GIAC Certified Forensic Analyst (GCFA)
Practical Assignment
Version 1.2 (January 2003)

Kamarul Baharin Khalid
NISER, Malaysia

Introduction

This paper represents my submission to GIAC for the practical certification requirements for the GIAC Certified Forensic Analyst Certification. This paper consists of three parts:

Part 1: Analyze an Unknown Binary File
Abstract: An unknown binary file was given to us for analysis. Our task is to identify and investigate the binary file 's characteristic by using forensic techniques and tools. Once identified, we will discuss on the legal expect and interview questions related to the b inary file.

Part 2 - Option 2: Perform Forensic Tool Validation
Abstract: A windows recovery tool was introduced to us which seem to be very useful for forensic analysis. Extensive tests will be done to verify that this recovery tool can recover files fo rensically. Test environment and procedures will be discuss ed to reduce outside interference.

Part 3: Legal Issues of Incident Handling
Abstract: As a system Administrator for an Internet Service Provider, we were contacted by the law enforcement officer for assistant in their investigation. H ere we will discuss on our limitation of assistant and the process which is required by the law enforcement officer to preserved and obtained evidence from us according to Malaysia Law.

Note: Some output lines are purposely removed due to its length. Only related outputs are left as is but complete outputs are attached as Appendixes. Highlighted texts outputs are answers to some of the question asked or important information.

Guideline: While writing this paper, I refer to four (4) others GIAC Certified Forensic Analyst (GCFA)[1] submitted assignment as my guideline. Thanks to Chris Calabrese (September 2002), Denis E. Brooker (April 2002), James A. Clausing (April 2002) and Greg Owen (April 2002).

Table of Contents

Introduction 2
Table of Contents 3
Part 1: Analyze an Unknown Binary File 5
Background Information 5
Preparation 6
Binary Detail 9
Program Description 13
Forensic Details 17
Program Identification 24
Legal Implications 24
Interview Questions 27
Additional Information 29
Part 2 – Option 2: Perform Forensic Tool Validation 30
Introduction 30
Scope 31
Tools Description 32
Test Apparatus 33
Environmental Conditions 34
Description of the Procedures 34
Data Recovery and Results 41
1. Permanently Deleted Files 41
2. Removed Partition table 47
3. Repartitioned and Reformatted with Same File system 53
4. Repartitioned and Reformatted with Different File system 59
5. Recovery from Real Case – Permanently deleted file 65
Analysis 66
Presentation 67
Conclusion 68
Summary 68
Part 3: Legal Issues of Incident Handling 69
Synopsis 69
Questions 69
Appendix 1: "*strings -a*" output (2 column - Knoppix) 74
Appendix 2: "*zipinfo -v*" output (Knoppix) 76
Appendix 3: "*debugfs*" output (Knoppix) 77
Appendix 4: "strace" output (RedHat ver 5.1) 78
Appendix 5: "*ps -ax*" output (RedHat ver 5.1) 79
Appendix 7: "*make linux*" output (RedHat ver 5.1) 84
Appendix 8: "readelf" output (Knoppix) 86
Appendix 9: Screenshots: ER Pro Installation 89
Appendix 10: Screenshots: EmergencyDiskette Creation 93
Appendix 11: Sample Screenshots during Data Recovery 95
Appendix 12: FAT32 HDD MD5 Value Result Summary 99
Appendix 13: FAT32 Files MD5 Value Result Summary 100
Appendix 14: NTFS HDD MD5 Value Result Summary 102

Appendix 15: NTFS Files MD5 Value Result Summary 103
Appendix 16: Case Result Summary 105
HDD MD5 Values 105
Files MD5 Values 105
Reference 106

Part 1: Analyze an Unknown Binary File

In this part of my assignment paper, we are analyzing an unknown binary file which was given to us by SANS [2] as part of our GIAC practical assignment.

Background Information

Because the binary file is likely to be malicious code, proper test setup will be considered.

1. Operating System (OS)

   The test workstation will be boot -up using an OS from a Compact Disk (CD) which to ensure that all system files won't be modified or erase. System setting, if modified, won't be save when the system rebooted.

2. Networking

   The test workstation will be disconnected for any network or if the binary file is related to network, the test workstation will only be connected to a small hub that only h as a sniffer attached for network analysis.

3. Hard disk space

   The hard disk space used for the test workstation to analyze the binary file is a large loopback filesystem volume file created using dd and mkfs that can then be totally wipe off from the sys tem. Another reason is that if required to change to another system, we only need to copy this large file.

   This file will be mount using '*`-o loop,noatime,noexec`*' options. Noatime mean the system won't change the access time on any file in the mounted file system. Noexec mean the system won't execute any binary program in the mounted file system. Loop option is required because the file system is within a file and not a physical device/hard disk.

4. Binary file

   The binary file will be downloaded from t he SANS GIAC website using another system which will then be copied to the test workstation using a floppy disk. This is to ensure that the test workstation will not be connected to the network at anytime.

These precautions are required to ensure that th e unknown binary file or malicious code will never leave the test workstation and avoid infection of other system on the real network.

Preparation

The test workstation is a Pentium III 1.0GHz with 256MB memory and 30GB hard disk notebook, which was originally formatted using FAT32, which was used with Microsoft[3] Windows Millennium. This notebook is boot-up using Knoppix Linux[4] CD version 3.1 released 04-08-2002-Beta. Knoppix Linux is a Linux OS that is boot-up directly from the CD without requirement of hard disk installation. Since it is boot-up from CD, the system files/folders are marks as read-only by the OS. This is very helpfully in preventing any modification of the system files/setting by the unknown malicious binary program that we are going to analyze.

After successfully boot-up using Knoppix Linux, we create a loopback file system as mention in early precaution/requirement steps. The process is as follows:

```
root@ttyp0[root]#  uname -a
Linux Knoppix 2.4.19-xfs #2 SMP Sam Aug 3 16:51:33 CEST 2002 i686 unknown unknown GNU/Linux
root@ttyp0[root]#  mount -t vfat -o noatime,noexec /dev/hda1 /mnt/hda1
root@ttyp0[root]#  cd /mnt/hda1
root@ttyp0[hda1]#  mkdir alltemp
root@ttyp0[hda1]#  cd alltemp
root@ttyp0[alltemp]#  mkdir Practical
root@ttyp0[alltemp]#  cd Practical
root@ttyp1[Practical]#  pwd
/mnt/hda1/alltemp/Practical
root@ttyp1[Practical]#  ls -al
total 10272
drwxr-xr-x    3 root     root          8192 Jan 12 19:16 .
drwxr-xr-x   10 root     root          8192 Jan 12 19:14 ..
```

"uname" command is use to display system name information. The parameter "-a" is to specify "uname" to display information on the CPU or machine type, displays the node name of this particular machine, displays the release (major version) number of the operating system, displays the name of the operating system and displays the version (minor version) number of the operating system.

Next we "mount" the FAT32 volume by using "-t vfat" parameter. "-t vfat" parameter is to inform "mount" command that we are mounting a vfat type volume (FAT32). After mounting the FAT32 volume, we create and change to a new subdirectory call "Practical" using command "mkdir" and "cd".

"pwd" command is to display current working directory that we are in. "ls" command is to list the directory contents. The parameter "-al" for the "ls" command is to specify "ls" to display it output including directory entries whose names begin with a dot (.) and list it in long format.

When we are already in the test directory, we can start creating our test EXT2 file system loopback volume.

```
root@ttyp0[Practical]#  dd if=/dev/zero of=Exam1.dd bs=1024k count=10
10+0 records in
10+0 records out
```

To create the loopback file system volume, "dd" command is used. "dd" is a utility that can copies the standard /file/device input to the standard /file/device output. The input and output parameter is specify using " if" for input and "of" for output. In this preparation, we use " /dev/zero" as it input parameter to create an empty/wiped loopback file system volume that is filled with zeros. "dd" will create an empty/wiped loopback file system volume file called "Exam1.dd" as we specify as the " of" parameter. The "bs" (block size) and "count" parameter is to specify the total size to copy. In this preparation, " bs" is specified as 1024k (1MB) and " count" is specified as 10 which give us total loopback file system volume of size 10MB.

```
root@ttyp0[Practical]#  ls -lh
total 11M
-rwxr-xr-x    1 root     root          10M Jan 12 19:16 Exam1.dd
root@ttyp0[Practical]#  losetup /dev/loop0  Exam1.dd
root@ttyp0[Practical]#  mkfs.ext2 /dev/loop0
mke2fs 1.27 (8-Mar-2002)
Filesystem label=
OS type: Linux
Block size=1024 (log=0)
Fragment size=1024 (log=0)
2560 inodes, 10240 blocks
512 blocks (5.00%) reserved for the super user
First data block=1
2 block groups
8192 blocks per group, 8192 fragments per group
1280 inodes per group
Superblock backups stored on blocks:
        8193

Writing inode tables: done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 26 mounts or
180 days, whichever comes first.  Use tune2fs   -c or -i to override.
root@ttyp0[Practical]#  losetup -d /dev/loop0
```

After we created the 10MB loopback file system volume file, we need to prepare the loopback file system volume file for the test. We need to create a linux partition inside the loopback file system volume file using " mkfs" command. Before we can use the "mkfs" command, we need to associate loop devices with our loopback file system file using " losetup".

"losetup" is used to associate loop devices with regular files or block devices, to detach loop devices and to query the status of a loop device. The "/dev/loop0" parameter is to specify the loop device name which is to be associated "Exam1.dd" with.

After associating the loopback file system volume file to "/dev/loop0", we use "mkfs" command to create and format EXT2 linux partition. "mkfs" creates a Linux file-system on a device (usually a disk partition). The first parameter, "ext2", is to specify what type of partition to create. The second parameter, "/dev/loop0", is the target device which we want to create partition.

Next we detach the loop device using "-d" parameter in "losetup" command.

After the loopback file system volume has been created, we mount the loopback file system to prepare for the test workstation for the analysis.

```
root@ttyp0[Practical]#  mkdir /mnt/Practical
root@ttyp0[Practical]#  mount -t ext2 -o loop,noatime,noexec ./Exam1.dd /mnt/Practical/
root@ttyp0[Practical]#  cd /mnt/Practical
root@ttyp0[Practical]#  pwd
/mnt/Practical
root@ttyp0[Practical]#  df -H .
Filesystem            Size  Used Avail Use% Mounted on
/dev/loop0             10M  632k  8.9M   7% /mnt/Practical
root@ttyp0[Practical]#  ls -al
total 22
drwxr-xr-x    3 root      root         1024 Jan 12 19:47 .
drwxr-xr-x    9 root     root          1024 Jan 12 19:46 ..
drwx------    2 root     root         12288 Jan 12 19:17 lost+found
```

Before mounting the loopback file system volume file, we need to create a directory to attach the loopback file system volume file using "mkdir" command. Once the directory created, we can use the "mount" command to mount the loopback file system volume file and attach it to the directory we just created. The parameter "-t ext2" is to specify that the type of the file system that we are going to mount is EXT2.

There are a few parameter that we specify after the "-o" option. "loop" parameter is to specify that the file system volume to be mounted is of type loopback file system. "noatime" parameter is to specify the operating system not to update inode access times on this file system. "noexec" Do not allow execution of any binaries on the mounted file system. This option is very useful on preventing execution of the unknown binary file.

An inode is the volume data structure used by the Extent (EXT2/3) file system to implement the abstraction of a file. An inode contains the type (for example, plain file, directory, symbolic link, or device file) of the file; its owner, group, and public access permissions; the owner and group ID numbers; its size in bytes; the number of links (directory references) to the file; and the times of last access and last modification to the file. In addition, there is a list of data blocks claimed by the file.

Now that the test workstation is prepared, the zip binary file is copy from a floppy disk. The zip binary file then we change it attribute to be read -only.

```
root@ttyp0[Practical]#  mount /dev/fd0 /mnt/floppy
root@ttyp0[Practical]#  cp /mnt/floppy/binary_v1.2. zip .
root@ttyp0[Practical]#  ls -al
total 22
drwxr-xr-x    3 root     root         1024 Jan 12 19:54 .
drwxr-xr-x    9 root     root         1024 Jan 12 19:46 ..
-rwxr-xr-x    1 root     root         7309 Jan 12 19:54 binary_v1.2.zip
drwx------    2 root     root        12288 Jan 12 19:17 lost+found
root@ttyp0[Practical]#  chmod a -w binary_v1.2.zi p
root@ttyp0[Practical]#  ls -al
total 22
drwxr-xr-x    3 root     root         1024 Jan 12 19:47 .
drwxr-xr-x    9 root     root         1024 Jan 12 19:46 ..
-r-xr-xr-x    1 root     root         7309 Jan 12 19:47 binary_v1.2.zip
drwx------    2 root     root        12288 Jan 12 19:17 lost+found
```

Binary Detail

1. Name of the program/file found on the system

   The first information that we try to get is the name of the program/binary file. To do this we have to run a '*strings -a*' command against the binary file and find any keyword, which related to the binary file real name. Before doing that, we have to extract the binary file from the zip binary file using '*unzip -X*' command.

```
root@ttyp0[Practical]#  mkdir Exam1
root@ttyp0[Practical]#  cd Exam1/
root@ttyp0[Exam1]#  pwd
/mnt/Practical/Exam1
root@ttyp0[Exam1]#  ls -al
total 2
drwxr-xr-x    2 root     root         1024 Jan 12 20:33 .
drwxr-xr-x    4 root     root         1  024 Jan 12 20:33 ..
root@ttyp0[Exam1]#  unzip -X ../binary_v1.2.zip
Archive:  ../binary_v1.2.zip
  inflating: atd.md5
  inflating: atd
root@ttyp0[Exam1]#  ls -al
total 19
drwxr-xr-x    2 root     root         1024 Jan 12 20:36 .
drwxr-xr-x    4 root     root          1024 Jan 12 20:33 ..
-rw-rw-rw-    1 root     root        15348 Aug 22 14:57 atd
-rw-rw-rw-    1 root     root           39 Aug 22 14:58 atd.md5
root@ttyp0[Exam1]#  chmod a -w atd
root@ttyp0[Exam1]#  ls -al
total 19
drwxr-xr-x    2 root     root          1024 Jan 12 20:36 .
drwxr-xr-x    4 root     root         1024 Jan 12 20:33 ..
-r--r--r--    1 root     root        15348 Aug 22 14:57 atd
-rw-rw-rw-    1 root     root           39 Aug 22 14:58 atd.md5
```

The command '*chmod a -w atd*' is to change the bin ary file attribute to read-only mode.

```
root@ttyp0[Exam1]#  strings -a atd > atd.strings
root@ttyp0[Exam1]#  grep -i "loki" atd.strings
lokid: Client database full
lokid version:          %s
lokid: inactive client <%d> expired from list [%d]
lokid -p (i|u) [  -v (0|1) ]
LOKI2   route [(c) 1997 guild corporation worldwide]
lokid: server is currently at capacity.  Try again later
                          (--The rest of the output removed --)
```

From this output we can see that this binary file is actually a LOKI [5] program as shown by '`LOKI2   route [(c) 1997 guild corporation worldwide]`' that have been rename to '*`atd`*'.

2. <u>File/MACTime information (last modified, last accessed, and last changed time</u>

   Next is to find out the MAC (**M**odified, **A**ccessed, and **C**hanged) time of the binary file. Due to the noatime option used during mounting the loopback file system, this will ensure that the system will never change the access time on any file in the loopback file system.

```
root@ttyp0[Exam1]#  zipinfo -l ../binary_v1.2.zip
Archive:  ../binary_v1.2.zip     7309 bytes   2 files
-rw-rw-rw-  2.0 fat       39 t -       38 defN  22-Aug-02 14:58  atd.md5
-rw-rw-rw-  2.0 fat    15348 b-      7077 defN  22-Aug-02 14:57  atd
2 files, 15387 bytes uncompressed, 7115 bytes compressed:  53.8%
root@ttyp0[Exam1]#  zipinfo -v ../binary_v1.2.zip
Archive:  ../binary_v1.2.zip   7309 bytes   2 files
                              (---The output removed ---)
Central directory entry #1:
---------------------------

  atd.md5

  offset of local header from start of archive:     0 (00000000h) bytes
  file system or operating system of origin:        MS-DOS, OS/2 or NT FAT
  version of encoding software:                        2.0
                              (---The output removed ---)
  file last modified on (DOS date/time):            2002 Aug 22 14:58:08
                              (---The output removed ---)
Central directory e ntry #2:
---------------------------

  atd

  offset of local header from start of archive:     75 (0000004Bh) bytes
  file system or operating system of origin:        MS-DOS, OS/2 or NT FAT
  version of encoding software:                        2.0
                              (---The output removed ---)
  file last modified on (DOS date/time):            2002 Aug 22 14:57:54
  32-bit CRC value (hex):                              d0ee3072
  compressed size:                                     7077 bytes
  uncompressed size:                                     15348 bytes
                              (---The output removed ---)
root@ttyp0[Exam1]#  unzip -v ../binary_v1.2.zip
Archive:  ../binary_v1.2.zip
 Length   Method    Size  Ratio   Date    Time    CRC   -32    Name
--------  ------  -------  -----   ----    ----   ------     ----
      39  Defl:N       38   3%    08-22-02 14:58   e5376cb4  atd.md5
   15348   Defl:N     7077  54%    08-22-02 14:57   d0ee3072  atd
--------          -------  ---                              -------
```

```
   15387             7115  54%                           2 file    s
root@ttyp0[Exam1]#  ls -i atd*
   1283 atd     1282 atd.md5
root@ttyp0[Exam1]#  debugfs -R "stat <1283>"  \
 /mnt/hda1/alltemp/Practical/Exam1.dd
debugfs 1.27 (8 -Mar-2002)
Inode: 1283   Type: regular    Mode:  0444   Flags: 0x0   Generation: 33279
User:     0   Group:     0    Size: 15348
File ACL: 0    Directory ACL: 0
Links: 1   Blockcount: 32
Fragment:  Address: 0    Number: 0    Size: 0
ctime: 0x3e21c3d5  -- Sun Jan 12 20:36:53 2003
atime: 0x3d64dfd2  -- Thu Aug 22 14:57:54 2002
mtime: 0x3d64dfd2  -- Thu Aug 22 14:57:54 2002
BLOCKS:
(0-11):8359 -8370, (IND):8371, (12 -14):8372 -8374
TOTAL: 16

root@ttyp0[Exam1]#  debugfs -R "stat <1282>"  \
 /mnt/hda1/alltemp/Practical/Exam1.dd
debugfs 1.27 (8 -Mar-2002)
                              (---The output removed ---)
ctime: 0x3e21c3ac  -- Sun Jan 12 2 0:36:12 2003
atime: 0x3d64dfe0  -- Thu Aug 22 14:58:08 2002
mtime: 0x3d64dfe0  -- Thu Aug 22 14:58:08 2002
BLOCKS:
(0):8358
TOTAL: 1
```

From these output we can justify that, the binary file was last modified/ accessed on 22 August 2002 at 2:57pm. But due to the zip file was created using MS-DOS/MS Windows zip program, this date and time doesn't reflect the actual date it was modified in the compromised system. This date and time reflected to the modification/accessing of the binary file during it was transferred from the compromised system to the MS - DOS/MS Windows system. There is no date and time that was stored in the zip file on when is the binary file was really created, modified (compiled) and accessed (executed) during the binary file was in the compromised system.

The created date and time is the date and time of the binary file created during it was extracted from the zip file.

3. File owner(s) – (user and/or group)

There was no file ownership information available. The file ownership information may be lost during transferring the binary file from the compromised system to MS DOS/Windows system and/or due to the binary file was zipped using MS -DOS/MS Windows zip program therefore the file ownership information (user and group) was not stored together in the zip file. MS-DOS/MS Windows zip file doesn't support storing Linux file ownership information.

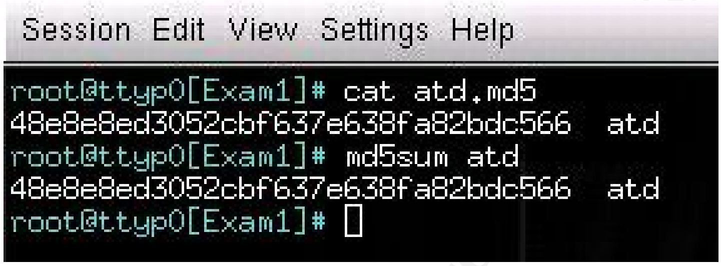
The file ownership which was shown in the '`ls -al`' command, is the owner of the Linux account used during extraction of the binary file. The account, which was used, is '`root`'.

4. File size (in bytes)

   From the output in part 2 of this section above, we can conclude that the binary file size is 15348 bytes which have been shown by using command *ls -al*, *zipinfo*, *unzip* and *debugfs*.

5. MD5 hash of the file (inc lude screenshot of the hash value obtained)

   The MD5 hash value of a file can be obtained using ' *md5sum*' command. Below is a screenshot which comparing the ' *md5sum*' result to the MD5 hash value in the file 'atd.md5'. The MD5 hash values are the same.



```
root@ttyp0[Exam1]# cat atd.md5
48e8e8ed3052cbf637e638fa82bdc566  atd
root@ttyp0[Exam1]# md5sum atd
48e8e8ed3052cbf637e638fa82bdc566  atd
root@ttyp0[Exam1]# 
```

6. Key words found that are associated with the program/file

   The key words can be display using the ' *strings -a*' command as mentioned in part 1 of this section above. The keyword found that are associated with the binary file are: LOKI2, route, lokid, client and server.

```
root@ttyp0[Exam1]#  strings -a atd
                                (---The output removed ---)
lokid: Client database full
DEBUG: stat_client nono
lokid version:              %s
                                (---The output removed ---)
lokid: inactive client <%d> expired from list [%d]
                                (---The output removed ---)
lokid -p (i|u) [  -v (0|1) ]
                                (---The output removed ---)
LOKI2           route [(c) 1997 guild corporation worldwide]
                                (---The output removed ---)
lokid: server is currently at capacity.  Try again later
lokid: Cannot add key
lokid: popen
                                (---The output removed ---)
lokid:  client <%d> requested an all kill
   sending L_QUIT: <%d> %s
lokid: clean exit (killed at client request)
                                (---The output removed ---)
lokid: cannot locate client entry in database
lokid: client <%d> freed from list [%d]
                                (---The output removed ---)
lokid: unsup ported or unknown command string
lokid: client <%d> requested a protocol swap
   sending protocol update: <%d> %s [%d]
lokid: transport protocol changed to %s
                                (---The output removed ---)
```

Program Description

1. What type of program is it?

The program which wa s found on the compromise system was renamed to ‘`atd`’. The original filename is ‘ `lokid`’. For more explanations, please refer to part 1 of section “**Forensic Detail**” below.

```
root@ttyp0[Exam1]#  file atd
atd: ELF 32 -bit LSB executable, Intel 80386, version 1   (SYSV), dynamically linked
(uses shared libs), stripped
```

From the analysis using ‘ *`file`*’ command, it was confirm that this binary file is an ELF executable, which have been compiled/ported on Intel x86 systems usually running Linux operating system (OS). The binary file is also not statically linked. This means that this binary file requires or dynamically linked with some of the system file (share libs) to execute.

Further analysis using ‘ *`strings -a`*’ command (shown in part 1 and 6 of section “**Binary Detail**” above), it is confirmed that this binary file is actually a LOKI2, an ICMP_ECHO tunneling backdoor program.

More analysis of the binary file behaviors will be discussed in part 4 of this section below.

2. What is it used for?

A backdoor program is a p rogram that gives a user an unrestricted access to a server without proper login. A covert channel is “ *…a process to transfer information in a manner that violates the systems security policy….”*[6] [7]. In this case, LOKI2 is an ICMP covert channel (ICMP_ECHO tunneling) backdoor within a network that transcends and bypasses firewalls and the Linux systems authentication mechanisms.

ICMP is an abbreviation of Internet Control Message Protocol . “Because IP wasn't designed to be absolutely reliable, ICMP came into the scene to provide feedback on problems which existed in the communication environment.”[8] For more detail about ICMP and how it work , we can visit http://www.firewall.cx/menu.php under ICMP option, for great ICMP explanation . ICMP packets were usu ally not blocked by the firewall.

“Tunneling is a technique used get one network protocol from A to B by using another protocol to encapsulate it. ”[9] Tunneling or c overt channel application uses raw sockets to reconstruct forged packets and encapsulate the data. The data itself can contain text or binary data as the user sees necessary.

Actually Loki is not a compromise tool. It has many uses, none of which are breaking into a machine. In a good hand, this program can be used to remotely manage a server without accessing the server physically. In the wrong hand, this program can be used for remotely access the compromise server without login to the server and give the hacker-unrestricted access as if he/she was accessing the server physically.

3. When was the last time it was used

   Unable to tell the last time this binary file was used from the downloaded zip file alone. Require further analysis on the compromise system itself.

4. Step-by-step analysis of the program actions

   For step-by-step analysis of the program actions, we need to execute this binary file through '`strace`' command. '`strace`' is use to capture/trace all the behaviors/actions done by the binary file during it execution. Before trying to execute the binary file, we need to change the file system mounting option without NOEXEC and change the binary file attribute to executable. We make another copy of the loop file system just for precaution.

```
root@ttyp0[Exam1]# cd /mnt/hda1/alltemp/Practical/
root@ttyp0[Practical]# umount /mnt/Practical
root@ttyp0[Practical]# cp Exam1.dd Exam1cpy.dd
root@ttyp0[Practical]# ls -al
total 20512
drwxr-xr-x    3 knoppix  knoppix      8192 Jan 29 22:07 .
drwxr-xr-x   12 knoppix  knoppix      8192 Jan 25 08:03 ..
-rwxr-xr-x    1 knoppix  knoppix  10485760 Jan 25 08:04 Exam1.dd
-rwxr-xr-x    1 knoppix  knoppix  10485760 Jan 29 22:07 Exam1cpy.dd
-r-xr-xr-x    1 knoppix  knoppix      7309 Jan 11 18:16 binary_v1.2.zip
root@ttyp0[Practical]# mount -o loop,noatime Exam1cpy.dd /mnt/Practical/
root@ttyp0[Practical]# cd /mnt/Practical/Exam1/
root@ttyp0[Exam1]# pwd
/mnt/Practical/Exam1
root@ttyp0[Exam1]# ls -al
total 25
drwxr-xr-x    5 root     root         1024 Jan 12 21:04 .
drwxr-xr-x    4 root     root         1024 Jan 12 20:33 ..
-r--r--r--    1 root     root        15348 Aug 22 14:57 atd
-rw-rw-rw-    1 root     root           39 Aug 22 14:58 atd.md5
-rw-r--r--    1 root     root         2820 Jan 12 20:38 atd.strings
drwxr-xr-x    3 root     root         1024 Jan 12 20:57 src1
drwxr-xr-x    3 root     root         1024 Jan 12 21:02 src2
root@ttyp0[Exam1]# strace ./atd
execve("./atd", ["./atd"], [/* 14 vars */]) = 0
strace: exec: Permission denied
root@ttyp0[Exam1]# chmod 755 ./atd
root@ttyp0[Exam1]# ls -al
total 25
drwxr-xr-x    5 root     root         1024 Jan 12 21:04 .
drwxr-xr-x    4 root     root         1024 Jan 12 20:33 ..
-rwxr-xr-x    1 root     root        15348 Aug 22 14:57 atd
-rw-rw-rw-    1 root     root           39 Aug 22 14:58 atd.md5
-rw-r--r--    1 root     root         2820 Jan 12 20:38 atd.strings
drwxr-xr-x    3 root     root         1024 Jan 12 20:57 src1
drwxr-xr-x    3 root     root         1024 Jan 12 21:02 src2
root@ttyp0[Exam1]# strace ./atd
execve("./atd", ["./atd"], [/* 14 vars */]) = 0
old_mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) =
0x40007000
mprotect(0x40000000, 21406, PROT_READ|PROT_WRITE|PROT_EXEC) = 0
mprotect(0x8048000, 13604, PROT_READ|PROT_WRITE|PROT_EXEC) = 0
stat("/etc/ld.so.cache", {st_mode=S_IFREG|0644, st_size=57162, ...}) = 0
open("/etc/ld.so.cache",  O_RDONLY)      = 3
old_mmap(NULL, 57162, PROT_READ, MAP_SHARED, 3, 0) = 0x40008000
close(3)                                = 0
stat("/etc/ld.so.preload", 0xbffffd68)  =   -1 ENOENT (No such file or directory)
open("/usr/lib/libc.so.5", O_RDONLY)    =   -1 ENOENT (No such file or directory)
open("/lib/libc.so.5", O_RDONLY)        =   -1 ENOENT (No such file or directory)
write(2, "./atd: can \'t load library  \'libc."..., 38./atd: can't load library
'libc.so.5') = 38
_exit(16)                               = ?
```

The binary file requires a system file to execute. It looks for system file call ‘libc.so.5’ which is not available to our current system.

```
root@ttyp0[Exam1]#  locate libc.so
locate: warning: database `/var/lib/locate/locatedb' is more than 8 days old
/lib/libc.so.6
/usr/lib/libc.so
```

From the output above, we can see that our system only have ‘ libc.so.6’ which is not the file needed by the binary file. Let find out which version of GCC[10] it was originally compiled from.

```
root@ttyp0[Exam1]#  grep -i “gcc” atd.strings
GCC: (GNU) 2.7.2.1
GCC: (GNU) 2.7.2.1
GCC: (GNU) 2.7.2.1
GCC: (GNU) 2.7.2.1
GCC: (GNU) 2.7.2.1
GCC: (GNU) 2.7.2.1
GCC: (GNU) 2.7.2.1
GCC: (GNU) 2.7.2.1
root@ttyp0[Exam1]#  gcc -v
Reading specs from /usr/lib/gcc-lib/i386-linux/2.95.4/specs
gcc version  2.95.4 20011002 (Debian prerelease)
```

From the combination command of ‘ *strings -a*’ and ‘*grep -I “gcc”*’, we can see that this binary file was compiled using GCC version 2.7.2.1 but our current GCC is version 2.95.4.

GCC usually were installed together during Linux OS installation. GCC version 2.7.2.1 is quite old which should be available on older Linux OS. Searching throughout our organization, we manage to get hold of an old unused RedHat[11] Linux OS version 5.1. Before using this system we make a backup copy of the hard disk as a precaution by using Norton Ghost[12] version 2002 from Symantec Corporation[13]. After making the backup copy, we check the system for ‘ libc.so.5’

```
[root@ftp home]#  uname -a
Linux RedHat 2.0.34 #1 Fri May 8 16:05:57 EDT 1998 i586 unknown
[root@ftp home]#  locate libc.so
locate: warning: database `/var/lib/locatedb' is more than 8 days old
/home/ftp/lib/libc.so.6
/lib/libc.so.6
/usr/i486-linux-libc5/lib/libc.so.5
/usr/i486-linux-libc5/lib/libc.so.5.3.12
/usr/i486-linuxaout/lib/libc.so.4
/usr/i486-linuxaout/lib/libc.so.4.7.2
```

```
/usr/lib/libc.so
```

Now that we confirm that the ‘ `libc.so.5` ’ exists on the system, we can now continue on our analysis of the binary file action. We do the ‘ `strace` ’ command again to the binary file that was copied to the system using a floppy disk.

```
root # mkdir Practical
root # cd Practical
root # cp /mnt/floppy/binary_v1.2.zip .
root # chmod a -w binary_v1.2.zip
root # mkdir Exam1
root # cd Exam1
root # unzip -X ../binary_v1.2.zip
Archive:  ../binary_v1.2.zip
  inflat ing: atd.md5
  inflating: atd
root # ls -al
total 19
drwxr-xr-x    2 root     root         1024 Jan 12 20:36 .
drwxr-xr-x    4 root     root         1024 Jan 12 20:33 ..
-rw-rw-rw-    1 root     root        15348 Aug 22 14:57 atd
-rw-rw-rw-    1 root     r oot           39 Aug 22 14:58 atd.md5
root # chmod 755 ./atd
root# strace ./atd
execve("./atd", ["./atd"], [/* 17 vars */]) = 0
mmap(0, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS,    -1, 0) = 0x40006000

                              (---The output removed ---)
semop(0x1, 0x1, 0 , 0xbffffd18)          = 0
_exit(0)                                = ?
```

Now we manage to execute the binary file and captured the ‘ `strace` ’ output. The length of the ‘ `strace` ’ output is quite long but we need to show all the output for analysis. Let confir m whether the binary file were executed by using ‘`ps -ax`’ command.

```
root# ps -ax
  PID TTY STAT TIME COMMAND
                              (---The output removed ---)
  503   3 S    0:00  -bash
  539  ?  S    0:00 ./atd
  597   2 R    0:00 ps ax
  243  ?  S    0:00 /usr/sbin/atd

                              (---The output removed ---)
```

Yes, the binary file was executed and stays resident in the memory.

From the ‘`strace`’ output we can see that, during the binary file executed, the binary file have done a few action.

```
stat("/etc/ld.so.cache", {st_mode=0, st_size  =0, ...}) = 0
open("/etc/ld.so.cache", O_RDONLY)      = 4
stat("/etc/ld.so.preload", 0xbffffd7c)  =   -1 ENOENT (No such file or directory)
open("/usr/i486 -linux -libc5/lib/libc.so.5", O_RDONLY) = 4
open("/usr/share/locale/C/LC_MESSAGES", O_RDONLY) = -1 ENOENT (No such file or directory)
stat("/etc/locale/C/libc.cat", 0xbffff8a0) = -1 ENOENT (No such file or directory)
stat("/usr/lib/locale/C/libc.cat", 0xbffff8a0) = -1 ENOENT (No such file or directory)
stat("/usr/lib/locale/libc/C", 0xbffff8a0) = -1 ENOENT (No such file or directory)
stat("/usr/share/locale/C/libc.cat", 0xbffff8a0) = -1 ENOENT (No such file or directory)
stat("/usr/local/share/locale/C/libc.cat", 0xbffff8a0) = -1 ENOENT (No such file or
directory)
```

The binary file try to search (get status, "`stat`") and access ("`open`") file "`ld.so.cache`", "`ld.so.preload`", "`LC_MESSAGES`" and "`libc.cat`".

```
personality(0 /* PER_??? */)            = 0
geteuid()                               = 0
getuid()                                = 0
getgid()                                  = 0
getegid()                               = 0
geteuid()                               = 0
getuid()                                = 0
```

The binary file is also trying to get the account ID/information ("`geteuid()`", "`getuid()`", "`getgid()`", "`getegid()`", "`geteuid()`", "`getuid()`") of the person running this binary file. The result "`0`" shows that the binary file is executed using "`root`" account.

```
getpid()                                = 615
getpid()                                = 615
```

Next, the binary file is trying to get it's process ID ("`getpid()`").

```
write(2, "\nLOKI2\troute [(c) 1997 guild c"..., 52) = 52
```

Next the binary file output to screen ("`write`") 'LOKI2   route [(c) 1997 guild corporation worldwide]'.

```
time([1043305782])                        = 1043305782
```

Next the binary file query the system time ("`time`") and the result are in UNIX binary time format. After conversion the time "`1043305782`" is result to "`Thu Jan 23 15:09:42 2003`" (GMT+0800) which is the time the binary file is executed.

Further investigation on the binary file action is not possible because we could not get LOKI2 client program. Without the client program to interact with the binary file, we are unable to monitor further actions done by the binary file and also the network traffic during the interaction. Please refer to part 1 of section "**Forensic Details**" below.

Forensic Details

1. What are the forensic footprints when this program installed?

   If the source codes were downloaded from the Phrack Magazine Volume 7, issue 51, article 06[14], then there should be an extractor program, which can be downloaded from Phrack Magazine Volume 7, issue 51, article 17[15]. The extractor program included is in C and Perl format. Here we use the Perl format.

```
root@ttyp0[Exam1]#  mkdir s rc1
root@ttyp0[Exam1]#  cd src1
root@ttyp0[src1]#  pwd
/mnt/Practical/Exam1/src1
root@ttyp0[src1]#  ls -al
total 116
drwxr-xr-x    2 root     root         1024 Jan 12 20:49 .
drwxr-xr-x    3 root     root         1024 Jan 12 20:47 ..
-rwxr-xr-x    1 root     root       111957 Jan 12 20:49 P51-06.txt
-rwxr-xr-x    1 root     root         2524 Jan 12 20:49 P51-17.txt
root@ttyp0[src1]#  mv P51-17.txt extract.pl
root@ttyp0[src1]#  vi extract.pl
```

'*vi*' is a text editor in linux we used to remove all unnecessary text i n the Phrack Magazine Volume 7 – article 17[12] text file and leave only the extraction Perl script. Then we execute the Perl script to extract LOKI2 source code from Phrack Magazine Volume 7 - article 06[11] text file.

```
root@ttyp0[src1]#  ls -al
total 122
drwxr-xr-x    2 root     root         1024 Jan 12 20:52 .
drwxr-xr-x    3 root     root         1024 Jan 12 20:47 ..
-rwxr-xr-x    1 root     root       111957 Jan 12 20:49 P51-06.txt
-rwxr-xr-x    1 root     root         1456 Jan 12 20:52 extract.pl
root@tty p0[src1]#  perl extract.pl P51 -06.txt
Attempting extraction of L2/Makefile
Attempting extraction of L2/client_db.c
Attempting extraction of L2/client_db.h
Attempting extraction of L2/crypt.c
Attempting extraction of L2/crypt.h
Attempting extraction of L2/lo  ki.c
Attempting extraction of L2/loki.h
Attempting extraction of L2/lokid.c
Attempting extraction of L2/md5/Makefile
Attempting extraction of L2/md5/global.h
Attempting extraction of L2/md5/md5.h
Attempting extraction of L2/md5/md5c.c
Attempting extraction  of L2/pty.c
Attempting extraction of L2/shm.c
Attempting extraction of L2/shm.h
Attempting extraction of L2/surplus.c
root@ttyp0[src1]#  ls -Ral
.:
total 124
drwxr-xr-x    3 root     root         1024 Jan 12 20:57 .
drwxr-xr-x    3 root     root         1024 Jan 12 20:47 ..
dr----x--t    3 root     root         1024 Jan 12 20:57 L2
-rwxr-xr-x    1 root     root       111957 Jan 12 20:49 P51-06.txt
-rwxr-xr-x    1 root     root          553 Jan 12 20:56 extract.pl

./L2:
total 90
dr----x--t    3 root     root         1024 Jan 12 20:57 .
drwxr-xr-x    3 root     root         1024 Jan 12 20:57 ..
-rw-r--r--    1 root     root         2651 Jan 12 20:57 Makefile
-rw-r--r--    1 root     root         6685 Jan 12 20:57 client_db.c
-rw-r--r--    1 root     root         1750 Jan 12 20:57 client_db.h
-rw-r--r--    1 root     root         3971 Jan 12 20:57 crypt.c
-rw-r--r--    1 root     root          470 Jan 12 20:57 crypt.h
-rw-r--r--    1 root     root        16720 Jan 12 20:57 loki.c
-rw-r--r--    1 root     root        14797 Jan 12 20:57 loki.h
-rw-r--r--    1 root     root        18876 Jan 12 20:57 lokid.c
dr----x--t    2 root     root         1024 Jan 12 20:57 md5
-rw-r--r--    1 root     root         3739 Jan 12 20:57 pty.c
-rw-r--r--    1 root     root         2813 Jan 12 20:57 shm.c
-rw-r--r--    1 root     root          645 Jan 12 20:57 shm.h
-rw-r--r--    1 root     root         8018 Jan 12 20:57 surplus.c
```

```
./L2/md5:
total 18
dr----x--t    2 root     root         1024 Jan 12 20:57 .
dr----x--t    3 root     root         1024 Jan 12 20:57 ..
-rw-r--r--    1 root     root          124 Jan 12 20:57 Makefile
-rw-r--r--    1 root     root          933 Jan 12 20:57 global.h
-rw-r--r--    1 root     root         1530 Jan 12 20:57 md5.h
-rw-r--r--    1 root     root        11353 Jan 12 20:57 md5c.c
```

There are also several websites, which have the LOKI2 source code available in '`tar/gzip`' archive format. Just for comparison purpose we download another LOKI2 source code from Packet Storm [16] website.

```
root@ttyp0[src1]#  cd ..
root@ttyp0[Exam1]#  mkdir src2
root@ttyp0[Exam1]#  cd src2
root@ttyp0[src2]#  pwd
/mnt/Practical/Exam1/src2
root@ttyp0[src2]#  ls -al
total 25
drwxr-xr-x    2 root     root          1024 Jan 12 21:00 .
drwxr-xr-x    4 root     root          1024 Jan 12 20:58 ..
-rwxr-xr-x    1 root     root         21526 Jan 12 21:00 Loki2.tar.tar
root@ttyp0[src2]#  file Loki2.tar.tar
Loki2.tar.tar: bzip2 compressed data, block size = 900k
root@ttyp0[src2]#  bunzip2 Loki2.tar.tar
bunzip2: Can't guess original name for Loki2.tar.t  ar -- using Loki2.tar.tar.out
root@ttyp0[src2]#  ls -al
total 113
drwxr-xr-x    2 root     root          1024 Jan 12 21:02 .
drwxr-xr-x    4 root     root          1024 Jan 12 20:58 ..
-rwxr-xr-x    1 root     root        112640 Jan 12 21:00 Loki2.tar.tar.out
root@ttyp0[src2]#  tar -xvf Loki2.tar.tar.out
L2/
L2/Makefile
L2/client_db.c
L2/client_db.h
L2/crypt.c
L2/crypt.h
L2/loki.c
L2/loki.h
L2/lokid.c
L2/md5/
L2/md5/Makefile
L2/md5/global.h
L2/md5/md5.h
L2/md5/md5c.c
L2/pty.c
L2/shm.c
L2/shm.h
L2/surplus.c
root@ttyp0[src2]#  ls -Ral
.:
total 114
drwxr-xr-x    3 root     root          1024 Jan 12 21:02 .
drwxr-xr-x    4 root     root          1024 Jan 12 20:58 ..
drwx------    3 root     root          1024 Nov  2  1998 L2
-rwxr-xr-x    1 root     root        112640 Jan   12 21:00 Loki2.tar.tar.out

./L2:
total 90
drwx------    3 root     root          1024 Nov  2  1998 .
drwxr-xr-x    3 root     root          1024 Jan 12 21:02 ..
-rw-r--r--    1 root     root          2651 Nov  2  1998 Makefile
-rw-r--r--    1 root     root           6685 Nov  2  1998 client_db.c
-rw-r--r--    1 root     root          1750 Nov  2  1998 client_db.h
```

```
-rw-r--r--    1 root     root         3971 Nov  2  1998 crypt.c
-rw-r--r--    1 root     root          470 Nov  2  1998 crypt.h
-rw-r--r--    1 root      root        16720 Nov  2  1998 loki.c
-rw-r--r--    1 root     root        14797 Nov  2  1998 loki.h
-rw-r--r--    1 root     root        18876 Nov  2  1998 lokid.c
drwx------    2 root     root         1024 Nov  2  1998 md5
-rw-r--r--    1 root     roo t         3739 Nov  2  1998 pty.c
-rw-r--r--    1 root     root         2813 Nov  2  1998 shm.c
-rw-r--r--    1 root     root          645 Nov  2  1998 shm.h
-rw-r--r--    1 root     root         8018 Nov  2  1998 surplus.c

./L2/md5:
total 18
drwx------    2 root     root         1024 Nov  2  1998 .
drwx------    3 root     root         1024 Nov  2  1998 ..
-rw-r--r--    1 root     root          124 Nov  2  1998 Makefile
-rw-r--r--    1 root     root          933 Nov  2  1998 global.h
-rw-r--r--    1 root      root         1530 Nov  2  1998 md5.h
-rw-r--r--    1 root     root        11353 Nov  2  1998 md5c.c
```

From the file listing we can see that there are no differences between the source codes we extracted from Phrack Magazine [11] and the one we downloaded from Packet Storm. Just to reconfirm on our comparison conclusion, we do a MD5 comparison.

```
root@ttyp0[src2]#  cd ../src1/L2
root@ttyp0[L2]#  pwd
/mnt/Practical/Exam1/src1/L2
root@ttyp0[L2]#  for i in *; do md5sum $i; md5sum ../../src2/L2/$i; done
06e1346590e d816d687c862755450fd3  Makefile
06e1346590ed816d687c862755450fd3  ../../src2/L2/Makefile
a7ece6d77f58d7e3fdc4676083bdc080  client_db.c
a7ece6d77f58d7e3fdc4676083bdc080  ../../src2/L2/client_db.c
130cb15e2e91337652b5c3f509ad6a6c  client_db.h
130cb15e2e91337 652b5c3f509ad6a6c  ../../src2/L2/client_db.h
a1eabedb587dabc4af937e6d5b0de695  crypt.c
a1eabedb587dabc4af937e6d5b0de695  ../../src2/L2/crypt.c
ce308873283d279bb6df215f167f03cd  crypt.h
ce308873283d279bb6df215f167f03cd  ../../src2/L2/crypt.h
22b987159702216 a749340d9345a3a06  loki.c
22b987159702216a749340d9345a3a06  ../../src2/L2/loki.c
bd7691320c05d34abeac6f9661a8b438  loki.h
bd7691320c05d34abeac6f9661a8b438  ../../src2/L2/loki.h
00b8bbdaf6d0939002959c48df9d7579  lokid.c
00b8bbdaf6d0939002959c48df9d7579  ../  ../src2/L2/lokid.c
error processing md5: failed in buffer_read(fd): mdfile: Is a directory
error processing ../../src2/L2/md5: failed in buffer_read(fd): mdfile: Is a
directory
08672c91bbf56b5a92b8798e2fc4ef9a  pty.c
08672c91bbf56b5a92b8798e2fc4ef9a  ../..  /src2/L2/pty.c
cbdce8a480066a073f0ed0e1561684cf  shm.c
cbdce8a480066a073f0ed0e1561684cf  ../../src2/L2/shm.c
f455cb39f7eb8d531f774266976e0aed  shm.h
f455cb39f7eb8d531f774266976e0aed  ../../src2/L2/shm.h
b25c223fb5cb0d68d2c95b43fb705ffe  surplus.c
b25c223fb 5cb0d68d2c95b43fb705ffe  ../../src2/L2/surplus.c
```

By comparing these two-source codes with MD5 checksum, we can conclude that both source codes are identical. So, we just use the source code we extracted from the Phrack Magazine [11].

Now, let try to compi le the binary file extracted. When we type, " `make`", it as us to specify which system we are compiling it from. So we type, " `make linux`".

```
root@ttyp0[L2]#  make

LOKI2 Makefile
Edit the Makefile and then invoke with one of the following:

linux openbsd fre ebsd solaris    clean

See Phrack Magazine issue 51 article 7 for verbose instructions

root@ttyp0[L2]# make linux
make[1]: Entering directory `/mnt/Practical/Exam1/src1/L2'
gcc -Wall -O6 -finline-functions  -funroll-all-loops -DLINUX -DWEAK_CRYPTO  -DPOPEN -
DSEND_PAUSE=100  -Dx86_FAST_CHECK      -c surplus.c  -o surplus.o
In file included from /usr/include/linux/signal.h:4,
                 from loki.h:38,
                 from surplus.c:10:
/usr/include/asm/signal.h:26: warning: `NSIG' redefined
                              (---The output  removed---)
/usr/include/bits/siginfo.h:289: warning: `sigevent_t' previously declared here
make[1]: *** [surplus.o] Error 1
make[1]: Leaving directory `/mnt/Practical/Exam1/src1/L2'
make: *** [linux] Error 2
```

From the output, we can seem that trying to c ompile the source code on our Knoppix Linux system cause too many warn ings/errors. Seem that we cannot compile it from our Knoppix Linux system. Maybe it needs an old Linux system. Let try compiling it on the old RedHat Linux version 5.1.

```
[root@ftp L2] # make linux
make[1]: Entering directory `/home/Practical/Exam1/src2/L2'
gcc -Wall -O6 -finline-functions -funroll-all-loops -DLINUX -DWEAK_CRYPTO  -DPOPEN -
DSEND_PAUSE=100  -Dx86_FAST_CHECK      -c surplus.c  -o surplus.o
In file included from /usr/include/li  nux/signal.h:4,
                 from loki.h:38,
                 from surplus.c:10:
/usr/include/asm/signal.h:60: warning: `SA_NOMASK' redefined
                              (---The output removed ---)
/usr/include/signal.h:48: warning: `__sighandler_t' previously declared here
/usr/include/asm/signal.h:86: redefinition of `struct sigaction'
In file included from surplus.c:10:
loki.h:357: field `iph' has incomplete type
make[1]: *** [surplus.o] Error 1
make[1]: Leaving directory `/home/Practical/Exam1/src2/L2'
make: *** [linux] Error 2
```

From the output we can see that trying to compile on the old RedHat version 5.1 still cause too many warnings/errors. We still could not compile the source code on this system.

We try to compile on two different system but unable to compile the LOKI2 source code on both system. So, further analysis that we can do is to compare between the "`strings`" and "`grep -I "loki"`" output of the binary file and the source code.

```
root@ttyp0[L2]#  grep -i "loki" ../../atd.strings
lokid: Client database full
lokid ve rsion:          %s
lokid: inactive client <%d> expired from list [%d]
lokid -p (i|u) [ -v (0|1) ]
LOKI2   route [(c) 1997 guild corporation worldwide]
lokid: server is currently at capacity.  Try again later
lokid: Cannot add key
lokid: popen
lokid: client  <%d> requested an all kill
lokid: clean exit (killed at client request)
lokid: cannot locate client entry in database
lokid: client <%d> freed from list [%d]
lokid: unsupported or unknown command string
lokid: client <%d> requested a protocol swap
lokid: transport protocol changed to %s
root@ttyp0[L2]#  grep -i "nloki" *
client_db.c:        if (verbose) fprintf(stderr, "   \nlokid: Client database full");
client_db.c:    n = sprintf(buf, "  \nlokid version: \t\t%s\n", VERSION);
client_db.c:                if (ver  bose) fprintf(stderr, " \nlokid: inactive client
<%d> expired from list [%d] \n", client[i].client_id, i);
loki.c:              if (verbose) fprintf(stderr, "   \nloki: %s", L_MSG_DHKEYGEN);
loki.c:          if (verbose) fprintf(stderr, "   \nloki: submiting o ur public key
to server");
loki.c:          if (verbose) fprintf(stderr, "   \nloki: Transport protocol changed
to %s.\n", pprot -> p_name);
loki.c:          fprintf(stderr, "  \nloki: clean exit \nroute [guild
worldwide]\n");
loki.c:       fprintf(stderr,  "\nloki: Alarm timer changed to %d seconds.",
*timer);
loki.c:       fprintf(stderr, "  \nloki: protocol swapping only supported in
Linux\n");
loki.h:#define L_MSG_BANNER    "  \nLOKI2\troute [(c) 1997 guild corporation
worldwide]\n"
loki.h:#define S_MSG_PACK ED    "\nlokid: server is currently at capacity.  Try
again later\n"
loki.h:#define S_MSG_UNKNOWN   "  \nlokid: cannot locate client entry in database  \n"
loki.h:#define S_MSG_UNSUP     "  \nlokid: unsupported or unknown command string  \n"
loki.h:#define S_MSG_I CMPONLY  "\nlokid: ICMP protocol only with strong
cryptography\n"
loki.h:#define S_MSG_CLIENTK   "  \nlokid: clean exit (killed at client request)  \n"
loki.h:#define S_MSG_DUP       "  \nlokid: duplicate client entry found, updating  \n"
loki.h:#define S_MSG_USAG E     "\nlokid -p (i|u) [ -v (0|1) ]\n"
loki.h:#define C_MSG_USAGE     "  \nloki -d dest -p (i|u) [ -v (0|1) ] [ -t (n>3)
]\n"
loki.h:#define C_MSG_TIMEOUT   "  \nloki: no response from server (expired timer)  \n"
loki.h:#define C_MSG_NOSWAP    "  \nloki: cannot s wap protocols with strong crypto  \n"
loki.h:#define C_MSG_MUSTQUIT  "  \nloki: received termination directive from
server\n"
lokid.c:    if (verbose) fprintf(stderr, "  \nlokid: %s", L_MSG_DHKEYGEN);
lokid.c:    if (verbose) fprintf(stderr, "  \nlokid: done. \n");
lokid.c:                  fprintf(stderr, "  \nlokid: public key submission and
request : %s <%d> ", host_lookup(rdg.iph.ip_dst), c_id);
lokid.c:                  fprintf(stderr, "  \nlokid: computing shared secret");
lokid.c:              if (verbose)   fprintf(stderr, " \nlokid: extracting 128 -bit
blowfish key");
lokid.c:                  err_exit(1, 0, verbose, "   \nlokid: Cannot add key \n");
lokid.c:                  fprintf(stderr, "   \nlokid: client <%d> added to list
[%d]", c_id, c);
lokid.c:                   fprintf(stderr, "  \nlokid: submiting my public key to
client");
lokid.c:              err_exit(1, 1, verbose, "   \nlokid: popen");
lokid.c:         if (verbose) fprintf(stderr, "   \nlokid: client <%d> requested an all
kill\n", c_id);
lokid.c:         else if (verbose) fprintf(stderr, "  \nlokid: client <%d> freed from
list [%d]", c_id, m);
```

```
lokid.c:    if (verbose) fprintf(stderr, "  \nlokid: client <%d> requested a protocol
swap\n", c_id);
grep: md5: Is a directory
```

After comparing the “`strings`” and “`grep -i “loki”`” output of the binary file to the source code, we can see that the most matching output strings are in the source code file “`client_db.c`”, “`loki.h`” and “`lokid.c`”. “`client_db.c`” and “`loki.h`” are only include/header files. So, we can conclude that this binary file is a compilation of “`lokid.c`”.

2. <u>What other files are used when the program is executed/implemented?</u>

   Using “`strace`” command, as shown in part 4 of section “ **Program Description**” above, we can see that, beside the system file `"libc.so.5"`, the binary file is searching and trying to access these files:

```
a. "/etc/ld.so.cache"
b. "/etc/ld.so.cache"
c. "/etc/ld.so.preload"
d. "/usr/share/locale/C/LC_MESSAGES"
e. "/etc/locale/C/libc.cat"
f. "/usr/lib/locale/C/libc.cat"
g. "/usr/lib/locale/libc/C"
h. "/usr/share/locale /C/libc.cat"
i. "/usr/local/share/locale/C/libc.cat"
```

   From here we can see that this binary file doesn’t open any log/record files. This program also doesn’t sniff or wiretap any information from the system/network.

3. <u>How is the file system affected by the ex ecution of the program?</u>

   This binary file doesn’t affect the compromise file system. This binary file only opens a backdoor gateway using ICMP covert channel (ICMP_ECHO tunneling). Please refer to part 2 of section “ **Program Description** ” above for more detail explanation. By using the binary file client program, the compromise system can be easily accessed.

4. <u>Does the program use, manipulate, or reference any other system files?</u>

   Yes, the binary file has a dynamic link to the system files. Command ’*readelf -a*’, ’*strace -o*’ (shown in part 4 of section “ **Program Description**” above) and even execute the binary file itself can shows which system files that this binary file need to access. The system file required on execution of the binary file is called ‘ `libc.so.5`’.

```
root@ttyp0[L2]#  cd ../..
root@ttyp0[Exam1]#  readelf atd -a;
                              (--- The output removed ---)
Dynamic segment at offset 0x3644 contains 17 entries:
  Tag        Type                         Name/Value
 0x00000001 (NEEDED)                     Shared libr   ary: [libc.so.5]
 0x0000000c (INIT)                       0x8048a70
 0x0000000d (FINI)                       0x804a8e0
 0x00000004 (HASH)                        0x80480e8
 0x00000005 (STRTAB)                      0x80486ac
 0x00000006 (SYMTAB)                        0x804828c
 0x0000000a (STRSZ)                       528 (bytes)
 0x0000000b (SYMENT)                      16 (bytes)
 0x00000015 (DEBUG)                       0x0
 0x00000003 (PLTGOT)                      0x804c570
 0x00000002 (PLTRELSZ)                      400 (bytes)
 0x00000014 (PLTREL)                      REL
 0x00000017 (JMPREL)                      0x80488dc
 0x00000011 (REL)                         0x80488bc
 0x00000012 (RELSZ)                       32 (bytes)
 0x00000013 (RELENT)                      8   (bytes)
 0x00000000 (NULL)                        0x0
                                (---The output removed ---)
root@ttyp0[Exam1]#  ./atd
./atd: can't load library 'libc.so.5'
```

When execute the binary file itself, it give us a warning saying that it's require a system file which does not exist in our current system. Without this system file, the binary file cannot be executed. For more explanations, please refer to part 4 of section ' **Program Description** ' above.

5. Are there any "leads" that could be pulled out of the file for further investigation (e.g., IP address, user information, etc.)?

   No, there is no "leads" that could be pulled out from the binary file for further investigation. Access to the compromise system is required for further investigation.

Program Identification

As mention in part 1 of section " **Program Description** " that this binary file is a LOKI2 program. Also as mention in Part 1 of section " **Forensic Detail** ", we can conclude that this binary file is a LOKI2 deamon (" `lokid`") executable file.

Legal Implications

1. Prove that this program was executed

   Analysis of the binary file extracted from the zip file gives us limited information. Please refer in section " **Binary Detail**" for analysis detail. From the binary file itself, we cannot determine whether the binary file was executed or not. Direct analysis from the compromise system is needed to determine whether the binary file was executed or not.

   Because the binary file needs to refer to system file for execution, we can only say that the binary file was compiled fro m the compromise system itself. Different system have different configuration and cause the binary file to be compiled differently and refer to different system file.

2. What Laws may have been violated?

   As describe earlier in part 2 of section " **Program Description**", LOKI2 is an ICMP covert channel (ICMP_ECHO tunneling) backdoor program.

   In Malaysia, the violation by executing this binary file for unauthorized access to any computer system fall under section 3 of Computer Crimes Bill 1997 [17] title "Unauthorised access to computer material" which state:

> **Computer Crimes Bill 1997**
> **Section 3: Unauthorised access to computer material**
>
> 4. a person shall be guilty of an offence if:
>
>   a. he causes a computer to perform any function with intent to secure access to any program or dat a held in any computer;
>   b. the access he intends to secure is unauthorised; and
>   c. he knows at the time when he causes the computer to perform the function that that is the case.
>
> 5. the intent a person has to have to commit an offence under this section need not be directed at:
>
>   a. any particular program or data;
>   b. a program or data of any particular kind; or
>   c. a program or data held in any particular computer.
>
> 6. a person guilty of an offence under this section shall on conviction be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding five years or to both.

3. The penalties if convicted

   As stated above, in part 2 of this section, in Malaysia, the penalty if convicted, the offender is liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding five years or to both.

4. Authorized use of the program

   As mention in part 2 of section " **Program Description** ", in the good hand this program, can be used as a helping tool. For example, a system administrator which is currently working off base (out station) and/or not near to server room, but need direct access to the server for urgent matter can use this program to have remote access to the server.

   The system administrator is the person who is already assigned to be in charge of the server maintenances and already has full access to the server. By using this program, the system administrator can make his/her work easier because he doesn't have to get direct physical access to the server.

5. Violation of internal policies

   But if this program was installed by a wrong hand, the program can give the unauthorized user a remote " `root`" access without needing to login to the server.

   The "`root`" access give the unauthorized user unlimited access to the server. Basically the unauthorized user can do anything he/she wanted with the compromised server.

   Due to this, every company should have a policy similar to section 3 of Computer Crimes Bill 1997 [14] title "Unauthorised access to computer material" which was mentioned in part 2 of this section. This policy is to protect the organization from any internal hacker.

Interview Questions

If we were given a chance to interview the suspect, these are the question that we might ask:

1. Even though we already know the answer but by asking the suspect a bout his name and job as an introduction can make the suspect feel a little bit comfortable.

   Explanation: By making the suspect feel easy and comfortable, we can aspect a better cooperation from the suspect.

2. Then we continue our interview by query whe ther he/she have any knowledge about the investigation.

   a. Why he/she was called for the interview?
   b. What/why/who is being investigated?
   c. What are the misconduct actions done?

   Depend on the suspect responds, and then we explain the situation of the investigation. Explain to the suspect why we need this information and what is currently going on.

   Explanation: By doing these, we can see how the suspect reacts to the question by monitoring his/her body language. From here we can judge on his/her level of cooperation with us.

3. Next we try to find-out his level of computer knowledge.

    a. Linux Operating System (OS) knowledge

        i. Different user privilege i.e. root
        ii. Accessing the server

    b. Network knowledge

        i. Knowledge of ICMP
        ii. Covert channel
        iii. Backdoor

    c. Programming/compiling knowledge

        i. GCC
        ii. Gather source code information
        iii. Knowledge on compiling the source code
        iv. Usage of the program compiled

    We can also find-out where he/she have learned about all this computer knowledge he/she know.

    Explanation: By knowing his/her level of computer knowledge, we can judge whether he/she has actually done misconduct action by him/herself or by the help of others. And by doing this, he/she should think that we respect his/her skill and we are on his/her side. This will make the suspect more comfortable.

4. Then we query about his/her access level on the compromise system.

    a. Console/Terminal/Remote access
    b. Become "`root`"/unauthorized access
    c. System administrator privilege
    d. During the incident, did he/she logged on the system

    We can also mention to him/her that without his/her cooperation, we can also find-out this information by ourselves but we have to call -in the law enforcement officer to do the investigation with us. With outside interference, this internal misconduct will become state criminal issues. We can also say that, with his/her full cooperation, we can avoid this situation.

    Explanation: We are trying to get his/her guilt to work with us. By adding outside factor and making the issue big, hopefully he/she will want to avoid this situation and give us his/her full cooperation.

5. Finally we need the suspect confirmation on installing the binary file on the compromise system.

    a. Authorization/permission on installing the binary program
    b. Reason for installing the binary program

    Here, we explain the used of the program in the good hand and also in the wrong hand. If we still didn't get full cooperation from the suspect, we can still add the outside factor i.e. the law enforcement officer, end up in jail etc and stress on it.

    Explanation: First we are trying to confirm, voluntarily, on installation of the binary file. If the outcome is not as we expected, we add more pressure by adding outside factor and make things look worst and out of our control. With this pressure, hopefully, we ge t the answer we need.

Additional Information

1. LOKI ICMP tunneling back door
    URL: http://www.iss.net/security_center/static/1452.php
    (February 2003)
2. Advanced/Other Techniques for ByPassing Firewalls
    URL: http://www.fromadia.com/newsread.php?newsid=469
    (February 2003)
3. Defensive recommendations
    URL: http://www.sans.org/y2k/practical/Mark_Cooper.doc
    (January 2003)
4. Strategies for Defeating Distributed Attacks
    URL: http://razor.bindview.com/publish/papers/strategies.html
    (February 2003)
5. ICMP Attacks Illustra ted
    URL: http://rr.sans.org/threats/ICMP_attacks.php (February 2003)

Part 2 – Option 2: Perform Forensic Tool Validation

Introduction

Microsoft (MS) has produced various types of Operating System (OS), which support various type of file system. The first OS that was produce d by MS is MS DOS (Disk Operating System). Later MS produce a Graphical User Interface (GUI) OS which was called MS Windows.

Operating System (OS)	File System Supported				
	FAT12	FAT16	FAT32	NTFS	NTFS5
MS DOS (version before 5.00)	✓				
MS DOS (version 5.00 to6.22)	✓	✓			
MS Windows 95 (before OSR2)	✓	✓			
MS Windows NT (highest version 4.0)	✓	✓		✓	✓SP4
MS Windows 95 (OSR2)	✓	✓	✓		
MS Windows 98 (and Second Edition)	✓	✓	✓		
MS Windows 2000	✓	✓	✓	✓	✓
MS Windows Millennium	✓	✓	✓		
MS Windows XP (Home and Pro)	✓	✓	✓	✓	✓
MS Windows 2003	✓	✓	✓	✓	✓
Maximum Volume Size	2Mb	2Gb	2Tb	16Eb	16Eb

```
Notes [18] [19] [20]:  FAT12 = File Allocation Table  (12-bit)
               FAT16 = File Allocation Table  (16-bit)
               FAT32 = File Allocation Table  (32-bit)
               NTFS  = New Technology File System (64-bit old standard )
               NTFS5 = New Technology File System ver 5.0 (64-bit new standard )
               Mb    = MegaBytes
               Gb    = GigaBytes
               Eb    = ExaBytes
```

Because of its nice and user friendly GUI, MS Windows are quickly becoming the standard OS in the world from a home user to the business world live server system.

Although MS Windows become the standard OS, its lack of integrated method in restoring files or partition that have been accidentally/purposely deleted, formatted, and re partitioned except Recycled Bin . The Recycled Bin function temporarily store deleted file (deleted by using the 'DEL' key or dragged to the Recycled Bin icon), which can then be restored back if it is not emptied. Recycled Bin cannot handle file deleted by using shift-'DEL', shift-dragged, 'del' command in DOS prompt, formatted or repartitioned.

Recovering these permanently deleted file is very critical to the Forensic Analyst in investigating a system that have been tempered or compromised as the offend ers or hackers may have delete files or even reformat or repartition the hard disk to cover their tracks.

In conclusion, we need third party software to recover these deleted files. After surveying several products, EasyRecovery Professional (ER Pro) fr om Ontrack was the product that supports various MS Windows file system. Not just that, after installation of ER Pro windows version, it can then create a disk, which is bootable and run an ER Pro in pure DOS mode (without installation).

In this report, several tests will be simulated on recovering data from various disaster situations. We were also asked to download and include a zipped binary file named "`sn.zip`" in our test. Assuming that this file is our crucial evidence file to be recovered which co ntain a sniffer program downloaded by the suspect. Because this tool is a media analysis tool, we will plant the zipped binary file into the media that we were going to analyzed. Here we want to investigate and validate whether ER Pro can be used as an evidence recovery tools in forensic analysis.

Scope

A forensic investigator receives a case regarding a system administrator which have misuse his/her capability/talent and office equipment in providing illegal services through internet. After hearing that the company is investigating his/her activities, he/she tries to cover his/her track by deleting logs files and reformat his/her office computer. After seizing and imaged all the necessary computer system, recovering the lost evidence files is one of necessary step during the forensic analysis.

ER Pro support data recovery on various file disaster situation that may be very useful during this type of forensic analysis:

1. Deleted file
2. Partition table removed
3. Repartition to same file system and reformat
4. Repartition to different file system and reformat

Both Windows and DOS version have the ability to recover file from these disaster situation.

Although MS Windows and ER Pro support various file system, we will only test ER Pro on two cloned hard disk (HDD) of real live MS Windows systems that are FAT32 file system and NTFS file system. We choose these file systems because they are the most commonly used file system either in the home desktop system and/or as commercial server systems.

These cloned HDD will be simulated on above disaster situation and both version of ER Pro will be used to recover a few selected data. Same data will be recovered from every simulated HDD to determine whether ER Pro capable of recovering the same data in all different situation.

To ensure the validity of the product as a forensic data recovery tool, these entire tests will be conducted in a manner as to simulate a forensic investigation.

Tools Description

At the time of writing this paper, Ontrack Inc. [21] is the developer of EasyRecovery Professional (ER Pro) [22], which is located at 9023 Columbine Road, Eden Prairie, MN 55347. Ontrack Inc. can be contacted by email at sales@ontrack.com or by phone at 1 -800-645-3649. ER Pro newest version is 6.01 (previous version wa s 5.12a) and the software cost is US$499.00.

A trial version of ER Pro can be downloaded from Ontrack Inc. site itself at http://www.ontrack.com/easyrecovery/info.asp but need to be registered first. The ER Pro Trial edition identifies and allows you t o view the deleted files and corrupted documents that you could recover and restore with a full edition of ER Pro. But the Zip repair component is fully functional and allows you to recover and repair deleted or corrupt Zip files.

ER Pro is primarily a d ata recovery[23] tools that is design to rec over accidentally/permanently deleted/lost of data either by deletion, repartitioned or formatted in MS Windows situation. The file system ER Pro supports are FAT12 (floppy), FAT16, FAT32, and NTFS. The media devi ces supported by ER Pro are any devices recognized by MS Windows system (IDE, SCSI, ZIP drive etc). Additional functions added in its newest version are the ability to repair corrupted MS Office documents, Zip files and MS Outlook mailbox. It can also rec over data in unallocated cluster by searching for file header signature info. In this test, we just evaluate the primary function of ER Pro that is data recovery .

ER Pro is a windows application, but after installation, ER Pro for windows can produce a b ootable diskette which contains ER Pro for DOS. With ER Pro DOS version, no installation is required for the data recovery process. This gives us the ability to recover data on any system with a working floppy drive by just adding another storage device to store recovered data. ER Pro DOS version function is limited. ER Pro DOS version only has the ability to recover data. The additional new functions are no t available in the DOS version.

ER Pro ability to recover lost evidence will be very useful to Forensic Analyst in their investigation. With this ability, investigation on any tempered or compromised machines can add more evidence and make their conclusion become much stronger because those deleted/lost evidence files with clues can be recovered.

One scenario, an employee resigned from an organization. Before resigning, the employee permanently reformats the machine hard disk and cause lots of company priceless documentation lost. Even if the employee was called back, those deleted documentatio n are still lost and the employee misconduct is still not proven. But using ER Pro, those priceless documents can be rescued. The rescued priceless documents can then be as part of evidences showing the employee misconduct.

Test Apparatus

The computer used for this testing was a Pentium celeron 566MHz , 128MB RAM and 10GB hard disk drive (HDD) desktop system configured with dual boot capability. Dual systems preinstalled are MS Windows 98se (without any patches and updates) and Redhat Linux 7.2 (Kernel version without any patches and updates). This system is configured for forensic investigation with two (2) HDD tray mounted for easy HDD exchange during forensic investigation and no network connection . The system BIOS is AMIBIOS version 1.22. The system is located in our secure Forensic Lab which can only be accessed by Computer Forensic Analysts only. The RedHat Linux is required during the testing for HDD (md5sum) checksum function.

After purchasing ER Pro online, we received an e -mail with an URL with username and password to download the ER Pro installer. The downloadable ER Pro installer size is 31.4MB. After copying the ER Pro installer into the CD-RW, now we are ready to instal l ER Pro into our test system. ER Pro installation is straight f orward. Please refer to Appendix 9 for screenshot during the installation.

First, ER Pro installer asks for language to use during installation and ER Pro usage. Next, a n installation welcome screen pop -up with a warning saying not to install the ER Pro on the disk which is to be recovered. Next, a Licensed Agreement screen displayed. Next , the ER Pro installer asks for location to install ER Pro. Here we use the default location given that is “C:\Program Files\Ontrack\EasyRecovery Professional”. Nex t, the ER Pro installer asks for location to create ER Pro shortcut in the Windows Start Menu folder. Here we also use the default location given that is Program Folder called “EasyRecovery Professional”. Next screen, the ER Pro installer shows a summary of parameters that it will use during the installation. These also include the folder asked previously. Next, the ER Pro installer starts copying ER Pro required files into the folder we specified earlier. After the copy process completed, a registrati on screen displayed asking us to register the ER Pro. When we press the “Registration” button shown on the screen, a registration webpage pop -up in our Internet Explorer. After the registration completed, the ER Pro show an installation completed screen.

Now when we go to the Windows Start Menu, we can see that EasyRecovery Professional items have been added. To execute the ER Pro, we can just select it icons from the Windows Start Menu. Next we create ER Pro EmergencyDiskette from the ER Pro applicati on itself. Please refer to Appendix 10 for screenshots during disk ette creation.

ER Pro EmergencyDiskette creation is also straight forward. From ER Pro screen, select DataRecovery from the left panel. Then on the right panel select EmergencyDiskette op tion. Then the ER Pro Diskette Creator welcome screen pop-up. After pressing the "Continue" button, a Licensed Agreement screen displayed. Next, ER Pro Diskette Creator main screen displayed giving a warning about any data contained in the floppy will b e destroyed. Then we insert a formatted empty disk in the floppy drive and press "Start" button to continue. ER Pro Diskette Creator give us a warning before overwrite the floppy disk. After pressing "OK" button, the ER Pro Diskette Creator start copyin g file onto the floppy disk. Finally a completion screen displayed saying that the floppy disk is successfully created.

Now that we have both of the ER Pro Windows and DOS versions, we are ready to start doing the testing.

Environmental Conditions

The test apparatus environments have been mention under " ***Test Apparatus*** " section. These controlled environment conditions are required to eliminate any outside interference i.e. network access and physical access which may effect the test result .

MD5 checksum will be used to verify whether the recovered HDD were untouched by ER Pro and whether all the recovered files are the same as the original. With MD5 checksum, we can also verify whether is there any outside interference during running the test.

Definition of MD5 is "MD5 is an algorithm that is used to verify data integrity through the creation of a 128 -bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to t he specific individual. "[24]

ER Pro is designed to recover and copy the data to another destination such as a removable drive, another hard drive, a floppy diskette, or a network volume. But in this testing situation, the recovered data will be copied into another local HDD. No network connection required. No external devices required.

Description of the Procedures

1. <u>Test Plan</u>

   Two (2) HDD will be used during these tests. These HDD will be cloned from two OS installation using Norton Ghost [12] for DOS (bootable disk) by Symantec Corp . Norton Ghost is a great tool to duplicated/cloned HDD for backup purpose.

   One (1) HDD will be cloned with FAT32 (MS Windows 98se installation) file system and another HDD will be cloned with NTFS (MS Windows 2000 installation) file system.

To verify that the cloned HDD were successfully cloned, we replace the cloned HDD with the original HDD and try to boot-up the system with the cloned HDD. If the system successfully boot-up, this mean that our cloning process is successful.

The zipped binary file, '`sn.zip`', downloaded from GIAC practical exam website will be planted in cloned HDD, FAT32 and NTFS file system, under folder "`\Download`". This file will be one of our simulated lost file to be recovered.

```
Sn.zip

D:\Download\sn.zip
   MD5: 5fea57f2a1546bc391c6b9cb1bbfc452

Zip file contain:
   sn.dat     389KB      11/04/2002 09:29
         MD5: 0e954f43fd73f56e812a7285f32e41d3
   sn.md5     37 bytes   11/04/2002 09:29
         MD5: fe89813cd0bdd13971e5c385c63930f4

Sn.md5 file contain:
   0e954f43fd73f56e812a728 5f32e41d3  sn
```

In addition to the zipped binary file, eight (8) other files are randomly chosen as our lost files that are to be recovered in each HDD. The eight files are chosen from these file types: GIF (Image), DOC (Document), JPG (Image), XLS (Document), PPT (Document), TXT (Text Notes), EXE (Application) and COM (Application). MD5 checksum values were also calculated for each file.

```
FAT32 Partition:

D:\Program Files\Paint Shop Pro 6\Anims\Tube.gif
   MD5: fac395242697347c2a24c17e4ec2aa59
D:\Program Files\Quick View Plus\SAMPLES\msword2.doc
   MD5: 89138783d69b7d7d8fbb86224bd1342a
D:\Program Files\Roxio\WinOnCD\Images\bck\canvas_dark_blue.jpg
   MD5: 8dbc7cc7a3feb7b8fde8edeeaa268c2a
D:\Program Files\Quick View Plus\SAMPLES\msexcel.xls
   MD5: 4ad2cfd5c730299 61fcbfb5b7330996d
D:\Program Files\Quick View Plus\SAMPLES\powerpt.ppt
   MD5: 4caf30766db0bc9eaf133e46049b41b6
D:\UTILS\dn\doc\english\history.txt
   MD5: 6cff95aa45756531484c7f760f9fe1f3
D:\Program Files\Adobe\Acrobat 5.0\Reader\AcroRd32.exe
   MD5: 358f5f9aaa7b576bb4fe74ce6e61323c
D:\DOS\4DOS.COM
   MD5: 5ba55680533727e153606947ae026286


NTFS Partition:

D:\Program Files\CacheSentry\Docs\CacheSentryWindowTips.gif
   MD5: 5a599350b5a46e56b9a4105fa4dd34bb
```

```
D:\Program Files\Quick View Plus\SAMPLES\msword2.doc
   MD5: 8913878 3d69b7d7d8fbb86224bd1342a
D:\Program Files\GPSoftware\Directory Opus\Images\Leaf.JPG
   MD5: a0565cb3cfc82ccb3509800f8ccab22b
D:\Program Files\Quick View Plus\SAMPLES\msexcel.xls
   MD5: 4ad2cfd5c73029961fcbfb5b7330996d
D:\Program Files\Quick View Plus\SAMPLES\powerpt.ppt
   MD5: 4caf30766db0bc9eaf133e46049b41b6
D:\DOS\TCMD32.TXT
   MD5: 65bf77fc5199fe3711f43cae10248d05
D:\Program Files\Adobe\Acrobat 5.0\Reader\AcroRd32.exe
   MD5: ba9a26a090809162ee06d6688f0ed4cf
D:\DOS\4DOS.COM
   MD5: 09fa40b1080e0b3a66f07adf5 ba05917
```

These MD5 checksum values will be used to compare with the recovered files in all test result. Here we can see whether ER Pro able to recover these file as its original.

An MD5 value of the HDD to be re covered is also calculated after disaster situation is simulated and before ER Pro is used. Another MD5 values is calculated after using ER Pro on the HDD recovered. Both of these MD5 then will be compared to verify whether or not that the ER Pro touched the recovered HDD.

Both of the HDD will b e simulated in 4 different disaster situations:

1. Permanently deleted files
2. Partition table removed
3. Reformatted with same file system
4. Reformatted with different file system

In all the disaster situations simulated, both the Windows and DOS version of ER Pro will be used to recover the lost files.

Because the test procedures for all disaster situations are very similar, we don't want to mention it repeatedly in the report section. Below is the basic procedure that we will go through for each test.

2. Pre-Test Procedure

Four (4) disaster situations will be simulated on both FAT32 file system and NTFS file system and for all four (4) disaster situation simulated; both ER Pro (Windows and DOS version) will be used to recover the nine (9) lost files. Total of sixteen (16) tests will be conducted.

1. Permanently deleted files

   Purpose: To test the basic recovery function of ER Pro by recovering deleted files where the HDD partition table and File Allocation Table (FAT) or Master File Table (MFT) are still intact.

The chosen files mention in part 1 of section " **Description of the Procedures**", were permanently deleted using Windows Explorer with combination of Shift-Del keys. Using this combination keys will permanently delete selected files without moving it to the Recycled Bin.

Another method for permanently deleted files is using MS -DOS command prompt windows. Anything deleted in this windows using "del <filename>" command, will permanently delete the file mention ed as it parameter.

But in this test we use the first method of deletion. Once the disaster simulated, we can continue with the test p rocedure mention below.

2. Partition table removed

Purpose: To test the recovery function of ER Pro by recovering deleted files from the HDD which the partition table where removed or corrupted. Even the without partition table, the original FAT or MFT are still intact.

To easily remove partition, a program called Partition Magic (PM) for DOS (bootable disk)[25] by Powerquest Corporation [26] is used. PM can manage HDD pa rtition without destroying the HDD existing data. With PM we can quickly and easily resize, split, merge, delete, undelete, create, format and convert partitions in GUI user friendly interface.

After successfully removed the partition table information, we can continue with the test procedure mention below.

To verified that the partition been removed, we can use Microsoft "fdisk" or Linux "fdisk –l" command to view partition table. If the no partition displayed, then the partition is successfully remove d.

3. Reformatted with same file system

Purpose: To test more advanced recovery function of ER Pro by recovering deleted files from the HDD which are not only the partition table where removed or corrupted but the original FAT or MFT were removed.

To simulate this situation, PM was also been used to reformat the partition. PM can reformat HDD and support many type of file system. File system supported by PM are FAT16, FAT32, NTFS and EXT2/3.

Here the FAT32 file system will be reformat with FAT32 (same) file system and NTFS file system will be reformat with NTFS (same) file system.

After reformatting both HDD, we can continue with the test procedure mentioned below.

To verified that the partition been reformatted with the same filesystem, we can use Micr osoft "fdisk" or Linux "fdisk –l" command to view partition table. If the partition displayed is the same filesystem type from the previous filesystem, then the partition is successfully reformatted with the same filesystem.

4. Reformatted with different file system

   Purpose: To test more complicated recovery function of ER Pro by recovering deleted files from the HDD which are not only the partition table where removed or corrupted and the original FAT or MFT were removed but also the original FAT or MFT were overwritten with other file system.

   In this disaster situation , PM was also been used to reformat the partition. But in this situation, the FAT32 file system HDD will be repartition and reformatted to become NTFS file system and NTFS file system HDD will be repartition and reformatted to become FAT32 file system.

   After repartition and reformatting both HDD, we can continue with the test procedure mentioned below.

   To verified that the partition been reformatted with the different filesystem, we can us e Microsoft "fdisk" or Linux "fdisk –l" command to view partition table. If the partition displayed is the different filesystem type from the previous filesystem, then the partition is successfully reformatted with the different filesystem

5. Real Case situ ation – Permanently deleted file

   Purpose: To test the recovery function of ER Pro in recovering permanently/purposely deleted evidence forensically sound .

   This is a real case situation we encountered . We receive this case while we are doing testing ER P ro. Several tests have been done on ER Pro and we can conclude that ER Pro can forensically recover the evidence. So we decided to use ER Pro on this case to recover the permanently deleted evidence files.

   Synopsis:

   A system administrator claims that he accidentally deleted the only backup copy of proxy log file s in his IBM notebook. These proxy logs are very import in our investigation. The se logs recorded all the internet transaction /activities for a whole two month s that was under our investigati on.

Background:

The HDD to be recovered was running MS Windows 2000 NTFS file system. The original 6GB HDD was seized from a IBM thinkpad notebook and was label 15/01/03(1)NB(1)ORG. An image copy was made using '`dd`' command and was label 15/01/03(1)NB(1)CPY1.

Using our forensic tools i.e EnCase[27] during investigation , we did not managed to recover these deleted files. So, we finally decided to try ER Pro on recovering the lost evidence files.

MD5 values will be calculated before and after using ER Pro. Both ER Pro Windows and DOS version will be used. The procedure we use is the same as the test procedure mention below.

3. Test Procedure

In this section we describe on how the test will be done. Here is the actual procedure that will test the function of ER Pro. Please refer to Appendix 11 for sample screenshots during the recovery process.

After simulated the disaster situation, the test apparatus will be boot -up using RedHat 7.2 to calculate the MD5 values of the HDD that have been simulated before recovery process.

Then the test apparatus will be boot -up using ER Pro diskette (ER Pro DOS version) and we will try to recover all the nine (9) lost files.

After the lost data have been recovered, the test apparatus will be boot -up using RedHat 7.2 again to recalculate the MD5 values of the HDD that have been recovered using ER Pro DOS version.

Then the test apparatus will be boot -up using MS Windows 98se and we will try to recover again all the nine (9) lost files using ER Pro windows version.

Finally, the test apparatus will be boot -up again using RedHat 7.2 to recalculate the MD5 values of the HDD that have been recovered using ER Pro windows version.

Last phase, we do an analysis on the recovered zipped binary file "`sn.zip`". First we use a program called WinZip[26] to test the zipped file for error. Winzip is an archive tool used for distributing and storing files in one zip file. Files archived in zip format are compressed to save disk space which can then easily be transport and copy. Second we calculate the MD5 value for all the files contain in the recovered zipped file.

After the test is complete, the HDD is now ready to be simulated with another disaster situation.

4. Criteria for Approval

   ER Pro can be executed from MS Windows (ER Pro w indows version) or boot from the bootable disk (ER Pro DOS version) created using ER Pro windows version. Risk when using ER Pro windows version is that MS Windows Operating System is capable of modifying suspect's HDD even during boot-up. This will be c onfirmed in our tests.

   Result we should be expected during recovering using ER Pro (Windows or DOS) is that ER Pro should have no problem recovering all nine (9) files in our entire 18 tests (all 4 different disaster situations in both FAT32 and NTFS and also case). This also will be confirmed in our tests.

   To verify that the ER Pro can be used as a forensic tool, ER Pro has to pass these criteria during the recovery process:

   a. MD5 before and after recovery process have to be the same.

      This criteria is to ensure that ER Pro doesn't modify the content of suspect's HDD during the recovering process. This is very important to ensure that ER Pro can recover evidence files forensically sound.

   b. MD5 files recovered have to be the same with the original file (be fore lost)

      This criteria is to ensure that the file recovered using ER Pro is the exact copy from it original file before removed. This also is very important to ensure that ER Pro can fully and accurately recover files without modifying the file content .

Data Recovery and Results

Refer to Appendix 12, 13, 14, 15 and 16 for data summaries and results.

1. Permanently Deleted Files

a. FAT32 file system with ER Pro DOS version

Hard Disk MD5 before recovery: `72ae12a54249ba1521840bd8ef5e0869`
`Sn.zip`
Path: `\DOWNLOAD\ N.ZIP`
MD5: `5fea57f2a1546bc391c6b9cb1bbfc452`
`Tube.gif`
Path: `\PROGRA~1\PAINTS~1\ANIMS\TUBE.GIF` MD5: `fac395242697347c2a24c17e4ec2aa59`
`msword2.doc`
Path: `\PROGRA~1\QUICKV~1\SAMPLES\MSWORD2.DOC`
MD5: `89138783d69b7d7d8fbb86224bd1342a`
`canvas_dark_blue.jpg`
Path: `\PROGRA~1\ROXIO\WINONCD\IMAGES\BCK\CANVAS~3.JPG`
MD5: `8dbc7cc7a3feb7b8fde8edeeaa268c2a`
`Msexcel.xls`
Path: `\PROGRA~1\QUICKV~1\SAMPLES\MSEXCEL.XLS`
MD5: `4ad2cfd5c73029961fcbfb5b7330996d`
`Powerpt.ppt`
Path: `\PROGRA~1\QUICKV~1\SAMPLES\POWERPT.PPT`
MD5: `4caf30766db0bc9eaf133e46049b41b6`
`history.txt`
Path: `\UTILS\DN\DOC\ENGLISH\HISTORY.TXT`
MD5: `6cff95aa45756531484c7f760f9fe1f3`
`AcroRd32.exe`
Path: `\PROGRA~1\ADOBE\ACROBA~2.0\READER\ACRORD32.EXE`
MD5: `358f5f9aaa7b576bb4fe74ce6e61323c`
`4DOS.COM`
Path: `\Exam2\Fat32\Test01\dos\_DOS.COM`
MD5: `5ba55680533727e153606947ae026286`
Hard Disk MD5 after recovery: `72ae12a54249ba1521840bd8ef5e0869`

LFN.BAT produced:

```
REM This file should be run under Windows to restore your long file names.
@echo off

ren   UTILS\DN\DOC\ENGLISH\HISTORY.TXT "history.txt
ren   PROGRA~1\PAINTS~1\ANIMS\TUBE.GIF "Tube.gif
ren   PROGRA~1\QUICKV~1\SAMPLES\MSEXCEL.XLS "msexcel.xls
ren   PROGRA~1\QUICKV~1\SAMPLES\MSWORD2.DOC "msword2.doc
ren   PROGRA~1\QUICKV~1\SAMPLES\POWERPT.PPT "powerpt.ppt
ren   PROGRA~1\ROXIO\WINONCD\IMAGES\BCK\CANVAS~3.JPG "canvas_dark_blue.jpg
ren   PROGRA~1\ADOBE\ACROBA~2.0\READER\ACRORD32.EXE "AcroRd32.exe
ren   DOS\_DOS.COM "_DOS.COM
ren   DOWNLOAD\_N.ZIP "_N.ZIP
```

SN.ZIP analysis:

```
WinZip Archive Test :

No errors  detected in compressed data of _N.ZIP.
Testing ...
testing: sn.dat                   OK
testing: sn.md5                   OK


MD5 contain of Zip File :

Name     Size      Attr   Modified           Type      MD5 Checksum
----     ----     -----   --------           ----      ------------
sn.dat   389 KB    -a----  11/04/2002 09:29   DAT File  0e954f43fd73f56e812a7285f32e41d3
sn.md5   37 bytes  -a----  11/04/2002 09:29   MD5 File  fe89813cd0bdd13971e5c385c63930f4
```

b. FAT32 file system with ER Pro Windows version

Hard Disk MD5 before recovery: `72ae12a54249ba1521840bd8ef5e086 9`
`Sn.zip`
Path: `\Download\_N.ZIP`
MD5: `5fea57f2a1546bc391c6b9cb1bbfc452`
`Tube.gif`
Path: `\Program Files\Paint Shop Pro 6\Anims\Tube.gif`
MD5: `fac395242697347c2a24c17e4ec2aa59`
`msword2.doc`
Path: `\Program Files\Quick View Plus\SAMPLES\msword2.doc`
MD5: `89138783d69b7d7d8fbb86224bd1342a`
`canvas_dark_blue.jpg`
Path: `\Program Files\Roxio\WinOnCD\Images\bck\canvas_dark_blue.jpg`
MD5: `8dbc7cc7a3feb7b8fde8edeeaa268c2a`
`msexcel.xls`
Path: `\Program Files\Quick View Plus\SAMPLES\msexcel.xls`
MD5: `4ad2cfd5c73029961fcb fb5b7330996d`
`powerpt.ppt`
Path: `\Program Files\Quick View Plus\SAMPLES\powerpt.ppt`
MD5: `4caf30766db0bc9eaf133e46049b41b6`
`history.txt`
Path: `\UTILS\dn\doc\english\history.txt`
MD5: `6cff95aa45756531484c7f760f9fe1f3`
`AcroRd32.exe`
Path: `\Program Files\Adobe\Acrobat 5.0\Reader\AcroRd32.exe`
MD5: `358f5f9aaa7b576bb4fe74ce6e61323c`
`4DOS.COM`
Path: `\dos\_DOS.COM`
MD5: `5ba55680533727e153606947ae026286`
Hard Disk MD5 after recovery: `72ae12a54249ba1521840bd8ef5e0869`

SN.ZIP analysis:

```
WinZip Archive Test :

No errors detected in compressed data of _N.ZIP.
Testing ...
testing: sn.dat                   OK
testing: sn.md5                   OK


MD5 contain of Zip File :

Name     Size       Attr   Modified           Type      MD5 Checksum
----     ----      -----   --------           ----      ------------
sn.dat   389 KB    -a----  11/04/2002 09:29   DAT File  0e954f43fd73f56e812a7285f32e41d3
sn.md5   37 bytes  -a----  11/04/2002 09:29   MD5 File  fe89813cd0bdd13971e5c385c63930f4
```

c. NTFS file system ER Pro DOS Version

Hard Disk MD5 before recovery: c2ea8a2e7f563163828d149235d5ab85
Sn.zip
Path: \DOWNLOAD\SN.ZIP
MD5: 5fea57f2a1546bc391c6b9cb1bbfc452
CacheSentryWindowTips.gif
Path: \progra~1\CACHES~2\DOCS\CACHES~4.GIF
MD5: 5a599350b5a46e56b9a4105fa4dd34bb
msword2.doc
Path: \progra~1\QUICKV~1\SAMPLES\MSWORD2.DOC
MD5: 89138783d69b7d7d 8fbb86224bd1342a
Leaf.JPG
Path: \progra~1\GPSOFT~1\DIRECT~1\IMAGES\LEAF.JPG
MD5: a0565cb3cfc82ccb3509800f8ccab22b
msexcel.xls
Path: \progra~1\QUICKV~1\SAMPLES\MSEXCEL.XLS
MD5: 4ad2cfd5c73029961fcbfb5b7330996d
powerpt.ppt
Path: \progra~1\QUICKV~1\SAMPLES\POWERPT.PPT
MD5: 4caf30766db0bc9eaf133e46049b41b6
TCMD32.TXT
Path: \dos\TCMD32.TXT
MD5: 65bf77fc5199fe3711f43cae10248d05
AcroRd32.exe
Path: \progra~1\ADOBE\ACROBA~1.0\READER\ACRORD32.EXE
MD5: ba9a26a090809162ee06d6688f0ed4cf
4DOS.COM
Path: \dos\4DOS.COM
MD5: 09fa40b1080e0b3a66f07adf5ba05917
Hard Disk MD5 after recovery: c2ea8a2e7f563163828d149235d5ab85

LFN.BAT produced:

```
REM This file should be run under Windows to restore your long file names.
@echo off

ren   Download\sn.zip "sn.zip
ren   DOS\4DOS.COM "4DOS.COM
ren   DOS\TCMD32.TXT "TCMD32.TXT
ren   PROGRA~1\Adobe\ACROBA~1.0\Reader\AcroRd32.exe "AcroRd32.exe
ren   PROGRA~1\QUICKV~1\SAMPLES\msexcel.xls "msexcel.xls
ren   PROGRA~1\QUICKV~1\SAMPLES\msword2.doc "msword2.doc
ren   PROGRA~1\QUICKV~1\SAMPLES\powerpt.ppt "powerpt.ppt
ren   PROGRA~1\GPSOFT~1\DIRECT~1\Images\Leaf.JPG "Leaf.JPG
ren   PROGRA~1\CACHES~2\Docs\CACHES~4.GIF "CacheSentryWindowTips.gif
```

SN.ZIP analysis:

```
WinZip Archive Test :

No errors detected in compressed data of   SN.ZIP.
Testing ...
testing: sn.dat                   OK
testing: sn.md5                   OK


MD5 contain of Zip File :

Name     Size      Attr   Modified           Type      MD5 Checksum
----     ----     -----   --------           ----      ------------
sn.dat   389 KB   -a----  11/04/2002 09:29   DAT File  0e954f43fd73f56e812a7285f32e41d3
sn.md5   37 bytes -a----  11/04/2002 09:29   MD5 File  fe89813cd0bdd13971e5c385c63930f4
```

d. NTFS file system ER Pro Windows Version

Hard Disk MD5 before recovery: c2ea8a2e7f563163828d149235d5ab85
Sn.zip
Path: \Download\sn.zip
MD5: 5fea57f2a1546bc391c6b9cb1bbfc452
CacheSentryWindowTips.gif
Path: \Program Files\CacheSentry\Docs\CacheSentryWindowTips.gif
MD5: 5a599350b5a46e56b9a4105fa4dd34bb
msword2.doc
Path: \Program Files\Quick View Plus\SAMPLES\msword2.doc
MD5: 89138783d69b7d7d8f bb86224bd1342a
Leaf.JPG
Path: \Program Files\GPSoftware\Directory Opus\Images\Leaf.JPG
MD5: a0565cb3cfc82ccb3509800f8ccab22b
msexcel.xls
Path: \Program Files\Quick View Plus\SAMPLES\msexcel.xls
MD5: 4ad2cfd5c73029961fcbfb5b7330996d
powerpt.ppt
Path: \Program Files\Quick View Plus\SAMPLES\powerpt.ppt
MD5: 4caf30766db0bc9eaf133e46049b41b6
TCMD32.TXT
Path: \dos\TCMD32.TXT
MD5: 65bf77fc5199fe3711f43cae10248d05
AcroRd32.exe
Path: \Program Files\Adobe\Acrobat 5.0\Reader\AcroRd32.exe
MD5: ba9a26a090 809162ee06d6688f0ed4cf
4DOS.COM
Path: \dos\4DOS.COM
MD5: 09fa40b1080e0b3a66f07adf5ba05917
Hard Disk MD5 after recovery: c2ea8a2e7f563163828d149235d5ab85

SN.ZIP analysis:

```
WinZip Archive Test :

No errors detected in compressed data of   sn.zip.
Testing ...
testing: sn.dat                  OK
testing: sn.md5                  OK


MD5 contain of Zip File :

Name     Size       Attr   Modified          Type      MD5 Checksum
----     ----      -----   --------          ----      ------------
sn.dat   389 KB    -a----  11/04/2002 09:29  DAT File  0e954f43fd73f56e812a7285f32e41d3
sn.md5   37 bytes  -a----  11/04/2002 09:29  MD5 File  fe89813cd0bdd13971e5c385c63930f4
```

2. Removed Partition table

a. FAT32 file system with ER Pro DOS version

Hard Disk MD5 before recovery: `a0fe4af410f25398572c338f8298bd7a`
Sn.zip
Path: `\DOWNLOAD\_N.ZIP`
MD5: `5fea57f2a1546bc391c6b9cb1bbfc452`
Tube.gif
Path: `\PROGRA~1\PAINTS~1\ANIMS\TUBE.GIF`
MD5: `fac395242697347c2a24c17e4ec2aa59`
msword2.doc
Path: `\PROGRA~1\QUICKV~1\SAMPLES\MSWORD2.DOC`
MD5: `89138783d69b7d7d8fbb86224bd1342a`
canvas_dark_blue.jpg
Path: `\PROGRA~1\ROXIO\WINONCD\IMAGES\BCK\CANVAS~3.JPG`
MD5: `8dbc7cc7a3feb7b8fde8edeeaa268c2a`
Msexcel.xls
Path: `\PROGRA~1\QUICKV~1\SAMPLES\MSEXCEL.XLS`
MD5: `4ad2cfd5c73029961fcbfb5b7330996d`
Powerpt.ppt Path: `\PROGRA~1\QUICKV~1\SAMPLES\POWERPT.PPT`
MD5: `4caf30766db0bc9eaf133e46049b41b6`
history.txt
Path: `\UTILS\DN\DOC\ENGLISH\HISTORY.TXT`
MD5: `6cff95aa45756531484c7f760f9fe1f3`
AcroRd32.exe
Path: `\PROGRA~1\ADOBE\ACROBA~2.0\READER\ACRORD32.EXE`
MD5: `358f5f9aaa7b576bb4fe74ce6e61323c`
4DOS.COM
Path: `\dos\_DOS.COM`
MD5: `5ba55680533727e153606947ae026286`
Hard Disk MD5 after recovery: `a0fe4af410f25398572c338f8298bd7a`

LFN.BAT produced:

```
REM This file should be run under Windows to restore your long file names.
@echo off

ren   UTILS\DN\DOC\ENGLISH\HISTORY.TXT "history.txt
ren   PROGRA~1\PAINTS~1\ANIMS\TUBE.GIF "Tube.gif
ren   PROGRA~1\QUICKV~1\SAMPLES\MSEXCEL.XLS "msexcel.xls
ren   PROGRA~1\QUICKV~1\SAMPLES\MSWORD2.DOC "msword2.doc
ren   PROGRA~1\QUICKV~1\SAMPLES\POWERPT.PPT "powerpt.ppt
ren   PROGRA~1\ROXIO\WINONCD\IMAGES\BCK\CANVAS~3.JPG "canvas_dark_blue.jpg
ren   PROGRA~1\ADOBE\ACROBA~2.0\READER\ACRORD32.EXE "AcroRd32.exe
ren   DOS\_DOS.COM "_DOS.COM
ren   DOWNLOAD\_N.ZIP "_N.ZIP
```

SN.ZIP analysis:

```
WinZip Archive Test :

No errors detected in compressed d  ata of _N.ZIP.
Testing ...
testing: sn.dat                   OK
testing: sn.md5                   OK


MD5 contain of Zip File :

Name     Size      Attr   Modified          Type      MD5 Checksum
----     ----     -----   --------          ----      ------------
sn.dat   389 KB   -a----  11/04/2002 09:29  DAT File  0e954f43fd73f56e812a7285f32e41d3
sn.md5   37 bytes -a----  11/04/2002 09:29  MD5 File  fe89813cd0bdd13971e5c385c63930f4
```

b. FAT32 file system with ER Pro Windows version

Hard Disk MD5 before recovery: a0fe4af410f25398572c338f8298bd7a
Sn.zip
Path: \Download_N.ZIP
MD5: 5fea57f2a1546bc391c6b9cb1bbfc452
Tube.gif
Path: \Program Files \Paint Shop Pro 6 \Anims \Tube.gif
MD5: fac395242697347c2a24c17e4ec2aa59
msword2.doc
Path: \Program Files \Quick View Plus \SAMPLES \msword2.doc
MD5: 89138783d69b7d7d8fbb86224bd 1342a
canvas_dark_blue.jpg
Path: \Program Files \Roxio\WinOnCD\Images \bck\canvas_dark_blue.jpg
MD5: 8dbc7cc7a3feb7b8fde8edeeaa268c2a
Msexcel.xls
Path: \Program Files \Quick View Plus \SAMPLES \msexcel.xls
MD5: 4ad2cfd5c73029961fcbfb5b7330996d
Powerpt.pp t
Path: \Program Files \Quick View Plus \SAMPLES \powerpt.ppt
MD5: 4caf30766db0bc9eaf133e46049b41b6
history.txt
Path: \UTILS \dn\doc\english \history.txt
MD5: 6cff95aa45756531484c7f760f9fe1f3
AcroRd32.exe
Path: \Program Files \Adobe\Acrobat 5.0 \Reader \AcroRd32.exe
MD5: 358f5f9aaa7b576bb4fe74ce6e61323c
4DOS.COM
Path: \dos_DOS.COM
MD5: 5ba55680533727e153606947ae026286
Hard Disk MD5 after recovery: a0fe4af410f25398572c338f8298bd7a

SN.ZIP analysis:

```
WinZip Archive Test :

No errors detected in compresse  d data of _N.ZIP.
Testing ...
testing: sn.dat                    OK
testing: sn.md5                    OK


MD5 contain of Zip File :

Name     Size       Attr   Modified           Type      MD5 Checksum
----     ----      -----   --------           ----      ------------
sn.dat   389 KB    -a----  11/04/2002 09:29   DAT File  0e954f43fd73f56e812a7285f32e41d3
sn.md5   37 bytes  -a----  11/04/2002 09:29   MD5 File  fe89813cd0bdd13971e5c385c63930f4
```

c. NTFS file system with ER Pro DOS version

Hard Disk MD5 before recovery: 8b4f2fea9d0aee07642313f51b484b4d
Sn.zip
Path: \DOWNLOAD\SN.ZIP
MD5: 5fea57f2a1546bc391c6b9cb1bbfc452
CacheSentryWindowTips.gif
Path: \PROGRA~1\CACHES~2\DOCS\CACHES~4.GIF
MD5: 5a599350b5a46e56b9a4105fa4dd34bb
msword2.doc
Path: \PROGRA~1\QUICKV~1\SAMPLES\MSWORD2.DOC
MD5: 89138783d69b7d7d8fbb86224bd1342a
Leaf.JPG
Path: \PROGRA~1\GPSOFT~1\DIRECT~1\IMAGES\LEAF.JPG
MD5: a0565cb3cfc82ccb3509800f8ccab22b
msexcel.xls
Path: \PROGRA~1\QUICKV~1\SAMPLES\MSEXCEL.XLS
MD5: 4ad2cfd5c73029961fcbfb5b7330996d
powerpt.ppt
Path: \PROGRA~1\QUICKV~1\SAMPLES\POWERPT.PPT
MD5: 4caf30766db0bc9eaf133e46049b41b6
TCMD32.TXT
Path: \dos\TCMD32.TXT
MD5: 65bf77fc5199fe3711f43cae10248d05
AcroRd32.exe
Path: \PROGRA~1\ADOBE\ACROBA~1.0\READER\ACRORD32.EXE
MD5: ba9a26a090809162ee06d6688f0ed4cf
4DOS.COM
Path: \dos\4DOS.COM
MD5: 09fa40b1080e0b3a66f07adf5ba05917
Hard Disk MD5 after recovery: 8b4f2fea9d0aee07642313f51b484b4d

LFN.BAT created:

```
REM This file should be run under Windows to restore your long file names.
@echo off

ren   Download\sn.zip "sn.zip
ren   DOS\4DOS.COM "4DOS.COM
ren   DOS\TCMD32.TXT "TCMD32.TXT
ren   PROGRA~1\Adobe\ACROBA~1.0\Reader\AcroRd32.exe "AcroRd32.exe
ren   PROGRA~1\QUICKV~1\SAMPLES\msexcel.xls "msexcel.xls
ren   PROGRA~1\QUICKV~1\SAMPLES\msword2.doc "msword2.doc
ren   PROGRA~1\QUICKV~1\SAMPLES\powerpt.ppt "powerpt.ppt
ren   PROGRA~1\GPSOFT~1\DIRECT~1\Images\Leaf.JPG "Leaf.JPG
ren   PROGRA~1\CACHES~2\Docs\CACHES~4.GIF "CacheSentryWindowTips.gif
```

SN.ZIP analysis:

```
WinZip Archive Test :

No errors detected in compressed data of   SN.ZIP.
Testing ...
testing: sn.dat                   OK
testing: sn.md5                   OK


MD5 contain of Zip File :

Name     Size      Attr   Modified           Type      MD5 Checksum
----     ----     -----   --------           ----      ------------
sn.dat   389 KB   -a----  11/04/2002 09:29   DAT File  0e954f43fd73f56e812a7285f32e41d3
sn.md5   37 bytes -a----  11/04/2002 09:29   MD5 File  fe89813cd0bdd13971e5c385c63930f4
```

d. NTFS file system with ER Pro Windows version

Hard Disk MD5 before recovery: 8b4f2fea9d0aee07642313f51b484b4d
Sn.zip
Path: \Download\sn.zip
MD5: 5fea57f2a1546 bc391c6b9cb1bbfc452
CacheSentryWindowTips.gif
Path: \Program Files\CacheSentry\Docs\CacheSentryWindowTips.gif
MD5: 5a599350b5a46e56b9a4105fa4dd34bb
msword2.doc
Path: \Program Files\Quick View Plus\SAMPLES\msword2.doc
MD5: 89138783d69b7d7d8fbb86224bd1 342a
Leaf.JPG
Path: \Program Files\GPSoftware\Directory Opus\Images\Leaf.JPG
MD5: a0565cb3cfc82ccb3509800f8ccab22b
msexcel.xls
Path: \Program Files\Quick View Plus\SAMPLES\msexcel.xls
MD5: 4ad2cfd5c73029961fcbfb5b7330996d
powerpt.ppt
Path: \Program Files\Quick View Plus\SAMPLES\powerpt.ppt
MD5: 4caf30766db0bc9eaf133e46049b41b6
TCMD32.TXT
Path: \dos\TCMD32.TXT
MD5: 65bf77fc5199fe3711f43cae10248d05
AcroRd32.exe
Path: \Program Files\Adobe\Acrobat 5.0\Reader\AcroRd32.exe
MD5: ba9a26a090809162ee06 d6688f0ed4cf
4DOS.COM
Path: \dos\4DOS.COM
MD5: 09fa40b1080e0b3a66f07adf5ba05917
Hard Disk MD5 after recovery: 8b4f2fea9d0aee07642313f51b484b4d

SN.ZIP analysis:

```
WinZip Archive Test :

No errors detected in compressed data of   sn.zip.
Testing ...
testing: sn.dat                   OK
testing: sn.md5                   OK


MD5 contain of Zip File :

Name     Size      Attr   Modified           Type      MD5 Checksum
----     ----     -----   --------           ----      ------------
sn.dat   389 KB   -a----  11/04/2002 09:29   DAT File  0e954f43fd73f56e812a7285f32e41d3
sn.md5   37 bytes -a----  11/04/2002 09:29   MD5 File  fe89813cd0bdd13971e5c385c63930f4
```

3. Repartitioned and Reformatted with Same File system

a. FAT32 file system with ER Pro DOS version

Hard Disk MD5 before recovery: `f8ac1318653d4dbd44f39852ffb9626e`
`Sn.zip`
Path: `\LOSTFILE\DIR20\_N.ZIP`
MD5: `5fea57f2a1546bc391c6b9cb1bbfc452`
`Tube.gif`
Path: `\LOSTFILE\DIR5\PAINTS~1\ANIMS\TUBE.GIF`
MD5: `fac395242697347c2a24c17e4ec2aa59`
`msword2.doc`
Path: `\LOSTFILE\DIR5\QUICKV~1\SAMPLES\MSWORD2.DOC`
MD5: `89138783d69b7d7d8fbb86224bd1342a`
`canvas_dark_blue.jpg`
Path: `\LOSTFILE\DIR5\ROXIO\WINONCD\IMAGES\BCK\CANVAS~3.JPG`
MD5: `8dbc7cc7a3feb7b8fde8edeeaa268c2a`
`Msexcel.xls`
Path: `\LOSTFILE\DIR5\QUICKV~1\SAMPLES\MSEXCEL.XLS`
MD5: `4ad2cfd5c73029961fcbfb5b7330996d`
`Powerpt.ppt`
Path: `\LOSTFILE\DIR5\QUICKV~1\SAMPLES\POWERPT.PPT`
MD5: `4caf30766db0bc9eaf133e46049b41b6`
`history.txt`
Path: `\LOSTFILE\DIR0\DN\DOC\ENGLISH\HISTORY.TXT`
MD5: `6cff95aa45756531484c7f760f9fe1f3`
`AcroRd32.exe`
Path: `\LOSTFILE\DIR5\ADOBE\ACROBA~2.0\READER\ACRORD32.EXE`
MD5: `358f5f9aaa7b576bb4fe74ce6e61323c`
`4DOS.COM`
Path: `\LOSTFILE\DIR17\_DOS.COM`
MD5: `5ba55680533727e153606947ae026286`
Hard Disk MD5 after recovery: `f8ac1318653d4dbd44f39852ffb9626e`

LFN.BAT created:

```
REM This file should be run under Windows to restore your long file names.
@echo off

ren   LOSTFILE\DIR0\DN\DOC\ENGLISH\HISTORY.TXT "history.txt
ren   LOSTFILE\DIR5\PAINTS~1\ANIMS\TUBE.GIF "Tube.gif
ren   LOSTFILE\DIR5\QUICKV~1\SAMPLES\MSEXCEL.XLS "msexcel.xls
ren   LOSTFILE\DIR5\QUICKV~1\SAMPLES\MSWORD2.DOC "msword2.doc
ren   LOSTFILE\DIR5\QUICKV~1\SAMPLES\POWERPT.PPT "powerpt.ppt
ren   LOSTFILE\DIR5\ROXIO\WINONCD\IMAGES\BCK\CANVAS~3.JPG
"canvas_dark_blue.jpg
ren   LOSTFILE\DIR5\ADOBE\ACROBA~2.0\READER\ACRORD32.EXE "AcroRd32.exe
ren   LOSTFILE\DIR17\_DOS.COM "_DOS.COM
ren   LOSTFILE\DIR20\_N.ZIP "_N.ZIP
```

SN.ZIP analysis:

```
WinZip Archive Test :

No errors detected in compressed data of _N.ZIP.
Testing ...
testing: sn.dat                   OK
testing: sn.md5                   OK


MD5 contain of Zip File :

Name     Size      Attr   Modified           Type      MD5 Checksum
----     ----     -----   --------           ----      ------------
sn.dat   389 KB   -a----  11/04/2002 09:29   DAT File  0e954f43fd73f56e812a7285f32e41d3
sn.md5   37 bytes -a----  11/04/2002 09:29   MD5 File  fe89813cd0bdd13971e5c385c63930f4
```

b. FAT32 file system with ER Pro Windows version

Hard Disk MD5 before recovery: f8ac1318653d4dbd44f39852ffb9626e
Sn.zip
Path: \LOSTFILE\DIR20_N.ZIP
MD5: 5fea57f2a1546bc391c6b9cb1bbfc452
Tube.gif
Path: \LOSTFILE\DIR5\Paint Shop Pro 6\Anims\Tube.gif
MD5: fac395242697347c2a24c17e4ec2aa59
msword2.doc
Path: \LOSTFILE\DIR5\Quick View Plus\SAMPLES\msword2.doc
MD5: 89138783d69b7d7d8fbb86224bd1342a
canvas_dark_blue.jpg
Path: \LOSTFILE\DIR5\Roxio\WinOnCD\Images\bck\canvas_dark_blue.jpg
MD5: 8dbc7cc7a3feb7b8fd e8edeeaa268c2a
Msexcel.xls
Path: \LOSTFILE\DIR5\Quick View Plus\SAMPLES\msexcel.xls
MD5: 4ad2cfd5c73029961fcbfb5b7330996d
Powerpt.ppt
Path: \LOSTFILE\DIR5\Quick View Plus\SAMPLES\powerpt.ppt
MD5: 4caf30766db0bc9eaf133e46049b41b6
history.txt
Path: \LOSTFILE\DIR0\dn\doc\english\history.txt
MD5: 6cff95aa45756531484c7f760f9fe1f3
AcroRd32.exe
Path: \LOSTFILE\DIR5\Adobe\Acrobat 5.0\Reader\AcroRd32.exe
MD5: 358f5f9aaa7b576bb4fe74ce6e61323c
4DOS.COM
Path: \LOSTFILE\DIR17_DOS.COM
MD5: 5ba55680533727e 153606947ae026286
Hard Disk MD5 after recovery: bd8b788c9a383d0d5a9ea5714714d19c

SN.ZIP analysis:

```
WinZip Archive Test :

No errors detected in compressed data of _N.ZIP.
Testing ...
testing: sn.dat                  OK
testing: sn.md5                   OK


MD5 contain of Zip File :

Name     Size       Attr   Modified          Type      MD5 Checksum
----     ----      -----   --------          ----      ------------
sn.dat   389 KB    -a----  11/04/2002 09:29  DAT File  0e954f43fd73f56e812a7285f32e41d3
sn.md5   37 bytes  -a----  11/04/2002 09:29  MD5 File  fe89813cd0bdd13971e5c385c63930f4
```

c. NTFS file system with ER Pro DOS version

Hard Disk MD5 before recovery: `cec00bea7f9ac1eb9ea02c25db63c334`
Sn.zip
Path: `\LOSTFILE\DIR218\SN.ZIP`
MD5: `5fea57f2a1546bc391c6b9cb1bbfc452`
CacheSentryWindowTips.gif
Path: `\LOSTFILE\DIR23\CACHES~2\DOCS\CACHES~4.GIF`
MD5: `5a599350b5a46e56b9a4105fa4dd34bb`
msword2.doc
Path: `\LOSTFILE\DIR82\MSWORD2.DOC`
MD5: `89138783d69b7d7d8fbb86224bd1342a`
Leaf.JPG
Path: `\LOSTFILE\DIR51\LEAF.JPG`
MD5: `a0565cb3cfc82ccb3509800f8ccab22b`
msexcel.xls
Path: `\LOSTFILE\DIR82\MSEXCEL.XLS`
MD5: `4ad2cfd5c73029961fcbfb5b7330996d`
powerpt.ppt
Path: `\LOSTFILE\DIR82\POWERPT.PPT`
MD5: `4caf30766db0bc9eaf133e46049b41b6`
TCMD32.TXT
Path: `\DOS\TCMD32.TXT`
MD5: `65bf77fc5199fe3711f43cae10248d05`
AcroRd32.exe
Path: `\LOSTFILE\DIR160\ACRORD32.EXE`
MD5: `ba9a26a090809162ee06d6688f0ed4cf`
4DOS.COM
Path: `\DOS\4DOS.COM`
MD5: `09fa40b1080e0b3a66f07adf5ba05917`
Hard Disk MD5 after recovery: `cec00bea7f9ac1eb9ea02c25db63c334`

LFN.BAT created:

```
REM This file should be run under Windo  ws to restore your long file names.
@echo off

ren   LOSTFILE\DIR23\CACHES~2\Docs\CACHES~4.GIF "CacheSentryWindowTips.gif
ren   LOSTFILE\DIR51\Leaf.JPG "Leaf.JPG
ren   LOSTFILE\DIR82\msexcel.xls "msexcel.xls
ren   LOSTFILE\DIR82\msword2.doc "msword2.doc
ren   LOSTFILE\DIR82\powerpt.ppt "powerpt.ppt
ren   LOSTFILE\DIR160\AcroRd32.exe "AcroRd32.exe
ren   LOSTFILE\DIR218\sn.zip "sn.zip
ren   DOS\4DOS.COM "4DOS.COM
ren   DOS\TCMD32.TXT "TCMD32.TXT
```

SN.ZIP analysis:

```
WinZip Archive Test :

No errors detected in  compressed data of  SN.ZIP.
Testing ...
testing: sn.dat                   OK
testing: sn.md5                   OK


MD5 contain of Zip File :

Name     Size      Attr   Modified          Type      MD5 Checksum
----     ----     -----   --------          ----      ------------
sn.dat   389 KB    -a----  11/04/20 02 09:29  DAT File  0e954f43fd73f56e812a7285f32e41d3
sn.md5   37 bytes  -a----  11/04/2002 09:29  MD5 File  fe89813cd0bdd13971e5c385c63930f4
```

d. NTFS file system with ER Pro Windows version

Hard Disk MD5 before recovery:	cec00bea7f9ac1eb9ea02c25db63c334
Sn.zip	
Path:	\LOSTFILE\DIR213\sn.zip
MD5:	5fea57f2a1546bc391c6b9cb1bbfc452
CacheSentryWindowTips.gif	
Path:	\LOSTFILE\DIR23\CacheSentry\Docs\CacheSentryWindowTips.gif
MD5:	5a599350b5a46e56b9a4105fa4dd34bb
msword2.doc	
Path:	\LOSTFILE\DIR82\msword2.doc
MD5:	89138783d69b7d7d8fbb86224bd1342a
Leaf.JPG	
Path:	\LOSTFILE\DIR51\Leaf.JPG
MD5:	a0565cb3cfc82ccb3509800f8ccab22b
Msexcel.xls	
Path:	\LOSTFILE\DIR82\msexcel.xls
MD5:	4ad2cfd5c73029961fcbfb5b7330996d
powerpt.ppt	
Path:	\LOSTFILE\DIR82\powerpt.ppt
MD5:	4caf30766db0bc9eaf133e46049b41b6
TCMD32.TXT	
Path:	\DOS\TCMD32.TXT
MD5:	65bf77fc5199fe3711f43cae10248d05
AcroRd32.exe	
Path:	\LOSTFILE\DIR314\AcroRd32.exe
MD5:	ba9a26a090809162ee06d6688f0ed4cf
4DOS.COM	
Path:	\DOS\4DOS.COM
MD5:	09fa40b1080e0b3a66f07adf5b a05917
Hard Disk MD5 after recovery:	cec00bea7f9ac1eb9ea02c25db63c334

SN.ZIP analysis:

```
WinZip Archive Test :

No errors detected in compressed data of   sn.zip.
Testing ...
testing: sn.dat                   OK
testing: sn.md5                   OK


MD5 contain of Zip File :

Name     Size      Attr   Modified           Type      MD5 Checksum
----     ----      -----  --------           ----      ------------
sn.dat   389 KB    -a---- 11/04/2002 09:29   DAT File  0e954f43fd73f56e812a7285f32e41d3
sn.md5   37 bytes  -a---- 11/04/2002 09:29   MD5 File  fe89813cd0bdd13971e5c385c63930f4
```

4. Repartitioned and Reformatted with Different File system

a. FAT32 file system with ER Pro DOS version

Hard Disk MD5 before recovery: 398f2febe28ca81ed4ce2f6817b4dae7
Sn.zip
Path: \LOSTFILE\DIR20_N.ZIP
MD5: 5fea57f2a1546bc391c6b9cb1bbfc452
Tube.gif
Path: \LOSTFILE\DIR5\PAINTS~1\ANIMS\TUBE.GIF
MD5: fac395242697347c2a24c17e4ec2aa59
msword2.doc
Path: \LOSTFILE\DIR5\QUICKV~1\SAMPLES\MSWORD2.DOC
MD5: 89138783d69b7d7d8fbb86224bd1342a
canvas_dark_blue.jpg
Path: \LOSTFILE\DIR5\ROXIO\WINONCD\IMAGES\BCK\CANVAS~3.JPG
MD5: 8dbc7cc7a3feb7b8fde8edeeaa268c2a
Msexcel.xls
Path: \LOSTFILE\DIR5\QUICKV~1\SAMPLES\MSEXCEL.XLS
MD5: 4ad2cfd5c73029961fcbfb5b7330996d
Powerpt.ppt
Path: \LOSTFILE\DIR5\QUICKV~1\SAMPLES\POWERPT.PPT
MD5: 4caf30766db0bc9eaf13 3e46049b41b6
history.txt
Path: \LOSTFILE\DIR0\DN\DOC\ENGLISH\HISTORY.TXT
MD5: 6cff95aa45756531484c7f760f9fe1f3
AcroRd32.exe
Path: \LOSTFILE\DIR5\ADOBE\ACROBA~2.0\READER\ACRORD32.EXE
MD5: 358f5f9aaa7b576bb4fe74ce6e61323c
4DOS.COM
Path: \LOSTFILE\DIR17_DOS.COM
MD5: 5ba55680533727e153606947ae026286
Hard Disk MD5 after recovery: 398f2febe28ca81ed4ce2f6817b4dae7

LFN.BAT Created:

```
REM This file should be run under Windows to restore your long file names.
@echo off

ren   LOSTFILE\DIR0\DN\DOC\ENGLISH\HISTORY.TXT "history.txt
ren   LOSTFILE\DIR5\PAINTS~1\ANIMS\TUBE.GIF "Tube.gif
ren   LOSTFILE\DIR5\QUICKV~1\SAMPLES\MSEXCEL.XLS "msexcel.xls
ren   LOSTFILE\DIR5\QUICKV~1\SAMPLES\MSWORD2.DOC "msword2.doc
ren   LOSTFILE\DIR5\QUICKV~1\SAMPLES\POWERPT.PPT "pow erpt.ppt
ren   LOSTFILE\DIR5\ROXIO\WINONCD\IMAGES\BCK\CANVAS~3.JPG
"canvas_dark_blue.jpg
ren   LOSTFILE\DIR5\ADOBE\ACROBA~2.0\READER\ACRORD32.EXE "AcroRd32.exe
ren   LOSTFILE\DIR17\_DOS.COM "_DOS.COM
ren   LOSTFILE\DIR20\_N.ZIP "_N.ZIP
```

SN.ZIP analysis:

```
WinZip Archive Test :

No errors detected in compressed data of _N.ZIP.
Testing ...
testing: sn.dat                   OK
testing: sn.md5                   OK


MD5 contain of Zip File :

Name     Size      Attr   Modified          Type      MD5 Checksum
----     ----     -----   --------          ----      ------------
sn.dat   389 KB   -a----  11/04/2002 09:29  DAT File  0e954f43fd73f56e812a7285f32e41d3
sn.md5   37 bytes -a----  11/04/2002 09:29  MD5 File  fe89813cd0bdd13971e5c385c63930f4
```

b. FAT32 file system with ER Pro Windows version

Hard Disk MD5 before recovery : 398f2febe28ca81ed4ce2f6817b4dae7
Sn.zip
Path: \LOSTFILE\DIR20_N.ZIP
MD5: 5fea57f2a1546bc391c6b9cb1bbfc452
Tube.gif
Path: \LOSTFILE\DIR5\Paint Shop Pro 6\Anims\Tube.gif
MD5: fac395242697347c2a24c17e4ec2aa59
msword2.doc
Path: \LOSTFILE\DIR5\Quick View Plus\SAMPLES\msword2.doc
MD5: 89138783d69b7d7d8fbb86224bd1342a
canvas_dark_blue.jpg
Path: \LOSTFILE\DIR5\Roxio\WinOnCD\Images\bck\canvas_dark_blue.jpg
MD5: 8dbc7cc7a3feb7b8fde8edeeaa268c2a
Msexcel.xls
Path: \LOSTFILE\DIR5\Quick View Plus\SAMPLES\msexcel.xls
MD5: 4ad2cfd5c73029961fcbfb5b7330996d
Powerpt.ppt
Path: \LOSTFILE\DIR5\Quick View Plus\SAMPLES\powerpt.ppt
MD5: 4caf30766db0bc9eaf133e46049b41b6
history.txt
Path: \LOSTFILE\DIR0\dn\doc\english\history.txt
MD5: 6cff95aa45756531484c7f760f 9fe1f3
AcroRd32.exe
Path: \LOSTFILE\DIR5\Adobe\Acrobat 5.0\Reader\AcroRd32.exe
MD5: 358f5f9aaa7b576bb4fe74ce6e61323c
4DOS.COM
Path: \LOSTFILE\DIR17_DOS.COM
MD5: 5ba55680533727e153606947ae026286
Hard Disk MD5 after recovery: 398f2febe28ca81ed4ce2f68 17b4dae7

SN.ZIP analysis:

```
WinZip Archive Test :

No errors detected in compressed data of _N.ZIP.
Testing ...
testing: sn.dat                  OK
testing: sn.md5                  OK


MD5 contain of Zip File :

Name     Size      Attr   Modified           Type      MD5 Checksum
----     ----     -----   --------           ----      ------------
sn.dat   389 KB   -a----  11/04/2002 09:29   DAT File  0e954f43fd73f56e812a7285f32e41d3
sn.md5   37 bytes -a----  11/04/2002 09:29   MD5 File  fe89813cd0bdd13971e5c385c63930f4
```

c. NTFS file system with ER Pro DOS version

Hard Disk MD5 before recovery: `914654a4ae8d5d3569f27325ccb75d22`
Sn.zip
Path: `\LOSTFILE\DIR218\SN.ZIP`
MD5: `5fea57f2a1546bc391c6b9cb1bbfc452`
CacheSentryWindowTips.gif
Path: `\LOSTFILE\DIR23\CACHES~2\DOCS\CACHES~4.GIF`
MD5: `5a599350b5a46e56b9a4105fa4dd34bb`
msword2.doc
Path: `\LOSTFILE\DIR82\MSWORD2.DOC`
MD5: `89138783d69b7d7d8fbb86224bd1342a`
Leaf.JPG
Path: `\LOSTFILE\DIR51\LEAF.JPG`
MD5: `a0565cb3cfc82ccb3509800f8ccab22b`
msexcel.xls
Path: `\LOSTFILE\DIR82\MSEXCEL.XLS`
MD5: `4ad2cfd5c73029961fcbfb5b7330996d`
powerpt.ppt
Path: `\LOSTFILE\DIR82\POWERPT.PPT`
MD5: `4caf30766db0bc9eaf133e46049b41b6`
TCMD32.TXT
Path: `\DOS\TCMD32.TXT`
MD5: `65bf77fc5199fe3711f43cae10248d05`
AcroRd32.exe
Path: `\LOSTFILE\DIR160\ACRORD32.EXE`
MD5: `ba9a26a090809162ee06d6688f0ed4cf`
4DOS.COM
Path: `\DOS\4DOS.COM`
MD5: `09fa40b1080e0b3a66f07adf5ba05917`
Hard Disk MD5 after recovery: `914654a4ae8d5d3569f27325ccb75d22`

LFN.BAT Created:

```
REM This file should be run under Windows to restore your long file names.
@echo off

ren   LOSTFILE\DIR23\CACHES~2\Docs\CACHES~4.GIF "CacheSentryWindowTips.gif
ren   LOSTFILE\DIR51\Leaf.JPG "Leaf.JPG
ren   LOSTFILE\DIR82\msexcel.xls "msexcel.xls
ren   LOSTFILE\DIR82\msword2.doc "msword2.doc
ren   LOSTFILE\DIR82\powerpt.ppt "powerpt.ppt
ren   LOSTFILE\DIR160\AcroRd32.exe "AcroRd32.exe
ren   LOSTFILE\DIR218\sn.zip "sn.zip
ren   DOS\4DOS.COM "4DOS.COM
ren   DOS\TCMD32.TXT "TCMD32.TXT
```

SN.ZIP analysis:

```
WinZip Archive Test :

No errors detected in compressed data of   SN.ZIP.
Testing ...
testing: sn.dat                     OK
testing: sn.md5                   OK


MD5 contain of Zip File :

Name     Size      Attr   Modified           Type      MD5 Checksum
----     ----     -----   --------           ----      ------------
sn.dat   389 KB    -a----  11/04/2002 09:29   DAT File  0e954f43fd73f56e812a7285f32e41d3
sn.md5   37 bytes  -a----  11/04/2002 09:29   MD5 File  fe89813cd0bdd13971e5c385c63930f4
```

d. NTFS file system with ER Pro Windows version

Hard Disk MD5 before recovery: 914654a4ae8d5d3569f27325ccb75d22
Sn.zip
Path: \LOSTFILE\DIR213\sn.zip
MD5: 5fea57f2a1546bc391c6b9cb1bbfc452
CacheSentryWindowTips.gif
Path: \LOSTFILE\DIR23\CacheSentry\Docs\CacheSentryWindowTips.gif
MD5: 5a599350b5a46e56b9a4105fa4dd34bb
msword2.doc
Path: \LOSTFILE\DIR82\msword2.doc
MD5: 89138783d69b7d7d8fbb86224bd1342a
Leaf.JPG
Path: \LOSTFILE\DIR51\Leaf.JPG
MD5: a0565cb3cfc82ccb3509800f8ccab22b
msexcel.xls
Path: \LOSTFILE\DIR82\msexcel.xls
MD5: 4ad2cfd5c73029961fcbfb5b7330996d
powerpt.ppt
Path: \LOSTFILE\DIR82\powerpt.ppt
MD5: 4caf30766db0bc9eaf133e46049b41b6
TCMD32.TXT
Path: \DOS\TCMD32.TXT
MD5: 65bf77fc5199fe3711f43cae10248d05
AcroRd32.exe
Path: \LOSTFILE\DIR159\AcroRd32.exe
MD5: ba9a26a090809162ee06d6688f0ed4cf
4DOS.COM
Path: \DOS\4DOS.COM
MD5: 09fa40b1080e0b3a66f07adf5ba05917
Hard Disk MD5 after recovery: f9ddcf054bdd25f7f85185b64afea735

SN.ZIP analysis:

```
WinZip Archive Test :

No errors detected in compressed data of   sn.zip.
Testing ...
testing: sn.dat                  OK
testing: sn.md5                  OK


MD5 contain of Zip File :

Name     Size       Attr   Modified           Type      MD5 Checksum
----     ----      -----   --------           ----      ------------
sn.dat   389 KB    -a----  11/04/2002 09:29   DAT File  0e954f43fd73f56e812a7285f32e41d3
sn.md5   37 bytes  -a----  11/04/2002 09:29   MD5 File  fe89813cd0bdd13971e5c385c63930f4
```

5. Recovery from Real Case – Permanently deleted file

a. NTFS file system with ER Pro DOS version

Hard Disk MD5 before recovery: `df4ef4731722ba722065a68528ace0a9`
`access_july2002.zip` `(size: 34.6MB)`
Path: `\DOCUME~1\LIMSR\MYDOCU~1\BACKUP\ACCESS~2.ZIP`
MD5: `2e1b9f2ee6e409ca818d7d81394c2a0c`
`access_sep2002.zip` `(size: 44 .7MB)`
Path: `\DOCUME~1\LIMSR\MYDOCU~1\BACKUP\ACCESS~1.ZIP`
MD5: `733d61834b28edb24f221555a9ec6d84`
Hard Disk MD5 after recovery: `df4ef4731722ba722065a68528ace0a9`

LFN.BAT created:

```
REM This file should be run under Windows to restore your long file names.
@echo off

ren   DOCUME~1\limsr\MYDOCU~1\backup\ACCESS~2.ZIP "access_july2002.zip
ren   DOCUME~1\limsr\MYDOCU~1\backup\ACCESS~1.ZIP "access_sep2002.zip
```

b. NTFS file system with ER Pro Windows version

Hard Disk MD5 before recovery: `df4ef4731722ba722065a6852 8ace0a9`
`access_july2002.zip` `(size: 34.6MB)`
Path: `\Documents and Settings\limsr\My Documents\backup\access_july2002.zip`
MD5: `2e1b9f2ee6e409ca818d7d81394c2a0c`
`access_sep2002.zip` `(size: 44.7MB)`
Path: `\Documents and Settings\limsr\My Documents\backup\access_sep2002.zip`
MD5: `733d61834b28edb24f221555a9ec6d84`
Hard Disk MD5 after recovery: `df4ef4731722ba722065a68528ace0a9`

Winzip[28] Archive Test result for both files:

```
No errors detected in compressed data of access_july2002.zip.
Testing ...
testing: access _july2002.log      OK
```

```
No errors detected in compressed data of access_sep2002.zip.
Testing ...
testing: access.18Sep -12PM        OK
```

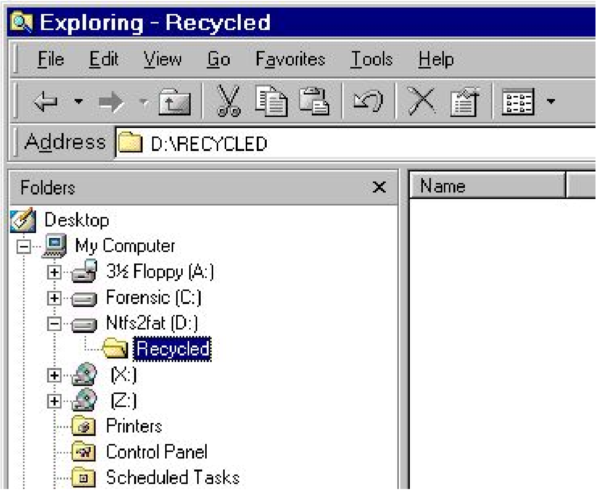
Analysis

After several tests have been done, we can conclude that ER Pro is a good data recovery tool. For ER Pro windows version (not required for ER Pro DOS version), if we can introduce hardware write block to the suspect's HDD, it can be a very useful forensic tool. Its ability in recovering data in most MS Windows filesystem, make it very useful for forensic analys t in their investigation.

From several tests that we have conducted, we verified that ER Pro can quickly and easily recovered data that have been permanently deleted, from HDD which partition table has been removed, reformatted with same file system and reformatted with different file system. But it required longer time for ER Pro to recover lost file from situation HDD reformatted with same file system and reformatted with different file system. In these situations, ER Pro needs to search and reconstruct the FAT for FAT32 file system and MFT for NTFS file system. After reconstruction of FAT or MFT, ER Pro put the reconstructed FAT or MFT under folder "`LOSTFILE`".

As mention in "Test Plan" of section "**Description of Procedures**", MD5 is an algorithm that is used to verify data integrity. By comparing the MD5 values of the recovered files with the original file, we can see that ER Pro recovered the lost file the same as the original. And by comparing the MD5 values of the HDD, before and after recovery, w e see that ER Pro doesn't modify the contents of the HDD during recovery process (forensically sound). Please refer to Appendix 12, 13, 14, 15 and 16 for MD5 comparisons.

In all eighteen (18) tests done, two (2) of them have different HDD MD5 values after the recovery process. After investigation, it seems that both recoveries, which MD5 values are different, were done on a reformatted FAT32 file system using ER Pro windows version. After further investigation we saw that a folder "Recycled" was automat ically created in it which does not exist during using ER Pro DOS version. Here we conclude that MS Windows 98se automatically created a "Recycled" folder when an empty formatted HDD was installed.

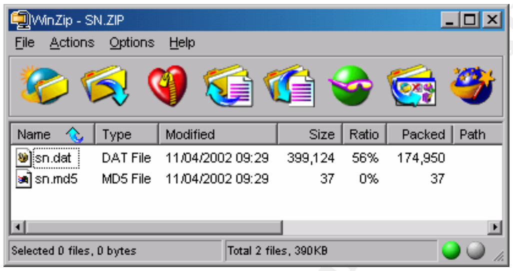
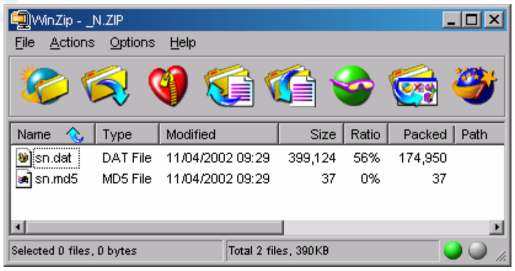
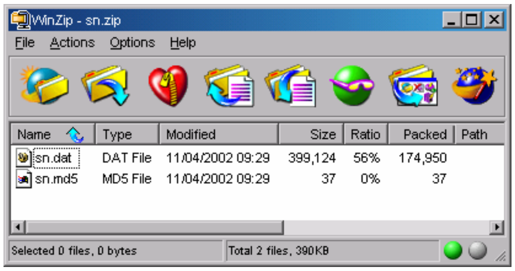


When recovering using ER Pro for DOS, LFN.BAT file wi ll be created. This file is created because ER Pro for DOS cannot save the recovered file s using long filename. This is due to the limitation in DOS [29]. LFN.BAT is a script automatically created to rename the entire recovered file in to their original long filename and this script should be executed in Windows environment.

Presentation

Evidences recovered by ER Pro with the support of MD5 hash values are presentable in the court of law. ER Pro has the ability to recover evidences without modifying the o riginal contain of recovered HDD. Several test with the help of MD5 hash values have confirmed that the original cont ents of the HDD recovered are not touched and/or modified.

Sample result for SN.ZIP:

Before	**After** (FAT32 – DOS)
Filename: SN.ZIP File size: 171KB MD5: 5fea57f2a1546bc391c6b9cb1bbfc452 Screenshot:  WinZip - SN.ZIP Name · Type · Modified · Size · Ratio · Packed · Path sn.dat · DAT File · 11/04/2002 09:29 · 399,124 · 56% · 174,950 sn.md5 · MD5 File · 11/04/2002 09:29 · 37 · 0% · 37 Selected 0 files, 0 bytes · Total 2 files, 390KB	Filename: _N.ZIP File size: 171KB MD5: 5fea57f2a1546bc391c6b9cb1bbfc452 Screenshot:  WinZip - _N.ZIP Name · Type · Modified · Size · Ratio · Packed · Path sn.dat · DAT File · 11/04/2002 09:29 · 399,124 · 56% · 174,950 sn.md5 · MD5 File · 11/04/2002 09:29 · 37 · 0% · 37 Selected 0 files, 0 bytes · Total 2 files, 390KB
	After (NTFS – WIN)
	Filename: sn.zip File size: 171KB MD5: 5fea57f2a1546bc391c6b9cb1bbfc452 Screenshot:  WinZip - sn.zip Name · Type · Modified · Size · Ratio · Packed · Path sn.dat · DAT File · 11/04/2002 09:29 · 399,124 · 56% · 174,950 sn.md5 · MD5 File · 11/04/2002 09:29 · 37 · 0% · 37 Selected 0 files, 0 bytes · Total 2 files, 390KB

Conclusion

Extensive test have been done to prove that the lost files recovered using ER Pro is reliable, forensically sound and suitable for presentation to the court of law. The program performed as what we expected and is very suitable if used in any forensic investigation.

With the existence of ER Pro DOS version, we can directly recover files from the suspect system without removing his/her HDD but additional storage is required to be attached i.e. extra HDD, Zip drive, or floppy di sk for destination location to copy recovered files .

Summary

1. Permanently deleted files are able to be recovered.
2. Lost files from HDD with partition table removed are also able to be recovered.
3. Lost files from HDD that have been reformatted either with s ame file system or different file system are also able to be recovered but longer time is required and the root files and/or folders name is unrecoverable.
4. ER Pro doesn't touched/modified the recovered HDD. This is confirmed by calculating and comparing t he MD5 hash values before and after recovery process.
5. File recovered with ER Pro is exactly the same as the original. This is confirmed by calculating and comparing the MD5 hash values of the original files and the recovered files.
6. ER Pro DOS version unab le to recreate long filenames but it will create a script call '`lfn.bat`' which can be executed in MS Windows MS -DOS prompt to rename them to the correct long filename.

Part 3: Legal Issues of Incident Handling

For my final part of the assignment pape r, we were asked to act as an Internet Service Provider system administrator and try to response to the question given, which relate to legal issues of incident handling.

Synopsis

You are the system administrator for an Internet Service Provider that provides Internet access to paying customers. You receive a telephone call from a law enforcement officer who informs you that an account on your system was used to hack into a government computer. He asks you to verify the activity by reviewing your logs and determine if your logs reflect whether or not the activity was initiated there or from another upstream provider. You review your logs and can only determine a valid user account logged in via a dialup account during the period of the suspicious activ ity.

NOTE: For the purposes of this scenario, assume you validated the identity of the law enforcement officer and this is not social engineering.

Questions

1. <u>What, if any, information can you provide to the law enforcement officer over the phone dur ing the initial contact?</u>

   As a system administrator of an Internet Service Provider company, we would have direct access to dial -up Internet account database. In this phone conversation, after we have validated the identity of the law enforcement officer , we would ask from the law enforcement officer for the hacker origin IP address and the account used during the hacking occurred.

   The IP address given is then compared to our range of assigned IP address to confirm that the hacker 's IP address belongs t o us. Then we scan and/or search through Internet account database to confirm that the internet account used is a valid internet account provided by us. We can only confirm to the law enforcement officer that the hacker's account and IP address belong to us.

   This information can be given in the initial contact to the law enforcement officer, as they are not confidential. Others information, evidence and/or detail of our subscribers are confidential and cannot be given during the initial contact, even th ough the initial contact are done by the law enforcement officer themselves.

2. What must the law enforcement officer do to ensure you to preserve this evidence if there is a delay in obtaining any required legal authority?

After the initial call, the law enforcement officer may ask us not to deleted logs information related to the IP address and account given. It is also our regulation to keep/backup logs information frequently. But if it is required to preserve/copy/image these evidences, the law enforcement officer have to provide to us a formal letter or with a court summons stating the offence done under this investigation and the report number lodged by the law enforcement officer. In the letter also, the law enforcement officer have to mention under which section act does the offence has been done.

In this case, hacking by unknown user into a system usually fall under Section 3 of Computer Crimes Bill 1997 [14] title “Unauthorised access to computer material” which state:

```
Computer Crimes Bill 1997
Section 3: Unauthorised access to computer material

1. a person shall be guilty of an offence if:

   a. he causes a computer to perform any function with intent to
      secure access to any program or data held in any computer;
   b. the access he intends to secure is unauthorised; and
   c. he knows at the time when he causes the computer to perform
      the function that that is the case.

2. the intent a person has to have to commit an offence under this
   section need not be directed at:

   a. any particular program or data;
   b. a program or data of any particular kind; or
   c. a program or data held in any particular computer.

3. a person guilty of an offence under this section shall on
   conviction be liable to a fine not exceeding fifty thousand
   ringgit or to imprisonment for a term not exceeding five years
   or to both.
```

What these mean is that an unauthorized user accessing a computer system with intention to access, upload, download, modify, delete, execute, etc. any malicious software (malware), programs, information, etc in the unauthorized accessed computer system, is an offence.

3. What legal authority, if any, does the law enforcement officer need to provide to you in order for you to send him your logs?

Log information’s are confidential evidence. From the logs information, we can trace the origin of the IP address/internet account connection either by dial-up or from another Internet Service Provider connection. If the connection if from dial -up account, then we can trace the origin telephone number which can then be trace to their physical location address.

So, for the law enforcement officer to get these confidential evidences from us, they have to make an official written request /order or with a court summons where the information need to be mentioned in the letter as described in part 2 of this section above .

These procedures are stated under Section 51 (1) Criminal Procedure Code[30], which stated that:

> **Criminal Procedure Code**
> **Section 51 (1):**
>
> "Whenever any Court or police officer making a police investigation considers that the production of any property or document is necessary or desirable for the purpose of any investigation, inquiry, trial or the proceeding under this Code by or before such /court or officer such Court may issue a summons or such officer a written order to the person in which possession or power such property or document is believed to be requiring him to attend and produce it or to produce it at the time and place stated in the summons or order."

4. What other "investigative" activity are you permitted to conduct at this time?

   Without official written request /order by the law enforcement officer, we as system administrator of an Internet Service Provider company cannot do any further investigation. We cannot monitor and even intercept any network traffic, Communication and Multimedia Act 1998 [31] Section 252:

> **Communication and Multimedia Act 1998**
> **Section 252: Power to intercept communications**
>
> 1. Notwithstanding the provisions of any other written law, the Public Prosecutor, if he considers that any communications is likely to contain any information which is relevant for the purpose of any investigation into an offence under this Act or its subsidiary legislation, may, on the application of an authorised officer or a police officer of or above the rank of Superintendent, authorise the officer to intercept or to listen to any communication transmitted or received by any communications.
>
> 2. When any person is charged with an offence under this Act or its subsidiary legislation, any information obtained by an authorised officer or a police officer under subsection (1), whether before or after the person is charged, shall be admissible at his trial in evidence.
>
> 3. An authorisation by the Public Prosecutor under subsection (1) may be given either orally or in writing; but if an oral authorisation is given, the Public Prosecutor shall, as soon as practicable, reduce the authorisation into writing.
>
> 4. A certificate by the Public Prosecutor stating that the action taken by an authorised officer or a police officer under subsection (1) had been authorised by him under that subsection shall be conclusive evidence that it had been so authorised, and

> the certificate shall be admissible in evidence without proof of his signature there.
>
> 5. No person shall be under any duty, obligation or liability, or be in any manner compelled, to disclose in any proceedings the procedure, method, manner or means, or any matter related to it, of anything done under subsection (1).

When the law enforcement officer have submitted to us an official written request/order and a court summons /order, then we are permitted to do further investigation i.e. monitoring, tapping, tracing etc. and preserved all finding. The findings are confidential evidence that only can be given to the requested law enforcement officer and cannot be disclosed to others.

This is stated under Section 234 in Communication and Multimedia Act 1998[25] which is:

> **Communication and Multimedia Act 1998**
> **Section 234: Interception and disclosure of communications prohibited:**
>
> 1. A person who, without lawful authority under this Act or any other written law -
>
>   a. intercepts, attempts to intercept, or procures any other person to intercept or attempt to intercept, any communications;
>
>   b. discloses, or attempts to disclose, to any other person the contents of any communications, knowing or having reason to believe that the information was obtained through the interception of any communications in contravention of this section; or
>
>   c. uses, or attempts to use, the contents of any communications, knowing or having reason to believe that the information was obtained through the interception of any communications in contravention of this section,
>   commits an offence.

5. <u>How would your actions change if your logs disclosed a hacker gained unauthorized access to your system at some point, created an account for him/her to use, and used THAT account to hack into the government system?</u>

   During the investigation, if we manage to identify that the account used by the hacker is not a valid internet account provided by us, we still do further investigation as requested by the law enforcement officer. We still need to find the origin of hacker IP address. With this information then we can identify whether the hacker connection is from a dial-up access or from another Internet Service Provider account.

With this information then we can lodge a report to the law agencies as with this report the investigation law enforcement officer can then continue their investigation to trace out the hacker. The report we lodged now as a victim of compromised system that was used to hack to another system.

Now with the help of computer forensics analyst, we need to determine on how does the hacker gained access to our system and create an invalid account that was use for hacking purpose. All computer forensic procedure i.e. media images, chain of custody, etc needs to be considered as all the findings can be used as evidence in the court of law.

The document which were produced by the computer during the investigation were admissible in court as evidence provided that it full fill the requirement of section 90A in Evidence (Amendment) Act 1993 [32]

Evidence (Amendment) Act 1993
Section 90A: Admissibility of documents produced by computer, and of statements contained therein

1. In any criminal or civil proceeding a document produced by a computer, or a statement contained in such document, shall be admissible as evidence of any fact stated therein if the document was produced by the computer in the course of its ordinary use, whether or not the person tendering the same is the maker of such document or statement.

5. A document shall be deemed to have been produced by a computer whether it was produced by it directly or by means of any appropriate equipment, and whether or not there was any direct or indirect human intervention

Appendix 1: "*strings -a*" output (2 column - Knoppix)

```
root@ttyp0[Exam1]#  strings -a atd
/lib/ld-linux.so.1
libc.so.5
longjmp
strcpy
ioctl
popen
shmctl
geteuid
_DYNAMIC
getprotobynumber
errno
__strtol_internal
usleep
semget
getpid
fgets
shmat
_IO_stderr_
perror
getuid
semctl
optarg
socket
__environ
bzero
_init
alarm
__libc_init
environ
fprintf
kill
inet_addr
chdir
shmdt
setsockopt
__fpu_control
shmget
wait
umask
signal
read
strncmp
sendto
bcopy
fork
strdup
getopt
inet_ntoa
getppid
time
gethostbyname
_fini
sprintf
difftime
atexit
_GLOBAL_OFFSET_TABLE_
semop
exit
__setfpucw
open
setsid
close
_errno
_etext
_edata
__bss_start
_end
WVS1
f91u
WVS1
pWVS
vuWj
<it          <ut
vudj
<it          <ut
3jTh
j7Wh
Wj7j
Vj7S
j8WS
Vj7S
j8WS
Vj7S
tVj8WS
Vj7S
t'j8WS
jTh8
Wj7j
j7hU
j@hL
@j@hL
jTh8
j            h@
}^j7
}1j7
<WVS
tDWS
lokid: Client database full
DEBUG: stat_client nono
lokid version:
             %s
remote interface:        %s
active transport:        %s
active cryptography:     %s
server uptime:
             %.02f minutes
client ID:               %d
packets written:         %ld
bytes written:
             %ld
requests:                %d
N@[fatal] cannot catch SIGALRM
lokid: inactive client <%d> expired
from list [%d]
@[fatal] shared mem segment request
error
[fatal] semaphore allocation error
[fatal] could not lock memory
[fatal] could not unlock  memory
[fatal] shared mem segment detach
error
[fatal] cannot destroy shmid
[fatal] cannot destroy semaphore
[fatal] name lookup failed
[fatal] cannot catch SIGALRM
[fatal] cannot catch SIGCHLD
[fatal] Cannot go daemon
[fatal] Cannot create session
```

```
/dev/tt y
[fatal] cannot detach from
controlling terminal
/tmp
[fatal] invalid user identification
value
v:p:
Unknown transport
lokid -p (i|u) [ -v (0|1) ]
[fatal] socket allocation error
[fatal] cannot catch SIGUSR1
Cannot set IP_HDRINCL socket option
[fatal] can not register with
atexit(2)
LOKI2       route [(c) 1997 guild
corporation worldwide]
[fatal] cannot catch SIGALRM
[fatal] cannot catch SIGCHLD
[SUPER fatal] control should NEVER
fall here
[fatal] forking error
lokid: server is currently at
capacity.  Try again l ater
lokid: Cannot add key
lokid: popen
[non fatal] truncated write
/quit all
lokid: client <%d> requested an all
kill
             sending L_QUIT: <%d> %s
lokid: clean exit (killed at client
request)
[fatal] could not signal process
group
/quit
lokid: cannot locate c lient entry
in database
lokid: client <%d> freed from list
[%d]
/stat
/swapt
[fatal] could not signal parent
lokid: unsupported or unknown
command string
```

```
lokid: client <%d> requested a
protocol swap
             sending protocol
update: <%d> %s [%d]
lokid: transport p rotocol changed
to %s
GCC: (GNU) 2.7.2.1
GCC: (GNU) 2.7.2.1
GCC: (GNU) 2.7.2.1
GCC: (GNU) 2.7.2.1
GCC: (GNU) 2.7.2.1
GCC: (GNU) 2.7.2.1
GCC: (GNU) 2.7.2.1
GCC: (GNU) 2.7.2.1
01.01
01.01
01.01
01.01
01.01
01.01
01.01
01.01
.symtab
.strtab
.shstrtab
.interp
.hash
.dynsym
.dynstr
.rel.bss
.rel.plt
.init
.plt
.text
.fini
.rodata
.data
.ctors
.dtors
.got
.dynamic
.bss
.comment
.note
```

Appendix 2: “*zipinfo -v*” output (Knoppix)

```
root@ttyp0[Exam1]#  zipinfo -v ../binary_v1.2.zip
Archive:  ../binary_v1.2.zip   7309 b  ytes   2 files

End-of-central-directory record:
-------------------------------

  Actual offset of end-of-central-dir record:        7287 (00001C77h)
  Expected offset of end-of-central-dir record:      7287 (00001C77h)
  (based on the length of the central directory and its expected offset)

  This zipfile constitutes the sole disk of a single-part archive; its
  central directory contains 2 entries.  The central directory is 102
  (00000066h) bytes long, and its (expected) offset in bytes from the
  beginning of the zipfile is 7185 (00001C11h).

  There is no zipfile comment.

Central directory entry #1:
---------------------------

  atd.md5

  offset of local header from start of archive:     0 (00000000h) bytes
  file system or operating system of origin:        MS-DOS, OS/2 or NT FAT
  version of encoding software:                     2.0
  minimum file system compatibility required:       MS-DOS, OS/2 or NT FAT
  minimum software version required to extract:     2.0
  compression method:                               deflated
  compression sub-type (deflation):                 normal
  file security status:                             not encrypted
  extended local header:                            no
  file last modified on (DOS date/time):            2002 Aug 22 14:58:08
  32-bit CRC value (hex):                           e5376cb4
  compressed size:                                  38 bytes
  uncompressed size:                                39 bytes
  length of filename:                               7 characters
  length of extra field:                            0 bytes
  length of file comment:                           0 characters
  disk number on which file begins:                 disk 1
  apparent file type:                               text
  non-MSDOS external file attributes:               81B600 hex
  MS-DOS file attributes (20 hex):                  arc

  There is no file comment.

Central directory entry #2:
---------------------------

  atd

  offset of local header from start of archive:     75 (0000004Bh) bytes
  file system or operating system of origin:        MS-DOS, OS/2 or NT FAT
  version of encoding software:                     2.0
  minimum file system compatibility required:       MS-DOS, OS/2 or NT FAT
  minimum software version required to extract:     2.0
  compression method:                               deflated
  compression sub-type (deflation):                 normal
  file security status:                             not encrypted
  extended local header:                            no
  file last modified on (DOS date/time):            2002 Aug 22 14:57:54
  32-bit CRC value (hex):                           d0ee3072
  compressed size:                                  7077 bytes
  uncompressed size:                                15348 bytes
  length of filename:                               3 characters
  length of extra field:                            0 bytes
  length of file comment:                           0 characters
  disk number on which file begins:                 disk 1
  apparent file type:                               binary
  non-MSDOS external file attributes:               81B600 hex
  MS-DOS file attributes (20 hex):                  arc

  There is no file comment.
```

Appendix 3: “*debugfs*” output (Knoppix)

```
root@ttyp0[Exam1]#  ls -i atd*
   1283 atd     1282 atd.md5     1284 atd.strings
root@ttyp0[Exam1]#  debugfs -R "stat <1283>"
/mnt/hda1/alltemp/Practical/Exam1.dd
debugfs 1.27 (8 -Mar-2002)
Inode: 1283   Type: regular    Mode:  0444   Flags: 0x0      Generation: 33279
User:     0   Group:     0   Size: 15348
File ACL: 0    Directory ACL: 0
Links: 1   Blockcount: 32
Fragment:  Address: 0    Number: 0    Size: 0
ctime: 0x3e21c3d5  -- Sun Jan 12 20:36:53 2003
atime: 0x3d64dfd2  -- Thu Aug 22 14:57:54 2002
mtime: 0x3d64dfd2  -- Thu Aug 22 14:57:54 2002
BLOCKS:
(0-11):8359-8370, (IND):8371, (12 -14):8372-8374
TOTAL: 16

root@ttyp0[Exam1]#  debugfs -R "stat <1282>"
/mnt/hda1/alltemp/Practical/Exam1.dd
debugfs 1.27 (8 -Mar-2002)
Inode: 1282   Type: regular    Mode:    0666   Flags: 0x0   Generation: 33276
User:     0   Group:     0   Size: 39
File ACL: 0    Directory ACL: 0
Links: 1   Blockcount: 2
Fragment:  Address: 0    Number: 0    Size: 0
ctime: 0x3e21c3ac  -- Sun Jan 12 20:36:12 2003
atime: 0x3d64dfe0  -- Thu Aug  22 14:58:08 2002
mtime: 0x3d64dfe0  -- Thu Aug 22 14:58:08 2002
BLOCKS:
(0):8358
TOTAL: 1
```

Appendix 4: “strace” output (RedHat ver 5.1)

```
[root@ftp Exam1]#  strace ./atd
execve("./atd", ["./atd"], [/* 17 vars */]) = 0
mmap(0, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x40006000
mprotect(0x40000000, 19984, PROT_READ|PROT_WRITE|PROT_EXEC) = 0
mprotect(0x8048000, 13604, PROT_READ|PROT_WRITE|PROT_EXEC) = 0
stat("/etc/ld.so.cache", {st_mode=0, st_size=0, ...}) = 0
open("/etc/ld.so.cache", O_RDONLY)      = 3
mmap(0, 18169, PROT_READ, MAP_SHARED, 3, 0) = 0x40007000
close(3)                                = 0
stat("/etc/ld.so.preload", 0xbffffd7c)  = -1 ENOENT (No such file or directory)
open("/usr/i486-linux-libc5/lib/libc.so.5", O_RDONLY) = 3
read(3, "\177ELF\1\1\1\0\0\0\0\0\0\0\0\0\3"..., 4096) = 4096
mmap(0, 823296, PROT_NONE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x4000c000
mmap(0x4000c000, 591973, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_FIXED, 3, 0) =
0x4000c000
mmap(0x4009d000, 23672, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED, 3, 0x90000) =
0x4009d000
mmap(0x400a3000, 201820, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -
1, 0) = 0x400a3000
close(3)                                = 0
mprotect(0x4000c000, 591973, PROT_READ|PROT_WRITE|PROT_EXEC) = 0
munmap(0x40007000, 18169)               = 0
mprotect(0x8048000, 13604, PROT_READ|PROT_EXEC) = 0
mprotect(0x4000c000, 591973, PROT_READ|PROT_EXEC) = 0
mprotect(0x40000000, 19984, PROT_READ|PROT_EXEC) = 0
personality(0 /* PER_??? */)            = 0
geteuid()                               = 0
getuid()                                = 0
getgid()                                = 0
getegid()                               = 0
geteuid()                               = 0
getuid()                                = 0
brk(0x804c818)                          = 0x804c818
brk(0x804d000)                          = 0x804d000
open("/usr/share/locale/C/LC_MESSAGES", O_RDONLY) = -1 ENOENT (No such file or
directory)
stat("/etc/locale/C/libc.cat", 0xbffff8a0) = -1 ENOENT (No such file or directory)
stat("/usr/lib/locale/C/libc.cat", 0xbffff8a0) = -1 ENOENT (No such file or directory)
stat("/usr/lib/locale/libc/C", 0xbffff8a0) = -1 ENOENT (No such file or directory)
stat("/usr/share/locale/C/libc.cat", 0xbffff8a0) = -1 ENOENT (No such file or
directory)
stat("/usr/local/share/locale/C/libc.cat", 0xbffff8a0) = -1 ENOENT (No such file or
directory)
socket(PF_INET, SOCK_RAW, IPPROTO_ICMP) = 3
sigaction(SIGUSR1, {0x804a6b0, [], 0}, {SIG_DFL}) = 0
socket(PF_INET, SOCK_RAW, IPPROTO_RAW)  = 4
setsockopt(4, IPPROTO_IP3, [1], 4)      = 0
getpid()                                = 454
getpid()                                = 454
shmget(696, 240, IPC_CREAT|0)           = 1
semget(878, 1, IPC_CREAT|0x180|0600)    = 0
shmat(1, 0, 0)                          = 0x40007000
write(2, "\nLOKI2\troute [(c) 1997 guild c"..., 52
LOKI2        route [(c) 1997 guild corporation worldwide]
) = 52
time([1043911073])                      = 1043911073
close(0)                                = 0
sigaction(SIGTTOU, {SIG_IGN}, {SIG_DFL}) = 0
sigaction(SIGTTIN, {SIG_IGN}, {SIG_DFL}) = 0
sigaction(SIGTSTP, {SIG_IGN}, {SIG_DFL}) = 0
fork()                                  = 455
close(4)                                = 0
close(3)                                = 0
semop(0, 0x2, 0, 0xbffffd18)            = 0
shmdt(0x40007000)                       = 0
semop(0, 0x1, 0, 0xbffffd18)            = 0
_exit(0)                                = ?
```

Appendix 5: “*ps -ax*” output (RedHat ver 5.1)

```
[root@ftp Exam1]#  ps -ax
  PID TTY STAT TIME COMMAND
    1  ?  S    0:03 init [3]
    2  ?  SW   0:00 (kflushd)
    3  ?  SW<  0:00 (kswapd)
   52  ?  S    0:00 /sbin/kerneld
  203  ?  S    0:00 /usr/bin/httpd
  223  ?  S    0:00 syslogd
  232  ?  S    0:00 klogd
  254  ?  S     0:00 crond
  265  ?  S    0:00 inetd
  282   1 S    0:00 /bin/login  -- root
  283   2 S    0:00 /bin/login  -- root
  284   3 S    0:00 /bin/login  -- root
  285   4 S    0:00 /sbin/mingetty tty4
  286   5 S    0:00 /sbin/mingetty tty5
  287   6 S     0:00 /sbin/mingetty tty6
  289  ?  S    0:00 update (bdflush)
  290   1 S    0:00  -bash
  487   2 S    0:00  -bash
  503   3 S    0:00  -bash
  539  ?  S    0:00 ./atd
  597   2 R    0:00 ps ax
  243  ?  S    0:00 /usr/sbin/atd
  210  ?  S    0:00  /usr/bin/httpd
  211  ?  S    0:00 /usr/bin/httpd
  212  ?  S    0:00 /usr/bin/httpd
  213  ?  S    0:00 /usr/bin/httpd
  214  ?  S    0:00 /usr/bin/httpd
  215  ?  S    0:00 /usr/bin/httpd
  216  ?  S    0:00 /usr/bin/httpd
  217  ?  S    0:00 /usr /bin/httpd
  218  ?  S    0:00 /usr/bin/httpd
  219  ?  S    0:00 /usr/bin/httpd
```

Appendix 6: “*make linux*” output (Knoppix)

```
root@ttyp0[L2]#  make linux
make[1]: Entering directory `/mnt/Practical/Exam1/src1/L2'
gcc -Wall -O6 -finline-functions -funroll-all-loops -DLINUX -DWEAK_CRYPTO -DPOPEN -
DSEND_PAUSE=100 -Dx86_FAST_CHECK     -c surplus.c -o surplus.o
In file included from /usr/include/linux/signal.h:4,
                 from loki.h:38,
                 from surplus.c:10:
/usr/include/asm/signal.h:26: warning: `NSIG' redefined
/usr/include/signal.h:179: warning: this is the location of the previous definition
/usr/include/asm/signal.h:70: warning: `SIGRTMIN' redefined
/usr/include/bits/signum.h:72: warning: this is the location of the previous
definition
/usr/include/asm/signal.h:71: warning: `SIGRTMAX' redefined
/usr/include/bits/signum.h:73: warning: this is the location of the previous
definition
/usr/include/asm/signal.h:87: warning: `SA_NOCLDSTOP' redefined
/usr/include/bits/sigaction.h:54: warning: this is the location of the previous
definition
/usr/include/asm/signal.h:88: warning: `SA_NOCLDWAIT' redefined
/usr/include/bits/sigaction.h:55: warning: this is the location of the previous
definition
/usr/include/asm/signal.h:89: warning: `SA_SIGINFO' redefined
/usr/include/bits/sigaction.h:57: warning: this is the location of the previous
definition
/usr/include/asm/signal.h:104: warning: `SS_ONSTACK' redefined
/usr/include/bits/sigstack.h:37: warning: this is the location of the previous
definition
/usr/include/asm/signal.h:105: warning: `SS_DISABLE' redefined
/usr/include/bits/sigstack.h:39: warning: this is the location of the previous
definition
/usr/include/asm/signal.h:131: warning: `SIG_DFL' redefined
/usr/include/bits/signum.h:24: warning: this is the location of the previous
definition
/usr/include/asm/signal.h:132: warning: `SIG_IGN' redefined
/usr/include/bits/signum.h:25: warning: this is the location of the previous
definition
/usr/include/asm/signal.h:133: warning: `SIG_ERR' redefined
/usr/include/bits/signum.h:23: warning: this is the location of the previous
definition
/usr/include/asm/signal.h:166: warning: `sa_handler' redefined
/usr/include/bits/sigaction.h:37: warning: this is the location of the previous
definition
/usr/include/asm/signal.h:167: warning: `sa_sigaction' redefined
/usr/include/bits/sigaction.h:38: warning: this is the location of the previous
definition
In file included from /usr/include/linux/signal.h:5,
                 from loki.h:38,
                 from surplus.c:10:
/usr/include/asm/siginfo.h:68: warning: `si_pid' redefined
/usr/include/bits/siginfo.h:111: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:69: warning: `si_uid' redefined
/usr/include/bits/siginfo.h:112: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:70: warning: `si_status' redefined
/usr/include/bits/siginfo.h:115: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:71: warning: `si_utime' redefined
/usr/include/bits/siginfo.h:116: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:72: warning: `si_stime' redefined
/usr/include/bits/siginfo.h:117: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:73: warning: `si_value' redefined
/usr/include/bits/siginfo.h:118: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:74: warning: `si_int' redefined
/usr/include/bits/siginfo.h:119: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:75: warning: `si_ptr' redefined
/usr/include/bits/siginfo.h:120: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:76: warning: `si_addr' redefined
```

```
/usr/include/bits/siginfo.h:121: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:77: warning: `si_band' redefined
/usr/include/bits/siginfo.h:122: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:78: warning: `si_fd' redefined
/usr/include/bits/siginfo.h:123: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:103: warning: `SI_USER' redefined
/usr/include/bits/siginfo.h:143: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:104: warning: `SI_KERNEL' redefined
/usr/include/bits/siginfo.h:145: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:105: warning: `SI_QUEUE' redefined
/usr/include/bits/siginfo.h:141: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:106: warning: `SI_TIMER' redefined
/usr/include/bits/siginfo.h:139: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:107: warning: `SI_MESGQ' redefined
/usr/include/bits/siginfo.h:137: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:108: warning: `SI_ASYNCIO' redefined
/usr/include/bits/siginfo.h:135: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:109: warning: `SI_SIGIO' redefined
/usr/include/bits/siginfo.h:133: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:117: warning: `ILL_ILLOPC' redefined
/usr/include/bits/siginfo.h:153: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:118: warning: `ILL_ILLOPN' redefined
/usr/include/bits/siginfo.h:155: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:119: warning: `ILL_ILLADR' redefined
/usr/include/bits/siginfo.h:157: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:120: warning: `ILL_ILLTRP' redefined
/usr/include/bits/siginfo.h:159: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:121: warning: `ILL_PRVOPC' redefined
/usr/include/bits/siginfo.h:161: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:122: warning: `ILL_PRVREG' redefined
/usr/include/bits/siginfo.h:163: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:123: warning: `ILL_COPROC' redefined
/usr/include/bits/siginfo.h:165: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:124: warning: `ILL_BADSTK' redefined
/usr/include/bits/siginfo.h:167: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:130: warning: `FPE_INTDIV' redefined
/usr/include/bits/siginfo.h:174: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:131: warning: `FPE_INTOVF' redefined
/usr/include/bits/siginfo.h:176: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:132: warning: `FPE_FLTDIV' redefined
/usr/include/bits/siginfo.h:178: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:133: warning: `FPE_FLTOVF' redefined
/usr/include/bits/siginfo.h:180: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:134: warning: `FPE_FLTUND' redefined
/usr/include/bits/siginfo.h:182: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:135: warning: `FPE_FLTRES' redefined
/usr/include/bits/siginfo.h:184: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:136: warning: `FPE_FLTINV' redefined
/usr/include/bits/siginfo.h:186: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:137: warning: `FPE_FLTSUB' redefined
/usr/include/bits/siginfo.h:188: warning: this is the location of the previous
definition
```

```
/usr/include/asm/siginfo.h:143: warning: `SEGV_MAPERR' redefined
/usr/include/bits/siginfo.h:195: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:144: warning: `SEGV_ACCERR' redefined
/usr/include/bits/siginfo.h:197: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:150: warning: `BUS_ADRALN' redefined
/usr/include/bits/siginfo.h:204: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:151: warning: `BUS_ADRERR' redefined
/usr/include/bits/siginfo.h:206: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:152: warning: `BUS_OBJERR' redefined
/usr/include/bits/siginfo.h:208: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:158: warning: `TRAP_BRKPT' redefined
/usr/include/bits/siginfo.h:215: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:159: warning: `TRAP_TRACE' redefined
/usr/include/bits/siginfo.h:217: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:165: warning: `CLD_EXITED' redefined
/usr/include/bits/siginfo.h:224: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:166: warning: `CLD_KILLED' redefined
/usr/include/bits/siginfo.h:226: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:167: warning: `CLD_DUMPED' redefined
/usr/include/bits/siginfo.h:228: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:168: warning: `CLD_TRAPPED' redefined
/usr/include/bits/siginfo.h:230: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:169: warning: `CLD_STOPPED' redefined
/usr/include/bits/siginfo.h:232: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:170: warning: `CLD_CONTINUED' redefined
/usr/include/bits/siginfo.h:234: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:176: warning: `POLL_IN' redefined
/usr/include/bits/siginfo.h:241: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:177: warning: `POLL_OUT' redefined
/usr/include/bits/siginfo.h:243: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:178: warning: `POLL_MSG' redefined
/usr/include/bits/siginfo.h:245: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:179: warning: `POLL_ERR' redefined
/usr/include/bits/siginfo.h:247: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:180: warning: `POLL_PRI' redefined
/usr/include/bits/siginfo.h:249: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:181: warning: `POLL_HUP' redefined
/usr/include/bits/siginfo.h:251: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:192: warning: `SIGEV_SIGNAL' redefined
/usr/include/bits/siginfo.h:299: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:193: warning: `SIGEV_NONE' redefined
/usr/include/bits/siginfo.h:301: warning: this is the location of the previous
definition
/usr/include/asm/siginfo.h:194: warning: `SIGEV_THREAD' redefined
/usr/include/bits/siginfo.h:303: warning: this is the location of the previous
definition
In file included from loki.h:36,
                 from surplus.c:10:
/usr/include/linux/icmp.h:67: parse error before `__u8'
/usr/include/linux/icmp.h:67: warning: no semicolon at end of struct or union
/usr/include/linux/icmp.h:68: warning: data definition has no type or storage class
/usr/include/linux/icmp.h:69: parse error before `checksum'
/usr/include/linux/icmp.h:69: warning: data definition has no type or storage class
/usr/include/linux/icmp.h:72: parse error before `__u16'
/usr/include/linux/icmp.h:72: warning: no semicolon at end of struct or union
/usr/include/linux/icmp.h:72: warning: no semicolon at end of struct or union
/usr/include/linux/icmp.h:73: warning: data definition has no type or storage class
```

```
/usr/include/linux/icmp.h:74: warning: data definition has no type or storage class
/usr/include/linux/icmp.h:75: parse error before `gateway'
/usr/include/linux/icmp.h:75: warning: data definition has no type or storage class
/usr/include/linux/icmp.h:77: parse error before `__u16'
/usr/include/linux/icmp.h:77: warning: no semicolon at end of struct or union
/usr/include/linux/icmp.h:78: warning: data definition has no type or storage class
/usr/include/linux/icmp.h:79: warning: data definition has no type or storage class
/usr/include/linux/icmp.h:80: parse error before `}'
/usr/include/linux/icmp.h:80: warning: data definition has no type or storage class
/usr/include/linux/icmp.h:81: parse error before `}'
/usr/include/linux/icmp.h:90: parse error before `__u32'
/usr/include/linux/icmp.h:90: warning: no semicolon at end of struct or union
In file included from /usr/include/linux/signal.h:4,
                 from loki.h:38,
                 from surplus.c:10:
/usr/include/asm/signal.h:27: conflicting types for `sigset_t'
/usr/include/sys/select.h:38: previous declaration of `sigset_t'
/usr/include/asm/signal.h:129: warning: redefinition of `__sighandler_t'
/usr/include/signal.h:71: warning: `__sighandler_t' previously declared here
/usr/include/asm/signal.h:156: redefinition of `struct sigaction'
/usr/include/asm/signal.h:171: redefinition of `struct sigaltstack'
/usr/include/asm/signal.h:175: warning: redefinition of `stack_t'
/usr/include/bits/sigstack.h:55: warning: `stack_t' previously declared here
In file included from /usr/include/linux/signal.h:5,
                 from loki.h:38,
                 from surplus.c:10:
/usr/include/asm/siginfo.h:8: redefinition of `union sigval'
/usr/include/asm/siginfo.h:11: warning: redefinition of `sigval_t'
/usr/include/bits/siginfo.h:37: warning: `sigval_t' previously declared here
/usr/include/asm/siginfo.h:16: redefinition of `struct siginfo'
/usr/include/asm/siginfo.h:63: warning: redefinition of `siginfo_t'
/usr/include/bits/siginfo.h:107: warning: `siginfo_t' previously declared here
/usr/include/asm/siginfo.h:199: redefinition of `struct sigevent'
/usr/include/asm/siginfo.h:211: warning: redefinition of `sigevent_t'
/usr/include/bits/siginfo.h:289: warning: `sigevent_t' previously declared here
make[1]: *** [surplus.o] Error 1
make[1]: Leaving directory `/mnt/Practical/Exam1/src1/L2'
make: *** [linux] Error 2
```

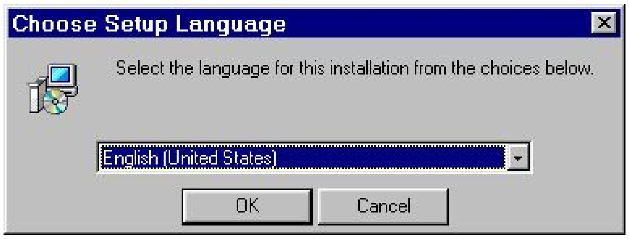
Appendix 7: “*make linux*” output (RedHat ver 5.1)

```
[root@ftp L2]#  make linux
make[1]: Entering directory `/home/Practical/Exam1/src2/L2'
gcc -Wall -O6 -finline-functions -funroll-all-loops -DLINUX -DWEAK_CRYPTO -DPOPEN -
DSEND_PAUSE=100 -Dx86_FAST_CHECK     -c surplus.c -o surplus.o
In file included from /usr/include/linux/signal.h:4,
                 from loki.h:38,
                 from surplus.c:10:
/usr/include/asm/signal.h:60: warning: `SA_NOMASK' redefined
/usr/include/sigaction.h:47: warning: this is the location of the previous definition
/usr/include/asm/signal.h:61: warning: `SA_ONESHOT' redefined
/usr/include/sigaction.h:48: warning: this is the location of the previous definition
/usr/include/asm/signal.h:82: warning: `SIG_DFL' redefined
/usr/include/signum.h:24: warning: this is the location of the previous definition
/usr/include/asm/signal.h:83: warning: `SIG_IGN' redefined
/usr/include/signum.h:25: warning: this is the location of the previous definition
/usr/include/asm/signal.h:84: warning: `SIG_ERR' redefined
/usr/include/signum.h:23: warning: this is the location of the previous definition
In file included from loki.h:36,
                 from surplus.c:10:
/usr/include/linux/icmp.h:66: parse error before `__u8'
/usr/include/linux/icmp.h:66: warning: no semicolon at end of struct or union
/usr/include/linux/icmp.h:67: warning: data definition has no type or storage class
/usr/include/linux/icmp.h:68: parse error before `checksum'
/usr/include/linux/icmp.h:68: warning: data definition has no type or storage class
/usr/include/linux/icmp.h:71: parse error before `__u16'
/usr/include/linux/icmp.h:71: warning: no semicolon at end of struct or union
/usr/include/linux/icmp.h:71: warning: no semicolon at end of struct or union
/usr/include/linux/icmp.h:72: warning: data definition has no type or storage class
/usr/include/linux/icmp.h:73: warning: data definition has no type or storage class
/usr/include/linux/icmp.h:74: parse error before `gateway'
/usr/include/linux/icmp.h:74: warning: data definition has no type or storage class
/usr/include/linux/icmp.h:75: warning: data definition has no type or storage class
/usr/include/linux/icmp.h:76: parse error before `}'
In file included from /usr/include/linux/ip.h:19,
                 from loki.h:37,
                 from surplus.c:10:
/usr/include/asm/byteorder.h:22: conflicting types for `ntohl'
/usr/include/netinet/in.h:198: previous declaration of `ntohl'
/usr/include/asm/byteorder.h:24: conflicting types for `htonl'
/usr/include/netinet/in.h:200: previous declaration of `htonl'
In file included from loki.h:37,
                 from surplus.c:10:
/usr/include/linux/ip.h:34: parse error before `__u8'
/usr/include/linux/ip.h:34: warning: no semicolon at end of struct or union
/usr/include/linux/ip.h:35: warning: data definition has no type or storage class
/usr/include/linux/ip.h:37: parse error before `flags'
/usr/include/linux/ip.h:45: warning: data definition has no type or storage class
/usr/include/linux/ip.h:46: parse error before `}'
/usr/include/linux/ip.h:71: parse error before `__u32'
/usr/include/linux/ip.h:71: warning: no semicolon at end of struct or union
/usr/include/linux/ip.h:76: parse error before `:'
/usr/include/linux/ip.h:88: parse error before `}'
/usr/include/linux/ip.h:92: parse error before `__u8'
/usr/include/linux/ip.h:92: warning: no semicolon at end of struct or union
/usr/include/linux/ip.h:100: warning: data definition has no type or storage class
/usr/include/linux/ip.h:101: parse error before `tot_len'
/usr/include/linux/ip.h:101: warning: data definition has no type or storage class
/usr/include/linux/ip.h:102: parse error before `id'
/usr/include/linux/ip.h:102: warning: data definition has no type or storage class
/usr/include/linux/ip.h:103: parse error before `frag_off'
/usr/include/linux/ip.h:103: warning: data definition has no type or storage class
/usr/include/linux/ip.h:104: parse error before `ttl'
/usr/include/linux/ip.h:104: warning: data definition has no type or storage class
/usr/include/linux/ip.h:105: parse error before `protocol'
/usr/include/linux/ip.h:105: warning: data definition has no type or storage class
/usr/include/linux/ip.h:106: parse error before `check'
/usr/include/linux/ip.h:106: warning: data definition has no type or storage class
/usr/include/linux/ip.h:107: parse error before `saddr'
/usr/include/linux/ip.h:107: warning: data definition has no type or storage class
/usr/include/linux/ip.h:108: parse error before `daddr'
/usr/include/linux/ip.h:108: warning: data definition has no type or storage class
In file included from /usr/include/linux/signal.h:4,
                 from loki.h:38,
                 from surplus.c:10:
/usr/include/asm/signal.h:4: conflicting types for `sigset_t'
/usr/include/signal.h:162: previous declaration of `sigset_t'
/usr/include/asm/signal.h:80: warning: redefinition of `__sighandler_t'
/usr/include/signal.h:48: warning: `__sighandler_t' previously declared here
/usr/include/asm/signal.h:86: redefinition of `struct sigaction'
In file included from surplus.c:10:
loki.h:357: field `iph' has incomplete type
make[1]: *** [surplus.o] Error 1
make[1]: Leaving directory `/home/Practical/Exam1/src2/L2'
make: *** [linux] Error 2
```

Appendix 8: “readelf” output (Knoppix)

```
root@ttyp0[Exam1]#  readelf atd -a;
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF32
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Intel 80386
  Version:                           0x1
  Entry point address:               0x8048db0
  Start of program headers:          52 (bytes into file)
  Start of section headers:          14508 (bytes into file)
  Flags:                             0x0
  Size of this header:               52 (bytes)
  Size of program headers:           32 (bytes)
  Number of program headers:         5
  Size of section headers:           40 (bytes)
  Number of section headers:         21
  Section header string table index: 20

Section Headers:
  [Nr] Name              Type            Addr     Off    Size   ES Flg Lk Inf Al
  [ 0]                   NULL            00000000 000000 000000 00      0   0  0
  [ 1] .interp           PROGBITS        080480d4 0000d4 000013 00   A  0   0  1
  [ 2] .hash             HASH            080480e8 0000e8 0001a4 04   A  3   0  4
  [ 3] .dynsym           DYNSYM          0804828c 00028c 000420 10   A  4   1  4
  [ 4] .dynstr           STRTAB          080486ac 0006ac 000210 00   A  0   0  1
  [ 5] .rel.bss          REL             080488bc 0008bc 000020 08   A  3  11  4
  [ 6] .rel.plt          REL             080488dc 0008dc 000190 08   A  3   8  4
  [ 7] .init             PROGBITS        08048a70 000a70 000008 00  AX  0   0 16
  [ 8] .plt              PROGBITS        08048a78 000a78 000330 04  AX  0   0  4
  [ 9] .text             PROGBITS        08048db0 000db0 001b28 00  AX  0   0 16
  [10] .fini             PROGBITS        0804a8e0 0028e0 000008 00  AX  0   0 16
  [11] .rodata           PROGBITS        0804a8e8 0028e8 000c3c 00   A  0   0  4
  [12] .data             PROGBITS        0804c528 003528 000038 00  WA  0   0  4
  [13] .ctors            PROGBITS        0804c560 003560 000008 00  WA  0   0  4
  [14] .dtors            PROGBITS        0804c568 003568 000008 00  WA  0   0  4
  [15] .got              PROGBITS        0804c570 003570 0000d4 04  WA  0   0  4
  [16] .dynamic          DYNAMIC         0804c644 003644 000088 08  WA  4   0  4
  [17] .bss              NOBITS          0804c6cc 0036cc 00012c 00  WA  0   0  8
  [18] .comment          PROGBITS        00000000 0036cc 0000a0 00      0   0  1
  [19] .note             NOTE            000000a0 00376c 0000a0 00      0   0  1
  [20] .shstrtab         STRTAB          00000000 00380c 0000a0 00      0   0  1
Key to Flags:
  W (write), A (alloc), X (execute), M (merge), S (strings)
  I (info), L (link order), G (group), x (unknown)
  O (extra OS processing required) o (OS specific), p (processor specific)

Program Headers:
  Type           Offset   VirtAddr   PhysAddr   FileSiz MemSiz  Flg Align
  PHDR           0x000034 0x08048034 0x08048034 0x000a0 0x000a0 R E 0x4
  INTERP         0x0000d4 0x080480d4 0x080480d4 0x00013 0x00013 R   0x1
      [Requesting program interpreter: /lib/ld-linux.so.1]
  LOAD           0x000000 0x08048000 0x08048000 0x03524 0x03524 R E 0x1000
  LOAD           0x003528 0x0804c528 0x0804c528 0x001a4 0x002d0 RW  0x1000
  DYNAMIC        0x003644 0x0804c644 0x0804c644 0x00088 0x00088 RW  0x4

 Section to Segment mapping:
  Segment Sections...
   00
   01     .interp
   02     .interp .hash .dynsym .dynstr .rel.bss .rel.plt .init .plt .text .fini
.rodata
   03     .data .ctors .dtors .got .dynamic .bss
   04     .dynamic

Dynamic segment at offset 0x3644 contains 17 entries:
  Tag        Type                         Name/Value
 0x00000001 (NEEDED)                     Shared library: [libc.so.5]
 0x0000000c (INIT)                       0x8048a70
 0x0000000d (FINI)                       0x804a8e0
 0x00000004 (HASH)                       0x80480e8
 0x00000005 (STRTAB)                     0x80486ac
 0x00000006 (SYMTAB)                     0x804828c
 0x0000000a (STRSZ)                      528 (bytes)
 0x0000000b (SYMENT)                     16 (bytes)
 0x00000015 (DEBUG)                      0x0
 0x00000003 (PLTGOT)                     0x804c570
 0x00000002 (PLTRELSZ)                   400 (bytes)
 0x00000014 (PLTREL)                     REL
 0x00000017 (JMPREL)                     0x80488dc
 0x00000011 (REL)                        0x80488bc
 0x00000012 (RELSZ)                      32 (bytes)
 0x00000013 (RELENT)                     8 (bytes)
 0x00000000 (NULL)                       0x0

Relocation section '.rel.bss' at offset 0x8bc contains 4 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
0804c6d8  00001005 R_386_COPY        0804c6d8   _IO_stderr_
0804c72c  00001405 R_386_COPY        0804c72c   optarg
0804c730  00002205 R_386_COPY        0804c730   __fpu_control
0804c6d0  00003d05 R_386_COPY        0804c6d0   _errno

Relocation section '.rel.plt' at offset 0x8dc contains 50 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
0804c57c  00000107 R_386_JUMP_SLOT   08048a88   longjmp
0804c580  00000207 R_386_JUMP_SLOT   08048a98   strcpy
0804c584  00000307 R_386_JUMP_SLOT   08048aa8   ioctl
0804c588  00000407 R_386_JUMP_SLOT   08048ab8   popen
0804c58c  00000507 R_386_JUMP_SLOT   08048ac8   shmctl
0804c590  00000607 R_386_JUMP_SLOT   08048ad8   geteuid
0804c594  00000807 R_386_JUMP_SLOT   08048ae8   getprotobynumber
0804c598  00000a07 R_386_JUMP_SLOT   08048af8   __strtol_internal
0804c59c  00000b07 R_386_JUMP_SLOT   08048b08   usleep
0804c5a0  00000c07 R_386_JUMP_SLOT   08048b18   semget
0804c5a4  00000d07 R_386_JUMP_SLOT   08048b28   getpid
0804c5a8  00000e07 R_386_JUMP_SLOT   08048b38   fgets
0804c5ac  00000f07 R_386_JUMP_SLOT   08048b48   shmat
0804c5b0  00001107 R_386_JUMP_SLOT   08048b58   perror
0804c5b4  00001207 R_386_JUMP_SLOT   08048b68   getuid
0804c5b8  00001307 R_386_JUMP_SLOT   08048b78   semctl
0804c5bc  00001507 R_386_JUMP_SLOT   08048b88   socket
0804c5c0  00001707 R_386_JUMP_SLOT   08048b98   bzero
0804c5c4  00001907 R_386_JUMP_SLOT   08048ba8   alarm
0804c5c8  00001a07 R_386_JUMP_SLOT   08048bb8   __libc_init
0804c5cc  00001c07 R_386_JUMP_SLOT   08048bc8   fprintf
0804c5d0  00001d07 R_386_JUMP_SLOT   08048bd8   kill
0804c5d4  00001e07 R_386_JUMP_SLOT   08048be8   inet_addr
0804c5d8  00001f07 R_386_JUMP_SLOT   08048bf8   chdir
0804c5dc  00002007 R_386_JUMP_SLOT   08048c08   shmdt
0804c5e0  00002107 R_386_JUMP_SLOT   08048c18   setsockopt
0804c5e4  00002307 R_386_JUMP_SLOT   08048c28   shmget
0804c5e8  00002407 R_386_JUMP_SLOT   08048c38   wait
0804c5ec  00002507 R_386_JUMP_SLOT   08048c48   umask
0804c5f0  00002607 R_386_JUMP_SLOT   08048c58   signal
0804c5f4  00002707 R_386_JUMP_SLOT   08048c68   read
0804c5f8  00002807 R_386_JUMP_SLOT   08048c78   strncmp
0804c5fc  00002907 R_386_JUMP_SLOT   08048c88   sendto
0804c600  00002a07 R_386_JUMP_SLOT   08048c98   bcopy
0804c604  00002b07 R_386_JUMP_SLOT   08048ca8   fork
0804c608  00002c07 R_386_JUMP_SLOT   08048cb8   strdup
0804c60c  00002d07 R_386_JUMP_SLOT   08048cc8   getopt
0804c610  00002e07 R_386_JUMP_SLOT   08048cd8   inet_ntoa
0804c614  00002f07 R_386_JUMP_SLOT   08048ce8   getppid
0804c618  00003007 R_386_JUMP_SLOT   08048cf8   time
0804c61c  00003107 R_386_JUMP_SLOT   08048d08   gethostbyname
0804c620  00003307 R_386_JUMP_SLOT   08048d18   sprintf
0804c624  00003407 R_386_JUMP_SLOT   08048d28   difftime
0804c628  00003507 R_386_JUMP_SLOT   08048d38   atexit
0804c62c  00003707 R_386_JUMP_SLOT   08048d48   semop
0804c630  00003807 R_386_JUMP_SLOT   08048d58   exit
0804c634  00003907 R_386_JUMP_SLOT   08048d68   __setfpucw
0804c638  00003a07 R_386_JUMP_SLOT   08048d78   open
0804c63c  00003b07 R_386_JUMP_SLOT   08048d88   setsid
0804c640  00003c07 R_386_JUMP_SLOT   08048d98   close
There are no unwind sections in this file.

Symbol table '.dynsym' contains 66 entries:
   Num:    Value  Size Type    Bind   Vis      Ndx Name
     0: 00000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 08048a88     0 FUNC    GLOBAL DEFAULT  UND longjmp
     2: 08048a98    30 FUNC    GLOBAL DEFAULT  UND strcpy
     3: 08048aa8     0 FUNC    WEAK   DEFAULT  UND ioctl
     4: 08048ab8     0 FUNC    WEAK   DEFAULT  UND popen
     5: 08048ac8    42 FUNC    GLOBAL DEFAULT  UND shmctl
     6: 08048ad8     0 FUNC    WEAK   DEFAULT  UND geteuid
     7: 0804c644     0 OBJECT  GLOBAL DEFAULT  ABS _DYNAMIC
     8: 08048ae8   292 FUNC    GLOBAL DEFAULT  UND getprotobynumber
     9: 0804c6d0     4 NOTYPE  WEAK   DEFAULT   17 errno
    10: 08048af8  1132 FUNC    GLOBAL DEFAULT  UND __strtol_internal
    11: 08048b08    99 FUNC    GLOBAL DEFAULT  UND usleep
    12: 08048b18    42 FUNC    GLOBAL DEFAULT  UND semget
    13: 08048b28     0 FUNC    WEAK   DEFAULT  UND getpid
    14: 08048b38     0 FUNC    WEAK   DEFAULT  UND fgets
    15: 08048b48    59 FUNC    GLOBAL DEFAULT  UND shmat
    16: 0804c6d8    84 OBJECT  GLOBAL DEFAULT   17 _IO_stderr_
    17: 08048b58     0 FUNC    WEAK   DEFAULT  UND perror
    18: 08048b68     0 FUNC    WEAK   DEFAULT  UND getuid
    19: 08048b78    47 FUNC    GLOBAL DEFAULT  UND semctl
    20: 0804c72c     4 OBJECT  GLOBAL DEFAULT   17 optarg
    21: 08048b88    94 FUNC    WEAK   DEFAULT  UND socket
    22: 0804c528     4 OBJECT  GLOBAL DEFAULT   12 __environ
    23: 08048b98    54 FUNC    GLOBAL DEFAULT  UND bzero
    24: 08048a70     0 FUNC    GLOBAL DEFAULT    7 _init
    25: 08048ba8     0 FUNC    WEAK   DEFAULT  UND alarm
    26: 08048bb8    70 FUNC    GLOBAL DEFAULT  UND __libc_init
    27: 0804c528     4 NOTYPE  WEAK   DEFAULT   12 environ
    28: 08048bc8     0 FUNC    WEAK   DEFAULT  UND fprintf
    29: 08048bd8     0 FUNC    WEAK   DEFAULT  UND kill
    30: 08048be8    57 FUNC    GLOBAL DEFAULT  UND inet_addr
    31: 08048bf8     0 FUNC    WEAK   DEFAULT  UND chdir
    32: 08048c08    36 FUNC    GLOBAL DEFAULT  UND shmdt
    33: 08048c18   111 FUNC    WEAK   DEFAULT  UND setsockopt
    34: 0804c730     2 OBJECT  GLOBAL DEFAULT   17 __fpu_control
    35: 08048c28    42 FUNC    GLOBAL DEFAULT  UND shmget
    36: 08048c38     0 FUNC    WEAK   DEFAULT  UND wait
    37: 08048c48     0 FUNC    WEAK   DEFAULT  UND umask
    38: 08048c58    84 FUNC    GLOBAL DEFAULT  UND signal
    39: 08048c68     0 FUNC    WEAK   DEFAULT  UND read
    40: 08048c78    38 FUNC    GLOBAL DEFAULT  UND strncmp
    41: 08048c88   124 FUNC    WEAK   DEFAULT  UND sendto
    42: 08048c98   146 FUNC    GLOBAL DEFAULT  UND bcopy
    43: 08048ca8     0 FUNC    WEAK   DEFAULT  UND fork
    44: 08048cb8    79 FUNC    GLOBAL DEFAULT  UND strdup
    45: 08048cc8    44 FUNC    GLOBAL DEFAULT  UND getopt
    46: 08048cd8    67 FUNC    GLOBAL DEFAULT  UND inet_ntoa
    47: 08048ce8     0 FUNC    WEAK   DEFAULT  UND getppid
    48: 08048cf8     0 FUNC    WEAK   DEFAULT  UND time
    49: 08048d08   292 FUNC    GLOBAL DEFAULT  UND gethostbyname
    50: 0804a8e0     0 FUNC    GLOBAL DEFAULT   10 _fini
    51: 08048d18    38 FUNC    WEAK   DEFAULT  UND sprintf
    52: 08048d28    16 FUNC    GLOBAL DEFAULT  UND difftime
    53: 08048d38    52 FUNC    GLOBAL DEFAULT  UND atexit
    54: 0804c570     0 OBJECT  GLOBAL DEFAULT  ABS _GLOBAL_OFFSET_TABLE_
    55: 08048d48    42 FUNC    GLOBAL DEFAULT  UND semop
    56: 08048d58   128 FUNC    GLOBAL DEFAULT  UND exit
    57: 08048d68    62 FUNC    GLOBAL DEFAULT  UND __setfpucw
    58: 08048d78     0 FUNC    WEAK   DEFAULT  UND open
    59: 08048d88     0 FUNC    WEAK   DEFAULT  UND setsid
    60: 08048d98     0 FUNC    WEAK   DEFAULT  UND close
    61: 0804c6d0     4 OBJECT  GLOBAL DEFAULT   17 _errno
    62: 0804a8d8     0 OBJECT  GLOBAL DEFAULT  ABS _etext
    63: 0804c6cc     0 OBJECT  GLOBAL DEFAULT  ABS _edata
    64: 0804c6cc     0 OBJECT  GLOBAL DEFAULT  ABS __bss_start
    65: 0804c7f8     0 OBJECT  GLOBAL DEFAULT  ABS _end

Histogram for bucket list length (total of 37 buckets):
 Length  Number     % of total  Coverage
      0  9          ( 24.3%)
      1  8          ( 21.6%)     12.3%
      2  10         ( 27.0%)     43.1%
      3  4          ( 10.8%)     61.5%
      4  5          ( 13.5%)     92.3%
      5  1          (  2.7%)    100.0%
No version information found in this file.
```

Appendix 9: Screenshots: ER Pro Installation

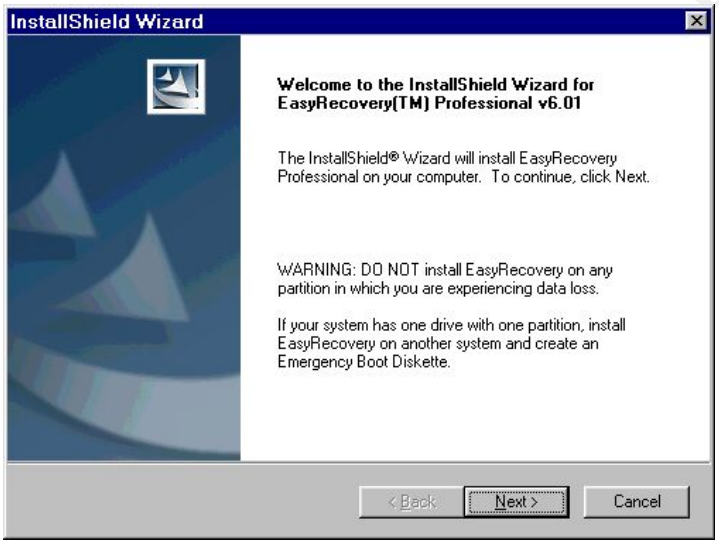


Choose Setup Language

Select the language for this installation from the choices below.

English (United States)

Figure 1: Select Language



InstallShield Wizard

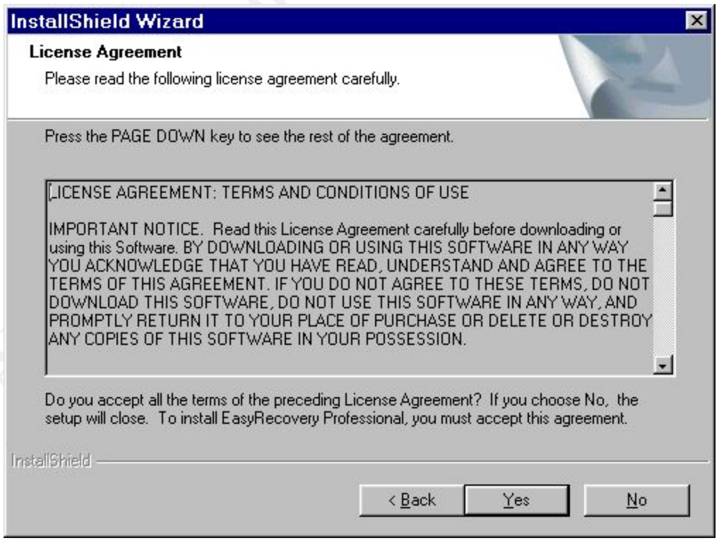
Welcome to the InstallShield Wizard for EasyRecovery(TM) Professional v6.01

The InstallShield® Wizard will install EasyRecovery Professional on your computer. To continue, click Next.

WARNING: DO NOT install EasyRecovery on any partition in which you are experiencing data loss.

If your system has one drive with one partition, install EasyRecovery on another system and create an Emergency Boot Diskette.

Figure 2: Installation Welcome Screen



InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

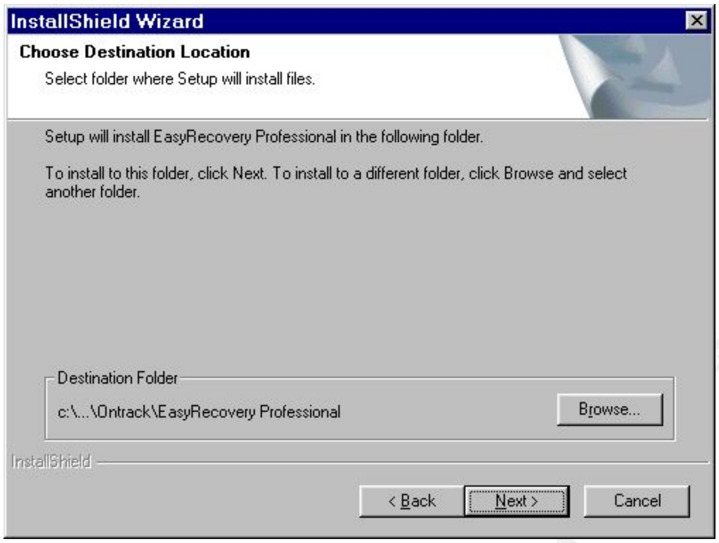
Press the PAGE DOWN key to see the rest of the agreement.

LICENSE AGREEMENT: TERMS AND CONDITIONS OF USE

IMPORTANT NOTICE. Read this License Agreement carefully before downloading or using this Software. BY DOWNLOADING OR USING THIS SOFTWARE IN ANY WAY YOU ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTAND AND AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT DOWNLOAD THIS SOFTWARE, DO NOT USE THIS SOFTWARE IN ANY WAY, AND PROMPTLY RETURN IT TO YOUR PLACE OF PURCHASE OR DELETE OR DESTROY ANY COPIES OF THIS SOFTWARE IN YOUR POSSESSION.

Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install EasyRecovery Professional, you must accept this agreement.

Figure 3: Lisenced Agreement Screen



InstallShield Wizard

Choose Destination Location

Select folder where Setup will install files.

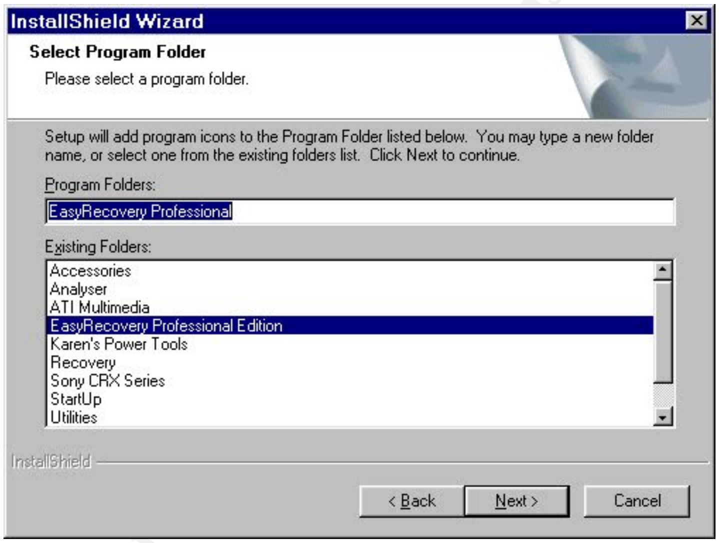
Setup will install EasyRecovery Professional in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

c:\...\Ontrack\EasyRecovery Professional

Figure 4: Installation Location



InstallShield Wizard

Select Program Folder

Please select a program folder.

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing folders list. Click Next to continue.

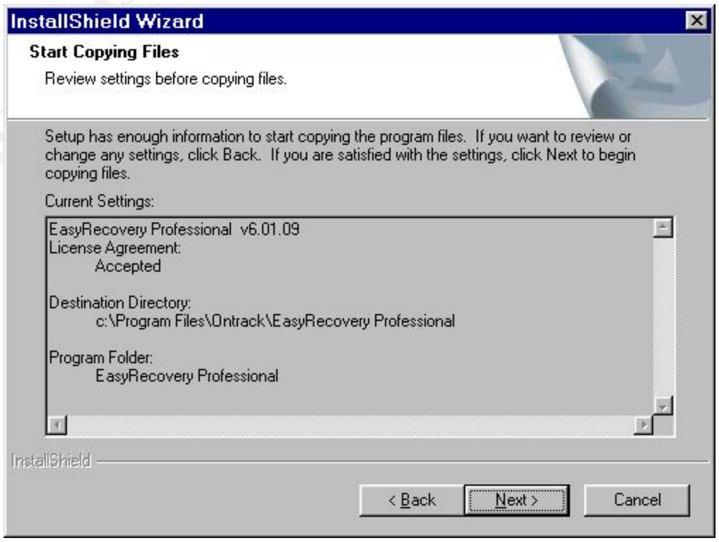
Program Folders:

EasyRecovery Professional

Existing Folders:

Accessories
Analyser
ATI Multimedia
EasyRecovery Professional Edition
Karen's Power Tools
Recovery
Sony CRX Series
StartUp
Utilities

Figure 5: Windows Start Menu Shortcut Location



InstallShield Wizard

Start Copying Files

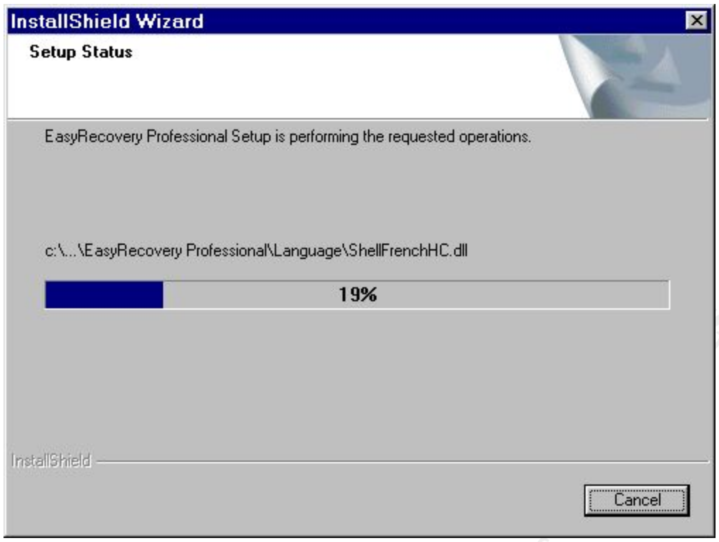
Review settings before copying files.

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

```
EasyRecovery Professional  v6.01.09
License Agreement:
        Accepted

Destination Directory:
        c:\Program Files\Ontrack\EasyRecovery Professional

Program Folder:
        EasyRecovery Professional
```

Figure 6: Parameters Summary Screen



InstallShield Wizard

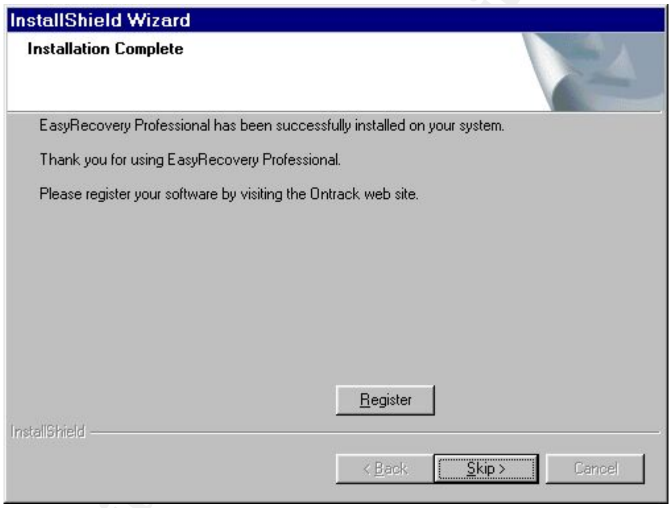
Setup Status

EasyRecovery Professional Setup is performing the requested operations.

c:\...\EasyRecovery Professional\Language\ShellFrenchHC.dll

19%

Figure 7: Installation in Progress



InstallShield Wizard

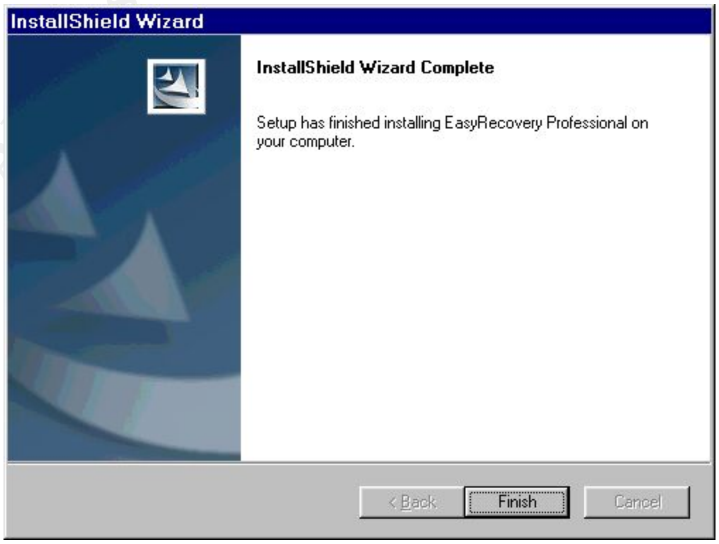
Installation Complete

EasyRecovery Professional has been successfully installed on your system.

Thank you for using EasyRecovery Professional.

Please register your software by visiting the Ontrack web site.

Figure 8: Registration Screen



InstallShield Wizard

InstallShield Wizard Complete

Setup has finished installing EasyRecovery Professional on your computer.

Figure 9: Installation Complete

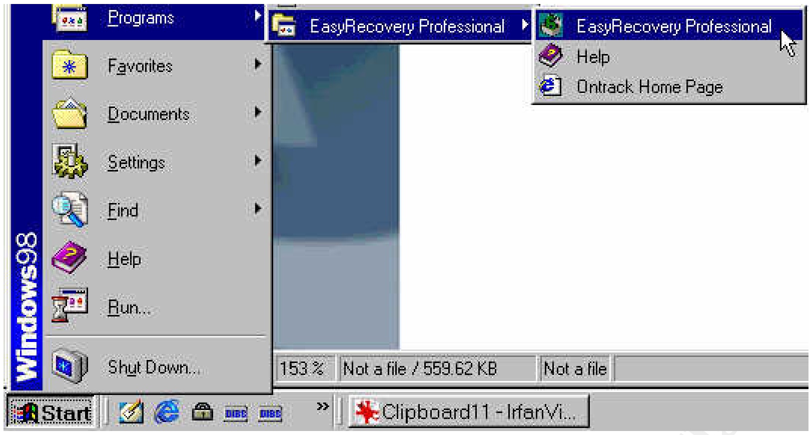


Figure 10: Windows Start Menu Item Created

Appendix 10: Screenshots: EmergencyDiskette Creation

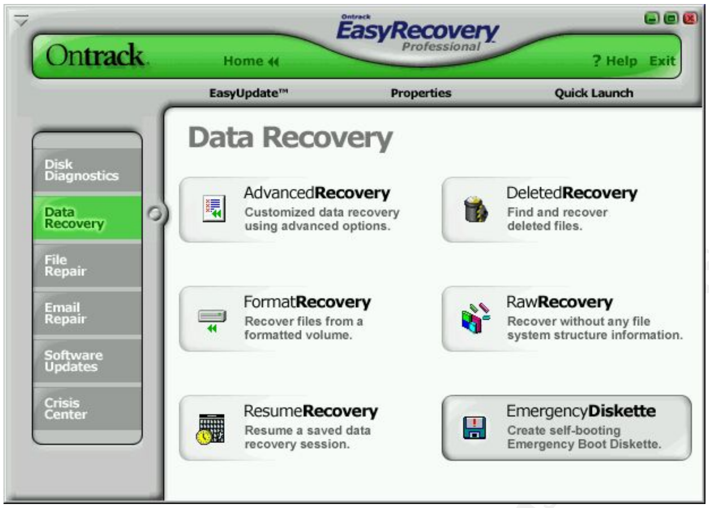
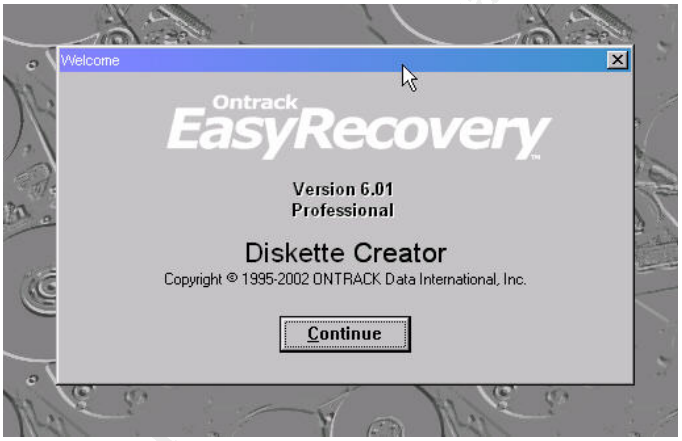

Ontrack
EasyRecovery Professional
Home
? Help
Exit
EasyUpdate™
Properties
Quick Launch
Disk Diagnostics
Data Recovery
File Repair
Email Repair
Software Updates
Crisis Center
Data Recovery
AdvancedRecovery
Customized data recovery using advanced options.
DeletedRecovery
Find and recover deleted files.
FormatRecovery
Recover files from a formatted volume.
RawRecovery
Recover without any file system structure information.
ResumeRecovery
Resume a saved data recovery session.
EmergencyDiskette
Create self-booting Emergency Boot Diskette.

Figure 11: Data Recovery Main Screen

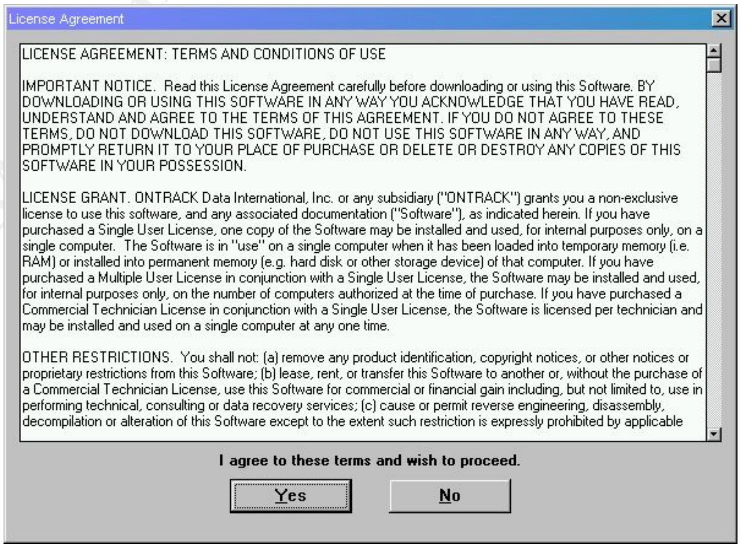


Version 6.01
Professional

Diskette Creator

Copyright © 1995-2002 ONTRACK Data International, Inc.

Figure 12: EmergencyDiskette Main Screen



LICENSE AGREEMENT: TERMS AND CONDITIONS OF USE

IMPORTANT NOTICE. Read this License Agreement carefully before downloading or using this Software. BY DOWNLOADING OR USING THIS SOFTWARE IN ANY WAY YOU ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTAND AND AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT DOWNLOAD THIS SOFTWARE, DO NOT USE THIS SOFTWARE IN ANY WAY, AND PROMPTLY RETURN IT TO YOUR PLACE OF PURCHASE OR DELETE OR DESTROY ANY COPIES OF THIS SOFTWARE IN YOUR POSSESSION.

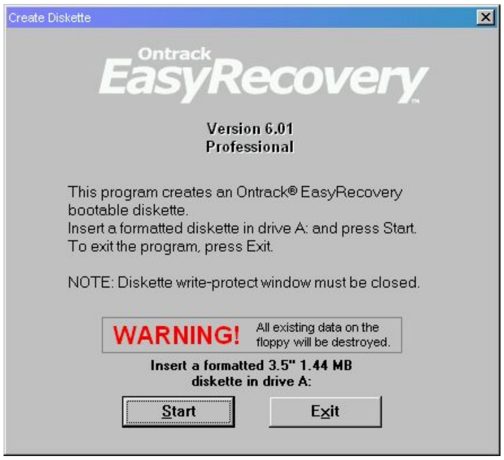
LICENSE GRANT. ONTRACK Data International, Inc. or any subsidiary ("ONTRACK") grants you a non-exclusive license to use this software, and any associated documentation ("Software"), as indicated herein. If you have purchased a Single User License, one copy of the Software may be installed and used, for internal purposes only, on a single computer. The Software is in "use" on a single computer when it has been loaded into temporary memory (i.e. RAM) or installed into permanent memory (e.g. hard disk or other storage device) of that computer. If you have purchased a Multiple User License in conjunction with a Single User License, the Software may be installed and used, for internal purposes only, on the number of computers authorized at the time of purchase. If you have purchased a Commercial Technician License in conjunction with a Single User License, the Software is licensed per technician and may be installed and used on a single computer at any one time.

OTHER RESTRICTIONS. You shall not: (a) remove any product identification, copyright notices, or other notices or proprietary restrictions from this Software; (b) lease, rent, or transfer this Software to another or, without the purchase of a Commercial Technician License, use this Software for commercial or financial gain including, but not limited to, use in performing technical, consulting or data recovery services; (c) cause or permit reverse engineering, disassembly, decompilation or alteration of this Software except to the extent such restriction is expressly prohibited by applicable

I agree to these terms and wish to proceed.

Yes No

Figure 13: License Agreement Screen



Create Diskette

Ontrack EasyRecovery

Version 6.01
Professional

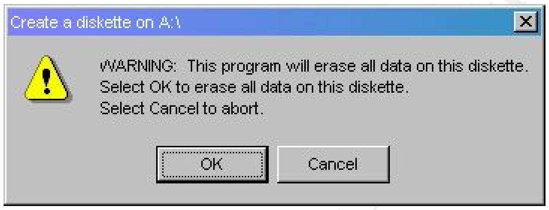
This program creates an Ontrack® EasyRecovery bootable diskette.
Insert a formatted diskette in drive A: and press Start.
To exit the program, press Exit.

NOTE: Diskette write-protect window must be closed.

WARNING! All existing data on the floppy will be destroyed.

Insert a formatted 3.5" 1.44 MB diskette in drive A:

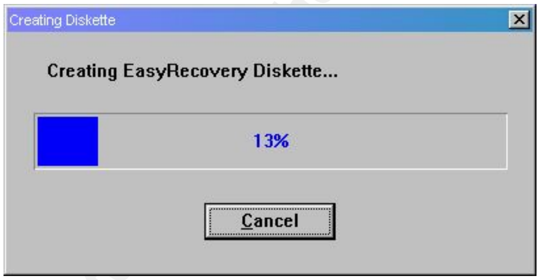
Figure 14: Instruction Screen



Create a diskette on A:\

WARNING: This program will erase all data on this diskette.
Select OK to erase all data on this diskette.
Select Cancel to abort.

Figure 15: Warning Screen

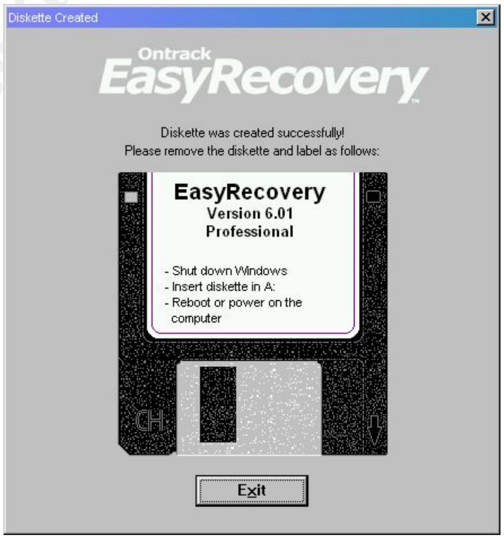


Creating Diskette

Creating EasyRecovery Diskette...

13%

Figure 16: Creating EmergencyDiskette



Diskette Created

Ontrack EasyRecovery

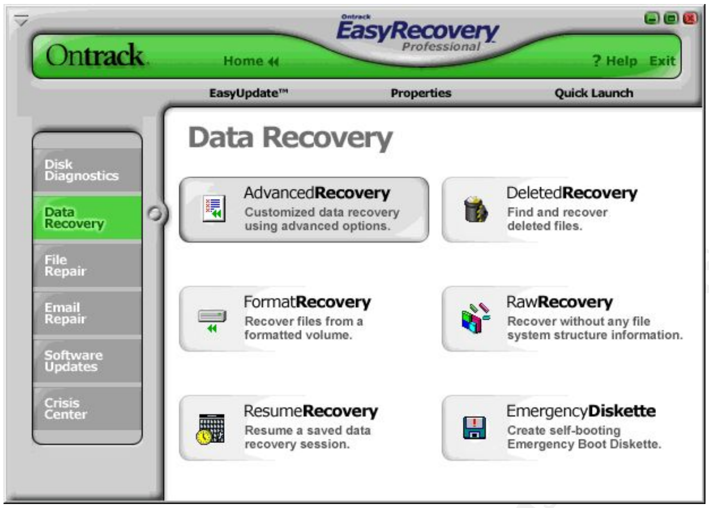
Diskette was created successfully!
Please remove the diskette and label as follows:

EasyRecovery
Version 6.01
Professional

- Shut down Windows
- Insert diskette in A:
- Reboot or power on the computer

Figure 17: EmergencyDiskette Created

Appendix 11: Sample Screenshots during Data Recovery



Data Recovery

AdvancedRecovery — Customized data recovery using advanced options.

DeletedRecovery — Find and recover deleted files.

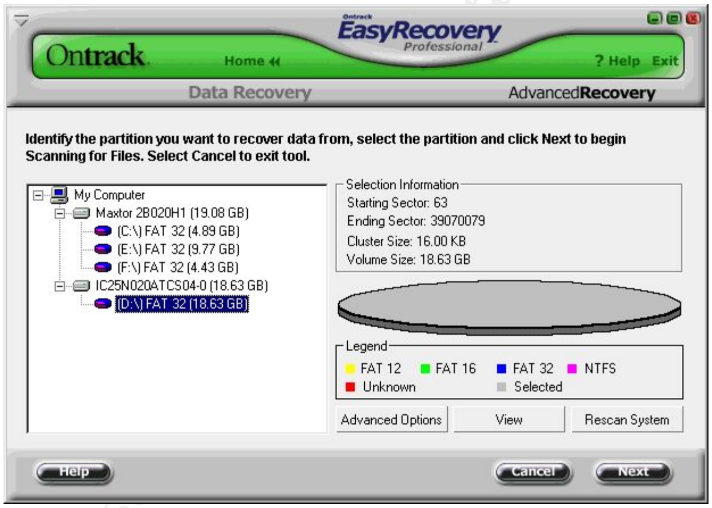
FormatRecovery — Recover files from a formatted volume.

RawRecovery — Recover without any file system structure information.

ResumeRecovery — Resume a saved data recovery session.

EmergencyDiskette — Create self-booting Emergency Boot Diskette.

Figure 18: Data Recovery Main Screen

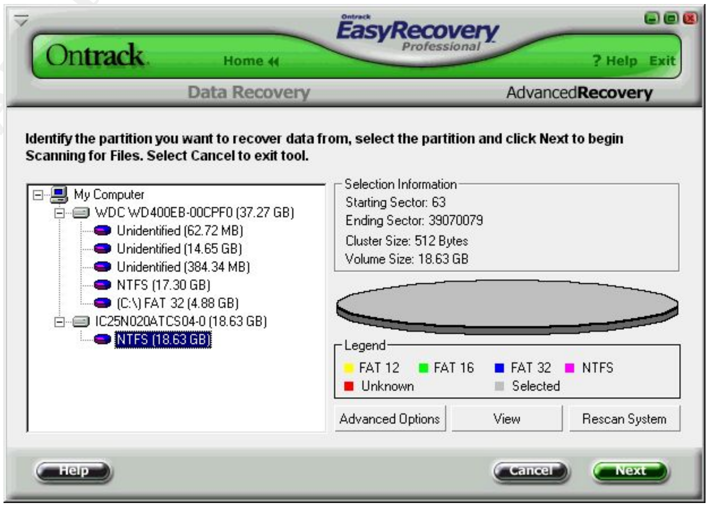


Identify the partition you want to recover data from, select the partition and click Next to begin Scanning for Files. Select Cancel to exit tool.

```
My Computer
  Maxtor 2B020H1 (19.08 GB)
    (C:\) FAT 32 (4.89 GB)
    (E:\) FAT 32 (9.77 GB)
    (F:\) FAT 32 (4.43 GB)
  IC25N020ATCS04-0 (18.63 GB)
    (D:\) FAT 32 (18.63 GB)
```

Selection Information
Starting Sector: 63
Ending Sector: 39070079
Cluster Size: 16.00 KB
Volume Size: 18.63 GB

Figure 19: AdvancedRecovery Screen (FAT32 media selected)

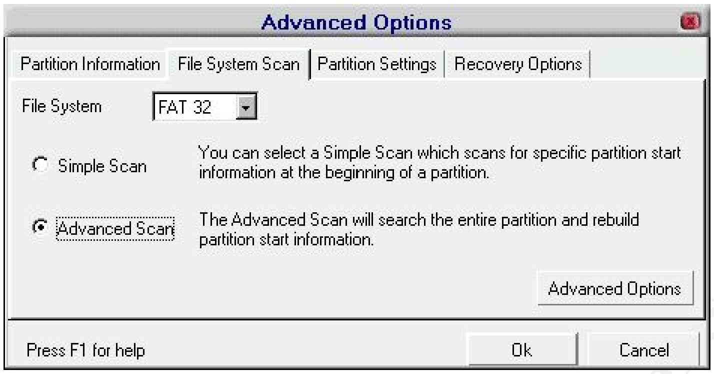


Identify the partition you want to recover data from, select the partition and click Next to begin Scanning for Files. Select Cancel to exit tool.

```
My Computer
  WDC WD400EB-00CPF0 (37.27 GB)
    Unidentified (62.72 MB)
    Unidentified (14.65 GB)
    Unidentified (384.34 MB)
    NTFS (17.30 GB)
    (C:\) FAT 32 (4.88 GB)
  IC25N020ATCS04-0 (18.63 GB)
    NTFS (18.63 GB)
```

Selection Information
Starting Sector: 63
Ending Sector: 39070079
Cluster Size: 512 Bytes
Volume Size: 18.63 GB

Figure 20: AdvancedRecovery Screen (NTFS media selected)

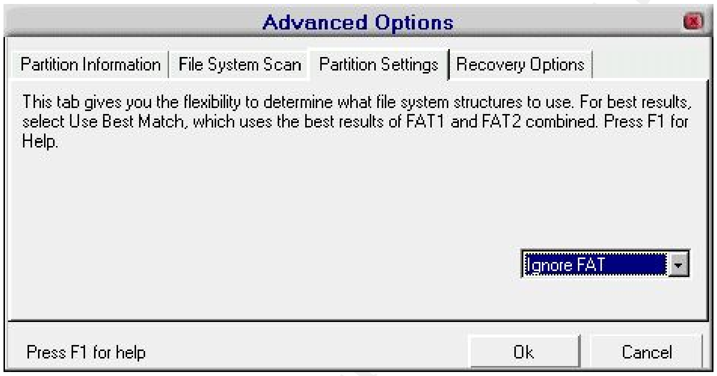


File System: FAT 32

○ Simple Scan — You can select a Simple Scan which scans for specific partition start information at the beginning of a partition.

● Advanced Scan — The Advanced Scan will search the entire partition and rebuild partition start information.

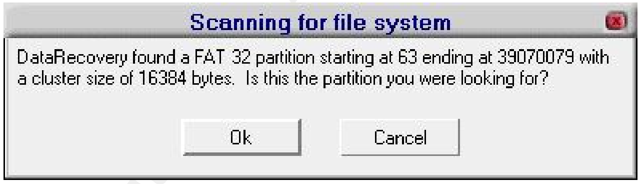
Figure 21: Advanced Options - File System Scan



This tab gives you the flexibility to determine what file system structures to use. For best results, select Use Best Match, which uses the best results of FAT1 and FAT2 combined. Press F1 for Help.

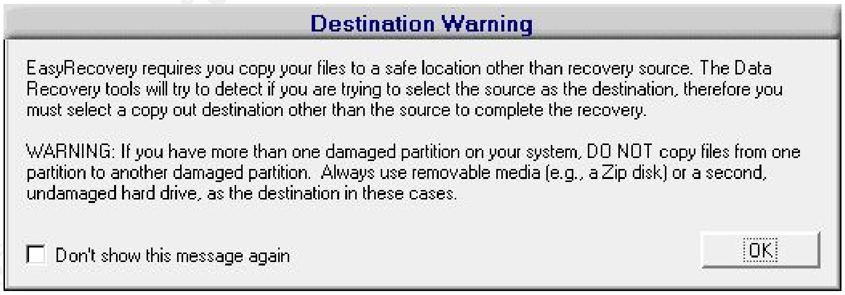
Ignore FAT

Figure 22: Advanced Option - Partition Setting



DataRecovery found a FAT 32 partition starting at 63 ending at 39070079 with a cluster size of 16384 bytes. Is this the partition you were looking for?

Figure 23: File System Found after Scanning

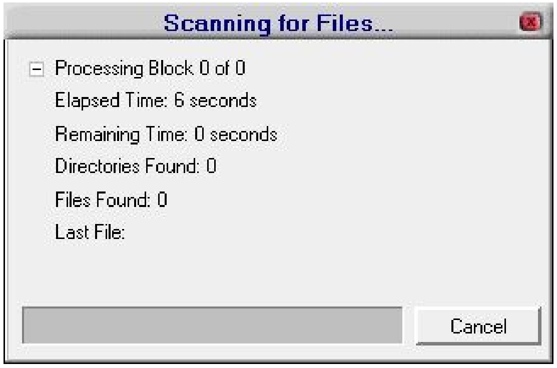


EasyRecovery requires you copy your files to a safe location other than recovery source. The Data Recovery tools will try to detect if you are trying to select the source as the destination, therefore you must select a copy out destination other than the source to complete the recovery.

WARNING: If you have more than one damaged partition on your system, DO NOT copy files from one partition to another damaged partition. Always use removable media (e.g., a Zip disk) or a second, undamaged hard drive, as the destination in these cases.

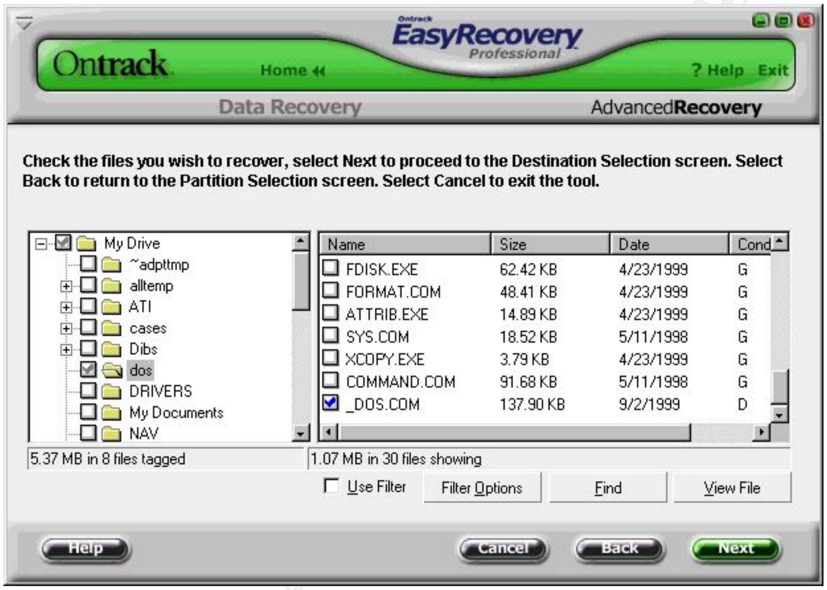
□ Don't show this message again

Figure 24: Destination Location Warning



⊟ Processing Block 0 of 0
Elapsed Time: 6 seconds
Remaining Time: 0 seconds
Directories Found: 0
Files Found: 0
Last File:

Figure 25: Scanning for files



Check the files you wish to recover, select Next to proceed to the Destination Selection screen. Select Back to return to the Partition Selection screen. Select Cancel to exit the tool.

- ☑ My Drive
  - □ ~adpttmp
  - □ alltemp
  - □ ATI
  - □ cases
  - □ Dibs
  - ☑ dos
  - □ DRIVERS
  - □ My Documents
  - □ NAV

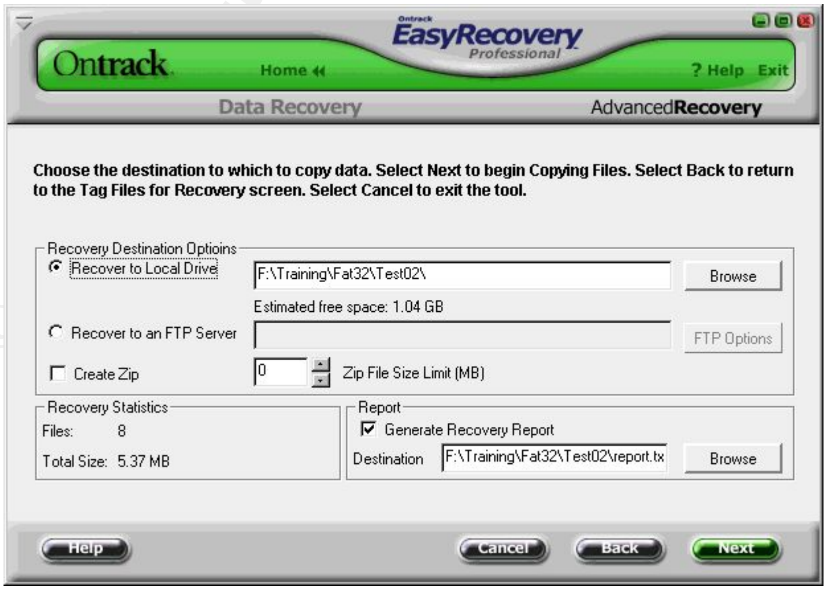
Name	Size	Date	Cond
□ FDISK.EXE	62.42 KB	4/23/1999	G
□ FORMAT.COM	48.41 KB	4/23/1999	G
□ ATTRIB.EXE	14.89 KB	4/23/1999	G
□ SYS.COM	18.52 KB	5/11/1998	G
□ XCOPY.EXE	3.79 KB	4/23/1999	G
□ COMMAND.COM	91.68 KB	5/11/1998	G
☑ _DOS.COM	137.90 KB	9/2/1999	D

5.37 MB in 8 files tagged

1.07 MB in 30 files showing

□ Use Filter | Filter Options | Find | View File

Figure 26: List of Files Found



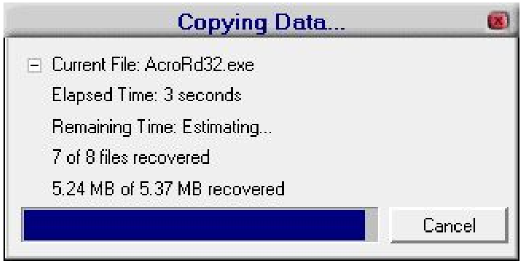
Choose the destination to which to copy data. Select Next to begin Copying Files. Select Back to return to the Tag Files for Recovery screen. Select Cancel to exit the tool.

Recovery Destination Options
● Recover to Local Drive: F:\Training\Fat32\Test02\
Estimated free space: 1.04 GB
○ Recover to an FTP Server
□ Create Zip: 0 Zip File Size Limit (MB)

Recovery Statistics
Files: 8
Total Size: 5.37 MB

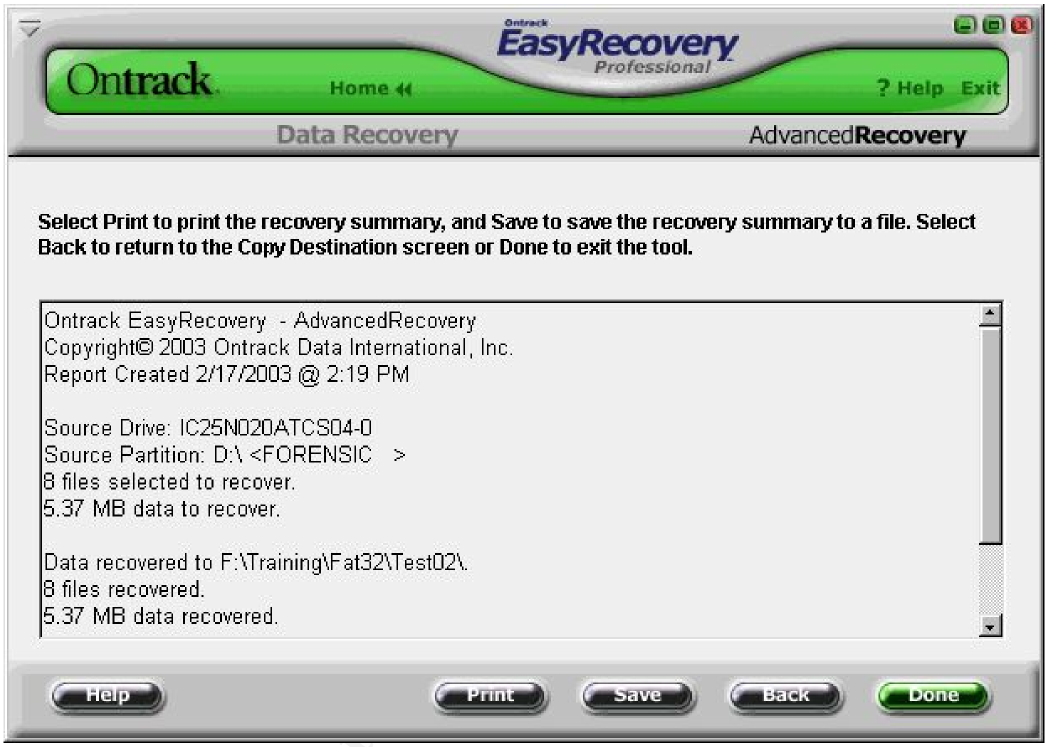
Report
☑ Generate Recovery Report
Destination: F:\Training\Fat32\Test02\report.tx

Figure 27: Select Destination Location



Current File: AcroRd32.exe
Elapsed Time: 3 seconds
Remaining Time: Estimating...
7 of 8 files recovered
5.24 MB of 5.37 MB recovered

Figure 28: Copying Recovered Data



Select Print to print the recovery summary, and Save to save the recovery summary to a file. Select Back to return to the Copy Destination screen or Done to exit the tool.

```
Ontrack EasyRecovery  - AdvancedRecovery
Copyright© 2003 Ontrack Data International, Inc.
Report Created 2/17/2003 @ 2:19 PM

Source Drive: IC25N020ATCS04-0
Source Partition: D:\ <FORENSIC   >
8 files selected to recover.
5.37 MB data to recover.

Data recovered to F:\Training\Fat32\Test02\.
8 files recovered.
5.37 MB data recovered.
```

Figure 29: Recovery Summary Screen

Appendix 12: FAT32 HDD MD5 Value Result Summary

```
Test01-DOS\MD5Before.txt
72ae12a54249ba1521840bd8ef5e0869  /dev/hdc

Test01-DOS\MD5After.txt
72ae12a54249ba1521840bd8ef5e0869  /dev/hdc

Test01-WIN\MD5Before.txt
72ae12a54249ba1521840bd8ef5e0869  /dev/hdc

Test01-WIN\MD5After.txt
72ae12a54249 ba1521840bd8ef5e0869  /dev/hdc

-------------------------------------------

Test02-DOS\MD5Before.txt
a0fe4af410f25398572c338f8298bd7a  /dev/hdc

Test02-DOS\MD5After.txt
a0fe4af410f25398572c338f8298bd7a  /dev/hdc

Test02-WIN\MD5Before.txt
a0fe4af410f25398 572c338f8298bd7a  /dev/hdc

Test02-WIN\MD5After.txt
a0fe4af410f25398572c338f8298bd7a  /dev/hdc

-------------------------------------------

Test03-DOS\MD5Before.txt
f8ac1318653d4dbd44f39852ffb9626e  /dev/hdc

Test03-DOS\MD5After.txt
f8ac1318653d4dbd44f39 852ffb9626e  /dev/hdc

Test03-WIN\MD5Before.txt
f8ac1318653d4dbd44f39852ffb9626e  /dev/hdc

Test03-WIN\MD5After.txt
bd8b788c9a383d0d5a9ea5714714d19c  /dev/hdc

-------------------------------------------

Test04-DOS\MD5Before.txt
398f2febe28ca81ed4ce2f681 7b4dae7  /dev/hdc

Test04-DOS\MD5After.txt
398f2febe28ca81ed4ce2f6817b4dae7  /dev/hdc

Test04-WIN\MD5Before.txt
398f2febe28ca81ed4ce2f6817b4dae7  /dev/hdc

Test04-WIN\MD5After.txt
398f2febe28ca81ed4ce2f6817b4dae7  /dev/hdc
```

Appendix 13: FAT32 Files MD5 Value Result Summary

```
5fea57f2a1546bc391c6b9cb1bbfc452  Original  \SN.ZIP
5fea57f2a1546bc391c6b9cb1bbfc452  Test01  -DOS\DOWNLOAD\_N.ZIP
5fea57f2a1546bc391c6b9cb1bbfc452  Test01  -WIN\Download\_N.ZIP
5fea57f2a1546bc391c6b9cb1bbfc452  Test02  -DOS\DOWNLOAD\_N.ZIP
5fea57f2a1546bc391c6b9cb1bbfc452  Test02  -WIN\Download\_N.ZIP
5fea57f2a1546bc391c6b9cb1bbfc452  Test03  -DOS\LOSTFILE\DIR20\_N.ZIP
5fea57f2a1546bc391c6b9cb1bbfc452  Test03  -WIN\LOSTFILE\DIR20\_N.ZIP
5fea57f2a1546bc391c6b9cb1bbfc452  Test04  -DOS\LOSTFILE\DIR20\_N.Z IP
5fea57f2a1546bc391c6b9cb1bbfc452  Test04  -WIN\LOSTFILE\DIR20\_N.ZIP

fac395242697347c2a24c17e4ec2aa59  Original  \Tube.gif
fac395242697347c2a24c17e4ec2aa59  Test01  -DOS\PROGRA~1\PAINTS~1\ANIMS\TUBE.GIF
fac395242697347c2a24c17e4ec2aa59  Test01  -WIN\Program Fi les\Paint Shop Pro 6 \Anims
                                            \Tube.gif
fac395242697347c2a24c17e4ec2aa59  Test02  -DOS\PROGRA~1\PAINTS~1\ANIMS\TUBE.GIF
fac395242697347c2a24c17e4ec2aa59  Test02  -WIN\Program Files \Paint Shop Pro 6 \Anims
                                            \Tube.gif
fac395242697347c2a24c17e4ec2aa59  Test03  -DOS\LOSTFILE\DIR5\PAINTS~1\ANIMS\TUBE.GIF
fac395242697347c2a24c17e4ec2aa59  Test03  -WIN\LOSTFILE\DIR5\Paint Shop Pro 6 \Anims
                                            \Tube.gif
fac395242697347c2a24c17e4ec2aa59  Test04  -DOS\LOSTFILE\DIR5\PAINTS~1\ANIMS\TUBE.GIF
fac395242697347c2a24c17e4ec2aa59  Test04  -WIN\LOSTFILE\DIR5\Paint Shop Pro 6 \Anims
                                            \Tube.gif

89138783d69b7d7d8fbb86224bd1342a  Original  \msword2.doc
89138783d69b7d7d8fbb86224bd1342a  Test01  -DOS\PROGRA~1\QUICKV~1\SAMPLES\MSWORD2.DOC
89138783d69b7d7d8fbb86224bd1342a  Test01  -WIN\Program Files \Quick View Pl us\SAMPLES
                                            \msword2.doc
89138783d69b7d7d8fbb86224bd1342a  Test02  -DOS\PROGRA~1\QUICKV~1\SAMPLES\MSWORD2.DOC
89138783d69b7d7d8fbb86224bd1342a  Test02  -WIN\Program Files \Quick View Plus \SAMPLES
                                            \msword2.doc
89138783d69b7d7d8fbb86224bd1342a  Test03  -DOS\LOSTFILE\DIR5\QUICKV~1\SAMPLES
                                            \MSWORD2.DOC
89138783d69b7d7d8fbb86224bd1342a  Test03  -WIN\LOSTFILE\DIR5\Quick View Plus \SAMPLES
                                            \msword2.doc
89138783d69b7d7d8fbb86224bd1342a  Test04  -DOS\LOSTFILE\DIR5\QUICKV~1\SAMPLES
                                            \MSWORD2.DOC
89138783d69b7d7d8fbb86224bd1342a  T  est04-WIN\LOSTFILE\DIR5\Quick View Plus \SAMPLES
                                            \msword2.doc

8dbc7cc7a3feb7b8fde8edeeaa268c2a  Original  \canvas_dark_blue.jpg
8dbc7cc7a3feb7b8fde8edeeaa268c2a  Test01  -DOS\PROGRA~1\ROXIO\WINONCD\IMAGES\BCK
                                            \CANVAS~3.JPG
8dbc7cc7a3feb7b8fde8edeeaa268c2a  Tes  t01-WIN\Program Files \Roxio\WinOnCD\Images\bck
                                            \canvas_dark_blue.jpg
8dbc7cc7a3feb7b8fde8edeeaa268c2a  Test02  -DOS\PROGRA~1\ROXIO\WINONCD\IMAGES\BCK
                                            \CANVAS~3.JPG
8dbc7cc7a3feb7b8fde8edeeaa268c2a  Test02  -WIN\Program Files \Roxio\WinOnCD\Images\bck
                                            \canvas_da rk_blue.jpg
8dbc7cc7a3feb7b8fde8edeeaa268c2a  Test03  -DOS\LOSTFILE\DIR5\ROXIO\WINONCD\IMAGES\BCK
                                            \CANVAS~3.JPG
8dbc7cc7a3feb7b8fde8edeeaa268c2a  Test03  -WIN\LOSTFILE\DIR5\Roxio\WinOnCD\Images\bck
                                            \canvas_dark_blue.jpg
8dbc7cc7a3feb7b8fde8edeeaa268c2a  Test04  -DOS\LOSTFILE\DIR5\ROXIO\WINONCD\IMAGES\BCK
                                            \CANVAS~3.JPG
8dbc7cc7a3feb7b8fde8edeeaa268c2a  Test04  -WIN\LOSTFILE\DIR5\Roxio\WinOnCD\Images\bck
                                            \canvas_dark_blue.jpg

4ad2cfd5c73029961fcbfb5b7330996d  Original  \msexcel.xls
4ad2cfd5c73029961fcbfb5b7330996d  Te  st01-DOS\PROGRA~1\QUICKV~1\SAMPLES\MSEXCEL.XLS
4ad2cfd5c73029961fcbfb5b7330996d  Test01  -WIN\Program Files \Quick View Plus \SAMPLES
                                            \msexcel.xls
4ad2cfd5c73029961fcbfb5b7330996d  Test02  -DOS\PROGRA~1\QUICKV~1\SAMPLES\MSEXCEL.XLS
4ad2cfd5c73029961fcbfb5b733099  6d  Test02-WIN\Program Files \Quick View Plus \SAMPLES
                                            \msexcel.xls
```

```
4ad2cfd5c73029961fcbfb5b7330996d  Test03  -DOS\LOSTFILE\DIR5\QUICKV~1\SAMPLES
                                    \MSEXCEL.XLS
4ad2cfd5c73029961fcbfb5b7330996d  Test03  -WIN\LOSTFILE\DIR5\Quick View Plus\SAMPLES
                                    \msexcel.xls
4ad2c fd5c73029961fcbfb5b7330996d  Test04  -DOS\LOSTFILE\DIR5\QUICKV~1\SAMPLES
                                    \MSEXCEL.XLS
4ad2cfd5c73029961fcbfb5b7330996d  Test04  -WIN\LOSTFILE\DIR5\Quick View Plus\SAMPLES
                                    \msexcel.xls

4caf30766db0bc9eaf133e46049b41b6  Original  \powerpt.ppt
4caf30766db0bc9eaf13 3e46049b41b6   Test01-DOS\PROGRA~1\QUICKV~1\SAMPLES\POWERPT.PPT
4caf30766db0bc9eaf133e46049b41b6  Test01  -WIN\Program Files\Quick View Plus\SAMPLES
                                    \powerpt.ppt
4caf30766db0bc9eaf133e46049b41b6  Test02  -DOS\PROGRA~1\QUICKV~1\SAMPLES\POWERPT.PPT
4caf30766db0bc 9eaf133e46049b41b6  Test02 -WIN\Program Files\Quick View Plus\SAMPLES
                                    \powerpt.ppt
4caf30766db0bc9eaf133e46049b41b6  Test03  -DOS\LOSTFILE\DIR5\QUICKV~1\SAMPLES
                                    \POWERPT.PPT
4caf30766db0bc9eaf133e46049b41b6  Test03  -WIN\LOSTFILE\DIR5\Quick View Plus\SAMPLES
                                    \powerpt.ppt
4caf30766db0bc9eaf133e46049b41b6  Test04  -DOS\LOSTFILE\DIR5\QUICKV~1\SAMPLES
                                    \POWERPT.PPT
4caf30766db0bc9eaf133e46049b41b6  Test04  -WIN\LOSTFILE\DIR5\Quick View Plus\SAMPLES
                                    \powerpt.ppt

6cff95aa45756531484c7f760f9fe1f3  Original  \history.txt
6cff95aa45756531484c7f760f9fe1f3  Test01  -DOS\UTILS\DN\DOC\ENGLISH\HISTORY.TXT
6cff95aa45756531484c7f760f9fe1f3  Test01  -WIN\UTILS\dn\doc\english\history.txt
6cff95aa45756531484c7f760f9fe1f3  Test02  -DOS\UTILS\DN\DOC\ENGLISH\HISTORY.TXT
6cff95aa45756531484c7f760f 9fe1f3  Test02 -WIN\UTILS\dn\doc\english\history.txt
6cff95aa45756531484c7f760f9fe1f3  Test03  -DOS\LOSTFILE\DIR0\DN\DOC\ENGLISH
                                    \HISTORY.TXT
6cff95aa45756531484c7f760f9fe1f3  Test03  -WIN\LOSTFILE\DIR0\dn\doc\english
                                    \history.txt
6cff95aa45756531484c7f760f9fe1 f3  Test04-DOS\LOSTFILE\DIR0\DN\DOC\ENGLISH
                                    \HISTORY.TXT
6cff95aa45756531484c7f760f9fe1f3  Test04  -WIN\LOSTFILE\DIR0\dn\doc\english
                                    \history.txt

358f5f9aaa7b576bb4fe74ce6e61323c  Original  \AcroRd32.exe
358f5f9aaa7b576bb4fe74ce6e61323c  Test01  -DOS\PROGRA~1\ADOBE\ACROBA~2.0\READER
                                    \ACRORD32.EXE
358f5f9aaa7b576bb4fe74ce6e61323c  Test01  -WIN\Program Files\Adobe\Acrobat 5.0\Reader
                                    \AcroRd32.exe
358f5f9aaa7b576bb4fe74ce6e61323c  Test02  -DOS\PROGRA~1\ADOBE\ACROBA~2.0\READER
                                    \ACRORD32.EXE
358f5f9aaa7b576bb4fe74ce6e613 23c  Test02-WIN\Program Files\Adobe\Acrobat 5.0\Reader
                                    \AcroRd32.exe
358f5f9aaa7b576bb4fe74ce6e61323c  Test03  -DOS\LOSTFILE\DIR5\ADOBE\ACROBA~2.0\READER
                                    \ACRORD32.EXE
358f5f9aaa7b576bb4fe74ce6e61323c  Test03  -WIN\LOSTFILE\DIR5\Adobe\Acrobat 5.0\Reader
                                    \AcroRd32.exe
358f5f9aaa7b576bb4fe74ce6e61323c  Test04  -DOS\LOSTFILE\DIR5\ADOBE\ACROBA~2.0\READER
                                    \ACRORD32.EXE
358f5f9aaa7b576bb4fe74ce6e61323c  Test04  -WIN\LOSTFILE\DIR5\Adobe\Acrobat 5.0\Reader
                                    \AcroRd32.exe

5ba55680533727e153606947ae026286  Original  \4DOS.COM
5ba55680533727e153606947ae026286  Test01  -DOS\DOS\_DOS.COM
5ba55680533727e153606947ae026286  Test01  -WIN\dos\_DOS.COM
5ba55680533727e153606947ae026286  Test02  -DOS\DOS\_DOS.COM
5ba55680533727e153606947ae026286  Test02  -WIN\dos\_DOS.COM
5ba55680533727e153606947 ae026286  Test03-DOS\LOSTFILE\DIR17\_DOS.COM
5ba55680533727e153606947ae026286  Test03  -WIN\LOSTFILE\DIR17\_DOS.COM
5ba55680533727e153606947ae026286  Test04  -DOS\LOSTFILE\DIR17\_DOS.COM
5ba55680533727e153606947ae026286  Test04  -WIN\LOSTFILE\DIR17\_DOS.COM
```

Appendix 14: NTFS HDD MD5 Value Result Summary

```
Test01-DOS\MD5Before.txt
c2ea8a2e7f563163828d149235d5ab85  /dev/hdc

Test01-DOS\MD5After.txt
c2ea8a2e7f563163828d149235d5ab85  /dev/hdc1
```

```
Test01-WIN\MD5Before.txt
c2ea8a2e7f563163828d149235d5ab85  /dev/hdc

Test01-WIN\MD5After.txt
c2ea8a2e7f563163828d149235d5ab85  /dev/hdc1

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

```
Test02-DOS\MD5Before.txt
8b4f2fea9d0aee07642313f51b484b4d  /dev/hdc

Test02-DOS\MD5After.txt
8b4f2fea9d0aee07642313f51b484b4d  /dev/hdc
```

```
Test02-WIN\MD5Before.txt
8b4f2fea9d0aee07642313f51b484b4d  /dev/hdc

Test02-WIN\MD5After.txt
8b4f2fea9d0aee07642313f51b484b4d  /dev/hdc

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

```
Test03-DOS\MD5Before.txt
cec00bea7f9ac1eb9ea02c25db63c334  /dev/hdc

Test03-DOS\MD5After.txt
cec00bea7f9ac1eb9ea02c25db63c334  /dev/hdc
```

```
Test03-WIN\MD5Before.txt
cec00bea7f9ac1eb9ea02c25db63c334  /dev/hdc

Test03-WIN\MD5After.txt
cec00bea7f9ac1eb9ea02c25db63c334  /dev/hdc

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

```
Test04-DOS\MD5Before.txt
914654a4ae8d5d3569f27325ccb75d22  /dev/hdc

Test04-DOS\MD5Before.txt
914654a4ae8d5d3569f27325ccb75d22  /dev/hdc
```

```
Test04-WIN\MD5Before.txt
914654a4ae8d5d3569f27325ccb75d22  /dev/hdc

Test04-WIN\MD5After.txt
f9ddcf054bdd25f7f85185b64afea735  /dev/hdc
```

Appendix 15: NTFS Files MD5 Value Result Summary

```
5fea57f2a1546bc391c6b9cb1bbfc452  Original  \SN.ZIP
5fea57f2a1546bc391c6b9cb1bbfc452  Test01  -DOS\DOWNLOAD\SN.ZIP
5fea57f2a1546bc391c6b9cb1bbfc452  Test01  -WIN\Download\sn.zip
5fea57f2a1546 bc391c6b9cb1bbfc452  Test02  -DOS\DOWNLOAD\SN.ZIP
5fea57f2a1546bc391c6b9cb1bbfc452  Test02  -WIN\Download\sn.zip
5fea57f2a1546bc391c6b9cb1bbfc452  Test03  -DOS\LOSTFILE\DIR218\SN.ZIP
5fea57f2a1546bc391c6b9cb1bbfc452  Test03  -WIN\LOSTFILE\DIR213\sn.zip
5fea57f2a15 46bc391c6b9cb1bbfc452  Test04  -DOS\LOSTFILE\DIR218\SN.ZIP
5fea57f2a1546bc391c6b9cb1bbfc452  Test04  -WIN\LOSTFILE\DIR213\sn.zip

5a599350b5a46e56b9a4105fa4dd34bb  Original  \CacheSentryWindowTips.gif
5a599350b5a46e56b9a4105fa4dd34bb  Test01  -DOS\PROGRA~1\CACHES~2\DOCS\CACHES~4.GIF
5a599350b5a46e56b9a4105fa4dd34bb  Test01  -WIN\Program Files\CacheSentry\Docs
                                            \CacheSentryWindowTips.gif
5a599350b5a46e56b9a4105fa4dd34bb  Test02  -DOS\PROGRA~1\CACHES~2\DOCS\CACHES~4.GIF
5a599350b5a46e56b9a4105fa4dd34bb  Test02  -WIN\Program Files\CacheSentry\Docs
                                            \CacheSentryWindowTips.gif
5a599350b5a46e56b9a4105fa4dd34bb  Test03  -DOS\LOSTFILE\DIR23\CACHES~2\DOCS
                                            \CACHES~4.GIF
5a599350b5a46e56b9a4105fa4dd34bb  Test03  -WIN\LOSTFILE\DIR23\CacheSentry\Docs
                                            \CacheSentryWindowTips.gif
5a599350b5a46 e56b9a4105fa4dd34bb  Test04  -DOS\LOSTFILE\DIR23\CACHES~2\DOCS
                                            \CACHES~4.GIF
5a599350b5a46e56b9a4105fa4dd34bb  Test04  -WIN\LOSTFILE\DIR23\CacheSentry\Docs
                                            \CacheSentryWindowTips.gif

89138783d69b7d7d8fbb86224bd1342a  Original  \msword2.doc
89138783d69b7d7d8fbb8 6224bd1342a  Test01 -DOS\PROGRA~1\QUICKV~1\SAMPLES\MSWORD2.DOC
89138783d69b7d7d8fbb86224bd1342a  Test01  -WIN\Program Files\Quick View  Plus\SAMPLES
                                            \msword2.doc
89138783d69b7d7d8fbb86224bd1342a  Test02  -DOS\PROGRA~1\QUICKV~1\SAMPLES\MSWORD2.DOC
89138783d69b7d7 d8fbb86224bd1342a  Test02 -WIN\Program Files\Quick View Plus\SAMPLES
                                            \msword2.doc
89138783d69b7d7d8fbb86224bd1342a  Test03  -DOS\LOSTFILE\DIR82\MSWORD2.DOC
89138783d69b7d7d8fbb86224bd1342a  Test03  -WIN\LOSTFILE\DIR82\msword2.doc
89138783d69b7d7d8fbb86224bd1342  a  Test04 -DOS\LOSTFILE\DIR82\MSWORD2.DOC
89138783d69b7d7d8fbb86224bd1342a  Test04  -WIN\LOSTFILE\DIR82\msword2.doc

a0565cb3cfc82ccb3509800f8ccab22b  Original  \Leaf.JPG
a0565cb3cfc82ccb3509800f8ccab22b  Test01  -DOS\PROGRA~1\GPSOFT~1\DIRECT~1\IMAGES
                                            \LEAF.JPG
a0565cb3cfc82ccb3509800f8ccab22b  Test01  -WIN\Program Files\GPSoftware\Directory
                                            Opus\Images\Leaf.JPG
a0565cb3cfc82ccb3509800f8ccab22b  Test02  -DOS\PROGRA~1\GPSOFT~1\DIRECT~1\IMAGES
                                            \LEAF.JPG
a0565cb3cfc82ccb3509800f8ccab22b  Test02  -WIN\Program Files\GPSoftwa re\Directory
                                            Opus\Images\Leaf.JPG
a0565cb3cfc82ccb3509800f8ccab22b  Test03  -DOS\LOSTFILE\DIR51\LEAF.JPG
a0565cb3cfc82ccb3509800f8ccab22b  Test03  -WIN\LOSTFILE\DIR51\Leaf.JPG
a0565cb3cfc82ccb3509800f8ccab22b  Test04  -DOS\LOSTFILE\DIR51\LEAF.JPG
a0565cb3cfc82cc b3509800f8ccab22b  Test04  -WIN\LOSTFILE\DIR51\Leaf.JPG

4ad2cfd5c73029961fcbfb5b7330996d  Original  \msexcel.xls
4ad2cfd5c73029961fcbfb5b7330996d  Test01  -DOS\PROGRA~1\QUICKV~1\SAMPLES\MSEXCEL.XLS
4ad2cfd5c73029961fcbfb5b7330996d  Test01  -WIN\Program Files\Quick View Plus\SAMPLES
                                            \msexcel.xls
4ad2cfd5c73029961fcbfb5b7330996d  Test02  -DOS\PROGRA~1\QUICKV~1\SAMPLES\MSEXCEL.XLS
4ad2cfd5c73029961fcbfb5b7330996d  Test02  -WIN\Program Files\Quick View Plus\SAMPLES
                                            \msexcel.xls
4ad2cfd5c73029961fcbfb5b7330996d  Test03  -DOS\LOSTFILE\DIR82\MSEXCEL.XLS
4ad2cfd5c73029961fcbfb5b7330996d  Test03  -WIN\LOSTFILE\DIR82\msexcel.xls
4ad2cfd5c73029961fcbfb5b7330996d  Test04  -DOS\LOSTFILE\DIR82\MSEXCEL.XLS
4ad2cfd5c73029961fcbfb5b7330996d  Test04  -WIN\LOSTFILE\DIR82\msexcel.xls

4caf30766db 0bc9eaf133e46049b41b6  Original  \powerpt.ppt
```

```
4caf30766db0bc9eaf133e46049b41b6  Test01  -DOS\PROGRA~1\QUICKV~1\SAMPLES\POWERPT.PPT
4caf30766db0bc9eaf133e46049b41b6  Test01  -WIN\Program Files\Quick View Plus\SAMPLES
                                    \powerpt.ppt
4caf30766db0bc9eaf133e46049b41b6  Test02  -DOS\PROGRA~1\QUICKV~1\SAMPLES\POWERPT.PPT
4caf30766db0bc9eaf133e46049b41b6  Test02  -WIN\Program Files\Quick View Plus\SAMPLES
                                    \powerpt.ppt
4caf30766db0bc9eaf133e46049b41b6  Test03  -DOS\LOSTFILE\DIR82\POWERPT.PPT
4caf30766db0bc9eaf133e46049b41b6  Test03  -WIN\LOSTFILE\DIR82\powerpt.ppt
4caf30766db0bc9eaf133e46049b41b6  Test04  -DOS\LOSTFILE\DIR82\POWERPT.PPT
4caf30766db0bc9eaf133e46049b41b6  Test04  -WIN\LOSTFILE\DIR82\powerpt.ppt

65bf77fc5199fe3711f43cae10248d05  Original  \TCMD32.TXT
65bf77fc5199fe3711f43cae10248d05  Test01  -DOS\DOS\TCMD32.TXT
65bf77fc5199fe3711f43cae10248d05  Test01  -WIN\DOS\TCMD32.TXT
65bf77fc5199fe3711f43cae10248d05  Test02  -DOS\DOS\TCMD32.TXT
65bf77fc5199fe3711f43cae10248d05  Test02  -WIN\DOS\TCMD32.TXT
65bf77fc5199fe3711f43cae10248d05  Test03  -DOS\DOS\TCMD32.TXT
65bf77fc5199fe3711f43cae10248d05  Test03  -WIN\DOS\TCMD32.TXT
65bf77fc5199fe3711f43cae10248d05  Test04  -DOS\DOS\TCMD32.TXT
65bf77fc5199fe3711f43cae10248d05  Test04  -WIN\DOS\TCMD32.TXT

ba9a26a090809162ee06d6688f0ed4cf  Original  \AcroRd32.exe
ba9a26a090809162ee06d6688f0ed4cf  Test01  -DOS\PROGRA~1\ADOBE\ACROBA~1.0\READER
                                    \ACRORD32.EXE
ba9a26a090809162ee06d6688f0ed4cf  Test01  -WIN\Program Files\Adobe\Acrobat 5.0\Reader
                                    \AcroRd32.exe
ba9a26a090809162ee06d6688f0ed4cf  Test02  -DOS\PROGRA~1\ADOBE\ACROBA~1.0\READER
                                    \ACRORD32.EXE
ba9a26a090809162ee06d6688f0ed4cf  Test02  -WIN\Program Files\Adobe\Acrobat 5.0\Reader
                                    \AcroRd32.exe
ba9a26a090809162ee06d6688f0ed4cf  Test03  -DOS\LOSTFILE\DIR160\ACRORD32.EXE
ba9a26a090809162ee06d6688f0ed4cf  Test03  -WIN\LOSTFILE\DIR159\AcroRd32.exe
ba9a26a090809162ee06d6688f0ed4cf  Test04  -DOS\LOSTFILE\DIR160\ACRORD32.EXE
ba9a26a090809162ee06d6688f0ed4cf  Test04  -WIN\LOSTFILE\DIR159\AcroRd32.exe

09fa40b1080e0b3a66f07adf5ba05917  Original  \4DOS.COM
09fa40b1080e0b3a66f07adf5ba05917  Test01  -DOS\DOS\4DOS.COM
09fa40b1080e0b3a66f07adf5ba05917  Test01  -WIN\DOS\4DOS.COM
09fa40b1080e0b3a66f07adf5ba05917  Test02  -DOS\DOS\4DOS.COM
09fa40b1080e0b3a66f07adf5ba05917  Test02  -WIN\DOS\4DOS.COM
09fa40b1080e0b3a66f07adf5ba05917  Test03  -DOS\DOS\4DOS.COM
09fa40b1080e0b3a66f07adf5ba05917  Test03  -WIN\DOS\4DOS.COM
09fa40b1080e0b3a66f07adf5ba05917  Test04  -DOS\DOS\4DOS.COM
09fa40b1080e0b3a66f07adf5ba05917  Test04  -WIN\DOS\4DOS.COM
```

Appendix 16: Case Result Summary

HDD MD5 Values

```
Case-DOS\MD5Before.txt
df4ef4731722ba722065a68528ace0a9  /dev/hdc

Case-DOS\MD5After.txt
df4ef4731722ba722065a68528ace0a9  /dev/hdc

Case-WIN\MD5Before.txt
df4ef4731722ba722065a68528ace0a9  /dev/hdc

Case-WIN\MD5After.txt
df4ef4731722ba722065a68528ace0a9  /dev/hdc
```

Files MD5 Values

```
2e1b9f2ee6e409ca818d7d81394c2a0c    \CASE-DOS\DOCUME~1\LIMSR\MYDOCU~1\BACKUP
                                    \ACCESS~2.ZIP
2e1b9f2ee6e409ca818d7d81394c2a0c    \CASE-WIN\Documents and Settings \limsr\My
                                    Documents\backup\access_july2002.zip

733d61834b28edb24f221555a9ec6d84    \CASE-DOS\DOCUME~1\LIMSR\MYDOCU~1\BACKUP
                                    \ACCESS~1.ZIP
733d61834b28edb24f221555a9ec6d84    \CASE-WIN\Documents and Settings \limsr\My
                                    Documents\backup\access_sep2002.zip
```

Reference

[1] GCFA: GIAC Computer Forensic Analyst. URL: http://www .giac.org/GCFA.php (January 2003)

[2] SANS (SysAdmin, Audit, Network, Security) Institute. URL: http://www.sans.org (January 2003)

[3] Microsoft Corporation. URL: http://www.microsoft.com (January 2003)

[4] Knoppix Live – Linux on CD. URL: http://www.knoppix.de (January 2003)

[5] Project Loki: ICMP Tunneling, Phrack Magazine Volume 7, Issue 49 August, 1996, file 06 of 16. URL: http://www.phrack.org/show.php?p=49&a=6 (January 2003)

[6] ICMP: Crafting and other uses. URL: http://www.giac.org/practical /STUART_THOMAS_G SEC.doc (January 2003)

[7] Northcutt Stephen, Novak, Judy. "Network Intrusion Detection, An Analyst's Handbook, Second Edition", New Riders, September 2000 - page 63 Malicious ICMP Activity (January 2003)

[8] Introduction To The Internet Control Message Protoc ol. URL: http://www.firewall.cx/icmp -intro.php (April 2003)

[9] What is tunneling. URL: http://www.zensecurity.co.uk/whatis/WhatIs.asp?URL=tunneling (April 2003)

[10] GCC (C compiler). URL: http://gcc.gnu.org (January 2003)

[11] RetHat Linux. URL: http://www.redha t.com (January 2003)

[12] Norton Ghost. URL: http://www.symantec.com/sabu/ghost/ghost_personal/ (February 2003)

[13] Symantec Corparation. URL: http://www.symantec.com (January 2003)

[14] LOKI2 (the implementation), Phrack Magazine Volume 7, Issue 51 September 01, 1997, article 06 of 17. URL: http://www.phrack.org/show.php?p=51&a=6 (January 2003)

[15] Extraction Utility, Phrack Magazine Volume 7, Issue 51 September 01, 1997, article 17 of 17. URL: http://www.phrack.org/show.php?p=51&a=17 (January 2003)

[16] .:[PACKET STOR M]:. URL: http://packetstormsecurity.nl/crypt/misc/ (January 2003)

[17] Computer Crimes Bill 1997 . URL: http://www.mycert.org.my/bill/crime.html (January 2003)

[18] AXCEL216's Glossary. URL: http://members.aol.com/axcel216/glossary.htm (March 2003)

[19] File System Identifiers . URL: http://www.maverick -os.dk/FileSystemFormats /FileSystemIdentifiers.html (March 2003)

[20] File System FAT16, FAT32 and NTFS. URL: http://www.alphastandard.net/os2.htm (March 2003)

[21] Ontrack Inc. URL: http://www.ontrack.com (February 2003)

[22] EasyRecovery Professional. URL: http://www.ontrack.com/easyrecovery/ (February 2003)

[23] EasyRecovery Professional features. URL: http://www.ontrack.com/easyrecovery /info.asp#erpro (February 2003)

[24] MD5 Definition. URL: http://searchsecurity.techtarget.com /sDefinition /0,,sid14_gci527453,00.html (March 2003)

[25] Partition Magic. URL: http://www.powerquest.com/partitionmagic/ (February 2003)

[26] Powerquest Corporation. URL: http://www.powerquest.com/ (February 2003)

[27] EnCase by GuidanceSoftware. URL: http://www. guidancesoftware.com/products/software /efev4/index.shtm (March 2003)

[28] WinZip - the archive utility for windows. URL: http://www.winzip.com (February 2003)

[29] Overview of common filesystems. URL: http://my.execpc.com/CE/AC/geezer/osd/fs /index.htm#overview (March 2003)

[30] Laws of Malaysia, Criminal Procedure Code, Penal Code and Evidence Act ,MDC publishers printers Sdn Bhd, 1996 page 19 (January 2003)

[31] Communication and Multimedia Act 1998. URL: http://www.mcmc.gov.my/mcmc/the_law /ViewAct.asp?lg=e&arid=90 0722 (January 2003)

[32] Laws of Malaysia, Criminal Procedure Code, Penal Code and Evidence Act ,MDC publishers printers Sdn Bhd, 1996 pg 394 (January 2003)