0,0,0 -data /var/tmp/expanded.cd
```

The hash of hdd1 is then taken to show it has not changed..

```
md5 /dev/hdd1
11ae9d098753557f0a1ff080c4b4f293        /dev/hdd1
```

The md5 hash is taken of /dev/cdrom and see that the md5 of it and expanded.cd are the same

```
md5 /dev/cdrom
ef860abc9dc78064ebd60dc970e758dd        /dev/cdrom
```

Now that drive E: has been extracted and the contents verified as forensically correct, further examination can proceed. Hashes collected by Autopsy are listed below.

Hashes – Compressed Drive

53AC7407E7CABD1DB281884AA59474BF	Drive_9.img
56A51A3591DE23DF2B2350E749417BE3	Drive_9.img.str
7042626D9BA7254055DCF46C56365E85	Drive_9.img.dls
9E3603E2E1D9CCD758462F8E797DE4C0	Drive_9.img.dls.str
EB98BE8299F4F0DFBC0736816C6BCF0E	body
6EDB6522E65A6C01C201314014CB480D	Drive9.timeline

Hashes – Uncompressed Drive

11AE9D098753557F0A1FF080C4B4F293	Drive_9_uncompressed.img
0D97CDED426CEEB4D10A3C8BEA054D88	Drive_9_uncompressed.img.str
5F78584178A3F440BE0181268E6D6445	Drive_9_uncompressed.img.dls
6CDC09A9E85BC01CFC22F268EA9B721D	Drive_9_uncompressed.img.dls.str
35AA4C1A36A7C770A802433D47BD17F7	body
35C4AE8A3459221C36D825E6D943B917	Drive_9_uncompressed.img.timeline

One of the first questions to answer is - when was the system was first installed and when were any upgrades done? As indicated earlier some of the dates in the time are from 1969. Since PC's were not invented until 1981 the earlier date is invalid. It might be possible to look at the timeline in such a way that a reasonable guess could be made. There are three problems with the time lines as they exist. The first is that if a program such as Microsoft ® Excel is used, there should be proper delimiters in place so that everything lines up in columns. This can be fixed by using the -d option in the mactime command. Another issue is that the time would be more readable if the year came first. This can be handled by the -y option in the mactime command which displays the date in yyyy/mm/dd format. The third issue is that in the existing timeline format, if there is a group of files, all with the same time and date, only the time and date for the first entry shows up. This is also fixed by using the –y option in the mactime command. The following information was created by importing the timelines into Microsoft ® Excel. The first thing done was to insert a column on the left so everything could be put back in the correct order if any analysis was done.

Table 19 - Timeline Entries from 1969 - 2004

	Timeline Entries	
Year	Original Image	Uncompressed Image
1969	14	2441
1980	0	126
1987	0	12
1988	0	21
1990	0	235
1991	0	5
1992	0	596
1993	3	377
1994	0	157
1995	18	1267
1996	0	296
1997	166	392
1998	0	6597
1999	591	2736
2000	0	2
2003	1	2
2004 (Before July 5)	175	573
2004 (July 5)	0	5851

Since this machine started off as a DOS 6 machine and it was received as a Windows 95 machine, when was it upgraded? The date that it was upgraded was Dec. 3, 1998. All the entries in the C:\FAILSAFE.DRV directory were created that day. This was also the last access date for COMMAND.DOS, a backup copy of the original COMMAND.COM from DOS 6.

One of the characteristics of all the items in the timeline was that entries that had a Create date of December 31, 1669 at 19:00.00.

In order to discover why the date and time is set to this we need to work backwards.

Here are two entries from the body file – one for IO.DOS and one for DRVSPACE.BIN.

IO.DOS has these dates in the timeline:

Modification date: 1993 Mar 10 Wed 06:00:00
Access date: 1998 Dec 03 Thu 00:00:00
Creation date: 1969 Dec 31 Wed 19:00:00

DRVSPACE.BIN has these dates in the timeline:

Modification date: 1998 Dec 03 Thu 13:40:58
Access date: 1998 Dec 23 Wed 00:00:00
Creation date: 1998 Dec 03 Thu 13:40:58

Note that the modification and creation dates are the same.

Looking at the body file – the intermediate file created before the timeline this information for IO.DOS is seen:

Modification date: 731761200 (number of seconds between 12/31/69 @ 19:00 and 3/10/93 @ 06:00:00
Access date: 912661200 (number of seconds between 12/31/69 @ 19:00 and 12/3/98 @ 00:00:00
Creation date: 0 (since this is zero it is set to 12/3/69)

Looking at the body file this information for DRVSPACE.BIN is seen:

Modification date: 912710458 (number of seconds between 12/31/69 @ 19:00 and 12/3/98 @ 13:40:58)
Access date: 914389200 (number of seconds between 12/31/69 @ 19:00 and 12/23/98 @ 00:00:00)
Creation date: 912710458 (number of seconds between 12/31/69 @ 19:00 and 12/3/98 @ 13:40:58)

The structure of a FAT16 directory entry can be found in the Long File Name Specification page (http://home.teleport.com/~brainy/lfn.htm) The format of a FAT entry is as follows:

Table 20 - FAT 16 Directory Entry Structure

Offset	Length	Value
0	8 bytes	Name
8	3 bytes	Extension
11	Byte	Attribute
12	Byte	Always 0
13	Byte	Create Time (milliseconds)
14	Word	Create Time (hour and min)
16	Word	Created Date
18	Word	Last Accessed Date
20	Word	Always 0
22	Word	Time
24	Word	Date
26	Word	Cluster
28	DoubleWord	File Size

Here is a comparison of the two FAT directory entries:

Screen shot of IO.DOS FAT entry: (from HexEdit Version 2.60 – see below). The creation time is highlighted and is set to zero.

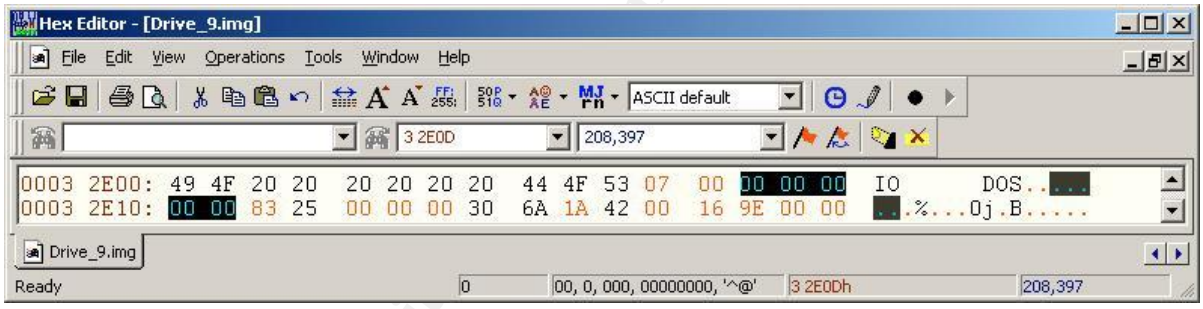


Figure 24 - HexEdit View of IO.DOS FAT Entry - Creation Time Is Zero

Screen shot of DRVSPACE.BIN FAT entry (from HexEdit Version 2.60). The creation time is highlighted and non-zero.

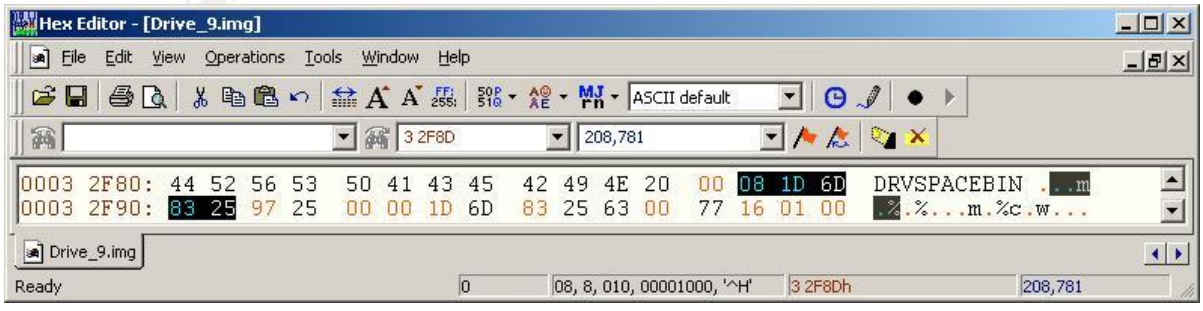


Figure 25 - HexEdit View of DRVSPACE.BIN FAT Entry - Creation Time Is Non-Zero

The reason there are so many directory entries with a date of 12/31/69 at 1900 is that when these directory entries were created under DOS 6, this field was left blank and MACtime puts in a default date of 12/31/1969 at 19:00. Windows 95 used all of the MAC fields and the MACtime program picked them all up and filled in the empty ones with a default date.

Software Used After the Acquisition is Complete

This software is listed alphabetically.

Ad-aware 6.0 Personal Edition (www.lavasoft.com) used to
> comprehensively scan your memory, registry, hard, removable and optical drives for known Datamining, aggressive advertising, Parasites, Scumware, Keyloggers, selected traditional Trojans, Dialers, Malware, Browser hijackers, and tracking components.

The results of this scan are in Appendix C. No software of this type was found.

HexEdit v 2.60 by Expert Commercial Software Pty Ltd, 2004. This softrware allows viewing of any Windows file so that all hexadecimal, ascii, and text characters can be seen. It is very useful for viewing file structures within non-readable files.

Internet History Viewer v. 1.4.2.6, © 1999, Phillips Ponder Company. This was written by Scott Ponder.

> The Internet Explorer History Viewer, will parse and print the history of URL's visited using the Microsoft Internet Explorer version 3.x, 4.x and 5.x.
> It can also read the INFO and INFO2 files from the recycle bins of Windows 95/98, NT 4.x and Windows 2000, the Netscape cache file "fat.db" and Netscape history file "Netscape.hst"

A nice program to look at cookie (Internet tracking files) is Karen's Cookie Viewer, v. 3.4, © 1998-2001 by Karen Kentworthy, is available for a free download from http://www.snapfiles.com/get/wmcookie.html. This program scans for cookies and when it finds them provides the following information - cookie location, cookie name, the site that the cookie is available to, the data contained in the cookie, the value of the data name, the create and expiration date, whether the cookie is secure, and its lifetime in days, hours, minutes, and seconds.

MailNavigator, V. 1.9, 6/21/2004, © 2000-2004 GEO Ltd. (http://www.MailNavigator.com), has the ability to import Outlook Express mailboxes (*.mbx files) and view them. This program was used to examine the five mailboxes found on the hard drive.

Norton Anti-Virus 9.05.15 by Symantec. (www.symantec.com) This program is one part of the Norton SystemWorks package. Scanning can occur for memory and any

combination of floppy disks and hard disks for viruses, Trojans, and many other kinds of offensive and damaging software. It has a LiveUpdate feature and will automatically "call home" and get the latest updates every time the machine is connected to the Internet. The results of this scan are in Appendix D. No viruses were found.

PWL and NetTools v 6.90 © Vitas Ramanchauskas & Eugene Korolev, 2002. (http://www.shareit.com) From their own description,

> Pwl&NetTools is a set of password recovery tools. The main program is RePwl. This program allows you to restore occasionally forgotten or lost logon password for Windows 3.11, Windows 95 (both original version and OSR2) and Windows 98. It also enables you to browse the passwords stored in PWL file.

Registry Viewer v 1.1 © AccessData Corp 2003. (www.accessdata.com)

> The AccessData Registry Viewer gives you the ability to view independent Windows registry files.

This software has an easy to use interface that makes examining and searching the registry files easy.

Looking for Log Files

Many times log files can tell us what kinds the dates and times that software was installed on the device. Here is what was found. The information format is the program name, the installation date, a description of the program owning the log, and the properties of the log when mounted under Linux including the creation date.

Grafixview was installed Dec. 6, 1998 at 6:11 a.m.
This is a Netscape plugin. A search for the executable, GFX-UP.EXE, showed that it had been deleted. The log indicated that the installation was completed successfully.

```
-rwxr-xr-x    1 root     root          999 Dec  6  1998 install.log
```

The scandisk log shows that there was a Drive H: attached to this device. Scandisk was run on April 29, 2004 at 3:58 p.m. No problems were found on drives C: or H:.

```
-rwxr-xr-x    1 root     root         1077 Apr 29 15:58 scandisk.log
```

Installation was started and completed successfully for Mustek Scanner Solutions for 600 III EP Plus v2.3 software. This was done on Nov. 30, 1998 at 1:43 p.m. From the contents of the log file twain drivers were installed. These drivers usually indicate the presence of a scanner attached to the PC. An update to the scanner software program was run from drive A: on Nov. 30, 1998 at 1:48 p.m. The version was upgraded to 600 III EP Plus v2.4.

```
-rwxr-xr-x    1 root     root         2135 Nov 30  1998 install.log
```

The drive was backed up on February 19, 1999. The backup was started 12:21:31 p.m. and completed successfully 12:23:02 p.m.

-rwxr-xr-x 1 root root 5938 Apr 29 15:57 ws2setup.log

The software installation for ACDSee was started Dec. 6, 1998 from E:\ACDSEE\ACDC32223.EXE but was aborted because there was not enough room on drive C: to install the software.
-rwxr-xr-x 1 root root 412 Dec 6 1998 install.log
The installation program needed an additional 774 K bytes to complete. This log shows that there was a drive E: attached to this device. In documentation for the program it proclaims that it is:

> the fastest and easiest-to-use image viewer available for Windows 95 and Windows NT! ACDSee is two tools in one. A full-featured image viewer quickly displays your images in high quality. The image browser lets you efficiently find and organize your images.

Another log file for this program was found that indicated it was installed successfully.
-rwxr-xr-x 1 root root 26590 Dec 6 1998 GLG31D5.TMP

The Mirabilis ICQ Installation (Ver 98a Dll 1.26 Win95 / NT) was started on November 27, 1998 at 4:27 p.m. and completed successfully.
-rwxr-xr-x 1 root root 59673 Nov 27 1998 install.log
There is another indication that drive E: was attached to the computer since the installation was run from E:\GOODIES\32-BIT\ICQ 98A\ICQ98A126.EXE.

A program named Internet Call Manager, v. 5.1.3 was installed on February 18, 1999 at 7:39 a.m. Internet Call Manager

> is the cost-effective solution to the problem of missed calls while your phone line is busy because you're on the Internet. It is ideal for anyone who wants the freedom to be on-line. You can comfortably do everything you do on the Internet worry-free while ICM monitors your telephone line. (http://www.internetcallmanager.com/CustomerService/faq.shtml#general01)

This program was installed so that it would have a link in C:\WINDOWS\Start Menu\Programs\StartUp so that when the computer was booted the program would start.
-rwxr-xr-x 1 root root 1583 Feb 18 1999 install.log
The ICM.INI file had many entries. A few of the interesting ones are listed below:

```
[PARAMS]
USERID=(407) 574-3169
PASSWORD=p*****
SOUND=1
RAS=1
USEAOL=1
SERVICE=3
VERSION=7.0
REDIRECTADDR=207.34.24.16/10002
SIGNATURE=031387
```

AOLTIMER=20
SERVER0=208.16.158.186/15001

The installation program for Yahoo! Pager was installed on Feb. 16, 1999 at 1:48 a.m.
-rwxr-xr-x 1 root root 1403 Feb 6 1999 install.log

Java was installed on November 28, 1998 at 8:13 a.m. In the log is the discovered version of Internet Explorer - IE Build 4.72.2106.7
-rwxr-xr-x 1 root root 1328 Nov 28 1998 javainst.log

Other Software Found

D:\PROGRAM_\NETSCAPE\NAVIGATO\PROGRAM\PLUGINS\ICHAT.TXT
The Ichat plugin for Netscape, v. 2.22, was installed January 7, 1999 (http://www.ichat.com)

D:\PROGRAM_\NETSCAPE\NAVIGATO\PROGRAM\REG.INI contains these lines:

[Server Info]
RegCGI=https://reggie1.bellsouth.net/cgi-bin/regserv1.12/reg.cgi

[Configuration]
REG_PLATFORM=WIN95
REG_SCRIPTING=No
REG_SOURCE=DUK

[Customer Information]
CST_PHONE=(407) 574-1532

D:\PROGRAM_\NETSCAPE\NAVIGATO contains three interesting files:
BOOKMARK.HTM
COOKIES.TXT
NETSCAPE.HST

D:\PROGRAM_\NETSCAPE\NAVIGATO\MAIL has the mailbox for Netscape
INBOX – viewable by notepad. Nothing significant was found.
Mail from: Wed, 13 Dec 1995 20:47:45
To: Thu, 18 Feb 1999 07:54:49

He is on the mailing lists for:
http://www.CompletelyFreeSoftware.com/ - a location for free software
http://miningco.com – a news digest
http://www.valupage.com – shopping guides for Winn-Dixie stores
http://www.valueamerica.com – a shopping site (this is a dead link)

www.evangelist.macaddict.com – a digest of MAC issues and correspondence (this is a dead link)
http://www.zws.com/classicmacs/ - classic MAC newsletter (this is a dead link)
http://www.virtual-electronics.com – a web based electronics store (this is a dead link)
http://www.buick.com – Buick events newsletter
http://home.netscape.com/netcenter/newsletter – a monthly travel newsletter
http://adultsingles.com/ - an adult site sponsored by http://absoluteagency.com/

Nickname and handle in relation to http://www.uproar.com

UPROAR Handle: o********
UPROAR Password: c*****

The Owner's Address (sanitized):

J*** F*****
*** C******* Street
*******, ******* *****

His ISP:

BitStorm, Inc.
780 Deltona Blvd.
Pickford Square Suite 101
Debary, FL 32725
407-668-0670

A request from his ISP to stop connecting through (407) 708-7867 and start using (904) 668-5494, 668-5876, or 668-6973

In here, the name of the business of the person owning the computer: D:\DOS\nsformHE.TMP

C******* H******* of F******

In here (D:\PROGRAM_\ICQ\UIN) there is one file of interest:

[ICQ User]
UIN=*******
Email=j******@bitstorm.net
NickName=o********
FirstName=J***
LastName=F******

Bookmarks from D:\PROGRAM_\ICQ\BOOKMARK\9******.HTM (all dead)

http://www.talstar.com/cat/jokes/C06.htm
http://surf.to/smile
http://www.marketez.com/kimmybaby

Netscape Navigator v. 3.01 was installed December 4, 1998 at 3:37 a.m..
drwxr-xr-x 3 root root 8192 Dec 4 1998 Netscape

Apple Quicktime Movieplayer v. 3.0.0.116 was installed November 30, 1998 at 8:38 a.m.
drwxr-xr-x 2 root root 8192 Nov 30 1998 QuickTime

Software called RapidCom was installed December 4, 1998 at 4:07 a.m.
drwxr-xr-x 7 root root 8192 Dec 4 1998 RapidComm
This software, v. 1.0.0.0, was published by Smith Micro Software, Inc. It worked through an dial-up connection and had chat, file transfer, and other components.

RealPlayer, v. 6.0.3.128, from RealNetworks, was installed December 12, 1998 at 1:39 p.m.
drwxr-xr-x 3 root root 8192 Dec 12 1998 Real

WinZip, v. 6.3 (32-bit) , from Nico Mak Computing, Inc., was installed November 28, 1998 at 7:33 a.m.

Software in a directory, created January 1, 1999 at 6:02 p.m., called TENBEST looks like it is a program that has lots of templates for form letters
drwxr-xr-x 2 root root 8192 Jan 1 1999 tenbest

Adobe Acrobat Reader, v. 2.1, Dec. 4, 1998 at 3:59. a.m.
drwxr-xr-x 5 root root 8192 Dec 4 1998 acroread

DeskMate, v. 1.3.0.1, from Oska Educational Systems Pty. Ltd, Smileware Pty. Ltd., was installed December 4, 1998 at 5:28 a.m.
drwxr-xr-x 2 root root 8192 Dec 4 1998 deskmate
On site (http://www.oska.com/deskmate_info.php) on August 8, 2004 was the description of an animated product described as

> an interactive cartoon character who lives on your Windows desktop.
> . . .
> When you leave Oska alone he will amuse himself and will randomly select one of the animations from about half of his library. After you click on Oska and activate his touch reactions he will then perform an animation selected from the other half of his library. We did this so that he will continue to do things you have not seen before for a long time after you buy him.

Version 3 was for sale. DeskMate sounds a lot like spyware because it looks attractive and (possibly) sends information back to headquarters.

An Internet relay chat client, mIRC, v. 5.31, from mIRC Co., Ltd. , was installed November 30, 1998 at 8:19 a.m.
drwxr-xr-x 5 root root 8192 Nov 30 1998 mirc

The homepage for this program is now http://www.mirc.com/ and the version is now 6.16.

Mopyfish and Mopyplay was installed November 27, 1998 at 8:47 a.m.
drwxr-xr-x 2 root root 8192 Dec 3 1998 mopyfish
At this site, http://www.mopyfish.net/, it is possible to download a virtual pet fish.

Software for a Mozart soundcard was installed November 27, 1998 at 8:47 a.m.
drwxr-xr-x 3 root root 8192 Nov 27 1998 mozart

An IRC program called PIRCH32.EXE was installed January 3, 1999 at 11:08 p.m.
drwxr-xr-x 2 root root 8192 Jan 3 1999 pirch32
Symantec (http://securityresponse.symantec.com/avcenter/venc/data/w97m.grouch.html) says that the W97M.Grouch macro virus does

> Checks whether the Mirc.ini file exists in any of the following folders:
> - C:\Mirc
> - C:\Mirc32
> - C:\Program Files\Mirc
> - C:\Programme\Mirc
> - C:\Programmi\Mirc
> - C:\Program Files\Mirc32
> - C:\Programme\Mirc32
> - C:\Programmi\Mirc32

This mirc.ini does exist in C:\MIRC

> If the Mirc.ini file does not exist in any of these folders, the virus creates the Script ini file. The Script.ini file includes the following text:
>
> ```
> [script]
> n5= on 1:JOIN:#:{
> n6= /if ( $nick == $me ) { halt }
> n7= /msg $nick Here is that document you wanted :)
> n8= /dcc send -c $nick " %the name of the word document %
> n9= }
> ```

The file script.ini does not exist.

> Checks whether the Pirch32.exe file exists in any of the following folders:
> - C:\Pirch
> - C:\Pirch32
> - C:\Program Files\Pirch
> - C:\Programme\Pirch
> - C:\Programmi\Pirch
> - C:\Program Files\Pirch32
> - C:\Programme\Pirch32\

- C:\Programmi\Pirch32\

If Pirch32.exe does not exist in any of these folders, the virus creates the file, Events.ini file, which the virus uses to store information about the infected Word documents.

The file pirch32.exe does exist in C:\Pirch32. Events.ini does exist but it contains none of the entries mentioned in the Symantec bulletin.

Who Were the Users?

In order to see who the users on the computer were it is necessary to look at the files with an extension of PWL. The software that was used to decipher these files was PWL and NetTools described earlier. There were three PWL files on the machine and after being deciphered by this tool here are the results. The ID's and passwords have been sanitized to hide the identities.

File: D:\WINDOWS\A*****.PWL
User name: 'A*****'
Password: 'A*****'

File: D:\WINDOWS\J******.PWL
User name: 'J******'
Password: ''

Dial-up:'*R**\BellSouth.net\j******'
Password:'cd5555'
Dial-up:'*R**\Bitstorm.net\a******'
Password:'p***'
Dial-up:'*R**\Bitstorm.net\j******'
Password:'cd5555'

File: D:\WINDOWS\R**.PWL
User name: '*R**'
Password: ''

Dial-up:'Sportster 9600 V.42bis'
Password:''
Dial-up:'Standard Modem'
Password:''
Dial-up:'Microsoft VPN Adapter'
Password:''

As can be seen creativity was not used in the passwords. Where the ID did have a password, it often was the same as the ID.

There are several types of accounts in evidence:

One account from bellshouth.net
Two accounts with bitstorm.net
An account for a Sportster modem
An account for a standard modem
An account for the Microsoft VPN adapter

It is not clear which of these accounts were used or if they ever were used at this time. The file locations and hashes of the password files are noted below. The names of the files have been sanitized.

Table 21 - md5 Hashes for PWL Files

Path to File	MD5 Hash
C:\windows\a*****.pwl	433A0E441C5C0D020D427CD69C212930
C:\windows\j******.pwl	49537C473E94E017FAB2286E58E4F58E
C:\windows\r**.pwl	F7AA3422EC4FCAFA8CB21E40DD96C14A

Registry Examination

The two files which make up the registry in Windows 95 are SYSTEM.DAT and USER.DAT. These files are found in the Windows directory, which was C:\Windows. These two files were extracted from the image and then burned to CD. Their hashes are:

SYSTEM.DAT BF12830FE32315D4BB3A1CD979B32136

USER.DAT 544D50DCB824F44E1A5580E7AEECF670

Using Registry Viewer ™ Copyright © AccessData Corp 2003 to open each file in turn, a registry report was created values of interesting keys. These reports are shown in Appendix Y (SYSTEM.DAT) and Appendix Z (USER.DAT). Summary information is shown below.

SYSTEM.DAT

Summary information from SYSTEM.DAT included this information.

Computer Name	My Internet
Drive D:	PIONEER CD-ROM DR-A02S
	TEAC CD-532E-B
Drive E:	MATSHITA CD-ROM CR-562
Monitor:	IBM 8515
Printer:	Canon BJC-2100

Run Command Contents loadwc.exe /u

USER.DAT

There were several pieces of information that were extracted from USER.DAT. These are listed below and include a description, the key the information came from, and if a file location is in the key that is included also.

Netscape User Profile - this is the user's name, organization, and email address.
.Default\Software\Netscape\Netscape Navigator\User

Since this device had Mirabilis ICQ installed, this key has the user's handle.
.Default\Software\Mirabilis\ICQ\Owners\9******

The Mirabilis ICQ preferences are found here, including the location of the received files (nothing significant), his description including height, weight and interests.
.Default\Software\Mirabilis\ICQ\Owners\9******\Prefs

Netscape News - nothing significant found here.
.Default\Software\Netscape\Netscape Navigator\News
C:\Program Files\Netscape\Navigator\news

Netscape Address Book - this file did not exist.
.Default\Software\Netscape\Netscape Navigator\Address Book
C:\Program Files\Netscape\Navigator\address.htm

NetScape History - this can be viewed by the Internet History Viewer
.Default\Software\Netscape\Netscape Navigator\History
C:\Program Files\Netscape\Navigator\Netscape.hst

Netscape Cache
.Default\Software\Netscape\Netscape Navigator\Cache
C:\Program Files\Netscape\Navigator\cache

Netscape Bookmarks
.Default\Software\Netscape\Netscape Navigator\Bookmark List
C:\Program Files\Netscape\Navigator\bookmark.htm

Netscape URL History - this is a list of the most recently viewer URL's
.Default\Software\Netscape\Netscape Navigator\URL History

What Did The User Do Last?

Typically Microsoft products keep track of the most recently accessed files. Microsoft ® Word tracks recently opened Word documents, for example. When doing a forensic

examination, review of the appropriate registry keys can enable an investigator to determine what the suspect was doing recently. Coupled with additional information from the MAC times, and file ownership much can be learned. For Windows 95 without Microsoft Office products, there are several keys that are noted in Appendix AA. that provide this information.

All of the information was found in USER.DAT.

Files to be Examined by the Internet History Viewer

Using the Internet History Viewer v. 1.4.2.6, © 1999, Phillips Ponder Company the following files will be examined. The files and their hashes are as follows:

NETSCAPE.HST is the browsing history from the Netscape browser. This file contains 5,654 entries. The dates are from 2/12/1999 to 2/20/1999. The URL and all he components of each web page are listed. Nothing remarkable or notable was found.

Table 22 - md5 Hash for netscape.hst File

Path to File	MD5 Hash
C:\Program Files\Netscape\Navigator\netscape.hst	E0D7C5EE46822F133E5AF24B767E37C9

INFO contains the names and delete time of files deleted (emptied) from the recycle bin. There are 809 deleted files. Two were deleted on 4/29/2004 at 3:49 p.m. The rest were deleted on 4/29/2004 at 10:29 p.m. In addition, the Internet History Browser shows the original path, the original file name, and the current file name.

Two Adobe Acrobat Reader ® files were found in INFO. The rest of the files came from the deletion of C:\Program Files\Juno directories.

Table 23 - md5 Hash for info File

Path to File	MD5 Hash
C:\recycled\info	0E8A95F0704C499B6FB059509EE42617

INDEX.DAT shows what sites have been visited using Microsoft's Internet Explorer (v. 4.x) browser. There are 303 entries starting at 11/28/1998 to12/2/1998. Nothing remarkable or unusual was found.

Table 24 - md5 Hash for History\index.dat File

Path to File	MD5 Hash
C:\windows\History\index.dat	56B0ED37355E5490DAC3C439CF1A09E7

In the Temporary Internet Files folder is another INDEX.DAT. This file, used by Internet Explorer, had 951 entries starting on 11/28/1998 to 12/2/1998. This file indexes components of web pages like image files (.GIF, .JPG) and other files.

Table 25 - md5 Hash for Temporary Internet Files\index.dat File

Path to File	MD5 Hash
C:\windows\Temporary Internet Files\index.dat	6C5719A93CB8220075BF4A020AADB9B0

The last INDEX.DAT file, that indexes the cookies used for tracking Internet usage by various sites, has 15 entries and the dates start at 11/28/1998 and go to 12/2/1998 - the same as the other two Internet Explorer index files.

Table 26 - md5 Hash for cookies\index.dat File

Path to File	MD5 Hash
C:\windows\cookies\index.dat	B6CE2E3D3ADA9461986183C5284202A4

More on Internet Cookies

Another file that tracks cookies is COOKIES.TXT. This file is a text file with tabs as delimiters. It can be exported into Excel. Because it is a text file it is impossible to determine when individual cookies were added. For Internet Explorer, each cookie is saved as a file so that the date of creation can be determined. By using Karen's Cookie Viewer it is possible to learn a lot about the contents of a cookie. Here is an example. Since the contents of the drive was burned to a CD, the drive letter is D:. There are 145 cookies stored in the COOKIES.TXT file.

The next figure highlights one cookie for further analysis.

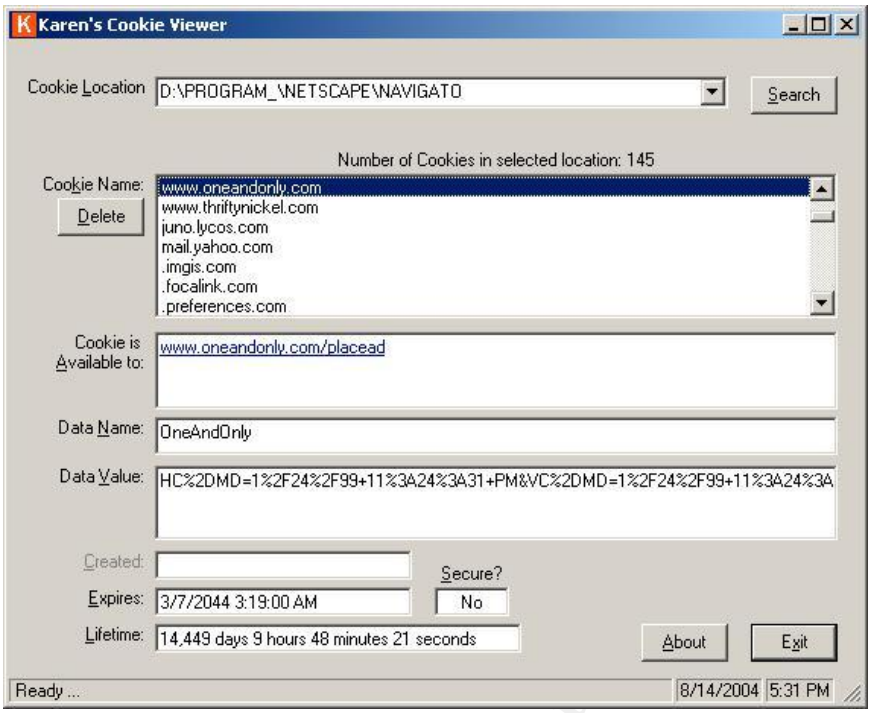


Figure 26 - Cookie from www.oneandonly.com Used as an Example

The site from the cookie used as an example, www.oneandonly.com is a dating site. This cookie does not expire until March 7, 2044. Documentation on Netscape's cookie format can be found. http://wp.netscape.com/newsref/std/cookie_spec.html

Table 27 - cookies.txt Path and md5 Hash

Path to File	MD5 Hash
C:\Program Files\Netscape\Navigator\cookies.txt	030BA00A5CC754FBDE70A73CF2BF5A03

Outlook Express

Microsoft's Outlook Express, © Microsoft Corporation, stores the information in files with an extension of MBX (MailBoX). The machine to be examined had five .MBX files.

Table 28 - Outlook Express Files and md5 Hash

Path to File	MD5 Hash
C:\windows\Application Data\Microsoft\Outlook Express\Mail\Deleted Items.mbx	5FA1EA55D0D3F3C924DD0B522BEB6FBC
C:\windows\Application Data\Microsoft\Outlook Express\Mail\Drafts.mbx	5FA1EA55D0D3F3C924DD0B522BEB6FBC

C:\windows\Application Data\Microsoft\Outlook Express\Mail\Inbox.mbx	B8A48D2311B4B1A1FEDC011501FD6037
C:\windows\Application Data\Microsoft\Outlook Express\Mail\Outbox.mbx	0066136AC3EAF7507D75788F5586DC93
C:\windows\Application Data\Microsoft\Outlook Express\Mail\Sent Items.mbx	0066136AC3EAF7507D75788F5586DC93

The first two mailboxes, Deleted Items.mbx, and Drafts.mbx were only 84 bytes long and when examined proved to be empty. The last two items, Outbox.mbx and Sent Items had the same hash so it is only necessary to examine one of them.

The Inbox.mbx had 35 messages and the dates for these messages ranged from 12/13/1995 at 8:47 p.m. to 12/1/1998 at 9:00 p.m. The majority of messages were from people who wanted to meet other people on the Internet. The owner of this drive placed an ad with http://www.classified2000.com and these were responses to the ad. Other messages included mailings about Apple Macintosh issues, etc., from the Classic Macs Digest. (http://www.hitznet.com)

The Outbox.mbx had 43 messages and dates for these messages ranged from 12/13/1995 at 8:47 p.m. to 12/2/1998 at 7:39 p.m. The messages in this mailbox had the same kind of information as Inbox.mbx.

Here are the MAC times from all of the mailboxes. The Access times for all of these files are invalid because they were in DBLSPACE.000 and this file was decompressed on July 5, 2004. This changed the Access time for all of the files

Modification / Create time - 1998 Nov 28 Sat 09:08:40
Access Time - 2004 Jul 05 Mon 00:00:00

Programs Invoked at Startup

There are four main places where programs can be started when the computer is started - CONFIG.SYS, AUTOEXEC.BAT, the registry, and startup folders.

CONFIG.SYS is the first file loaded at startup. It exists because in the early days of PC development, manufacturers were given the technical information needed to allow almost any device work with a Microsoft operating system. These manufacturers created device drivers and enabled devices to communicate with the operating system. What is found in this file are the location, the names, and any parameters needed to enable devices attached to a PC to operate.

CONFIG.SYS

DEVICE=C:\MOZART\MZTINIT.SYS /A220 /I5 /D1 /P /CA340 /CI9 /G /V7

This device driver allowed the operating system to talk to and initialize the Mozart sound card.

DEVICE=C:\WINDOWS\SETVER.EXE
As development of Microsoft operating systems progressed, the decision was made to be backward compatible with older versions. Some device drivers needed specific operating system versions in order to function. Microsoft solved this problem by using SETVER.EXE.

> SETVER.EXE loads into memory the MS-DOS version table, which lists names of programs and the number of the MS-DOS version with which each program is designed to run. (http://users.cybercity.dk/~bse26236/batutil/help/SETVERS.HTM)

SHELL=C:\COMMAND.COM C:\ /P /E:512
Many pieces of the operating system are replaceable or extendable. One of these pieces is the command shell. The command shell is the program that lets users use a command line interface rather than a graphical user interface (GUI) to interact with the operating system. COMMAND.COM was the standard DOS / Windows command shell and was loaded here.

DEVICE=C:\DOS\DBLSPACE.SYS /MOVE
This device driver is what is needed to use the contents of the compressed drive DBLSPACE.000.

DEVICE=C:\CDROMDRV\CDMKE41.SYS /D:MVCD001
A CD-ROM was attached to the computer and here is the device driver that allowed the operating system to initialize it.

AUTOEXEC.BAT

SET SOUND=C:\MOZART
This line does not execute anything but tells inquiring programs that an environment variable stored by the operating system that any inquiries about SOUND should reference the C:\MOZART directory. An environment variable is managed by the operating system and is available to all running programs.

SET BLASTER=A220 I5 D1 T4
Many sound cards had Sound Blaster (another type of sound card) compatibility. This tells programs inquiring about BLASTER that what is needed is in the BLASTER environment variable.

C:\MOZART\MZTVOL.EXE
This line is the program that starts the Mozart sound program running on the PC.

@ECHO OFF
This line prevents any further on-screen display of information from started commands.

PATH C:\WINDOWS;C:\WINDOWS\COMMAND;C:\DOS;C:\
The environment variable PATH shows where to look if operators or programs are trying to run another program. The first place to look is C:\WINDOWS; the second place to look is C:\WINDOWS\COMMAND; the third place to look is C:\DOS; and the last place to look is the root of C: or C:\.

SET TEMP=C:\DOS
If programs need to create temporary files, they can store them C:\DOS.

C:\DOS\MOUSE
By running this program, users will be able to use the mouse when running in the graphical user interface.

The registry - from SYSTEM.DAT

Key - SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
Value - this key is empty

Key - SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce
Value - this key is empty

Key - SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
Value - this key is empty

Key - SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Value - loadwc.exe /u
According to Microsoft,
Loadwc.exe, also known as Load WebCheck, customizes some of the settings in Internet Explorer. Loadwc.exe adds, removes, and updates subscriptions. Loadwc.exe also propagates settings for user profiles.

Information about loadwc.exe can be found at the Microsoft site. (http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/q176/9/60.asp&NoWebContent=1)

The registry - from USER.DAT

.Default\Software\Microsoft\Windows\CurrentVersion\RunOnce
Value - this key is empty

.Default\Software\Microsoft\Windows\CurrentVersion\Run
Value - this key is empty

Special folders such as:
C:\windows\All Users\Start Menu\Programs\StartUp folder

- this folder is empty

C:\windows\Start Menu\Programs\StartUp folder
- this folder starts up links to:

Internet Call Manager
This is the Internet Call Manager program.

Mopy Points Collector
This loads the virtual fish screen saver.

Watchdog
This starts a program that loads twain drivers. This usually means that a scanner is attached tot the system. The link points to D:\WINDOWS\TWAIN\A4S2\Watchdog.exe. In that directory is a bitmap file that shows what this device looks like.

Figure 27 - Scanner Illustration

Information from Unallocated Space

Several techniques were used to see what kind of information was contained in unallocated space. As the hard drive was examined a list of words was collected to do string searches. Although most of the hardware questions have been answered, the type of modem used was still undetermined.

There were several instances of the word "modem" along with a brand name in both the compressed and uncompressed image. Here is what was found in the compressed image in images-Drive_9.img-Sector273330.raw:

[Configuration]
Juno Version=Juno 2.0.11
Evlog Upload=TRUE
Upgrading=
Supported Transports=TCP,JTP
Machine ID=BW437C4AAA5GDC6BAAA7594DXCUF57

[Communications]
Modem Name=US Robotics Sportster 28800 / 33600
Modem Configuration String=&FX4&B1&H1&R2&K0
Port=COM1

Speed=38400

Note that software from Juno, version 2.0.11 was installed and used with the modem.

The words that were used in this search were:

breast	bitstorm	casino
cheat	coke	computer hardware
connect	credit card	drug
dungeon	fraud	gambl
iwantu	luckykittie	marij
modem	orange	nylon
photo	piracy	pooh
pot	porn	private
pwl	sex	single
slave	slut	smoke
smuggle	sportster	swap
warez		

Since the user liked to go to Internet dating sites, I wanted to look for these words to see if there was any correspondence. These were names of image files on the hard drive.

ann3	ann4	anne
christmaskiss	danny	debby12
helen	hornydawn	huneb
kimmybaby	ladytessa	pearls
sexydoll	shelly2232	smurk
swinger	sxysarah	wetscarlet
yesmiss		

None of these words was found.

Since Autopsy was used for the searches, the syntax of the commands was hidden. Here is an example of what was going on behind the scenes.

'/bin/grep' -i 'warez' '/mnt/analysis//Drive9/Host_9//output/Drive_9.img.str'

In the search the grep command is used and does a case insensitive search (-i) and looks in the file, Drive_9.img.str, containing the strings from the compressed drive: The search results can be easily checked.

The Beginning and The End of the Drive Timeline

Looking at the timeline taken from the drive when DRVSPACE.000 was present gives start and end dates for drive activity. As already discussed, anything happening on 12/31/1969 cannot be counted. This timeline, Drive9.timeline, has been imported into

Excel so that mining activities can be done easily. Microsoft changed the dates on its files in successive releases to be March 10, 1993 for DOS 6 (noted earlier in the COMMAND.DOS example) and July 11, 1995 for Windows 95. These dates are also invalid.

Two assumptions will be made.
1. Lower Inodes will be written earlier.
2. Any date of 12/31/69 is invalid.

Let's look at the Inodes and the MAC dates:

Table 29 - Inode and MACTime Date Relationship

Inode	File Name	M Date	A Date	C Date
3	C:/IO.DOS	1993 Mar 10 Wed 06:00:00	1998 Dec 03 Thu 00:00:00	1969 Dec 31 Wed 19:00:00
4	C:/MSDOS.DOS	1993 Mar 10 Wed 06:00:00	1998 Dec 03 Thu 00:00:00	1969 Dec 31 Wed 19:00:00
5	C:/CONFIG.DOS	1998 Nov 27 Fri 11:49:24	1998 Dec 03 Thu 00:00:00	1969 Dec 31 Wed 19:00:00
6	C:/COMMAND.DOS	1993 Mar 10 Wed 06:00:00	1998 Dec 03 Thu 00:00:00	1969 Dec 31 Wed 19:00:00
7	C:/AUTOEXEC.DOS	1998 Nov 27 Fri 11:47:34	1998 Dec 03 Thu 00:00:00	1969 Dec 31 Wed 19:00:00
8	C:/COMMAND.COM	1995 Jul 11 Tue 09:50:00	1998 Dec 23 Wed 00:00:00	1969 Dec 31 Wed 19:00:00
10	C:/MSDOS.SYS	1998 Dec 23 Wed 08:39:04	2004 Apr 29 Thu 00:00:00	1969 Dec 31 Wed 19:00:00
11	C:/CONFIG.SYS	1998 Dec 23 Wed 08:39:10	1998 Dec 23 Wed 00:00:00	1969 Dec 31 Wed 19:00:00
12	C:/AUTOEXEC.BAT	1998 Dec 23 Wed 08:39:10	1998 Dec 23 Wed 00:00:00	1969 Dec 31 Wed 19:00:00
13	C:/IO.SYS	1995 Jul 11 Tue 09:50:00	2004 Apr 29 Thu 00:00:00	1969 Dec 31 Wed 19:00:00
14	C:/DBLSPACE.INI	1998 Dec 23 Wed 08:39:06	1998 Dec 23 Wed 00:00:00	1969 Dec 31 Wed 19:00:00
15	C:/DRVSPACE.BIN	1998 Dec 03 Thu 13:40:58	1998 Dec 23 Wed 00:00:00	1998 Dec 03 Thu 13:40:58
16	C:/DBLSPACE.BIN	1998 Dec 03 Thu 13:40:58	1998 Dec 23 Wed 00:00:00	1998 Dec 03 Thu 13:40:58
17	C:/FAILSAFE.DRV	1998 Dec 03 Thu 13:40:58	1998 Dec 03 Thu 00:00:00	1998 Dec 03 Thu 13:40:58
18	C:/RECYCLED	1998 Dec 25 Fri 13:18:54	1998 Dec 25 Fri 00:00:00	1998 Dec 25 Fri 13:18:54
19	C:/DBLSPACE.000	2004 Jun 09 Wed 15:36:18	2004 Apr 29 Thu 00:00:00	1969 Dec 31 Wed 19:00:00
20	C:/BOOTLOG.TXT	1998 Dec 23 Wed 08:38:04	1998 Dec 23 Wed 00:00:00	1969 Dec 31 Wed 19:00:00

Key:
Invalid Date - Filled in by MACTime
Invalid Date - Microsoft Date 1 - DOS 6
Invalid Date - Microsoft Date 2 - Windows 95

Eliminating all the invalid dates gives Dec. 3, 1998 for the installation of DOS 6 and December 23, 1998 as the date of upgrade to Windows 95.

Looking at the drive timeline gives June 9, 2004 as the date of last activity.

Conclusions

Forensic analysis of this hard drive posed several interesting challenges. Among them was the struggle to extract the data from the compressed drive in a forensically correct manner. A second challenge was trying to determine the meaning of the dates in 1969. Working through these challenges made a very interesting experience. A third challenge was the discovery of the Internet usage by the two browsers, Netscape Navigator and Internet Explorer. This required the use of special software and the knowledge of the file locations.

By looking at the timeline entries in Table 19 it was possible to see that this machine was used most heavily in 1998 and 1999, and rarely after that. Of the machine's three users, J****** used the machine the most. J****** sent out the most emails, surfed the Internet the most, liked to share information about Apple computers and liked to go to chat and dating sites on the Internet.

Viruses or malware did not infect the machine. Also, there was no ad-ware on the machine - possibly because ad-ware had not come into wide use by 1999.

The machine a lot of software on it and nothing was found that was illegal or questionable. The hard drive was probably discarded because it was too small, at just over 300 megabytes, even with disk compression, for any more upgrades.

Appendix A – Text of Acceptable_Encryption_Policy.doc (Tag # fl-260404-RJL1)

Acceptable Encryption Policy

1.0 Purpose
The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

2.0 Scope
This policy applies to all Ballard Industries employees and affiliates.

3.0 Policy
Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Bright Industriess key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by InfoSec. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
Proprietary Encryption	An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.
Symmetric Cryptosystem	A method of encryption in which the same key is used for both encryption and decryption of the data.
Asymmetric Cryptosystem	A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

6.0 Revision History

Information Sensitivity Policy

Purpose
The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Ballard Industries without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect Ballard Industries Confidential information (e.g., Ballard Industries Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to Infosec.

Scope
All Ballard Industries information is categorized into two main classifications:
Ballard Industries Public
Ballard Industries Confidential

Ballard Industries Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to Ballard Industries Systems, Inc.

Ballard Industries Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Also included in Ballard Industries Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of Ballard Industries Confidential information is "Ballard Industries Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to Ballard Industries by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into Bright Industries's network to support our operations.

Ballard Industries personnel are encouraged to use common sense judgment in securing Ballard Industries Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager

Policy
The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as Ballard Industries Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the Ballard Industries Confidential information in question.

Minimal Sensitivity: General corporate information; some personnel and technical information

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".

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "Ballard Industries Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "Ballard Industries Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, Ballard Industries information is presumed to be "Ballard Industries Confidential" unless expressly determined to be Ballard Industries Public information by a Ballard Industries employee with authority to do so.

Access: Ballard Industries employees, contractors, people with a business need to know.
Distribution within Bright Industries: Standard interoffice mail, approved electronic mail and electronic file transmission methods.
Distribution outside of Ballard Industries internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.
Electronic distribution: No restrictions except that it be sent to only approved recipients.
Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.
Disposal/Destruction: Deposit outdated paper information 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.

More Sensitive: Business, financial, technical, and most personnel information

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". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "Ballard Industries Confidential" or "Ballard Industries Proprietary", wish to label the information "Ballard Industries Internal Use Only" or other similar labels at the discretion of your individual business unit or

department to denote a more sensitive level of information. However, marking is discretionary at all times.

Access: Ballard Industries employees and non-employees with signed non-disclosure agreements who have a business need to know.
Distribution within Bright Industries: Standard interoffice mail, approved electronic mail and electronic file transmission methods.
Distribution outside of Ballard Industries internal mail: Sent via U.S. mail or approved private carriers.
Electronic distribution: No restrictions to approved recipients within Bright Industries, but should be encrypted or sent via a private link to approved recipients outside of Ballard Industries premises.
Storage: Individual access controls are highly recommended for electronic information.
Disposal/Destruction: 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.

Most Sensitive: Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that Ballard Industries Confidential information is very sensitive, you may should label the information "Ballard Industries Internal: Registered and Restricted", "Ballard Industries Eyes Only", "Ballard Industries Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of Ballard Industries Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (Ballard Industries employees and non-employees) designated with approved access and signed non-disclosure agreements.
Distribution within Bright Industries: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.
Distribution outside of Ballard Industries internal mail: Delivered direct; signature required; approved private carriers.
Electronic distribution: No restrictions to approved recipients within Bright Industries, but it is highly recommended that all information be strongly encrypted.
Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.
Disposal/Destruction: Strongly Encouraged: In specially marked disposal bins on Ballard Industries premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions
Terms and Definitions

Appropriate measures
To minimize risk to Ballard Industries from an outside business connection. Ballard Industries computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access Ballard Industries corporate information, the amount of information at risk is minimized.

Configuration of Bright Industries-to-other business connections
Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required
Do not leave in interoffice mail slot, call the mail room for special pick-up of mail.

Approved Electronic File Transmission Methods
Includes supported FTP clients and Web browsers.

Envelopes Stamped Confidential
You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

Approved Electronic Mail
Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mailers here]. If you have a business need to use other mailers contact the appropriate support organization.

Approved Encrypted email and files
Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within Ballard Industries is done via a license. Please contact the appropriate support organization if you require a license.

Company Information System Resources
Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge
To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

Individual Access Controls
Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use *man chmod* to find out more about it). On Macs and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links
Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of Bright Industries.

Encryption
Secure Ballard Industries Sensitive information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow

corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

One Time Password Authentication
One Time Password Authentication on Internet connections is accomplished by using a one time password token to connect to Bright Industries's internal network over the Internet. Contact your support organization for more information on how to set this up.

Physical Security
Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link
A Private Link is an electronic communications path that Ballard Industries has control over it's entire distance. For example, all Ballard Industries networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer have established a private link. ISDN lines to employee's homes is a private link. Ballard Industries also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies which Ballard Industries has established private links include all announced acquisitions and some short-term temporary links

Revision History

Internal Lab Security Policy

1.0 Purpose
This policy establishes information security requirements for Ballard Industries labs to ensure that Ballard Industries confidential information and technologies are not compromised, and that production services and other Ballard Industries interests are protected from lab activities.

2.0 Scope
This policy applies to all internally connected labs, Ballard Industries employees and third parties who access Ballard Industries labs. All existing and future equipment, which fall under the scope of this policy, must be configured according to the referenced documents. DMZ Labs and stand-alone, air-gapped labs are exempt from this policy. DMZ labs must comply with the *DMZ Lab Security Policy*.

3.0 Policy

3.1 Ownership Responsibilities
1. Lab owning organizations are responsible for assigning lab managers, a point of contact (POC), and a back-up POC for each lab. Lab owners must maintain up-to-date POC information with InfoSec and the Corporate Enterprise Management Team. Lab managers or their backup must be available around-the-clock for emergencies, otherwise actions will be taken without their involvement.

2. Lab managers are responsible for the security of their labs and the lab's impact on the corporate production network and any other networks. Lab managers are responsible for adherence to this policy and associated processes. Where policies and procedures are undefined lab managers must do their best to safeguard Ballard Industries from security vulnerabilities.

3. Lab managers are responsible for the lab's compliance with all Ballard Industries security policies. The following are particularly important: *Password Policy for networking devices and hosts, Wireless Security Policy, Anti-Virus Policy, and physical security*.

4. The Lab Manager is responsible for controlling lab access. Access to any given lab will only be granted by the lab manager or designee, to those individuals with an immediate business need within the lab, either short-term or as defined by their ongoing job function. This includes continually monitoring the access list to ensure that those who no longer require access to the lab have their access terminated.

5. The Network Support Organization must maintain a firewall device between the corporate production network and all lab equipment.

6. The Network Support Organization and/or InfoSec reserve the right to interrupt lab connections that impact the corporate production network negatively or pose a security risk.

7. The Network Support Organization must record all lab IP addresses, which are routed within Ballard Industries networks, in Enterprise Address Management database along with current contact information for that lab.

8. Any lab that wants to add an external connection must provide a diagram and documentation to InfoSec with business justification, the equipment, and the IP address space information. InfoSec will review for security concerns and must approve before such connections are implemented.

9. All user passwords must comply with Bright Industries's *Password Policy*. In addition, individual user accounts on any lab device must be deleted when no longer authorized within three (3) days. Group account passwords on lab computers (Unix, windows, etc) must be changed quarterly (once every 3 months). For any lab device that contains Ballard Industries proprietary information, group account passwords must be changed within three (3) days following a change in group membership.

10. No lab shall provide production services. Production services are defined as ongoing and shared business critical services that generate revenue streams or provide customer capabilities. These should be managed by a <proper support> organization.

11. InfoSec will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

3.2 General Configuration Requirements

1. All traffic between the corporate production and the lab network must go through a Network Support Organization maintained firewall. Lab network devices (including wireless) must not cross-connect the lab and production networks.

2. Original firewall configurations and any changes thereto must be reviewed and approved by InfoSec. InfoSec may require security improvements as needed.

3. Labs are prohibited from engaging in port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact the corporate network and/or non-Ballard Industries networks. These activities must be restricted within the lab.

4. Traffic between production networks and lab networks, as well as traffic between separate lab networks, is permitted based on business needs and as long as the traffic does not negatively impact on other networks. Labs must not advertise network services that may compromise production network services or put lab confidential information at risk.

5. InfoSec reserves the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls and network peripherals.

6. Lab owned gateway devices are required to comply with all Ballard Industries product security advisories and must authenticate against the Corporate Authentication servers.

7. The enable password for all lab owned gateway devices must be different from all other equipment passwords in the lab. The password must be in accordance with Bright Industries's *Password Policy*. The password will only be provided to those who are authorized to administer the lab network.

8. In labs where non-Ballard Industries personnel have physical access (e.g., training labs), direct connectivity to the corporate production network is not allowed. Additionally, no Ballard Industries confidential information can reside on any computer equipment in these labs. Connectivity for authorized personnel from these labs can be allowed to the corporate production network only if authenticated against the Corporate

Authentication servers, temporary access lists (lock and key), SSH, client VPNs, or similar technology approved by InfoSec.

9. Infrastructure devices (e.g. IP Phones) needing corporate network connectivity must adhere to the *Open Areas Policy.*

10. All lab external connection requests must be reviewed and approved by InfoSec. Analog or ISDN lines must be configured to only accept trusted call numbers. Strong passwords must be used for authentication.

11. All labs networks with external connections must not be connected to Ballard Industries corporate production network or any other internal network directly or via a wireless connection, or via any other form of computing equipment. A waiver from InfoSec is required where air-gapping is not possible (e.g., Partner Connections to third party networks).

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions
Internal - A lab that is within Bright Industries's corporate firewall and connected to Bright Industries's corporate production network
Network Support Organization - Any InfoSec approved Ballard Industries support organization that manages the networking of non-lab networks.
Lab Manager - The individual responsible for all lab activities and personnel
Lab - A Lab is any non-production environment, intended specifically for developing, demonstrating, training and/or testing of a product.
External Connections (also known as DMZ) - External connections include (but not limited to) third-party data network-to-network, analog and ISDN data lines, or any other Telco data lines.
Lab Owned Gateway Device - A lab owned gateway device is the lab device that connects the lab network to the rest of Ballard Industries network. All traffic between the lab and the corporate production network must pass through the lab owned gateway device unless approved by InfoSec.
Telco - A Telco is the equivalent to a service provider. Telcos offer network connectivity, e.g., T1, T3, OC3, OC12 or DSL. Telcos are sometimes referred to as "baby bells", although Sprint and AT&T are also considered Telcos. Telco interfaces include BRI, or Basic Rate Interface - a structure commonly used for ISDN service, and PRI, Primary Rate Interface - a structure for voice/dial-up service.
Traffic - Mass volume of unauthorized and/or unsolicited network Spamming/Flooding traffic.
Firewall - A device that controls access between networks. It can be a PIX, a router with access control lists or similar security devices approved by InfoSec.
Extranet - Connections between third parties that require access to connections non-public Ballard Industries resources, as defined in InfoSec's Extranet policy (link).
DMZ (De-Militarized Zone) - This describes network that exists outside of primary corporate firewalls, but are still under Ballard Industries administrative control.

6.0 Revision History

Internal Lab Security Policy

1.0 Purpose
This policy establishes information security requirements for Ballard Industries labs to ensure that Ballard Industries confidential information and technologies are not compromised, and that production services and other Ballard Industries interests are protected from lab activities.

2.0 Scope
This policy applies to all internally connected labs, Ballard Industries employees and third parties who access Ballard Industries labs. All existing and future equipment, which fall under the scope of this policy, must be configured according to the referenced documents. DMZ Labs and stand-alone, air-gapped labs are exempt from this policy. DMZ labs must comply with the *DMZ Lab Security Policy*.

3.0 Policy

3.1 Ownership Responsibilities
1. Lab owning organizations are responsible for assigning lab managers, a point of contact (POC), and a back-up POC for each lab. Lab owners must maintain up-to-date POC information with InfoSec and the Corporate Enterprise Management Team. Lab managers or their backup must be available around-the-clock for emergencies, otherwise actions will be taken without their involvement.

2. Lab managers are responsible for the security of their labs and the lab's impact on the corporate production network and any other networks. Lab managers are responsible for adherence to this policy and associated processes. Where policies and procedures are undefined lab managers must do their best to safeguard Ballard Industries from security vulnerabilities.

3. Lab managers are responsible for the lab's compliance with all Ballard Industries security policies. The following are particularly important: *Password Policy for networking devices and hosts, Wireless Security Policy, Anti-Virus Policy, and physical security*.

4. The Lab Manager is responsible for controlling lab access. Access to any given lab will only be granted by the lab manager or designee, to those individuals with an immediate business need within the lab, either short-term or as defined by their ongoing job function. This includes continually monitoring the access list to ensure that those who no longer require access to the lab have their access terminated.

5. The Network Support Organization must maintain a firewall device between the corporate production network and all lab equipment.

6. The Network Support Organization and/or InfoSec reserve the right to interrupt lab connections that impact the corporate production network negatively or pose a security risk.

7. The Network Support Organization must record all lab IP addresses, which are routed within Ballard Industries networks, in Enterprise Address Management database along with current contact information for that lab.

8. Any lab that wants to add an external connection must provide a diagram and documentation to InfoSec with business justification, the equipment, and the IP address space information. InfoSec will review for security concerns and must approve before such connections are implemented.

9. All user passwords must comply with Bright Industries's *Password Policy*. In addition, individual user accounts on any lab device must be deleted when no longer authorized within three (3) days. Group account passwords on lab computers (Unix, windows, etc) must be changed quarterly (once every 3 months). For any lab device that contains Ballard Industries proprietary information, group account passwords must be changed within three (3) days following a change in group membership.

10. No lab shall provide production services. Production services are defined as ongoing and shared business critical services that generate revenue streams or provide customer capabilities. These should be managed by a <proper support> organization.

11. InfoSec will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

3.2 General Configuration Requirements

1. All traffic between the corporate production and the lab network must go through a Network Support Organization maintained firewall. Lab network devices (including wireless) must not cross-connect the lab and production networks.

2. Original firewall configurations and any changes thereto must be reviewed and approved by InfoSec. InfoSec may require security improvements as needed.

3. Labs are prohibited from engaging in port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact the corporate network and/or non-Ballard Industries networks. These activities must be restricted within the lab.

4. Traffic between production networks and lab networks, as well as traffic between separate lab networks, is permitted based on business needs and as long as the traffic does not negatively impact on other networks. Labs must not advertise network services that may compromise production network services or put lab confidential information at risk.

5. InfoSec reserves the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls and network peripherals.

6. Lab owned gateway devices are required to comply with all Ballard Industries product security advisories and must authenticate against the Corporate Authentication servers.

7. The enable password for all lab owned gateway devices must be different from all other equipment passwords in the lab. The password must be in accordance with Bright Industries's *Password Policy*. The password will only be provided to those who are authorized to administer the lab network.

8. In labs where non-Ballard Industries personnel have physical access (e.g., training labs), direct connectivity to the corporate production network is not allowed. Additionally, no Ballard Industries confidential information can reside on any computer equipment in these labs. Connectivity for authorized personnel from these labs can be allowed to the corporate production network only if authenticated against the Corporate

Authentication servers, temporary access lists (lock and key), SSH, client VPNs, or similar technology approved by InfoSec.

9. Infrastructure devices (e.g. IP Phones) needing corporate network connectivity must adhere to the *Open Areas Policy.*

10. All lab external connection requests must be reviewed and approved by InfoSec. Analog or ISDN lines must be configured to only accept trusted call numbers. Strong passwords must be used for authentication.

11. All labs networks with external connections must not be connected to Ballard Industries corporate production network or any other internal network directly or via a wireless connection, or via any other form of computing equipment. A waiver from InfoSec is required where air-gapping is not possible (e.g., Partner Connections to third party networks).

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions
Internal - A lab that is within Bright Industries's corporate firewall and connected to Bright Industries's corporate production network
Network Support Organization - Any InfoSec approved Ballard Industries support organization that manages the networking of non-lab networks.
Lab Manager - The individual responsible for all lab activities and personnel
Lab - A Lab is any non-production environment, intended specifically for developing, demonstrating, training and/or testing of a product.
External Connections (also known as DMZ) - External connections include (but not limited to) third-party data network-to-network, analog and ISDN data lines, or any other Telco data lines.
Lab Owned Gateway Device - A lab owned gateway device is the lab device that connects the lab network to the rest of Ballard Industries network. All traffic between the lab and the corporate production network must pass through the lab owned gateway device unless approved by InfoSec.
Telco - A Telco is the equivalent to a service provider. Telcos offer network connectivity, e.g., T1, T3, OC3, OC12 or DSL. Telcos are sometimes referred to as "baby bells", although Sprint and AT&T are also considered Telcos. Telco interfaces include BRI, or Basic Rate Interface - a structure commonly used for ISDN service, and PRI, Primary Rate Interface - a structure for voice/dial-up service.
Traffic - Mass volume of unauthorized and/or unsolicited network Spamming/Flooding traffic.
Firewall - A device that controls access between networks. It can be a PIX, a router with access control lists or similar security devices approved by InfoSec.
Extranet - Connections between third parties that require access to connections non-public Ballard Industries resources, as defined in InfoSec's Extranet policy (link).
DMZ (De-Militarized Zone) - This describes network that exists outside of primary corporate firewalls, but are still under Ballard Industries administrative control.

6.0 Revision History

Password Policy

1.0 Overview
Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Ballard Industries entire corporate network. As such, all Ballard Industries employees (including contractors and vendors with access to Ballard Industries systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose
The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope
The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Ballard Industries facility, has access to the Ballard Industries network, or stores any non-public Ballard Industries information.

4.0 Policy
4.1 General
All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
All production system-level passwords must be part of the InfoSec administered global password management database.
All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
Passwords must not be inserted into email messages or other forms of electronic communication.
Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines
A. General Password Construction Guidelines
Passwords are used for various purposes at Bright Industries. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

The password contains less than eight characters
The password is a word found in a dictionary (English or foreign)
The password is a common usage word such as:
Names of family, pets, friends, co-workers, fantasy characters, etc.
Computer terms and names, commands, sites, companies, hardware, software.
The words "Bright Industries", "sanjose", "sanfran" or any derivation.
Birthdays and other personal information such as addresses and phone numbers.
Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.

Any of the above spelled backwards.
Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

Contain both upper and lower case characters (e.g., a-z, A-Z)
Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
Are at least eight alphanumeric characters long.
Are not a word in any language, slang, dialect, jargon, etc.
Are not based on personal information, names of family, etc.
Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards
Do not use the same password for Ballard Industries accounts as for other non-Ballard Industries access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Ballard Industries access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share Ballard Industries passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Ballard Industries information.

Here is a list of "dont's":

Don't reveal a password over the phone to ANYONE
Don't reveal a password in an email message
Don't reveal a password to the boss
Don't talk about a password in front of others
Don't hint at the format of a password (e.g., "my family name")
Don't reveal a password on questionnaires or security forms
Don't share a password with family members
Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to InfoSec and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by InfoSec or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards
Application developers must ensure their programs contain the following security precautions. Applications:
should support authentication of individual users, not groups.
should not store passwords in clear text or in any easily reversible form.
should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users
Access to the Ballard Industries Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases
Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

5.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Terms	**Definitions**
Application Administration Account	Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

7.0 Revision History

Remote Access Policy

1.0 Purpose
The purpose of this policy is to define standards for connecting to Ballard Industries network from any host. These standards are designed to minimize the potential exposure to Ballard Industries from damages which may result from unauthorized use of Ballard Industries resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Ballard Industries internal systems, etc.

2.0 Scope
This policy applies to all Ballard Industries employees, contractors, vendors and agents with a Bright Industries-owned or personally-owned computer or workstation used to connect to the Ballard Industries network. This policy applies to remote access connections used to do work on behalf of Bright Industries, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy
3.1 General
It is the responsibility of Ballard Industries employees, contractors, vendors and agents with remote access privileges to Ballard Industries corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Bright Industries. General access to the Internet for recreational use by immediate household members through the Ballard Industries Network on personal computers is permitted for employees that have flat-rate services. The Ballard Industries employee is responsible to ensure the family member does not violate any Ballard Industries policies, does not perform illegal activities, and does not use the access for outside business interests. The Ballard Industries employee bears responsibility for the consequences should the access be misused.
Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Ballard Industries network:
Acceptable Encryption Policy
Virtual Private Network (VPN) Policy
Wireless Communications Policy
Acceptable Use Policy
For additional information regarding Ballard Industries remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

3.2 Requirements
Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.
At no time should any Ballard Industries employee provide their login or email password to anyone, not even family members.
Ballard Industries employees and contractors with remote access privileges must ensure that their Bright Industries-owned or personal computer or workstation, which is remotely connected to Ballard Industries corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
Ballard Industries employees and contractors with remote access privileges to Ballard Industries corporate network must not use non-Ballard Industries email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Ballard Industries business, thereby ensuring that official business is never confused with personal business.

Routers for dedicated ISDN lines configured for access to the Ballard Industries network must meet minimum authentication requirements of CHAP.
Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
Frame Relay must meet minimum authentication requirements of DLCI standards.
Non-standard hardware configurations must be approved by Remote Access Services, and InfoSec must approve security configurations for access to hardware.
All hosts that are connected to Ballard Industries internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
Personal equipment that is used to connect to Ballard Industries networks must meet the requirements of Bright Industries-owned equipment for remote access.
Organizations or individuals who wish to implement non-standard Remote Access solutions to the Ballard Industries production network must obtain prior approval from Remote Access Services and InfoSec.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	Definition
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCIData Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a Bright Industries-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into Ballard Industries and an ISP, depending on packet destination.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Frame Relay	A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.
ISDN	There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

Remote Access	Any access to Ballard Industries corporate network through a non-Ballard Industries controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-Ballard Industries network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Ballard Industries corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

6.0 Revision History

Appendix G - Document MetaData

Table 30 - Document MetaData

Document Name	Author	Revision Number	Company Name	Creation Date	Date Last Saved
Acceptable Encryption Policy	Ballard	11	Ballard Industries, Inc.	8/9/2001	4/20/2004
Information Sensitivity Policy	Ballard	10	Ballard Industries, Inc.	8/13/2001	4/20/2004
Internal Lab Security Policy	Ballard	8	Ballard Industries, Inc.	10/9/2001	4/20/2004
Internal Lab Security Policy1	Ballard	8	Ballard Industries, Inc.	10/9/2001	4/20/2004
Password Policy	Ballard	10	Cisco Systems	8/8/2001	4/23/2004
Remote Access Policy	Ballard	8	Cisco Systems	8/8/2001	4/23/2004

Appendix H - Document Statistics

Table 31 - Document Statistics

Document Name	Word Count	Character Count (Not Including Spaces)	Character Count (Including Spaces)	Length (Bytes)
Acceptable Encryption Policy	343	1,915	2,357	22,548
Information Sensitivity Policy	2,045	12,208	14,460	42,496
Internal Lab Security Policy	1,329	7,663	8,973	33,423
Internal Lab Security Policy1	1,329	7,663	8,973	32,256
Password Policy	1,257	6,806	8,126	307,935
Remote Access Policy	1,144	6,559	7,767	215895
Sample Document 1 (Text from Acceptable Encryption Policy)	343	1,915	2,357	21,504
Sample Document 2 (Text from Remote Access Policy)	1,144	6,559	7,767	7,913

Camouflage v1.2.1

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

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 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.

Camouflaging Files

After installing Camouflage you will find two new menu options when right-clicking files in Windows Explorer; 'Camouflage' and 'Uncamouflage'.

You can camouflage a file or several files at a time by highlighting them in Windows Explorer, then clicking the right mouse button and choosing 'Camouflage' from the pop-up menu.

A list of the files chosen is displayed in the Camouflage dialog.
You can view/edit the files by double-clicking them with the mouse, or by highlighting and right-clicking them, then choosing 'Open' from the pop-up menu. Selecting 'Properties' from this menu will display an information page similar to that in Windows Explorer.
Anyway, to continue click 'Next'.

In the second screen choose a file to be used as camouflage. This can be any type of file, but some files work better than others. For example, avoid choosing a text file because Notepad would display the entire contents of it, including the scrambled files attached. Most other files work well.
Camouflage remembers the last 10 files used and you can reuse one of them by selecting it from the drop-down list.
Note that Camouflage will simply use a copy of the selected file. The original chosen file will not be altered in any way.
Once you have selected a file, click 'Next'.

From the third screen choose the folder and filename of the camouflaged file that will be created. The default folder is the folder where you selected the files in Windows

Explorer, and the default filename is the name of the file you selected for use as camouflage in the previous screen.
Check 'Read-only' to create the camouflaged file with its 'Read-Only' attribute set. This is recommended because it makes the file safer, and prevents other applications from modifying it and destroying the camouflaged section.
Click 'Next'.

From the final screen you can type in a password if you wish. This password will be required when extracting files from your camouflaged file. If you do not wish to add a password just click 'Finish'.
Clicking 'Finish' will create the camouflaged file and then exit.

Uncamouflaging Files

To extract the files hidden within a camouflaged file, right-click it in Windows Explorer and choose 'Uncamouflage' from the pop-up menu.

A password prompt appears in the Uncamouflage dialog. If this file was created with a password, type it in.
Note that Camouflage was designed so that it doesn't reveal camouflaged files to the casual observer. For this reason the password screen is always displayed whether the file is a camouflaged file or not, or whether or not it contains a password.
Once you have entered the correct password (if applicable), click 'Next'.

The second screen displays a list of the files hidden within the camouflaged file. The first file in the list is the file originally used as camouflage.
To extract all files from the camouflaged file, either select them all, or just click 'Next' without selecting any files. You can extract certain files by selecting them, then clicking 'Next'. Note that you can deselect files by holding down CTRL and left-clicking them with the mouse.
You can view the files by double-clicking them with the mouse, or by highlighting and right-clicking them, then choosing 'Open' from the pop-up menu. Note that files modified in this way will not be changed in the archive. You can display further information about the files by choosing 'Properties' from this menu.

From the final screen, choose the folder where the files are to be extracted. If you're not extracting the first file in the list (the file originally used as camouflage), the default folder will be the folder where you right-clicked on the camouflaged file in Windows Explorer.
Click 'Finish' to extract the files and exit.

Uncamouflaging several files at once

It is possible to uncamouflage several files at once by selecting them in Windows Explorer and choosing 'Uncamouflage' from the pop-up menu.

Note that Camouflage will only allow you to do this if all the files are using the same password, or if none of the files are using a password.

The contents of each file is displayed in the second screen, and you can uncamouflage them in the usual way.

Configuring Camouflage Settings

You can modify Camouflage settings by running Camouflage from the Windows Start Menu shortcut, by opening the folder where you installed Camouflage and double-

clicking Camouflage.exe from Windows Explorer, or by clicking the 'Settings' button on the first screen.

The Camouflage Settings screen will appear. The version number is displayed in the title bar.

You can add or remove columns in the file selection screens (Size, Creation Date/Time, Modified Date/Time, Accessed Date, File Attributes) by checking or unchecking items in the 'Show File Details' area.

You can switch the pop-up help messages on or off by checking or unchecking 'Tool Tips'.

You can hide Camouflage from Windows Explorer by unchecking 'Show Camouflage menu options when right-clicking on files in Windows Explorer'.
When checked, Camouflage is enabled and you can right-click on files in Windows Explorer to use the Camouflage options.
When unchecked, Camouflage is disabled and the menu options do not appear when right-clicking on files in Windows Explorer.

Or you can disguise Camouflage in Windows Explorer by changing the 'Camouflage' or 'Uncamouflage' pop-up menu captions to whatever you want. When changed, the Camouflage icons do not appear.
To return the prompts and icons to normal, you can delete the text in the 'Camouflage' or 'Uncamouflage' fields.

By checking 'Make camouflaged files Read-Only', all files created by Camouflage have their Read-Only attribute set by default. This is highly recommended and prevents the camouflaged file from being modified by certain applications when you open it.

You can also display this Readme.txt file from Camouflage by clicking the 'View Readme File' button.

Tips for Using Camouflage

Although they do work well, text files are not recommended to be used as camouflage. Files with '.txt' extensions are usually opened with Notepad by default. Notepad will display the entire file, including the encrypted camouflaged section which might give the game away.
Most other applications will just open their part of the file, and ignore the camouflaged section.

Certain files, for example, Microsoft Excel files, are often modified by their native application when opened by it. It is recommended that you always make camouflaged files Read-Only. This prevents these applications from modifying the camouflaged file and therefore destroying the camouflaged section.

Be careful when uploading camouflaged files (especially text files) to an FTP site. Many FTP applications will 'auto-detect' the transfer type, and will upload text files as ASCII.
This would destroy the binary section of the file (the camouflaged section), so you must make sure that when uploading camouflaged files, you always set the transfer type to BINARY.

Be careful to remember your password, if you use one. We can't help you if you forget it and can't open your camouflaged file.

For additional tips, check out the FAQ on our web site.

Technical Support and Feedback

This product is completely free, we ask only that you show your support by visiting our web site at http://www.camouflagesoftware.com where you can freely download the latest version.

When using Camouflage you can click on the link 'Click here to get the latest version' to automatically go to the Camouflage web site. The current version you are using is displayed when you move the mouse pointer over this link.

Unfortunately Camouflage is no longer supported, but you can still use the web forum and guest book.

History

Camouflage v1.2.1
---
* Users can now uncamouflage multiple files in one session
* Added option to write-protect camouflaged files (by default)
* 'Settings' button added to first screen
* The version of Camouflage used to camouflage the files is now displayed
* Prompt for overwrite when creating the camouflage file, if the output file already exists
* User is prevented from specifying an output file that would overwrite one of the selected files for camouflaging
* Web page references now point to www.camouflagesoftware.com
* Cleaned up resize limiter
* Other miscellaneous changes

Camouflage v1.1.2
---
* Added support for additional regional standards, e.g. Brazilian.
* Updated runtime files in installation.
* Cleaned up the user prompt when overwriting files.

Camouflage v1.1.1
---
* Added option to open files when displaying them (double-click or right-click for menu).
* Added 'Properties' page for files (right-click for menu).
* Added file sizes, dates/times and attributes when displaying files.
* Added feature to change Windows Explorer pop-up menu captions.
* Added file icons in selection screens.
* Camouflage is now resizable. Settings and file selection column widths are saved.
* Added user prompts when overwriting files.
* Added prompt to create folder when extracting files.
* Camouflage version appears briefly in the title bar.
* Added 'email us' link in Settings.
* Added Tool Tips (can be switched off in Settings).

Camouflage v1.0.4
---
* First release.

www.camouflagesoftware.com

Appendix J - Camouflage End User License Agreement

Camouflage is Freeware. You are encouraged to freely use and distribute it provided that no files are added or removed from the archive, and that all files contained within the archive are distributed together.

All titles and copyrights in and to Camouflage are owned exclusively by Twisted Pear Productions. You may not reverse engineer, decompile, disassemble or alter Camouflage software in any way.

To the maximum extent permitted by applicable law, in no event shall the individual author(s) or Twisted Pear Productions be liable for any special, incidental, indirect, or consequential damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use Camouflage or the provision of or failure to provide Support Services.

You may not use Camouflage for unlawful activities.

If you decide to use Camouflage, please show your support by visiting our web site at http://www.camouflagesoftware.com where you can freely download the latest version.

Feedback is always encouraged. Please email bug-reports, comments, ideas or criticism to feedback@camouflagesoftware.com. Please include the version number of your copy and where you found it.

If you find any bugs with Camouflage, please email as much information as possible. Make sure you mention exactly what you were doing when the error occurred. When the bug has been fixed we can let you know via email.

http://www.camouflagesoftware.com
feedback@camouflagesoftware.com

Appendix K - Hex / Character Translation Table

Table 32 - Hex / Character Translation Table

Hex / Text		Hex / Text		Hex / Text	
61	a	41	A	30	0
62	b	42	B	31	1
63	c	43	C	32	2
64	d	44	D	33	3
65	e	45	E	34	4
66	f	46	F	35	5
67	g	47	G	36	6
68	h	48	H	37	7
69	i	49	I	38	8
6A	j	4A	J	39	9
6B	k	4B	K		
6C	l	4C	L		
6D	m	4D	M		
6E	n	4E	N		
6F	o	4F	O		
70	p	50	P		
71	q	51	Q		
72	r	52	R		
73	s	53	S		
74	t	54	T		
75	u	55	U		
76	v	56	V		
77	w	57	W		
78	x	58	X		
79	y	59	Y		
7A	z	5A	Z		

Internal Lab Security Policy

1.0 Purpose
This policy establishes information security requirements for Ballard Industries labs to ensure that Ballard Industries confidential information and technologies are not compromised, and that production services and other Ballard Industries interests are protected from lab activities.

2.0 Scope
This policy applies to all internally connected labs, Ballard Industries employees and third parties who access Ballard Industries labs. All existing and future equipment, which fall under the scope of this policy, must be configured according to the referenced documents. DMZ Labs and stand-alone, air-gapped labs are exempt from this policy. DMZ labs must comply with the *DMZ Lab Security Policy*.

3.0 Policy

3.1 Ownership Responsibilities
1. Lab owning organizations are responsible for assigning lab managers, a point of contact (POC), and a back-up POC for each lab. Lab owners must maintain up-to-date POC information with InfoSec and the Corporate Enterprise Management Team. Lab managers or their backup must be available around-the-clock for emergencies, otherwise actions will be taken without their involvement.

2. Lab managers are responsible for the security of their labs and the lab's impact on the corporate production network and any other networks. Lab managers are responsible for adherence to this policy and associated processes. Where policies and procedures are undefined lab managers must do their best to safeguard Ballard Industries from security vulnerabilities.

3. Lab managers are responsible for the lab's compliance with all Ballard Industries security policies. The following are particularly important: *Password Policy for networking devices and hosts, Wireless Security Policy, Anti-Virus Policy, and physical security*.

4. The Lab Manager is responsible for controlling lab access. Access to any given lab will only be granted by the lab manager or designee, to those individuals with an immediate business need within the lab, either short-term or as defined by their ongoing job function. This includes continually monitoring the access list to ensure that those who no longer require access to the lab have their access terminated.

5. The Network Support Organization must maintain a firewall device between the corporate production network and all lab equipment.

6. The Network Support Organization and/or InfoSec reserve the right to interrupt lab connections that impact the corporate production network negatively or pose a security risk.

7. The Network Support Organization must record all lab IP addresses, which are routed within Ballard Industries networks, in Enterprise Address Management database along with current contact information for that lab.

8. Any lab that wants to add an external connection must provide a diagram and documentation to InfoSec with business justification, the equipment, and the IP address space information. InfoSec will review for security concerns and must approve before such connections are implemented.

9. All user passwords must comply with Bright Industries's *Password Policy*. In addition, individual user accounts on any lab device must be deleted when no longer authorized within three (3) days. Group account passwords on lab computers (Unix, windows, etc) must be changed quarterly (once every 3 months). For any lab device that contains Ballard Industries proprietary information, group account passwords must be changed within three (3) days following a change in group membership.

10. No lab shall provide production services. Production services are defined as ongoing and shared business critical services that generate revenue streams or provide customer capabilities. These should be managed by a <proper support> organization.

11. InfoSec will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

3.2 General Configuration Requirements

1. All traffic between the corporate production and the lab network must go through a Network Support Organization maintained firewall. Lab network devices (including wireless) must not cross-connect the lab and production networks.

2. Original firewall configurations and any changes thereto must be reviewed and approved by InfoSec. InfoSec may require security improvements as needed.

3. Labs are prohibited from engaging in port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact the corporate network and/or non-Ballard Industries networks. These activities must be restricted within the lab.

4. Traffic between production networks and lab networks, as well as traffic between separate lab networks, is permitted based on business needs and as long as the traffic does not negatively impact on other networks. Labs must not advertise network services that may compromise production network services or put lab confidential information at risk.

5. InfoSec reserves the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls and network peripherals.

6. Lab owned gateway devices are required to comply with all Ballard Industries product security advisories and must authenticate against the Corporate Authentication servers.

7. The enable password for all lab owned gateway devices must be different from all other equipment passwords in the lab. The password must be in accordance with Bright Industries's *Password Policy*. The password will only be provided to those who are authorized to administer the lab network.

8. In labs where non-Ballard Industries personnel have physical access (e.g., training labs), direct connectivity to the corporate production network is not allowed. Additionally, no Ballard Industries confidential information can reside on any computer equipment in these labs. Connectivity for authorized personnel from these labs can be

allowed to the corporate production network only if authenticated against the Corporate Authentication servers, temporary access lists (lock and key), SSH, client VPNs, or similar technology approved by InfoSec.

9. Infrastructure devices (e.g. IP Phones) needing corporate network connectivity must adhere to the *Open Areas Policy.*

10. All lab external connection requests must be reviewed and approved by InfoSec. Analog or ISDN lines must be configured to only accept trusted call numbers. Strong passwords must be used for authentication.

11. All labs networks with external connections must not be connected to Ballard Industries corporate production network or any other internal network directly or via a wireless connection, or via any other form of computing equipment. A waiver from InfoSec is required where air-gapping is not possible (e.g., Partner Connections to third party networks).

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

- Internal - A lab that is within Bright Industries's corporate firewall and connected to Bright Industries's corporate production network
- Network Support Organization - Any InfoSec approved Ballard Industries support organization that manages the networking of non-lab networks.
- Lab Manager - The individual responsible for all lab activities and personnel
- Lab - A Lab is any non-production environment, intended specifically for developing, demonstrating, training and/or testing of a product.
- External Connections (also known as DMZ) - External connections include (but not limited to) third-party data network-to-network, analog and ISDN data lines, or any other Telco data lines.
- Lab Owned Gateway Device - A lab owned gateway device is the lab device that connects the lab network to the rest of Ballard Industries network. All traffic between the lab and the corporate production network must pass through the lab owned gateway device unless approved by InfoSec.
- Telco - A Telco is the equivalent to a service provider. Telcos offer network connectivity, e.g., T1, T3, OC3, OC12 or DSL. Telcos are sometimes referred to as "baby bells", although Sprint and AT&T are also considered Telcos. Telco interfaces include BRI, or Basic Rate Interface - a structure commonly used for ISDN service, and PRI, Primary Rate Interface - a structure for voice/dial-up service.
- Traffic - Mass volume of unauthorized and/or unsolicited network Spamming/Flooding traffic.
- Firewall - A device that controls access between networks. It can be a PIX, a router with access control lists or similar security devices approved by InfoSec.
- Extranet - Connections between third parties that require access to connections non-public Ballard Industries resources, as defined in InfoSec's Extranet policy (link).
- DMZ (De-Militarized Zone) - This describes network that exists outside of primary corporate firewalls, but are still under Ballard Industries administrative control.

6.0 Revision History

Appendix M - opportunity.txt (Recovered from Internal_Lab_Security_Policy.doc (Tag # fl-260404-RJL1))

I am willing to provide you with more information for a price. I have included a sample of our Client Authorized Table database. I have also provided you with our latest schematics not yet available. They are available as we discussed - "First Name".
My price is 5 million.

R***** J. L*********

(Note: the name is sanitized)

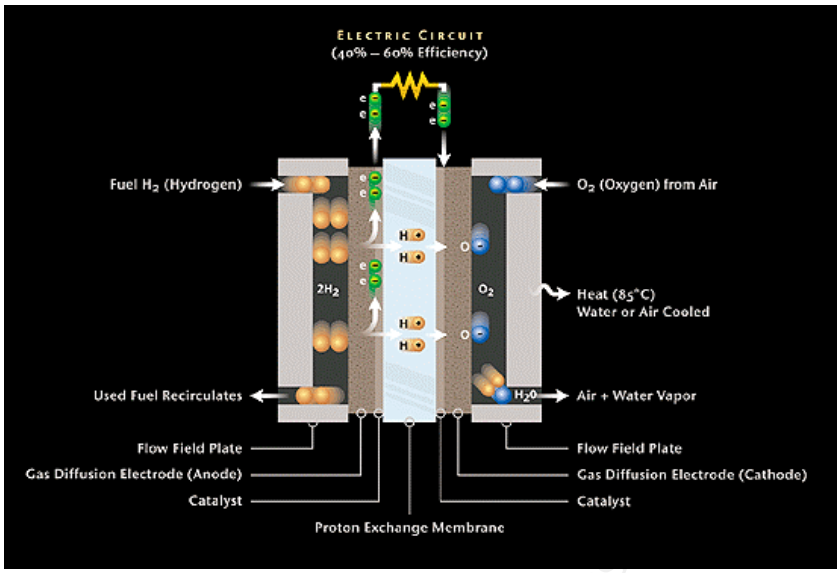


Figure 28 - Recovered Image (pem-fuelcell.gif) Showing Flows Across Proton Exchange Membrane

Password Policy

1.0 Overview
Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Ballard Industries entire corporate network. As such, all Ballard Industries employees (including contractors and vendors with access to Ballard Industries systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose
The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope
The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Ballard Industries facility, has access to the Ballard Industries network, or stores any non-public Ballard Industries information.

4.0 Policy
4.1 General
- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the InfoSec administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines
A. General Password Construction Guidelines
Passwords are used for various purposes at Bright Industries. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "Bright Industries", "sanjose", "sanfran" or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards
Do not use the same password for Ballard Industries accounts as for other non-Ballard Industries access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Ballard Industries access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share Ballard Industries passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Ballard Industries information.

Here is a list of "dont's":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to InfoSec and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by InfoSec or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards
Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users
Access to the Ballard Industries Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases
Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

5.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Terms	Definitions
Application Administration Account	Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

7.0 Revision History

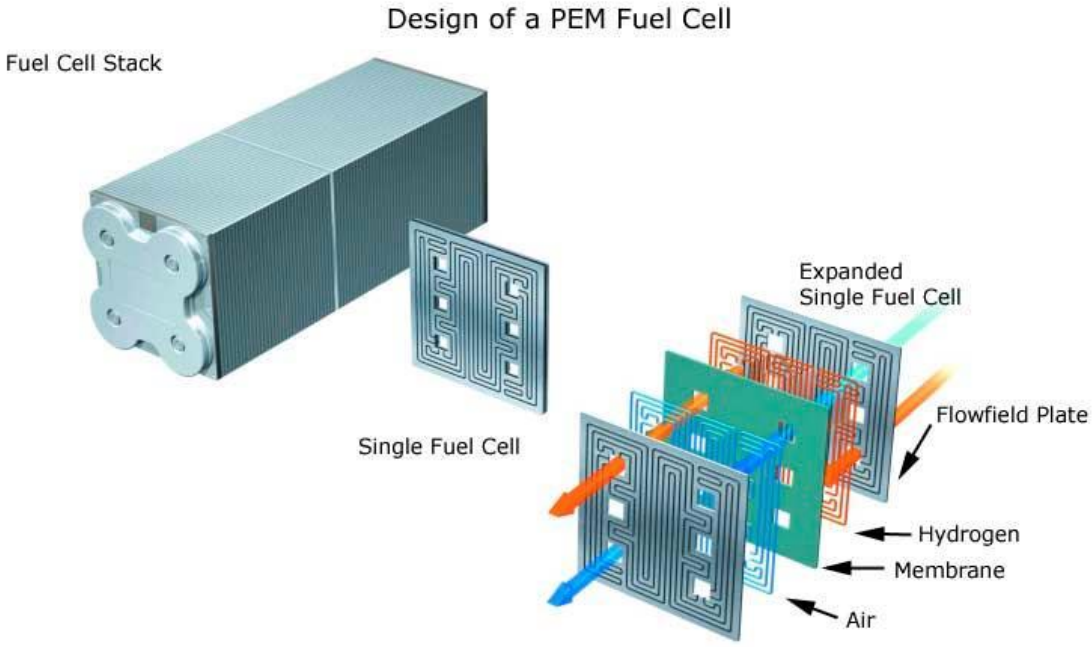


Figure 29 - Recovered Image (PEM-fuel-cell-large.jpg) Showing PEM Fuel Cell Design

Viewing this file with a hex editor shows the string "Adobe" starting at location 2B (hex).

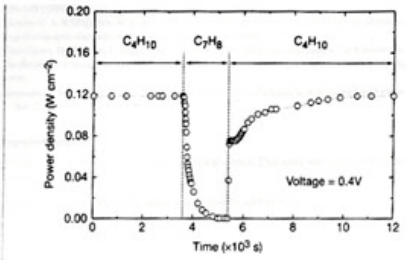


Figure 3 Effect of switching fuel type on the cell with the Cu-ceria composite anode at 973 K. The power density of the cell is shown as a function of time. The fuel was switched from *n*-butane (C_4H_{10}) to toluene (C_7H_8), and back to *n*-butane.

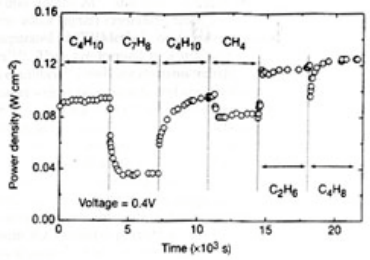


Figure 4 Effect of switching fuel type on the cell with the Cu-(doped ceria) composite anode at 973 K. The power density is shown as a function of time. The fuels were: *n*-butane (C_4H_{10}), toluene (C_7H_8), *n*-butane, methane (CH_4), ethane (C_2H_6), and 1-butene (C_4H_8).

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

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

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

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

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

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

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

The role of samaria in enhancing the results for toluene and some of the other hydrocarbons is uncertain. While samaria is used to enhance mixed (ionic and electronic) conductivity in ceria and could increase the active, three-phase boundary in the anode, samaria is also an active catalyst[12]. Other improvements in the performance of SOFCs are possible. For example, the composite anodes could be easily attached to the cathode-supported, thin-film electrolytes that have been used by others to achieve very high power densities[3]. In addition to raising the power density, thinner electrolytes may also allow lower operating temperatures.

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

Received 13 September 1999; accepted 26 January 2000.

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

Figure 30 - Recovered Image Showing Internal Fuel Cell Processes and Description

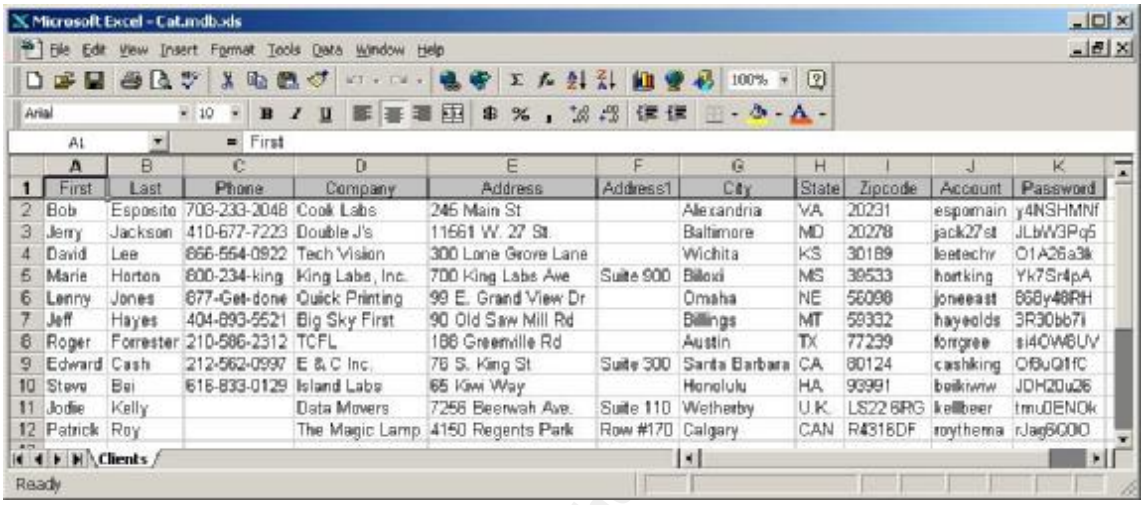
Examination of this file shows the strings:

"Photoshop 3.0" starting at location 18 (hex).

"File written by Adobe Photoshop 4.0" starting at location 154 (hex)

This file could not be read by Microsoft ® Access 97 SR-1 but was read by Microsoft ® Access 2000. It contained a customer database. In order to include this information in this appendix, the Clients table (the only table - no queries or other objects were found in the database) was copied to a Microsoft ® Excel spreadsheet.

Figure 31 - Recovered Database Sample from CAT.mdb



	First	Last	Phone	Company	Address	Address1	City	State	Zipcode	Account	Password
2	Bob	Esposito	703-233-2048	Cook Labs	245 Main St		Alexandria	VA	20231	espomain	y4NSHMNf
3	Jerry	Jackson	410-677-7223	Double J's	11661 W. 27 St.		Baltimore	MD	20278	jack27st	JLbW3Pq5
4	David	Lee	666-564-0922	Tech Vision	300 Lone Grove Lane		Wichita	KS	30189	leetechv	O1A26a3k
5	Marie	Horton	600-234-king	King Labs, Inc.	700 King Labs Ave	Suite 900	Biloxi	MS	39533	hortking	Yk7Sr4pA
6	Lenny	Jones	877-Get-done	Quick Printing	99 E. Grand View Dr		Omaha	NE	56098	joneeast	868y48RH
7	Jeff	Hayes	404-893-5521	Big Sky First	90 Old Saw Mill Rd		Billings	MT	59332	hayeolds	3R30bb7I
8	Roger	Forrester	210-586-2312	TCFL	186 Greenville Rd		Austin	TX	77239	forrgree	si4OW6UV
9	Edward	Cash	212-562-0997	E & C Inc.	76 S. King St	Suite 300	Santa Barbara	CA	80124	cashking	Of9uQ1fC
10	Steve	Bei	616-833-0129	Island Labs	65 Kiwi Way		Honolulu	HA	93991	beikiwsw	JDH2Du26
11	Jodie	Kelly		Data Movers	7256 Beerwah Ave.	Suite 110	Wetherby	U.K.	LS22 6RG	kellbeer	tmuDENOk
12	Patrick	Roy		The Magic Lamp	4150 Regents Park	Row #170	Calgary	CAN	R4316DF	roythema	rJag6Q0O

Remote Access Policy

1.0 Purpose

The purpose of this policy is to define standards for connecting to Ballard Industries network from any host. These standards are designed to minimize the potential exposure to Ballard Industries from damages which may result from unauthorized use of Ballard Industries resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Ballard Industries internal systems, etc.

2.0 Scope

This policy applies to all Ballard Industries employees, contractors, vendors and agents with a Bright Industries-owned or personally-owned computer or workstation used to connect to the Ballard Industries network. This policy applies to remote access connections used to do work on behalf of
Bright Industries, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy

3.1 General

1. It is the responsibility of Ballard Industries employees, contractors, vendors and agents with remote access privileges to Ballard Industries corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Bright Industries.
2. General access to the Internet for recreational use by immediate household members through the Ballard Industries Network on personal computers is permitted for employees that have flat-rate services. The Ballard Industries employee is responsible to ensure the family member does not violate any Ballard Industries policies, does not perform illegal activities, and does not use the access for outside business interests. The Ballard Industries employee bears responsibility for the consequences should the access be misused.
3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Ballard Industries network:
   a. *Acceptable Encryption Policy*
   b. *Virtual Private Network (VPN) Policy*
   c. *Wireless Communications Policy*
   d. *Acceptable Use Policy*
4. For additional information regarding Ballard Industries remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.
2. At no time should any Ballard Industries employee provide their login or email password to anyone, not even family members.

3. Ballard Industries employees and contractors with remote access privileges must ensure that their Bright Industries-owned or personal computer or workstation, which is remotely connected to Ballard Industries corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. Ballard Industries employees and contractors with remote access privileges to Ballard Industries corporate network must not use non-Ballard Industries email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Ballard Industries business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the Ballard Industries network must meet minimum authentication requirements of CHAP.
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. Frame Relay must meet minimum authentication requirements of DLCI standards.
8. Non-standard hardware configurations must be approved by Remote Access Services, and InfoSec must approve security configurations for access to hardware.
9. All hosts that are connected to Ballard Industries internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
10. Personal equipment that is used to connect to Ballard Industries networks must meet the requirements of Bright Industries-owned equipment for remote access.
11. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Ballard Industries production network must obtain prior approval from Remote Access Services and InfoSec.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCIData Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a Bright Industries-provided Remote Access home network,

and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into Ballard Industries and an ISP, depending on packet destination.

DSL Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

Frame Relay A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.

ISDN There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

Remote Access Any access to Ballard Industries corporate network through a non-Ballard Industries controlled network, device, or medium.

Split-tunneling Simultaneous direct access to a non-Ballard Industries network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Ballard Industries corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

6.0 Revision History

Date	Size	MAC Time	Permissions			Node	File Name
Sat Feb 03 2001 19:44:16	36864	m..	-/-rwxrwxrwx	0	0	5	a:\CamShell.dll (_AMSHELL.DLL) (deleted)
Sat Feb 03 2001 19:44:16	36864	m..	-rwxrwxrwx	0	0	5	<v1_5.gz-_AMSHELL.DLL-dead-5>
Thu Apr 22 2004 16:31:06	32256	m..	-/-rwxrwxrwx	0	0	13	a:\Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)
Thu Apr 22 2004 16:31:06	33423	m..	-/-rwxrwxrwx	0	0	17	a:\Internal_Lab_Security_Policy.doc (INTERN~2.DOC)
Fri Apr 23 2004 10:53:56	727	m..	-rwxrwxrwx	0	0	28	<v1_5.gz-_ndex.htm-dead-28>
Fri Apr 23 2004 10:53:56	727	m..	-/-rwxrwxrwx	0	0	28	a:_ndex.htm (deleted)
Fri Apr 23 2004 11:54:32	215895	m..	-/-rwxrwxrwx	0	0	23	a:\Remote_Access_Policy.doc (REMOTE~1.DOC)
Fri Apr 23 2004 11:55:26	307935	m..	-/-rwxrwxrwx	0	0	20	a:\Password_Policy.doc (PASSWO~1.DOC)
Fri Apr 23 2004 14:10:50	22528	m..	-/-rwxrwxrwx	0	0	27	a:\Acceptable_Encryption_Policy.doc (ACCEPT~1.DOC)
Fri Apr 23 2004 14:11:10	42496	m..	-/-rwxrwxrwx	0	0	9	a:\Information_Sensitivity_Policy.doc (INFORM~1.DOC)
Sun Apr 25 2004 00:00:00	0	.a.	-/-rwxrwxrwx	0	0	3	a:\RJL (Volume Label Entry)
Sun Apr 25 2004 10:53:40	0	m.c	-/-rwxrwxrwx	0	0	3	a:\RJL (Volume Label Entry)
Mon Apr 26 2004 00:00:00	32256	.a.	-/-rwxrwxrwx	0	0	13	a:\Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)
Mon Apr 26 2004 00:00:00	727	.a.	-rwxrwxrwx	0	0	28	<v1_5.gz-_ndex.htm-dead-28>
Mon Apr 26 2004 00:00:00	727	.a.	-/-rwxrwxrwx	0	0	28	a:_ndex.htm (deleted)
Mon Apr 26 2004 00:00:00	36864	.a.	-rwxrwxrwx	0	0	5	<v1_5.gz-_AMSHELL.DLL-dead-5>
Mon Apr 26 2004 00:00:00	36864	.a.	-/-rwxrwxrwx	0	0	5	a:\CamShell.dll (_AMSHELL.DLL) (deleted)
Mon Apr 26 2004 00:00:00	22528	.a.	-/-rwxrwxrwx	0	0	27	a:\Acceptable_Encryption_Policy.doc (ACCEPT~1.DOC)
Mon Apr 26 2004 00:00:00	215895	.a.	-/-rwxrwxrwx	0	0	23	a:\Remote_Access_Policy.doc (REMOTE~1.DOC)
Mon Apr 26 2004 00:00:00	33423	.a.	-/-rwxrwxrwx	0	0	17	a:\Internal_Lab_Security_Policy.doc (INTERN~2.DOC)
Mon Apr 26 2004 00:00:00	307935	.a.	-/-rwxrwxrwx	0	0	20	a:\Password_Policy.doc (PASSWO~1.DOC)
Mon Apr 26 2004 00:00:00	42496	.a.	-/-rwxrwxrwx	0	0	9	a:\Information_Sensitivity_Policy.doc (INFORM~1.DOC)
Mon Apr 26 2004 09:46:18	36864	..c	-/-rwxrwxrwx	0	0	5	a:\CamShell.dll (_AMSHELL.DLL) (deleted)
Mon Apr 26 2004 09:46:18	36864	..c	-rwxrwxrwx	0	0	5	<v1_5.gz-_AMSHELL.DLL-dead-5>
Mon Apr 26 2004 09:46:20	42496	..c	-/-rwxrwxrwx	0	0	9	a:\Information_Sensitivity_Policy.doc (INFORM~1.DOC)
Mon Apr 26 2004 09:46:22	32256	..c	-/-rwxrwxrwx	0	0	13	a:\Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)
Mon Apr 26 2004 09:46:24	33423	..c	-/-rwxrwxrwx	0	0	17	a:\Internal_Lab_Security_Policy.doc (INTERN~2.DOC)
Mon Apr 26 2004 09:46:26	307935	..c	-/-rwxrwxrwx	0	0	20	a:\Password_Policy.doc (PASSWO~1.DOC)
Mon Apr 26 2004 09:46:36	215895	..c	-/-rwxrwxrwx	0	0	23	a:\Remote_Access_Policy.doc (REMOTE~1.DOC)
Mon Apr 26 2004 09:46:44	22528	..c	-/-rwxrwxrwx	0	0	27	a:\Acceptable_Encryption_Policy.doc (ACCEPT~1.DOC)
Mon Apr 26 2004 09:47:36	727	..c	-/-rwxrwxrwx	0	0	28	a:_ndex.htm (deleted)
Mon Apr 26 2004 09:47:36	727	..c	-rwxrwxrwx	0	0	28	<v1_5.gz-_ndex.htm-dead-28>

Figure 32 - Timeline from Seized Floppy Disk Imported into Excel

Appendix U - Analysis of Drive_9.img Partition Types

Ran mmls on Drive_9.img to determine partition types:

```
[root@LinuxForensics images]# mmls -v -t dos Drive_9.img
dos_load_prim: Table Sector: 0
load_pri:0:0    Start: 1919950958   Size: 544437093  Type: 32
load_pri:0:1    Start: 1330184202   Size: 538976288  Type: 107
load_pri:0:2    Start: 538989391   Size: 1398362912  Type: 83
load_pri:0:3    Start: 1394627663   Size: 21337  Type: 73
DOS Partition Table
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  -----   0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000001   0538989390   0538989390   Unallocated
02:  00:02   0538989391   1937352302   1398362912   OnTrack Disk Manager (0x53)
03:  00:01   1330184202   1869160489   0538976288   Unknown Type (0x6B)
04:  00:03   1394627663   1394648999   0000021337   Unknown Type (0x49)
05:  -----   1394649000   1919950957   0525301958   Unallocated
06:  00:00   1919950958   2464388050   0544437093   Unknown Type (0x20)
[root@LinuxForensics images]#
```

A little research from here might shed some light on the types:

http://www.win.tue.nl/~aeb/partitions/partition_types-1.html

0x20 - Unused
0x49 – not listed
0x53 – Disk manager 6.0 Aux3
0x6B – not listed

I was unable to determine the partition types except for the OnTrack Disk Manager partition.

Appendix V - Extracts of rlb.exec.log

Explanations of these commands come from the manual pages for each command.

1. Display information about the file system layer – the FAT details.
   '/usr/local/src/sleuthkit/bin/fsstat' -f fat16 '/mnt/analysis/Drive_9/Drive_9.img'

2. Move the image file to the evidence locker.
   /bin/mv '/mnt/analysis/Drive_9/Drive_9.img'
   '/mnt/analysis//Drive9/Host_9//images/Drive_9.img'

3. Create an md5 signature of Drive_9.img image
   '/usr/local/src/sleuthkit/bin/md5' '/mnt/analysis//Drive9/Host_9//images/Drive_9.img'

4. Look for human readable information, or strings, in the image and put them into a file.
   -a = scan all of the file
   -t d = when the radix is printed use a decimal number as opposed to a hex number)
   '/usr/local/bin/strings' -a -t d '/mnt/analysis//Drive9/Host_9/images/Drive_9.img' >
   '/mnt/analysis//Drive9/Host_9/output/Drive_9.img.str'

5. Create an md5 signature for the file containing the strings – created in step 4.
   '/usr/local/src/sleuthkit/bin/md5'
   '/mnt/analysis//Drive9/Host_9/output/Drive_9.img.str'

6. List the content of the unallocated data within the image so that string searches can be done as desired later.
   '/usr/local/src/sleuthkit/bin/dls' -f fat16
   '/mnt/analysis//Drive9/Host_9/images/Drive_9.img' >
   '/mnt/analysis//Drive9/Host_9/output/Drive_9.img.dls'

7. Create an md5 signature for the file created in step 6 – contents of unallocated data.
   '/usr/local/src/sleuthkit/bin/md5'
   '/mnt/analysis//Drive9/Host_9/output/Drive_9.img.dls'

8. Look for strings in the unallocated data and put them into a file.
   -a = scan all of the file
   -t d = when the radix is printed use a decimal number as opposed to a hex number)
   '/usr/local/bin/strings' -a -t d '/mnt/analysis//Drive9/Host_9/output/Drive_9.img.dls' >
   '/mnt/analysis//Drive9/Host_9/output/Drive_9.img.dls.str'

9. Create an md5 signature for the file created in step 8 – contents strings found in unallocated data areas.
'/usr/local/src/sleuthkit/bin/md5'
'/mnt/analysis//Drive9/Host_9/output/Drive_9.img.dls.str'

10 The investigator can now look at the image and see the file names and directories within that image. This information is put into the body file.
-z 'EST' = timezone is set to EST
-s 0 = there is no clock skew (adjustment to times in the file).
-m 'C:/' = display in MACtime format with C:\ as the mount point of the image
-f fat16 = the file system type is fat16
-r = Recursively go through all directories
'/usr/local/src/sleuthkit/bin/fls' -z 'EST' -s 0 -m 'C:/' -f fat16 -r
'/mnt/analysis//Drive9/Host_9/images/Drive_9.img' >>
'/mnt/analysis//Drive9/Host_9/output/body'

11. Display information about all nodes and add it to the end of the body file.
-s 0 = there is no clock skew (adjustment to times in the file).
-m = display in MACtime format.
-t fat16 = the file system type is fat16
'/usr/local/src/sleuthkit/bin/ils' -s 0 -m -f fat16
'/mnt/analysis//Drive9/Host_9/images/Drive_9.img' >>
'/mnt/analysis//Drive9/Host_9/output/body'

12. Create an md5 signature for the file created in steps 10 and 11.
'/usr/local/src/sleuthkit/bin/md5' '/mnt/analysis//Drive9/Host_9/output/body'

13. Create a timeline file using mactime.using the body file created in steps 10 and 11
LANG=C LC_ALL=C - set environment variables for this command
-b …/body = body is the body file
-z 'EST = is the eastern time zone
-I day = a day is used as the time unit when the index file is created
Drive9.timeline.sum is the index file
Drive9.timeline is the timeline file
LANG=C LC_ALL=C '/usr/local/src/sleuthkit/bin/mactime' -b
'/mnt/analysis//Drive9/Host_9/output/body' -z 'EST' -i day
'/mnt/analysis//Drive9/Host_9/output/Drive9.timeline.sum' >
'/mnt/analysis//Drive9/Host_9/output/Drive9.timeline'

14. Create an md5 signature for the timeline created in step 13.
'/usr/local/src/sleuthkit/bin/md5'
'/mnt/analysis//Drive9/Host_9/output/Drive9.timeline'

The drives were clean and contained no offensive software. Here is the scan of drive C:

Figure 33 - Ad-Aware Scan of Drive C:

Here is the scan of drive E:

Figure 34 - Ad-Aware Scan of Drive E:

The drives were clean and contained no viruses, worms or other destructive software.

Here is the scan of drive C:

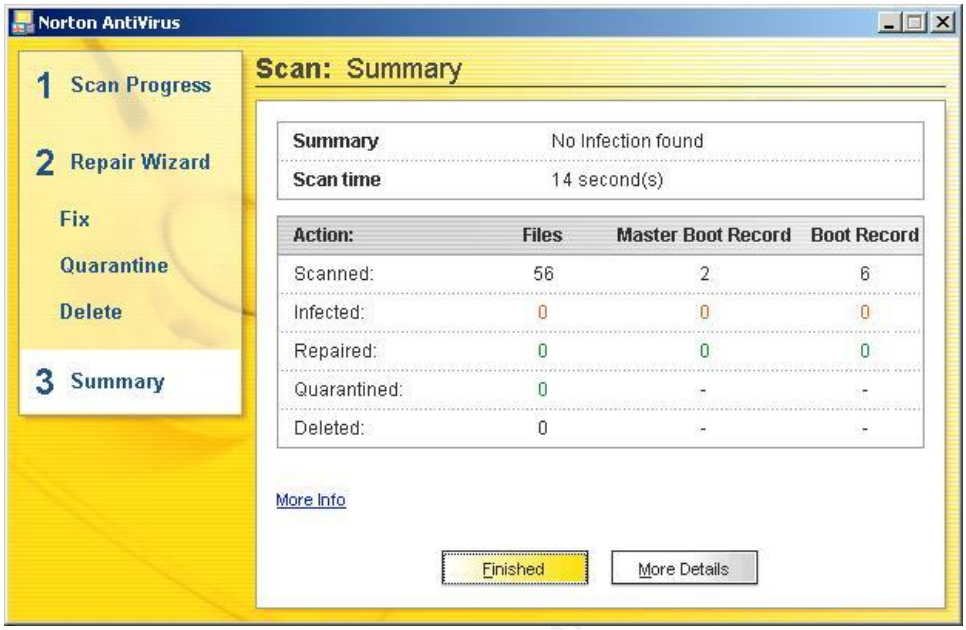


Figure 35 - Anti-Virus Scan of Drive C:

Here is the scan of Drive E:

Figure 36 - Anti-Virus Scan of Drive E:

Registry Report

System\CurrentControlSet\control\ComputerName\ComputerName

Name	Type	Data
ComputerName	REG_SZ	My Internet

Enum\SCSI\MATSHITACD-ROM_CR-562___0\ROOT&*PNPA003&000000

Name	Type	Data
AutoInsertNotification	REG_BINARY	01
UserDriveLetterAssignment	REG_SZ	EE
SCSITargetID	REG_SZ	0
SCSILUN	REG_SZ	0
RevisionLevel	REG_SZ	0.75
ProductId	REG_SZ	CD-ROM CR-562
Manufacturer	REG_SZ	MATSHITA
DeviceType	REG_BINARY	05
Removable	REG_BINARY	01
CurrentDriveLetterAssignment	REG_SZ	E
HardwareID	REG_SZ	MATSHITACD-ROM_CR-562___0,GenCD,SCSI\MATSHITACD-ROM_CR-562___0
Class	REG_SZ	CDROM
Driver	REG_SZ	CDROM\0000
Mfg	REG_SZ	(Standard CD-ROM device)
DeviceDesc	REG_SZ	MATSHITA CD-ROM CR-562

Enum\SCSI\PIONEER_CD-ROM_DR-A02S__1\ROOT&*PNP0600&000100

Name	Type	Data
AutoInsertNotification	REG_BINARY	01
SCSITargetID	REG_SZ	0
SCSILUN	REG_SZ	0
RevisionLevel	REG_SZ	1.07
ProductId	REG_SZ	CD-ROM DR-A02S
Manufacturer	REG_SZ	PIONEER
DeviceType	REG_BINARY	05
Removable	REG_BINARY	01
CurrentDriveLetterAssignment	REG_SZ	D
HardwareID	REG_SZ	PIONEER_CD-ROM_DR-A02S__1,GenCD,SCSI\PIONEER_CD-ROM_DR-A02S__1
Class	REG_SZ	CDROM
Driver	REG_SZ	CDROM\0001
Mfg	REG_SZ	(Standard CD-ROM device)
DeviceDesc	REG_SZ	PIONEER CD-ROM DR-A02S

Enum\SCSI\TEAC____CD-532E-B_____1\ROOT&*PNP0600&000100

Name	Type	Data
AutoInsertNotification	REG_BINARY	01
SCSITargetID	REG_SZ	0
SCSILUN	REG_SZ	0
RevisionLevel	REG_SZ	1.0B
ProductId	REG_SZ	CD-532E-B
Manufacturer	REG_SZ	TEAC
DeviceType	REG_BINARY	05
Removable	REG_BINARY	01
CurrentDriveLetterAssignment	REG_SZ	D
HardwareID	REG_SZ	TEAC____CD-532E-B_____1,GenCD,SCSI\TEAC____CD-532E-B_____1
Class	REG_SZ	CDROM
Driver	REG_SZ	CDROM\0002
Mfg	REG_SZ	(Standard CD-ROM device)
DeviceDesc	REG_SZ	TEAC CD-532E-B

Enum\Monitor\Default_Monitor\0001

Name	Type	Data
DeviceDesc	REG_SZ	IBM 8515
Class	REG_SZ	Monitor
Driver	REG_SZ	Monitor\0000
Mfg	REG_SZ	IBM PC Company
HardwareID	REG_SZ	Monitor\IBM8515

SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
UserDataUninstall	REG_SZ	loadwc.exe /u

Enum\LPTENUM\CANONBJC-2100FE1C\ROOT&*PNP0400&0000

Name	Type	Data
Model	REG_SZ	BJC-2100
Manufacturer	REG_SZ	Canon
DeviceDesc	REG_SZ	Canon BJC-2100
Class	REG_SZ	PRINTER
HardwareID	REG_SZ	LPTENUM\CANONBJC-2100FE1C

Registry Report

.Default\Software\Netscape\Netscape Navigator\User

Name	Type	Data
User_Name	REG_SZ	J*** F*****
User_Organization	REG_SZ	C******* H******* of F******
User_Addr	REG_SZ	j******@bitstorm.net
Reply_To	REG_SZ	j******@bitstorm.net

.Default\Software\Mirabilis\ICQ\Owners\9******

Name	Type	Data
Name	REG_SZ	o********

.Default\Software\Mirabilis\ICQ\Owners\9******\Prefs

Name	Type	Data
Default File Dir	REG_SZ	C:\Program Files\ICQ\Received Files
SMTP Address	REG_SZ	mail.bitstorm.net
Chat Message	REG_SZ	I would like to chat about anything
Save User File	REG_SZ	Yes
Auto Update	REG_SZ	Yes
Log History Events	REG_SZ	Yes
Connection Type	REG_SZ	Dynamic
ocksPort	REG_DWORD	0x00000438 (1080)
ProxySocks4Port	REG_DWORD	0x00000438 (1080)
FirewallFromPort	REG_DWORD	0x000007D0 (2000)
FirewallToPort	REG_DWORD	0x00000FA0 (4000)
Random Name	REG_SZ	o********
Random Comment	REG_SZ	Single,white,male,but engaged,** yrs,*' *'',*** lbs,lt brown hair, hazel eyes.Looking to chat with new friends.I like disco,lt rock,classics in music.Like to surf the web,meet new friends.E-mail or ICQ me !Love to here from you! J***
Chat RoomName	REG_SZ	My Chat Session
Auto Join Chat Room	REG_SZ	Yes

.Default\Software\Netscape\Netscape Navigator\News

Name	Type	Data
News Directory	REG_SZ	C:\Program Files\Netscape\Navigator\news

.Default\Software\Netscape\Netscape Navigator\Address Book

Name	Type	Data
File Location	REG_SZ	C:\Program Files\Netscape\Navigator\address.htm

.Default\Software\Netscape\Netscape Navigator\History

Name	Type	Data
History File	REG_SZ	C:\Program Files\Netscape\Navigator\Netscape.hst

.Default\Software\Netscape\Netscape Navigator\Cache

Name	Type	Data
Cache Dir	REG_SZ	C:\Program Files\Netscape\Navigator\cache
Disk Cache SSL	REG_SZ	no
Disk Cache Size	REG_DWORD	0x00001388 (5000)
Memory Cache Size	REG_DWORD	0x00000400 (1024)

.Default\Software\Netscape\Netscape Navigator\Bookmark List

Name	Type	Data
File Location	REG_SZ	C:\Program Files\Netscape\Navigator\bookmark.htm
Start Menu With	REG_SZ	Entire Listing
Add URLs Under	REG_SZ	Top Level of Listing

.Default\Software\Netscape\Netscape Navigator\Main

Name	Type	Data
Install Directory	REG_SZ	C:\Program Files\Netscape\Navigator
Mozilla	REG_SZ	Good-3.01
Home Page	REG_SZ	http://dir.yahoo.com/Regional/U_S__States/Alabama/Cities/Valley/
Default Save Dir	REG_SZ	A:\
Temp Directory	REG_SZ	C:\DOS

.Default\Software\Netscape\Netscape Navigator\URL History

Name	Type	Data
URL_1	REG_SZ	http://dir.yahoo.com/Regional/U_S__States/Alabama/Cities/Valley/
URL_2	REG_SZ	http://mail.yahoo.com/
URL_3	REG_SZ	http://edit.my.yahoo.com/config/eval_register?.src=pg&.done=http://pager.yahoo.com
URL_4	REG_SZ	http://www.yahoo.com/?http://calendar.yahoo.com/
URL_5	REG_SZ	http://edit.my.yahoo.com/config/set_sports?.done=http://my.yahoo.com/
URL_6	REG_SZ	http://www.hotmail.com/
URL_7	REG_SZ	http://dir.yahoo.com/Regional/U_S__States/Florida/Cities/Deltona/
URL_8	REG_SZ	file://C:/Program Files/ICQ/Bookmark/Bookmark.html
URL_9	REG_SZ	http://www.disney.go.com/disneytelevision/onesaturdaymorning/poohvalentine/Photo2.html?poohphoto2
URL_10	REG_SZ	http://www.disney.go.com/disneytelevision/onesaturdaymorning/poohvalentine/video.html?pooh2

.Default\Software\Netscape\Netscape Navigator\Services

Name	Type	Data
Mapi	REG_SZ	no
SMTP_Server	REG_SZ	mail.bitstorm.net
NNTP_Server	REG_SZ	news.bitstorm.net
POP_Server	REG_SZ	mail.bitstorm.net
SOCKS_ServerPort	REG_DWORD	0x00000438 (1080)
SOCKS_Server	REG_SZ	(value not set)
Socks Conf	REG_SZ	c:\windows\socks.cnf

.Default\Software\Microsoft\Windows\CurrentVersion\Applets\WordPad\Recent File List

Name	Type	Data
File1	REG_SZ	A:\poem1.txt
File2	REG_SZ	A:\SPS_cl162v.html
File3	REG_SZ	A:\SPS_cl105v.html
File4	REG_SZ	A:\SCOTT'S RESUM`E.doc

.Default\Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List

Name	Type	Data
File1	REG_SZ	A:\tn-loveballon.jpg
File2	REG_SZ	A:\tn-tiglove.jpg
File3	REG_SZ	A:\web41.bmp
File4	REG_SZ	A:\web16.bmp

.Default\Network

Name	Type	Data
(default)	REG_TYPE_SZ	(value not set)

.Default\Network\Recent

Name	Type	Data
(default)	REG_TYPE_SZ	(value not set)

.Default\Software\Microsoft\Windows\CurrentVersion\Applets\Paint

Name	Type	Data
(default)	REG_TYPE_SZ	(value not set)

.Default\Software\Microsoft\Windows\CurrentVersion\Applets\WordPad

Name	Type	Data
(default)	REG_TYPE_SZ	(value not set)

.Default\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Name	Type	Data
MRUList	REG_SZ	gnacmfojhdeklbi
g	REG_BINARY	4F 45 4D 53 45 54 55 50 2E 49 4E 46 00 1C 00 30 00 00 00 00 00 00 00 00 00 00 00 00 4F 65 6D 73 65 74 75 70 2E 6C 6E 6B 00 00 00 00
	(String1)	OEMSETUP.INF...0.....Oemsetup.lnk....
	(String2)	OEMSETUP.INF
n	REG_BINARY	78 2D 6D 61 73 2E 73 63 72 00 19 00 30 00 00 00 00 00 00 00 00 00 00 00 78 2D 6D 61 73 2E 6C 6E 6B 00 00 00 00
	(String1)	x-mas.scr...0.....x-mas.lnk....
	(String2)	x-mas.scr
a	REG_BINARY	44 49 53 50 4C 41 59 2E 54 58 54 00 1B 00 30 00 00 00 00 00 00 00 00 00 00 00 44 69 73 70 6C 61 79 2E 6C 6E 6B 00 00 00 00
	(String1)	DISPLAY.TXT...0.....Display.lnk....
	(String2)	DISPLAY.TXT
c	REG_BINARY	50 50 48 45 41 52 54 2E 53 43 52 00 1B 00 30 00 00 00 00 00 00 00 00 00 00 00 50 70 68 65 61 72 74 2E 6C 6E 6B 00 00 00 00

	(String1)	PPHEART.SCR...0.....Ppheart.lnk....
	(String2)	PPHEART.SCR
m	REG_BINARY	70 70 68 65 61 72 74 2E 7A 69 70 00 1F 00 30 00 00 00 00 00 00 00 00 00 00 00 70 70 68 65 61 72 74 20 28 32 29 2E 6C 6E 6B 00 00 00 00
	(String1)	ppheart.zip...0.....ppheart (2).lnk....
	(String2)	ppheart.zip
f	REG_BINARY	58 2D 4D 61 73 32 2E 73 63 72 00 1A 00 30 00 00 00 00 00 00 00 00 00 00 58 2D 4D 61 73 32 2E 6C 6E 6B 00 00 00 00
	(String1)	X-Mas2.scr...0.....X-Mas2.lnk....
	(String2)	X-Mas2.scr
o	REG_BINARY	54 49 47 47 45 52 2E 49 4E 49 00 1A 00 30 00 00 00 00 00 00 00 00 00 00 54 69 67 67 65 72 2E 6C 6E 6B 00 00 00 00
	(String1)	TIGGER.INI...0.....Tigger.lnk....
	(String2)	TIGGER.INI
j	REG_BINARY	53 59 53 54 45 4D 54 4F 2E 47 52 50 00 1C 00 30 00 00 00 00 00 00 00 00 00 00 00 53 79 73 74 65 6D 74 6F 2E 6C 6E 6B 00 00 00 00
	(String1)	SYSTEMTO.GRP...0.....Systemto.lnk....
	(String2)	SYSTEMTO.GRP
h	REG_BINARY	53 4E 41 4B 36 34 30 2E 53 43 52 00 1B 00 30 00 00 00 00 00 00 00 00 00 00 00 53 6E 61 6B 36 34 30 2E 6C 6E 6B 00 00 00 00
	(String1)	SNAK640.SCR...0.....Snak640.lnk....
	(String2)	SNAK640.SCR
d	REG_BINARY	53 43 52 4E 53 41 56 45 2E 53 43 52 00 1C 00 30 00 00 00 00 00 00 00 00 00 00 00 53 63 72 6E 73 61 76 65 2E 6C 6E 6B 00 00 00 00
	(String1)	SCRNSAVE.SCR...0.....Scrnsave.lnk....
	(String2)	SCRNSAVE.SCR
e	REG_BINARY	4D 4F 50 59 46 49 53 48 2E 53 43 52 00 1C 00 30 00 00 00 00 00 00 00 00 00 00 00 4D 6F 70 79 66 69 73 68 2E 6C 6E 6B 00 00 00 00
	(String1)	MOPYFISH.SCR...0.....Mopyfish.lnk....
	(String2)	MOPYFISH.SCR
k	REG_BINARY	53 53 53 54 41 52 53 2E 53 43 52 00 1B 00 30 00 00 00 00 00 00 00 00 00 00 00 53 73 73 74 61 72 73 2E 6C 6E 6B 00 00 00 00
	(String1)	SSSTARS.SCR...0.....Ssstars.lnk....
	(String2)	SSSTARS.SCR
l	REG_BINARY	53 53 4D 41 52 51 55 45 2E 53 43 52 00 1C 00 30 00 00 00 00 00 00 00 00 00 00 00 53 73 6D 61 72 71 75 65 2E 6C 6E 6B 00 00 00 00
	(String1)	SSMARQUE.SCR...0.....Ssmarque.lnk....
	(String2)	SSMARQUE.SCR
b	REG_BINARY	53 53 4D 59 53 54 2E 53 43 52 00 1A 00 30 00 00 00 00 00 00 00 00 00 00 53 73 6D 79 73 74 2E 6C 6E 6B 00 00 00 00
	(String1)	SSMYST.SCR...0.....Ssmyst.lnk....
	(String2)	SSMYST.SCR
i	REG_BINARY	50 41 57 53 2E 53 43 52 00 18 00 30 00 00 00 00 00 00 00 00 00 00 00 50 61 77 73 2E 6C 6E 6B 00 00 00 00
	(String1)	PAWS.SCR...0.....Paws.lnk....
	(String2)	PAWS.SCR

Appendix AB - References

Books

Salgado, R.P., (2004), Forensics Frameworks and Best Practices: Managerial and Legal Issues, 8.5, pages 17, 18)

Table 33 - Index of Internet Sites Used

Site	On Page	Description
http://absoluteagency.com/	69	An adult site
http://adultsingles.com/	69	A dating site
http://camouflage.unfiction.com/Overview.html	13	Site to download Camouflage software+C32
http://home.att.net/~rayknights/pc_boot/w95aboot.htm	47	Windows 95a Boot sector page
http://home.earthlink.net/~rlively/MANUALS/VERSIONS/INDEX.HTM	51	Versions of COMMAND.COM
http://home.netscape.com/netcenter/newsletter	69	Monthly travel newsletter
http://home.sol.no/~espensa/khexedit/	11	KhexEdit v. 0.8.5 by Espen Sand
http://home.teleport.com/~brainy/lfn.htm	64	FAT 16 File system entry structure
http://miningco.com/	68	A news digest site
http://msnbc.msn.com/id/5173972/	42	Original article for Part 2
http://securityresponse.symantec.com/avcenter/venc/data/w97m.grouch.html	71	Information about W97M.Grouch macro virus
http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/q176/9/60.asp&NoWebContent=1	80	Microsoft information about loadwc.exe
http://users.cybercity.dk/~bse26236/batutil/help/SETVERS.HTM	79	Information about SETVER.EXE
http://users.iafrica.com/c/cq/cquirke/win95ver.htm	49	Windows 95 versions reference
http://wp.netscape.com/newsref/std/cookie_spec.html	77	Netscape cookie documentation
http://www.ballard.com/be_informed/fuel_cell_technology/abouttechnology/how_the_technology_works	32	Source for jpg similar to PEM-fuel-cell-large.jpg
http://www.ballard.com/be_informed/fuel_cell_technology/abouttechnology/how_the_technology_works	31	Source for pem_fuelcell.gif
http://www.buick.com/	69	Site for Buick Automobiles
http://www.byte.com/art/9402/sec6/art1.htm	51	Information about DoubleSpace compression
http://www.classified2000.com	78	A classified ad site
http://www.CompletelyFreeSoftware.com/	68	A source for free software (subscription)
http://www.duxcw.com/dcforum/DCForumID6/381.html	52	Information about DoubleSpace compression
http://www.eBay.com	42	An Auction site
http://www.fact-index.com/t/tr/truth_table.html	22	Truth table for XOR
http://www.geocities.com/politalk/dos/dbldos.htm	51	General information of DoubleSpace

http://www.guidancesoftware.com/support/EnCaseForensic/version4/acquisition.shtm	53	EnCase forensic software vendor
http://www.hitznet.com	78	Site for Classic Mac Digest
http://www.ichat.com	68	An Internet chat program
http://www.internetcallmanager.com/CustomerService/faq.shtml#general01	67	Source for InternetCallManager
http://www.lavasoft.com/	65	Source for Ad-Aware
http://www.MailNavigator.com	65	Source for MailNavigator
http://www.melron.com/Maxtor.html	44	Source for Maxtor hard drive jumper info.
http://www.mirc.com/	71	Site for Internet Relay Chat program
http://www.mopyfish.net/	71	Virtual pet fish screensaver
http://www.oneandonly.com/	77	Internet dating site
http://www.oska.com/deskmate_info.php	70	Animated cartoon screensavers
http://www.reuters.com/	42	An international news agency
http://www.shareit.com/	65	Source for PWL and Net Tools
http://www.sleuthkit.org/autopsy/	2	Autopsy forensic toolkit by Brian Carver
http://www.snapfiles.com/get/wmcookie.html	65	Source for cookie viewer
http://www.symantec.com/index.htm	14	Norton Anti-Virus vendor site
http://www.usdoj.gov/criminal/cybercrime/1030_new.html	37	Source for From 18 U.S.C. §1030
http://www.usdoj.gov/criminal/cybercrime/18usc1831.htm	38	Source for From 18 U.S.C. §1831
http://www.usdoj.gov/criminal/cybercrime/18usc1832.htm	39	Source for From 18 U.S.C. §1832
http://www.valupage.com/	68	Shopping guides for Winn-Dixie stores
http://www.win.tue.nl/~aeb/partitions/partition_types-1.html	128	Site with information about partition types
http://www.winhex.com	24	Source for WinHex editor