Global Information Assurance Certification Paper

A Forensic Validation of ils and icat

GCFA Practical Assignment
Version 1.3

David Gabler
Submitted 08/10/2003

Abstract
This paper discusses a forensic investigation into an unknown binary, the validation of two forensic tools, 'ils' and 'icat', and a question/answer about how the Electronic Communications Privacy Act applies to a public Internet Service Provider. The forensic investigation into the binary was done through the use of a mixed environment of Red Hat Linux 8.0 and Microsoft Windows XP. It was discovered that the unknown binary had two purposes. The first purpose was to install a service that started with the computer. This service attempted to execute another binary, smsses.exe. Secondly the binary provides a means for covert channel communication. This finding shows that covert channels are out in the wild and are not something that is only talked about but not implemented. The validation was able to determine that 'ils' and 'icat' are forensically sound in their methods and their output. These findings are important because they can be used, in part, for building a library of forensic tools that have been validated as forensically sound. The Electronic Communications Privacy Act questions and answers bring further understanding to the complex nature of the Act itself.

Part 1 - Analyze an Unknown Binary

The purpose of this section is show that as an investigator you have the ability to take an unknown binary file and determine what the purpose of that file would be. As an investigator there will be a time when you will be tasked with analyzing a file that has never before been seen in an investigative circle. The proper analysis of such a file has the potential to either solve a case or make clear exactly what an intruder has done on a system.

Throughout this section, there are grey boxes containing text. Typically, these boxes will contain example Unix commands. Alternatively, they will contain a Unix command and the output from that command. The purpose of them is to call your attention to the specific command(s) and possibly their output.

Binary Details

Program Name and MACTime

The file name of the program that was given for analysis is target2.exe. Basic information about this file: size, owner, **M**odification date, last **A**ccessed date and **C**hange/**C**reation date (MACTime), was retrieved with a Perl[1] script[2], Mac.pl, written by H. Carvey. Using the executable file, provided on the SANS System Forensics, Investigation and Response class CD-ROM[3] created from H. Carvey's Perl script, and redirecting the output through grep[4], specific information about the binary was retrieved. Below is the MACTime information of the unknown binary.

[1] http://www.perl.com
[2] http://patriot.net/~carvdawg/scripts/mac.pl
[3] Handed out at the SANS System Forensics, Investigation and Response class held in San Diego CA, March 7-12, 2003.
[4] http://www.gnu.org/software/grep/grep.html

```
D:\response_kit\win2k_xp>mac.exe -d c:\ | grep.exe target2.exe

MAC.pl
Collect MAC times and owner from files in a directory.

Usage: [perl] mac.pl [-d dir] [-s] [-h/?] [> myfile.csv]
  -d   Directory to search.  May be a mapped dir, or UNC path
       (default: current working directory)
  -s   Check subdirectories

By default, search starts at current dir, looking at all files.
NOTE: Beginning and end of search are timestamped.  Output is in CSV format
      for easy opening in Excel.

Copyright 2000/2001 H. Carvey  keydet89@yahoo.com.
c:\\target2.exe,26793,TEXTBOX\Administrator,Tue May 27 20:45:19 2003,Thu Feb 20
12:45:48 2003,Mon May 19 20:45:17 2003

D:\response_kit\win2k_xp>
```

As can be seen in the above output, the file size of the unknown binary, target2.exe, is 26793 Bytes. The MAC times, -7 hours offset from UTC[5], are:

- **M**odify: Tue May 27 20:45:19 2003
- **A**ccessed: Thu Feb 20 12:45:48 2003
- **C**hanged/**C**reated: Mon May 19 20:45:17 2003.

The C time in this case is most likely the Change time not the Created time. This assumption is made because the C time is later than the Modify time and a file can not be Modified before it is Created. One must keep in mind however that these timestamps should not be considered infallible, as they can be modified by a variety of tools[6]. Although Mac.pl states that the C time is Creation time in its header field, the documentation from the underlying compiler/scripting language, Perl, states that the C time may not be the inode[7] change time but the creation time. (Perlfunc)

File Owner

The owner of the file is the local administrator. More specifically, the owner is TEXTBOX\Administrator, where TEXTBOX is the name of the local Windows XP instance.

[5] http://aa.usno.navy.mil/faq/docs/UT.html
[6] For example http://www.bykeyword.com/pages/detail11/download-11868.html
[7] http://www.webopedia.com/TERM/I/inode.html

MD5 Hash

The MD5 hash[8] of the file target2.exe is: 848903a92843895f3ba7fb77f02f9bf1
A screen capture of the MD5 hash can be seen below in Figure 1

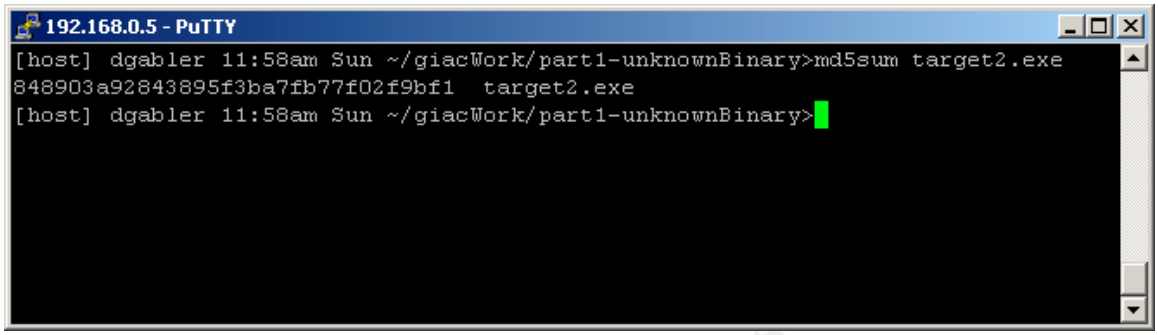

Figure 1 - MD5 hash of target2.exe

Key Words

The following command was used to retrieve the strings from the binary. The '-a' option retrieves all strings. This option will produce a tremendous amount of output that will likely give you more useless information than clues. However, without using this option, the clues that are discovered would not have been retrieved.

```
[host] dgabler 8:08pm Mon ~/giacWork/part1-unknownBinary>strings -a target2.exe
```

All of the helpful strings within target2.exe are listed in Appendix A. Strings that were meaningful are:

- ========== Icmp BackDoor V0.1 ==========
- ========= Code by Spoof. Enjoy Yourself!
- Your PassWord:
- loki
- impossibile creare raw ICMP socket
- CreateService failed:%d
- Hello from MFC!
- smsses.exe
- cmd.exe
- -i (determined to be of interest at a later point in the analysis)

[8] http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html

- -d (determined to be of interest at a later point in the analysis)

Other Information

The Unix utility 'zipinfo'[9] was also used to determine whether or not the archive itself contained any more information that could be used to further the investigation. The command that was used and its output follows:

[9] http://linuxcommand.org/man_pages/zipinfo1.html

```
[root@localhost root]# zipinfo -v binary_v1.3.zip
Archive:  binary_v1.3.zip   5687 bytes   1 file

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

  Actual offset of end-of-central-dir record:        5665 (00001621h)
  Expected offset of end-of-central-dir record:      5665 (00001621h)
  (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 1 entry.  The central directory is 57
  (00000039h) bytes long, and its (expected) offset in bytes from the
  beginning of the zipfile is 5608 (000015E8h).

  There is no zipfile comment.

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

  target2.exe

  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):            2003 Feb 20 12:45:48
  32-bit CRC value (hex):                           d185fd18
  compressed size:                                  5567 bytes
  uncompressed size:                                26793 bytes
  length of filename:                               11 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:               81FF00 hex
  MS-DOS file attributes (20 hex):                  arc

  There is no file comment.
```

Unfortunately the information produced by zipinfo was not able to provide any information to further the investigation. This is because much of this information was already discovered. However, it did reveal very detailed information about the archive and the contents of the file in that archive. Although the information from zipinfo was not considered useful, it is important to note that it is better to check for potentially useful information and not find any than to not check and miss it.

Program Description

Program Type and Use

The program, target2.exe, appears to be an ICMP[10] covert channel[11] program. The program uses ICMP packets[12] to communicate covertly. The program also installs a Microsoft Windows service[13], which has the goal of executing an additional unknown binary, smsses.exe. It appears that this binary, target2.exe, is part of a toolkit to assist in the take over of a computer.

Last Use

It is unknown when this tool was last used, however the file, target2.exe, was last modified on Feb 20 at 12:45:48 2003 -0700 and accessed on Feb 20 12:45:48 2003.

Methods and Program Analysis

These conclusions were reached by using both a Microsoft Windows XP[14] and a Red Hat Linux[15] test environment. The test equipment consists of VMware[16] Workstation 3.2.0 build-2330 running two different operating systems as virtual machines. The first virtual machine was a stock Red Hat 8.0 custom installation. This virtual machine is running the 2.4.18-14 kernel. The second Virtual machine was Microsoft Windows XP Professional with no updates or patches applied. After each operating system was configured, they were each suspended using the suspend feature in VMware workstation and their respective directories were named <OS>-master. Copies were then made from these master copies and used for testing.

[10] http://www.webopedia.com/TERM/I/ICMP.html
[11] http://www.sans.org/resources/idfaq/covert_chan.php
[12] http://www.webopedia.com/TERM/P/packet.html
[13] http://www.codeguru.com/cs_network/DotNet200304.html
[14] http://www.microsoft.com/windowsxp/default.asp
[15] http://www.redhat.com/
[16] http://www.vmware.com

The In the first phase, the binary was downloaded to a Unix environment from the Global Information Assurance Certification (GIAC) GIAC Certified Forensic Analysis (GCFA) practical assignment web page and the following steps were preformed on the file:

1. create MD5 hash of the file and take screen capture,
2. verify that the file is a zip archive,
3. determine if the archive has any relevant information,
4. extract the files from the archive,
5. create a MD5 hash of the archive contents and take a screen capture,
6. determine the file type,
7. retrieve the 'strings' from the file.

Next, the archive was copied to the Windows environment and extracted. The following steps detail how this was done:

1. copy unknown binary archive to floppy,
2. copy archive from floppy to the Windows virtual machine,
3. verify the MD5 hash of the copy matches the original,
4. extract the file from the archive,
5. get the MACTimes for the file.

Retrieving the MACTimes for the file in a Windows environment rather than a Unix environment allowed for file permission and ownership information to be retrieved in addition to the MACTimes.

Once all of the information gathering was complete, an analysis of the information was preformed. It was determined from the 'file' command output that the binary was a MS-DOS[17] based program. From the strings output, the meaningful keywords were selected and searched for on the internet in an attempt to locate the source code for the unknown binary. The only results pointed to source code[18] to create an Internet Control Message Protocol (ICMP)[19] covert channel. Nothing was found that matched any closer to the target2.exe binary strings than this code.

Next, the Microsoft Windows XP virtual machine was set up in preparation to run the binary. Two utilities, Filemon[20] and Regmon[21], both free from Sysinternals[22] that watch the file system and system registry for activity were started. Use of these applications allows us to capture most of the 'invisible' or behind the scenes activity. After these utilities were in position to capture data, the binary, target2.exe, was run without any options. When the binary finished running, the

[17] http://www.computerhope.com/msdos.htm#01
[18] http://www.s0ftpj.org/bfi/online/bfi7/bfi07-13.html
[19] http://dictionary.reference.com/search?q=icmp
[20] http://www.sysinternals.com/ntw2k/source/filemon.shtml
[21] http://www.sysinternals.com/ntw2k/source/regmon.shtml
[22] http://www.sysinternals.com

capture was stopped for both Filemon and Regmon. The capture was then saved to disk.

The captures from each Filemon and Regmon give little if any clues as to what is going on. The Filemon log only shows target2.exe loading libraries needed for execution, a log snippet is below.

```
42      2:52:53 PM      target2.exe:796 OPEN    C:\     SUCCESS
Options: Open Directory  Access: Traverse
47      2:52:53 PM      target2.exe:796 OPEN
C:\WINDOWS\System32\WS2_32.dll  SUCCESS Options: Open  Access:
Execute
53      2:52:53 PM      target2.exe:796 OPEN
C:\WINDOWS\System32\WS2HELP.dll SUCCESS Options: Open  Access:
Execute
67      2:52:53 PM      target2.exe:796 OPEN
C:\WINDOWS\System32\MFC42.DLL   SUCCESS Options: Open  Access:
Execute
142     2:52:53 PM      target2.exe:796 OPEN
C:\WINDOWS\System32\MSVCP60.dll SUCCESS Options: Open  Access:
Execute
```

The Regmon log only shows target2.exe opening and reading various registry keys. No writing to registry keys was performed.

After not being able to determine what target2.exe was trying to do, it was loaded into OllyDbg[23], a free shareware decompiler. Once the binary was loaded into the decompiler, two strings that previously not of interest presented themselves as more interesting, '-i' and '-d'. Again, the test environment was prepared. For this next test, a fresh Windows installation was used so that possible remnants from the first test would not affect subsequent ones. In this test, instead of running the binary without any options, it was run with the option '-i test'. This command and its output follows.

[23] http://home.t-online.de/home/Ollydbg/

```
C:\>target2.exe –i test

Create Service Local Partners Access ok!
starting the service <Local Partners Access>...
Starting the service failed!


Error Installing Service

C:\>
```

In the test, with the '-i' option, target2.exe produced some valuable visible output. At this point, Filemon and Regmon were stopped and their capture saved to disk. The output printed by target2.exe from this test appears promising as it is our first lead into what the program is doing. This output prompted a look at the installed services. Since this instantiation of Windows is a VMware virtual machine, a 'clean' instance of the test environment was easily started up. Comparing the services installed on both machines it was noticed that a new service was installed on the machine that the latest test was run on. The display name of the new service is 'Local Printer Manager Service'. At system startup this newly installed service automatically loads a program named 'smsses.exe' as the 'Local System Account'. A screen shot of this service can be seen in Figure 2.

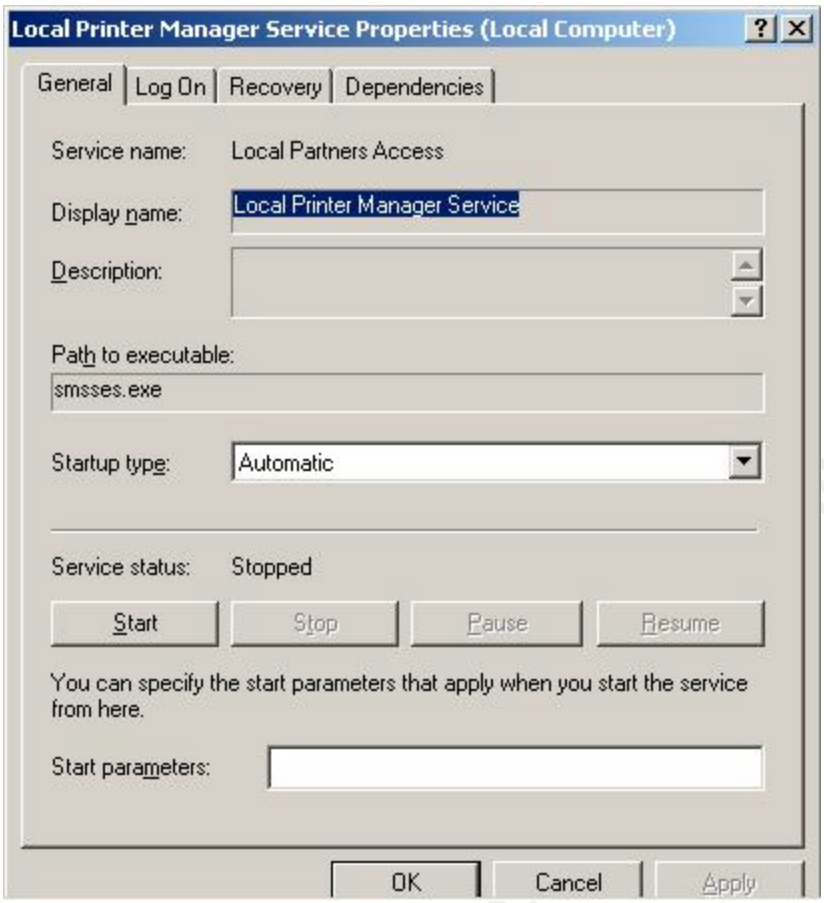

Figure 2 - Service Added by target2.exe

After this service is installed by target2.exe, an attempt is made to start the service. Because the service is trying to run a file that is not present on the system, it cannot be started, hence the 'Starting the service failed!' message when running target2.exe. The failure to start the service is logged by the system in the system log file and can be see in Figure 3

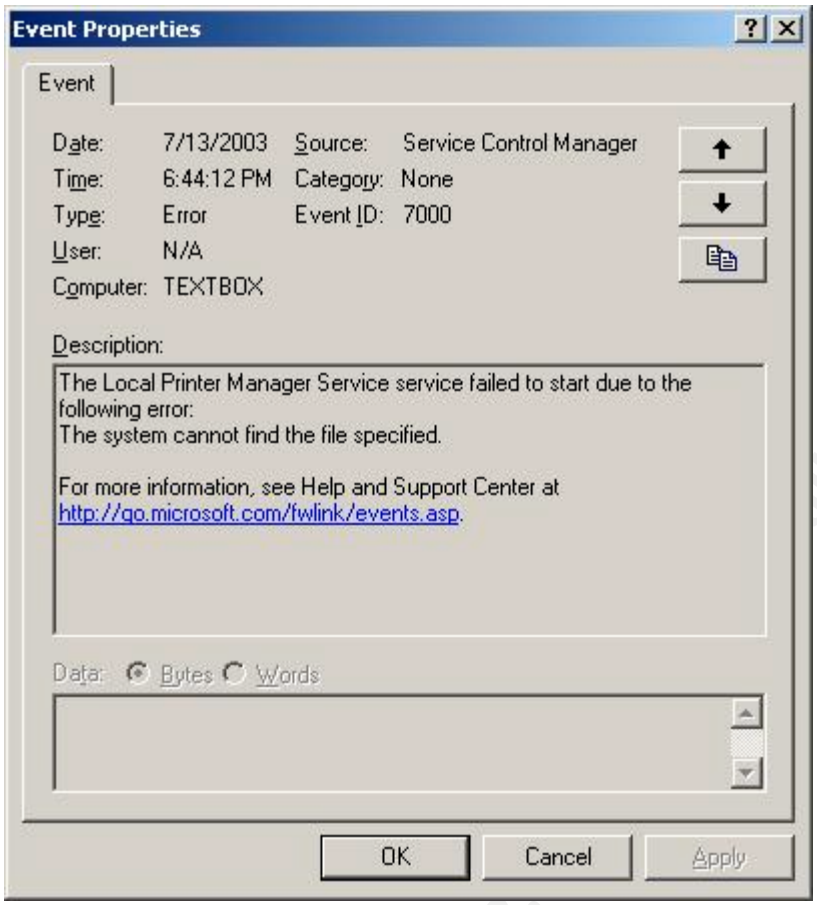

Figure 3 - Event Generated by Added Service

Filemon does not log the creation of the service however, it does capture services.exe logging data to the system.log log file as well as attempting to run smsses.exe. Some Filemon log excerpts depicting the services.exe logging information and attempting to execute smsses.exe are in the following text box.

```
…
98     7:19:34 PM     services.exe:664       SET INFORMATION
C:\WINDOWS\system32\config\system.LOG   SUCCESS Length: 45056
99     7:19:34 PM     services.exe:664       QUERY INFORMATION
C:\WINDOWS\system32\smsses.exe  FILE NOT FOUND  Attributes: Error
100    7:19:34 PM     services.exe:664       QUERY INFORMATION
C:\WINDOWS\system32\smsses.exe  FILE NOT FOUND  Attributes: Error
101    7:19:34 PM     services.exe:664       QUERY INFORMATION
C:\WINDOWS\System32\smsses.exe  FILE NOT FOUND  Attributes: Error
102    7:19:34 PM     services.exe:664       QUERY INFORMATION
C:\WINDOWS\system\smsses.exe    FILE NOT FOUND  Attributes: Error
103    7:19:34 PM     services.exe:664       QUERY INFORMATION
C:\WINDOWS\smsses.exe   FILE NOT FOUND  Attributes: Error
104    7:19:34 PM     services.exe:664       QUERY INFORMATION
C:\WINDOWS\system32\smsses.exe  FILE NOT FOUND  Attributes: Error
105    7:19:34 PM     services.exe:664       QUERY INFORMATION
C:\WINDOWS\smsses.exe   FILE NOT FOUND  Attributes: Error
106    7:19:34 PM     services.exe:664       QUERY INFORMATION
C:\WINDOWS\System32\Wbem\smsses.exe     FILE NOT FOUND  Attributes: Error
…
```

Regmon did not log target2.exe writing any registry keys during the second test however, it does show services.exe creating and writing to keys. The creation and writing of keys can be seen below in the Regmon log excerpts. The keys are created because the 'Local Partners Access' service has been installed.

```
…
63      30.21120835     services.exe:664        OpenKey
HKLM\System\CurrentControlSet\Services  SUCCESS Key: 0xE1138D58
64      30.21367822     services.exe:664        CreateKey
HKLM\System\CurrentControlSet\Services\Local Partners Access    SUCCESS Key:
0xE1138C40
65      30.21377543     services.exe:664        CloseKey
HKLM\System\CurrentControlSet\Services  SUCCESS Key: 0xE1138D58
66      30.21434785     services.exe:664        SetValue
HKLM\System\CurrentControlSet\Services\Local Partners Access\Type       SUCCESS
0x10
67      30.21478031     services.exe:664        SetValue
HKLM\System\CurrentControlSet\Services\Local Partners Access\Start      SUCCESS
0x2
68      30.21511387     services.exe:664        SetValue
HKLM\System\CurrentControlSet\Services\Local Partners Access\ErrorControl
SUCCESS 0x1
69      30.21537201     services.exe:664        SetValue
HKLM\System\CurrentControlSet\Services\Local Partners Access\ImagePath
SUCCESS "smsses.exe"
70      30.21577429     services.exe:664        SetValue
HKLM\System\CurrentControlSet\Services\Local Partners Access\DisplayName
SUCCESS "Local Printer Manager Service"
71      30.21693254     services.exe:664        CreateKey
HKLM\System\CurrentControlSet\Services\Local Partners Access\Security
SUCCESS Key: 0xE115B700
72      30.21726861     services.exe:664        SetValue
HKLM\System\CurrentControlSet\Services\Local Partners Access\Security\Security
SUCCESS 01 00 14 80 90 00 00 00…
...
```

Next target2.exe is run with the other option, -d. The command used and its output is below.

```
C:\>target2.exe -d test

1062


Service UnInstalled Sucessfully

C:\>
```

When using the -d option, the service that was installed with the -i option is uninstalled from the system. Once again, the output contained in the log files shows similar entries as when the binary was executed with the -i option.

Although communication from target2.exe to the system is not seen in Filemon, it can be observed that the process of events is as follows: target2.exe is executed with either the -d or -i option. If the -i option is specified, services.exe adds the service to the local computer and attempt is made to start the service. If, instead, the -d option is specified, the service is removed from the local computer. Lastly, in either case, svchost.exe is executed on the operating system. The purpose of svchost.exe goal is to prepare the installed services for the startup of the system[24]. This is very similar to changing what programs get started at the different run levels[25] on Unix.

The complete log files for Filemon and Regmon can be found in Appendices B, C, D and E.

Forensic Details

Footprints

If target2.exe is run without options there are will not be any footprints[26] left on the file system. When target2.exe is run with the -i option, it installs a service that has the purpose of running the program smsses.exe at system startup. The name of the service installed is 'Local Partners Access'. The display name for the service is 'Local Printer Manager Service'. See Figure 2 for a screen capture of the service.

Files Used

When target2.exe is executed without any options or with the -i option the files that it opens, according to Filemon, are:

- C:\WINDOWS\System32\WS2_32.dll
- C:\WINDOWS\System32\WS2HELP.dll
- C:\WINDOWS\System32\MFC42.DLL
- C:\WINDOWS\System32\MSVCP60.dll

When target2.exe is executed with the -d option the files that it opens, according to Filemon, are:

- C:\WINDOWS\SYSTEM32\ADVAPI32.DLL
- C:\WINDOWS\SYSTEM32\CTYPE.NLS

[24] http://www.igknighttec.com/Windows/WindowsXP/svchost_exe.php
[25] http://www.chicagotribune.com/technology/local/chi-000804finaldebug,0,2948151.story
[26] http://www.catb.org/~esr/jargon/html/F/footprint.html

- C:\WINDOWS\SYSTEM32\GDI32.DLL
- C:\WINDOWS\SYSTEM32\KERNEL32.DLL
- C:\WINDOWS\SYSTEM32\MFC42.DLL
- C:\WINDOWS\SYSTEM32\MSVCP60.DLL
- C:\WINDOWS\SYSTEM32\MSVCRT.DLL
- C:\WINDOWS\SYSTEM32\NTDLL.DLL
- C:\WINDOWS\SYSTEM32\RPCRT4.DLL
- C:\WINDOWS\SYSTEM32\USER32.DLL
- C:\WINDOWS\SYSTEM32\WS2_32.DLL
- C:\WINDOWS\SYSTEM32\WS2HELP.DLL

In either case, with or without options (-i, -d), OllyDbg sees all 11 DLLs as in use.

System files other than listed above are not directly used by target2.exe when the binary is run without options or with the -d or -i options. However, multiple system files are used by the programs that setup and start the services.

Filesystem Changes

The filesystem is changed by the binary, target2.exe, only when it is run with options. These changes are due to the service that is added to or removed from the system. When a service change takes place, the system registry is modified. If a service is being added, multiple keys are created. One 'parent' key created is created under HKLM\System\CurrentControlSet\Services\. The keys here have the name of the services installed on the machine. The key created here is 'Local Partners Access'. Multiple sub keys and values are created under this node. Another location that a 'parent' key is created under is: HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\ROOT\. Here, the key created is not just the service name, but the service name prefixed with 'LEGACY_' and all spaces replaced with underscores. The key created here is 'LEGACY_LOCAL_PARTNERS_ACCESS'. Multiple sub keys and values are here as well. When this service is deleted, the new registry entries are also removed. Because of the service start type, automatic, the system starts the service automatically after it is created. However, since the program that it is configured to execute, smsses.exe, does not exist, an error is logged to disk. This error is shown above in Figure 3,

Leads

Many times there will reside information inside of a binary that can take an investigation in a new direction. Unfortunately, the only item, or lead, that can be retrieved from the binary is what appears to be a password, 'loki'. This is not a very concrete piece of information that could drive an investigation forward however, it could end up being a critical piece of the puzzle latter on. 'Loki' was also the name of the project that came out in Phrack Volume 7 Issue 49 File 6[27].

[27] http://www.2600.com/phrack/p49-06.html

In this issue, the 'covert channel through ICMP' topic was first publicly discussed. This password also becomes more interesting when looking into the binary itself and seeing that it appears to have mechanisms for communication in it. Having a password of loki in conjunction with methods for communication drives home the likelihood that this binary can communicate through covert channels. Part of this capability is highlighted in grey below in Figure 4. Although there appears to be this potential for communication in the binary's code does not mean that this capability is being used correctly or at all. It is simply a call to the c++ function[28] 'socket' in the form of socket(AF_INET, SOCK_RAW, IPPROTO_IP)[29] or similar. There is not proof that this function is being used correctly.

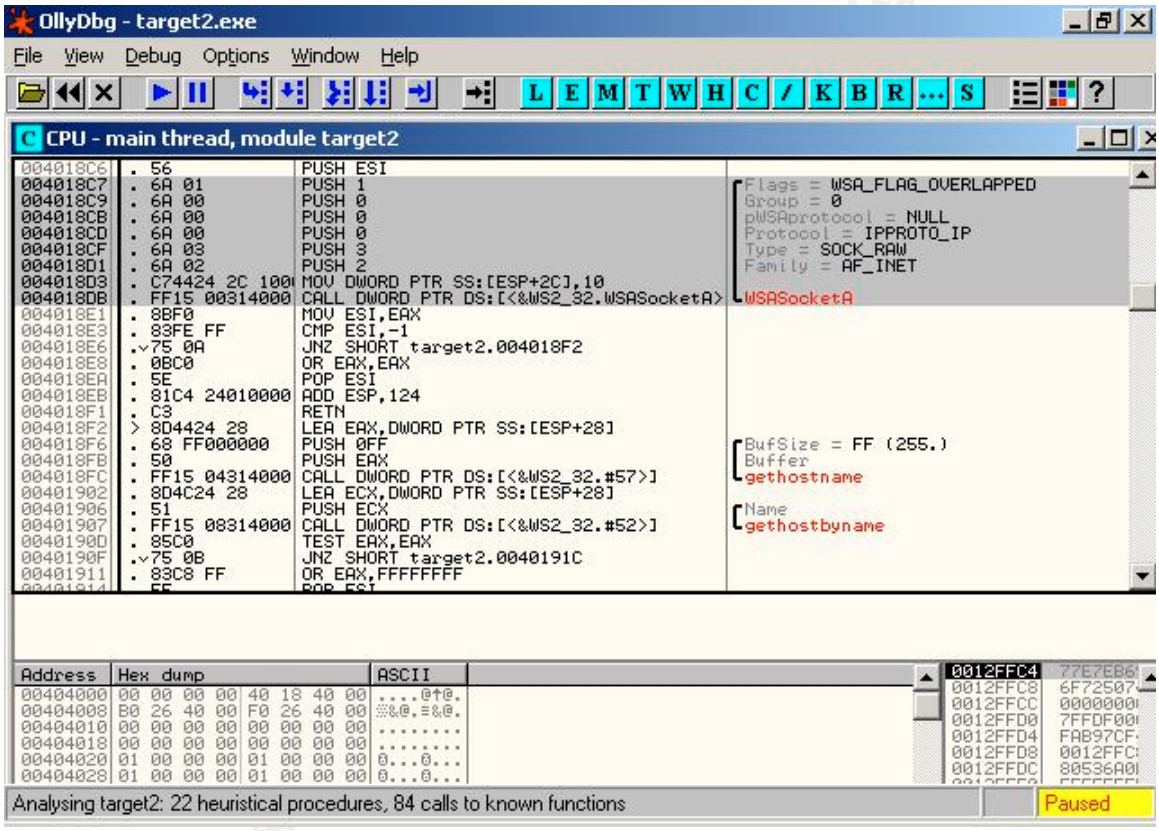

Figure 4 - OllyDbg Screen Capture of Socket Creation

Program Identification

Source code for target2.exe could not be located on the internet however, a program with similar parts was found. After looking through the strings in target2.exe, it appears that it is either written by the same author or is a derivative of the ICMP covert channel program at http://www.s0ftpj.org/bfi/online/bfi7/bfi07-13.html. Both tools contain similar spelling and grammar in their strings. Most likely, the program is a derivative and not coded by the original author because of the 'Hello from MFC!' string found in

[28] http://dictionary.reference.com/search?q=function&r=67 definition 8
[29] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winsock/winsock/socket_2.asp

the target2.exe binary. The string is a stock message[30] from Microsoft from the Visual C++ development environment.

Legal Implications

Due to the variety of laws in place throughout the United States, running programs with a malicious intent provides the victim or government with many legal recourses. In the case of the unknown binary analyzed in this section it is not possible to prove that this program was run without access to the system that it was potentially executed on. The reason that this is that the program does not modify itself during runtime. Running this program would violate multiple internal policies with the organization for which I am employed. These policies include both 'acceptable use' and 'security policies'. Our acceptable use policy states that unapproved software as well as downloaded software is not to be run on company computers with out expressed permission from your supervisor. This program could potentially violate our security policy if it is successful in starting the smsses.exe application. The binary, target2.exe, in and of itself does not violate our security policy because it does not bypass the requirement for administrator-like privileges when creating the service.

Interview Questions

Given the opportunity to perform an interview with the person who installed and executed this binary, the bulleted questions below would be asked. Professionalism is required when performing an interview. The person who is responsible for administering the computer that the binary was discovered on will probably feel personally violated. It is recommended to remove that person from the investigation so that no personal bias could influence the outcome. Have a co-worker or someone independent of the situation perform the interview. That aside, the following are potential interview questions:

- We found this application on Jane's computer the other day. Did you install it?
  - What was the use of that application?
- I imagine you noticed some problems on Jane's computer that she needed help with?
  - What were the specific problems with her computer that she needed help with?
- What were all the capabilities of the application?
- Were there any lag times when using the tool?
- When did you start helping Jane?
- How fast did the program take to setup on Jane's computer?
- Where did you find the tool or did you write it yourself?
  - (If self written) what language did you write it in?
- What privileges does the program require to run?

[30] http://www.visualcomponentlibrary.com/cpp/functions.htm list item 27

Additional Information

The following are some additional links where more information can be found on the topic of covert channels.

- http://www.phrack.org/show.php?p=49&a=6
- http://www.phrack.org/show.php?p=51&a=6
- http://www.if.uidaho.edu/~ghura/Advanced%20network%20surveillance.ppt
- http://www.s0ftpj.org/docs/covert_shells.htm
- http://www.firstmonday.dk/issues/issue2_5/rowland/

Part 2 - Option 2: Perform Forensic Tool Validation

Scope

The purpose of the following tests is to verify that two tools, 'icat'[31] and 'ils'[32], properly present to the investigator correct information about removed files and if that information can be trusted. 'ils' is used by investigators to list inodes[33] on the file system. 'icat' is used to copy information from inodes on the file system. Both tools get their usefulness from the ability to tell and present to an investigator information about and from deleted files. These two tools are a sub-set of tools made available to the investigator through 'The Sleuth Kit'[34], formerly known as TASK[35]. If the output from the tools can be proven to be accurate and reliable, then evidence found by these tools can be entered into a court of law with the knowledge that their output is forensically sound.

After the tools have shown the ability to recover files, their results will be verified in part by a independent tool, debugfs[36]. 'debugfs' is a tool published for debugging Linux ext2[37] and ext3[38] type filesystems.

Throughout this section, there are grey boxes containing text. Typically, these boxes will contain example Unix commands. Alternatively, they will contain a Unix command and the output from that command. The purpose of them is to call your attention to the specific command(s) and possibly their output.

Tool Description

Tools Being Tested

The products that were tested are 'ils' version 1.61 and 'icat' version 1.61. Both of these tools are included in 'The Sleuth Kit.' The author of 'The Sleuth Kit' is Brian Carrier, who based these tools on 'The Coroner's Toolkit.' These tools can be downloaded as part of The Sleuth Kit in source form from http://www.sleuthkit.org/sleuthkit/download.php.

Purpose of Tools

The function of 'ils' is to list the inodes of files on a particular device. A device can be either a physical device, such as a hard disk, or a file, such as a disk

[31] http://www.sleuthkit.org/sleuthkit/man/icat.html
[32] http://www.sleuthkit.org/sleuthkit/man/ils.html
[33] http://www.webopedia.com/TERM/I/inode.html
[34] http://www.sleuthkit.org/index.php
[35] http://www.sleuthkit.org/about.php
[36] http://www.die.net/doc/linux/man/man8/debugfs.8.html
[37] http://e2fsprogs.sourceforge.net/ext2intro.html
[38] http://batleth.sapienti-sat.org/projects/FAQs/ext3-faq.html

image. 'icat's' purpose is to copy a file from the inode(s) that are associated with it.

Value of Tools

'ils' and 'icat' both provide invaluable help to the forensic investigator by giving them easy access to files that have been removed from a file system. With this easy access, there is no need to do the tedious work of finding and re-constructing a removed file from the raw data residing on disk. By using these tools, the forensic investigator would be able to save time and possibly gain leads, for further investigation, from files that were removed.

Tool Details

The Sleuth Kit v1.61 can be compiled statically with the command 'make static' from the source's root directory. By compiling these tools statically, they can be used to respond to an incident on a live system without needing to access potentially compromised system libraries. In this same vein, once compiled statically the tools can be run from any media that they can fit on, either in piecemeal or as a whole. A statically compiled version of all of 'The Sleuth Kit' tools would require approximately 12MB of disk space, well within the size constraints of a mini CD-ROM, 50-120MB. When using these statically compiled tools, the forensic investigator should be more concerned about the mount[39] binary being compromised; a statically compiled binary does not utilize any outside libraries when running.

Test Apparatus

The test equipment consists of VMware Workstation[40] 3.2.0 build-2330 running a virtual machine. The virtual machine used was a stock Red Hat 8.0 custom installation running the 2.4.18-14 kernel.

The packages installed on this operating system can be found in Appendix F. Additionally the 'VMware Guest OS Tools' for VMware version 3.2.0 build 2230 are installed on this workstation as well as Brian Carrier's 'The Sleuth Kit'. The Sleuth Kit however, has not been installed, but is statically compiled from source using the following command:

```
[root@localhost sleuthkit-1.61]# make static
```

[39] http://www.die.net/doc/linux/man/man8/mount.8.html
[40] http://www.vmware.com/

The hardware that this virtual machine was run on also doubles as a personal computer which is located in a home office.

The tool used to verify results, debugfs, is a part of the e2fsprogs[41] tool kit. This toolkit was installed on the test machine by the e2fsprogs-1.27-9 rpm[42]. The version of debugfs used in these tests is 1.27.

Environmental Conditions

The tests were completed on the two identical copies of the Linux VMware virtual machine. The virtual machine was set with the network in host-only mode. This provides for a private RFC1918[43] network. After the virtual machine was fully configured, it was suspended using the VMware 'suspend' button. Suspending a virtual machine provides for fast 'power on' and is very similar to the suspend feature available in Windows XP. After the virtual machine was suspended, a copy was created and the original was labeled 'Master Copy'. This was done to ensure that an identical copy was readily available. Having this identical copy readily available provided a reproducible environment in a minimal amount of time. The machines were on their own network segment; no external communication could be initiated or received. The only communication that could be initiated with these virtual machines was through some media device, such as a floppy disk.

Description of the Procedures

Equipment Preparation

The equipment used in the testing of these tools was the Linux Virtual Machine, described above, and a single high density floppy disk. To prepare the floppy for the test, it was first physically labeled with the phrase 'Test Floppy' and then electronically wiped, or sanitized, of data. The floppy disk was wiped of data through Unix with the command dd[44]. An example of how this command was used is below.

```
[root@localhost root]# dd if=/dev/zero of=/dev/fd0
```

[41] http://e2fsprogs.sourceforge.net
[42] http://www.rpm.org/
[43] http://www.faqs.org/rfcs/rfc1918.html
[44] http://www.research.att.com/sw/tools/uwin/man/man1/dd.html

After the disk was wiped an ext2 filesystem was created on it with the command mke2fs[45] as can be seen below.

```
[root@localhost root]# mke2fs /dev/fd0
```

Files were then copied over to the new file system. A complete listing of the files copied can be found in Appendix G. Next, an image of the floppy was created to create a known good base image. This image that was created is important because it provides a checkpoint that can be returned to if the need exists. After the image was created, the MD5 hash of both the image and floppy were taken. The MD5 hash of the floppy is a4ee292feed7a6d851c3d53154542549. A screen shot of this hash can be seen in Figure 5.

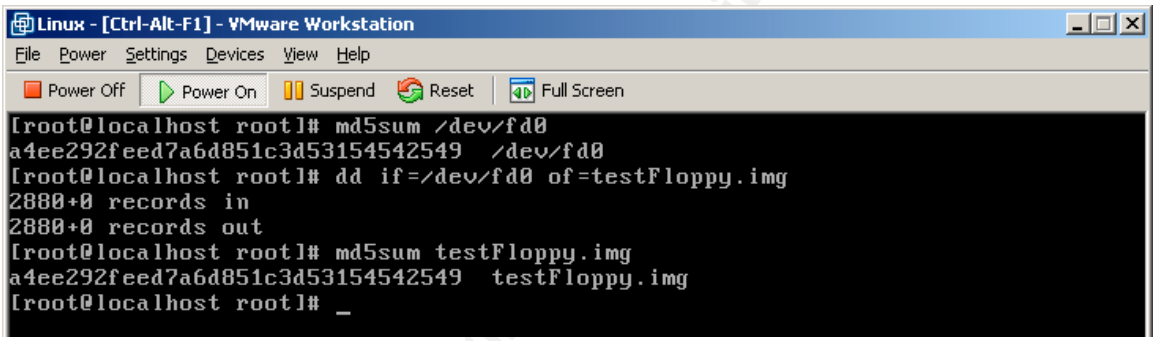

Figure 5 - Test Floppy MD5 Hash

After the base image was created, the following files were arbitrarily selected for removal:

- ./target2.exe
- ./level1/md5.c
- ./level1/level2/print.c
- ./level1/level2/level3/ifind.c

The MD5 hashes of the files before removal can be seen in Figure 6.

[45] http://unixhelp.ed.ac.uk/CGI/man-cgi?mke2fs+8

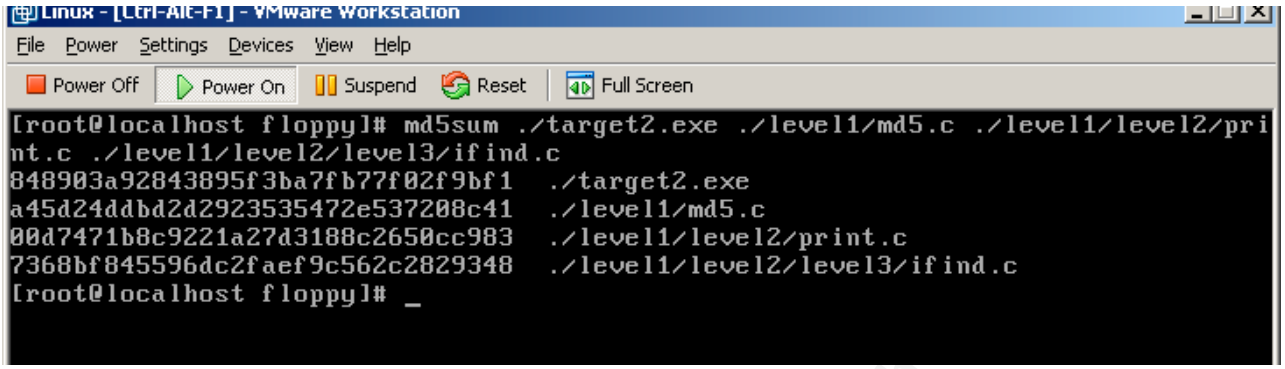

Figure 6 - MD5 Hash of Files Selected for Removal

After the md5 hashes of the files were recorded, other specific information was gathered: file size and file modification time. The information gathered is below in Table 1.

Table 1 - Detailed Information of Files Selected for Removal

File Name	Size (Bytes)	Modification Time
./target2.exe	26793	2003 May 27 21:32
./level1/md5.c	1759	2003 May 27 21:35
./level1/level2/print.c	5285	2003 May 27 21:36
./level1/level2/level3/ifind.c	12944	2003 May 27 22:38

Next, the chosen files were removed with the 'rm'[46] command and the time that each file was deleted was logged. These times can be found in Table 2. The commands used to remove the files are listed below.

```
[root@localhost root]# rm -f ./target2.exe
[root@localhost root]# rm -f ./level1/md5.c
[root@localhost root]# rm -f ./level1/level2/print.c
[root@localhost root]# rm -f ./level1/level2/level3/ifind.c
```

Table 2 Deletion Times of Files Selected for Removal

File Name	Deletion Time
./target2.exe	2003 May 28 20:53
./level1/md5.c	2003 May 28 20:53
./level1/level2/print.c	2003 May 28 20:53
./level1/level2/level3/ifind.c	2003 May 28 20:53

[46] http://unixhelp.ed.ac.uk/CGI/man-cgi?rm

After the removal of the chosen files, another image of the floppy was taken to create a checkpoint. This image was used to re-image the floppy disk between each of the tests preformed. The MD5 hash of this image was cf09908e574bd1b198dc8e572942102 and can be seen below in Figure 7.

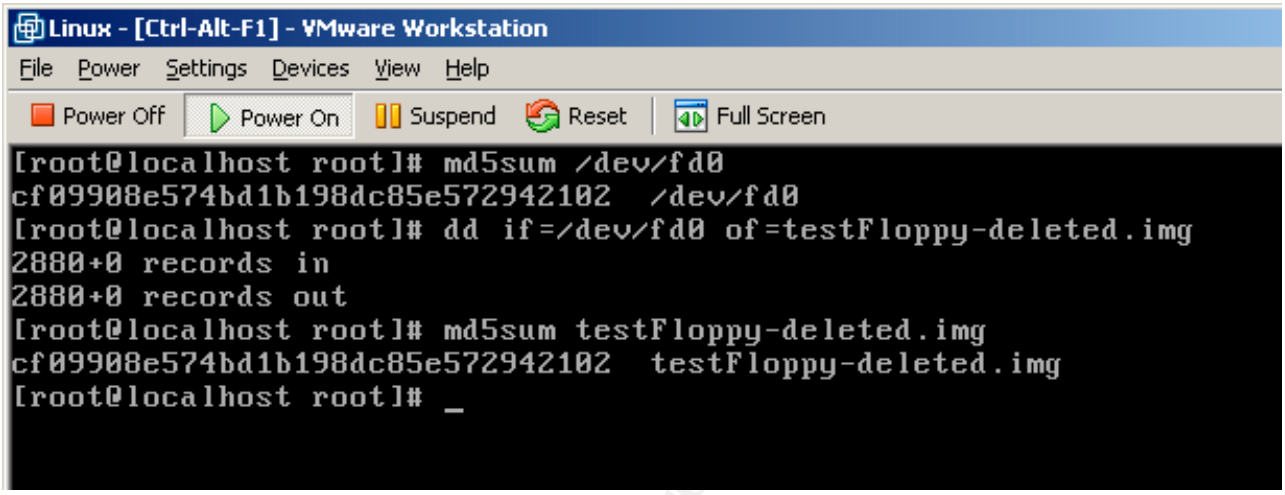

Figure 7 - Test Floppy MD5 Hash After Files Have Been Removed

File Naming Convention

As files were recovered they were named in the format of <inode number>-<YYMMDD>-<test run> until it can be determined, through their MD5 hashes, specifically what file name each recovered inode maps to.

Procedures

The integrity of test results were protected from tampering with the use of the virtual machines as well as having a controlled work environment.

The steps that will be used in the testing of 'ils' and 'icat' are:

1. sanitize floppy;
2. load image with the deleted files onto floppy;
3. verify the MD5 hash;
4. list deleted inodes on the floppy;
5. verify that the times stamps and file information is correct for the deleted inodes (MACTimes);
6. recover each of the deleted inodes to a temporary file;
7. verify the MD5 hashes of each of the files against the MD5 hashes for the files before they were deleted;
8. repeat the steps again on a duplicate installation and verify that the results are identical.

Once the tests have been shown the ability to correctly reproduce the removed inodes and recover the information in the removed files, the inodes for the removed files will be verified by using the 'debugfs' tool. The commands used to do this are:

```
[root@localhost root]# debugfs -R 'ls -l' <device>
[root@localhost root]# debugfs -R 'ls -ld <directory>' <device>
```

Criteria for Approval

'ils' Expected Results

ils is used to list the inodes on a file system. The default option for ils is to only list the inodes of removed files. Run with out any options ils should show us the inode information for the four files that were removed in the preparation steps.

For the purposes of this test the tool is executed in the following format:

```
[root@localhost root]# sleuthkit-1.61/bin/ils <device>
```

'ils' Details

Running 'ils' as shown in the above format will only show those inodes that have been removed. 'ils' automatically detects the filesystem type, so it is not required to be specified for these tests. If one wishes to specify the filesystem type, they can use the -f <type> option. In our tests, we specified the 'device' as the floppy disk, /dev/fd0. 'ils' runs in read-only mode, so there is no manipulation of the evidence as the tool is running. The proof that ils does not manipulate data on the floppy can be shown with identical before and after md5sums.

'icat' Expected Results

When running 'icat' the unmodified content of the deleted files is expected to be printed to the screen. For the purposes of this test, the tool is executed in the following format:

```
[root@localhost root]# sleuthkit-1.61/bin/icat <device> <inode>
```

'icat' Details

The syntax listed above will copy contents of the file residing at the inode specified on the device specified to standard out[47] but can be redirected to any file. For our tests we will specified 'device' as the floppy disk, '/dev/fd0'. When 'icat' is run as shown above, it copies the file as stored on disk. This ensures that the MD5 hashes match on the files. This tool will only access the 'device' specified. The device may be a physical device, such as a floppy, or logical such as a file system image. When executed, 'icat' runs in read-only mode, never changing the target filesystem. There is no manipulation of the evidence as the tool is running. Proof that this tool does not manipulate the data can be shown by before and after md5sums of the 'device' that it was run against.

Data and Results

During the first run to validate 'icat' and 'ils', the data was recovered without encountering any problems. Following the steps outlined previously, in the description of procedures, the test floppy was first sanitized, the deleted file image was loaded onto the floppy and the MD5 hash was verified. The Unix commands used to perform these tasks are below.

Sanitize the floppy:

```
[root@localhost root]# dd if=/dev/zero of=/dev/fd0
```

Load the deleted file image onto the test floppy:

```
[root@localhost root]# dd if=testImage-deleted.img of=/dev/fd0
```

Verify the integrity of the floppy:

```
[root@localhost root]# md5sum /dev/fd0
```

[47] http://java.sun.com/docs/books/tutorial/essential/system/iostreams.html

A screen shot of these commands being used to perform the tasks can be seen below in Figure 8.

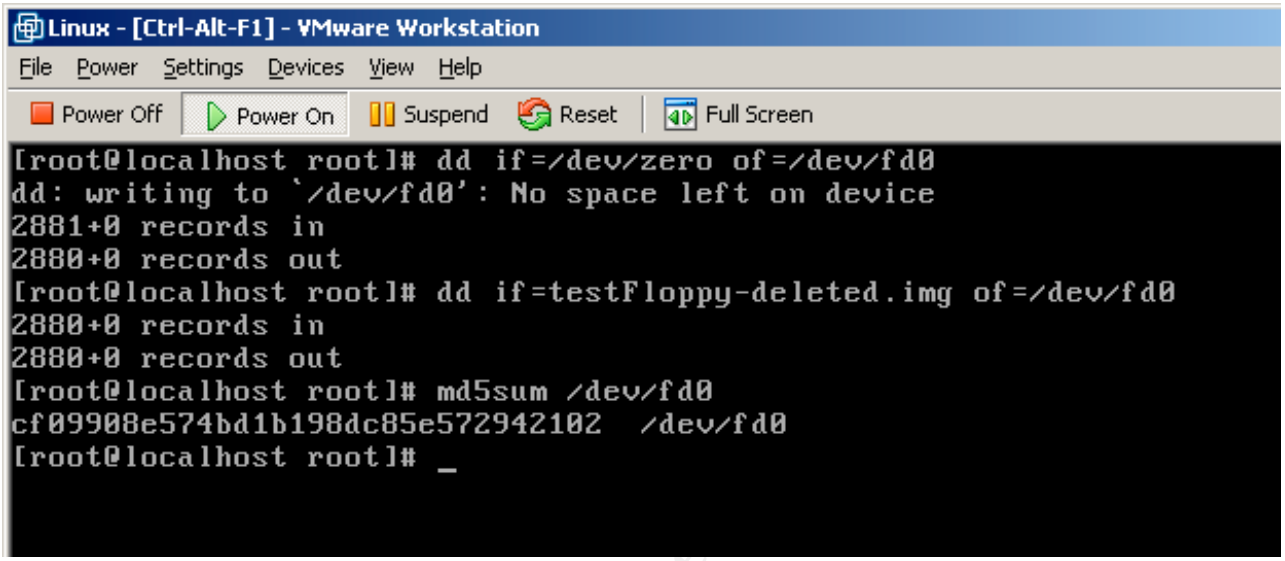

Figure 8 - Creation of the Test Floppy

Next, the inodes that were marked as deleted were listed on the floppy using 'ils'. Once the inodes for the deleted files were obtained they were recovered with 'icat'. The last step is to generate the md5 hash for each of the recovered files. This hash will allow the files, which are only identified by their inode number, to primarily be identified by name and secondly prove that the file was not modified in the recovery process. The Unix commands used to perform these tasks are listed below.

List deleted inodes:

```
[root@localhost root]# sleuthkit-1.61/bin/ils /dev/fd0
```

In this screen capture from the first run, the dates and file sizes can be seen.

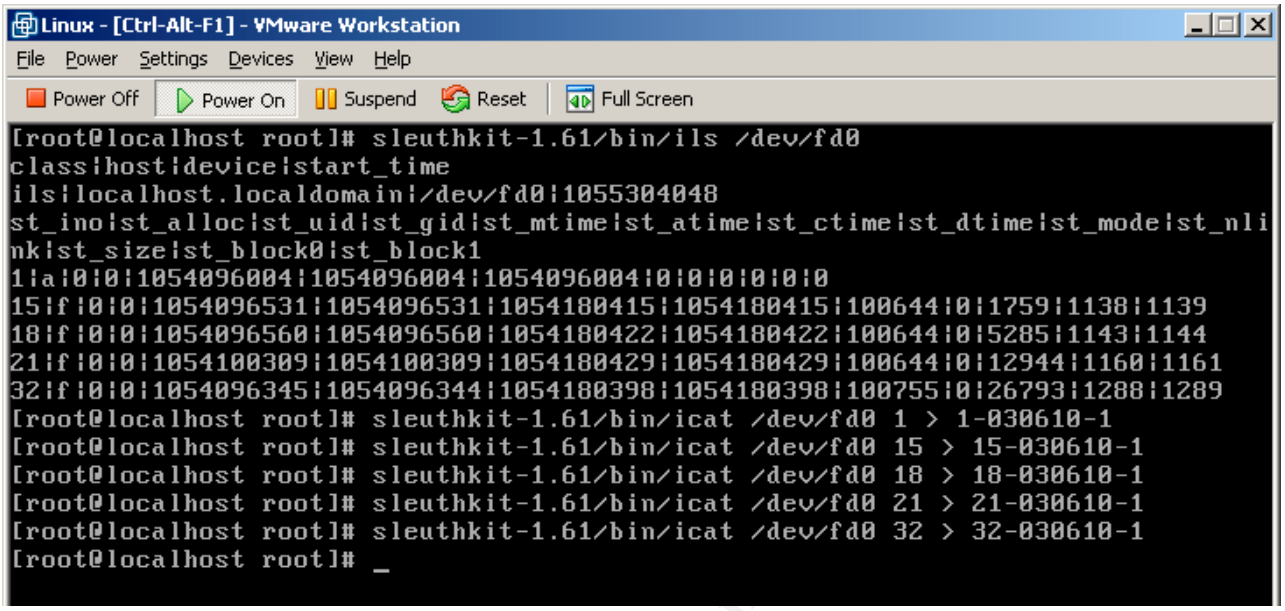

Figure 9 - Removed Inode Listing and File Recovery

A simple Perl[48] script in Appendix H can be used to convert epoch time stamps to a human readable format. Below is an example on how to execute the Perl script.

```
[root@localhost root]# ./epochToDate <epoch time stamp>
```

Using the above script, the dates from 'ils' can be compared to what is recorded in Table 1 and Table 2. Comparing the dates yields duplicate results.

To recover files that were removed and later found with 'ils', the following options were used with 'icat'

```
[root@localhost root]# sleuthkit-1.61/bin/icat /dev/fd0 <inode>
<destination file>
```

The process for generating the MD5 hashes of the recovered files is the same as the process for verifying the integrity of the test floppy.

[48] http://www.perl.com/

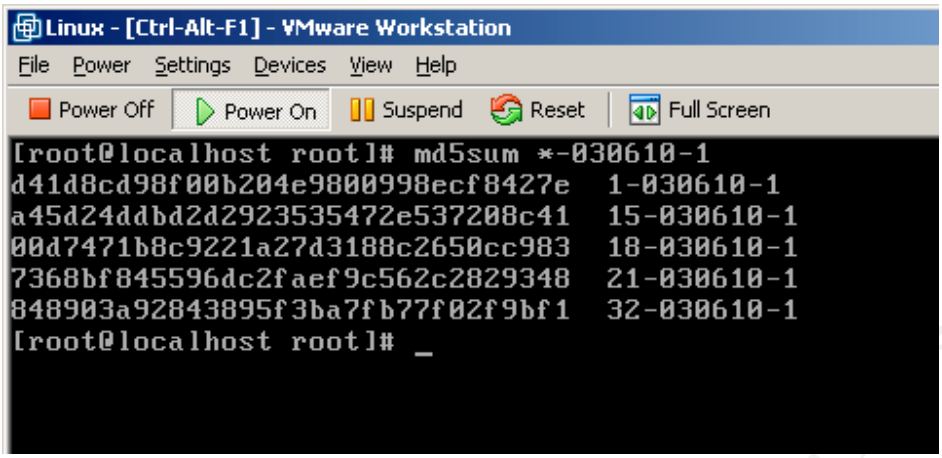

Figure 10 - MD5 Hashes of Recovered Files

In order to map the recovered inodes to their original file names, the MD5 hash values were used. The MD5 hash values of the recovered files are:

d41d8cd98f00b204e9800998ecf8427e 1-030610-1
a45d24ddbd2d2923535472e537208c41 15-030610-1
00d7471b8c9221a27d3188c2650cc983 18-030610-1
7368bf845596dc2faef9c562c2829348 21-030610-1
848903a92843895f3ba7fb77f02f9bf1 32-030610-1

The hash values for the original files are:

848903a92843895f3ba7fb77f02f9bf1 target2.exe
a45d24ddbd2d2923535472e537208c41 level1/md5.c
00d7471b8c9221a27d3188c2650cc983 level1/level2/print.c
7368bf845596dc2faef9c562c2829348 level1/level2//level3/ifind.c

It can be observed that all of the deleted files (except the file residing at inode 1) can be matched to the proper name as shown in .

Table 3 - Removed File to Inode Matches

File	Inode	MD5 hash
target2.exe	32	848903a92843895f3ba7fb77f02f9bf1
level1/md5.c	15	a45d24ddbd2d2923535472e537208c41
level1/level2/print.c	18	00d7471b8c9221a27d3188c2650cc983
level1/level2/level3/ifind.c	21	7368bf845596dc2faef9c562c2829348

The recovered file at inode 1 does not match any of the removed files and is an empty file.

The final MD5 hash for the test floppy in Figure 11, matches the starting MD5 hash in Figure 7. This proves that the tools, 'ils' and 'icat', do not make any modifications to the file system that they are working on.

Figure 11 - Run 1 Final MD5 Hash of Test Floppy

After running the debugfs commands, as listed in the above procedures, the following output was generated. This data was generated from the untouched floppy image. The files that were selected to be deleted are highlighted for easy reference.

```
[root@localhost root]# debugfs -R 'ls -l' testFloppy.img
debugfs 1.27 (8-Mar-2002)
     2   40755 (2)      0      0    1024 27-May-2003 22:47 .
     2   40755 (2)      0      0    1024 27-May-2003 22:47 ..
    11    40700 (2)     0      0   12288 27-May-2003 21:26 lost+found
    12   100755 (1)     0      0  910016 27-May-2003 22:44 dcat
    13   100755 (1)     0      0  205570 27-May-2003 22:45 file
    14    40755 (2)     0      0    1024 27-May-2003 21:35 level1
    24    40755 (2)     0      0    1024 27-May-2003 22:43 level1d
    30   100755 (1)     0      0   22470 27-May-2003 22:45 mactime
    31   100755 (1)     0      0   38770 27-May-2003 22:45 sorter
    32   100755 (1)     0      0   26793 27-May-2003 21:32 target2.exe

[root@localhost root]# debugfs -R 'ls -ld level1' testFloppy.img
debugfs 1.27 (8-Mar-2002)
    14   40755 (2)      0      0    1024 27-May-2003 21:35 .
     2   40755 (2)      0      0    1024 27-May-2003 22:47 ..
    15   100644 (1)     0      0    1759 27-May-2003 21:35 md5.c
    16   100644 (1)     0      0    1345 27-May-2003 21:35 md5.h
    17    40755 (2)     0      0    1024 27-May-2003 22:40 level2

[root@localhost root]# debugfs -R 'ls -ld level1/level2' testFloppy.img
debugfs 1.27 (8-Mar-2002)
    17   40755 (2)      0      0    1024 27-May-2003 22:40 .
    14   40755 (2)      0      0    1024 27-May-2003 21:35 ..
    18   100644 (1)     0      0    5285 27-May-2003 21:36 print.c
    19   100644 (1)     0      0    9540 27-May-2003 21:36 patchlevel.h
    20   40755 (2)      0      0    1024 27-May-2003 22:38 level3

[root@localhost root]# debugfs -R 'ls -ld level1/level2/level3' testFloppy.img
debugfs 1.27 (8-Mar-2002)
    20   40755 (2)      0      0    1024 27-May-2003 22:38 .
    17   40755 (2)      0      0    1024 27-May-2003 22:40 ..
    21   100644 (1)     0      0   12944 27-May-2003 22:38 ifind.c
    22   100644 (1)     0      0   31685 27-May-2003 22:38 ffs.c
    23   100644 (1)     0      0    6760 27-May-2003 22:38 ffs.h

[root@localhost root]#
```

From this output, it can be observed that 'debugfs' gives the same information that 'ils' presents.

After the first test run was completed, a second test run was preformed. The purpose of this second test run was to verify that the results of the first run were

reproducible. To ensure an identical virtual machine setup was used, a copy was made of the master image. This copy was named 'linux - second run'. Since all of the steps are identical to the first run, screen shots from this second run are below in Figure 12 through Figure 15.

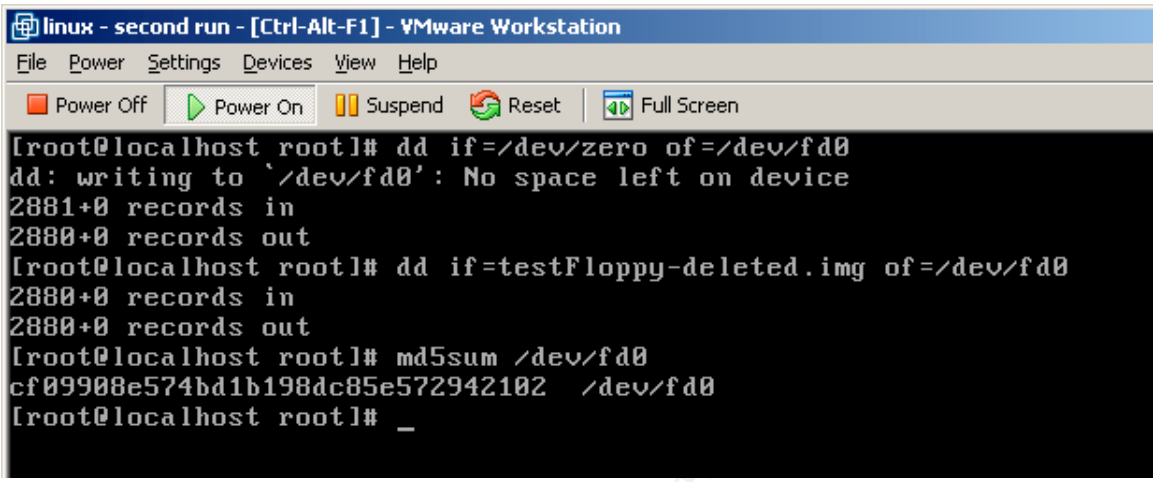

Figure 12 - Creation of Test Floppy and MD5 Hash of Test Floppy

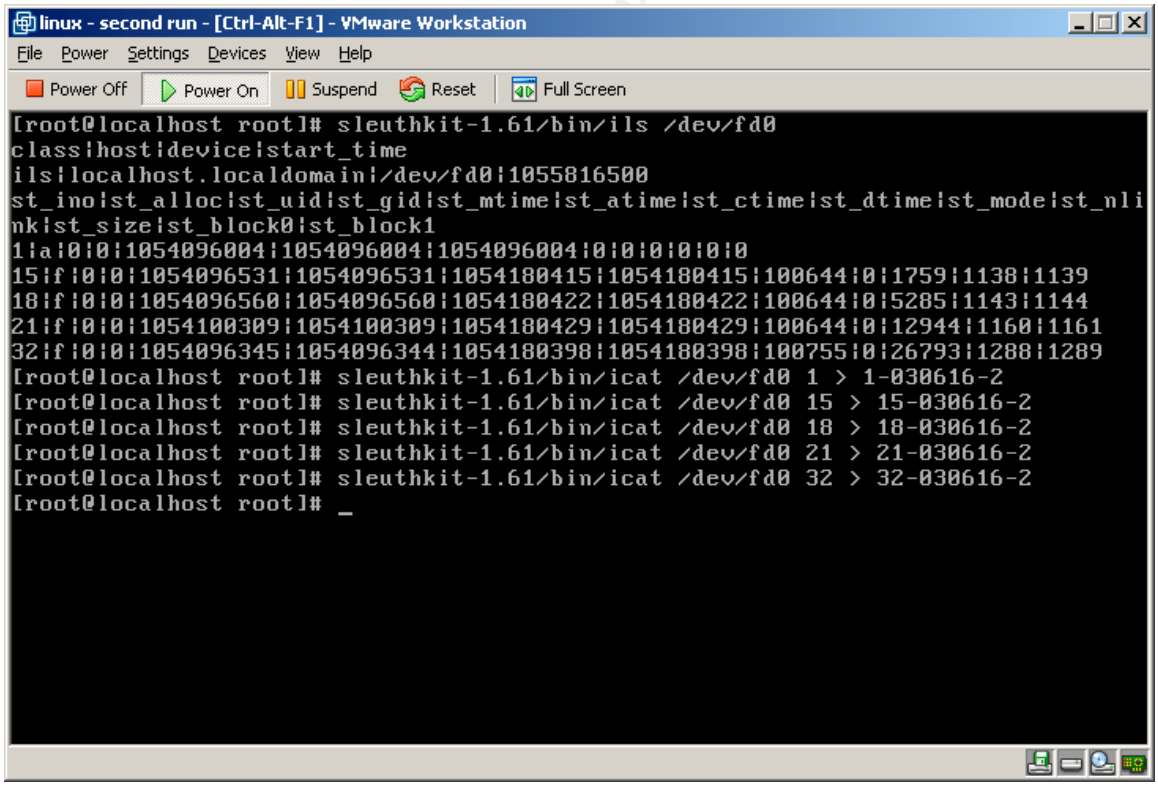

Figure 13 - Ils Inode Listing of Removed Files on Test Floppy and Icat Recovery of Files

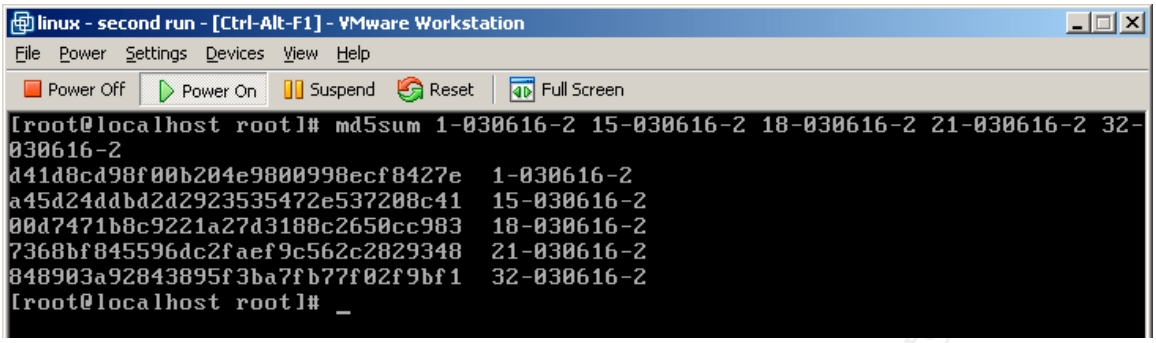

Figure 14 - MD5 Hashes of Recovered Files

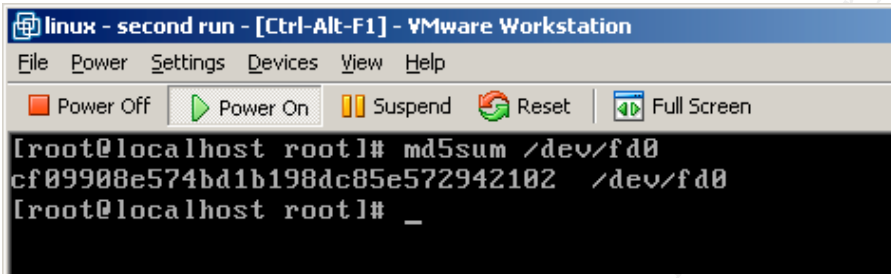

Figure 15 - Run 2 Final MD5 Hash of Test Floppy

The results from all of the tests performed in the second run were identical to those from the first run. 'ils' and 'icat' both present the information in a reproducible manner and in a format that is understandable.

Analysis

The data generated from running the 'ils' tool with its default options will present to the investigator a list of removed inodes and information about the files associated with those inodes that still reside on the file system. To make the most out of the output, the investigator would need to correlate the inodes to file names, where possible. Even without this ability to correlate inodes to file names, the data provided by 'ils' will still give the investigator critical information about the files. From the output of 'ils', a timeline can be created, allowing the investigator to correlate other events happening on the system with file activity.

Using 'icat', the investigator can recover or list the contents of the files that have been removed. Analyzing the data presented by this tool is trivial because this tool reveals to the investigator what was in the removed file. To the investigator, the data recovered could be the evidence needed to apprehend an individual.

Presentation

The data presented by 'ils' is fairly straight forward, as it is in a tabular format. The largest confusion in the data being presented comes from the column

names. There are two sets of data presented in the output from 'ils'. The fist line is the header line for the first section which contains information about the machine and image. It contains the *class* (program that is run), *host* that the program was run on, *device* that was scanned and the *start_time* that the program was initiated at (in seconds since midnight 1970, epoch local time). The second line is the line that this previous header applies to. The third line is the header line for the second section where the data gathered is presented.

From the 'ils' man page[49], the following Table 1 lists the descriptions of each of the fields.

Table 4 - 'ils' Column Descriptions

Label	Description
st_ino	The inode number.
st_alloc	Allocation status: 'a' for allocated inode, 'f' for free inode.
st_uid	Owner user ID.
st_gid	Owner group ID.
st_mtime	UNIX time (seconds) of last file modification.
st_atime	UNIX time (seconds) of last file access.
st_ctime	UNIX time (seconds) of last inode status change.
st_dtime	UNIX time (seconds) of file deletion (LINUX only).
st_mode	File type and permissions (octal).
st_nlink	Number of hard links.
st_size	File size in bytes.
st_block0,st_block	The first two entries in the direct block address list.

An example output from the 'ils' tool is:

```
[root@localhost root]# sleuthkit-1.61/bin/ils testFloppy.img
class|host|device|start_time
ils|localhost.localdomain|testFloppy.img|1057029796
st_ino|st_alloc|st_uid|st_gid|st_mtime|st_atime|st_ctime|st_dtim
e|st_mode|st_nlink|st_size|st_block0|st_block1
1|a|0|0|1054096004|1054096004|1054096004|0|0|0|0|0|0
```

The output from 'ils' could be presented in court as is, however it would require the judge and or jury to learn a significant amount of information. Specifically, it would require basic knowledge about inodes, UID/GID's (User ID, Group ID), MAC (Modification, Access, Change) times etc. They would need a crash course on filesystem structures. Because filesystem structures do not appeal to most

[49] http://www.catb.org/~esr/jargon/html/M/man-page.html

people, the best option would be to trim what was presented to a minimal amount, such as inode and times. This minimal amount could then be explained in simplistic terms, giving the audience a good explanation of what is going on, while at the same time not overloading them with information that would be forgotten as soon as the topic was finished.

Conversely, the data presented by 'icat' is unambiguous as it is simply copying the contents of the file at a given inode to standard out. Explaining this output to a judge and or a jury would be fairly trivial as the output and what is being done is trivial. However, if the details on how the tool worked were required to be explained, a fairly simplistic explanation on how file space is linked could be given. A creative individual could give a good explanation that would convey all of the necessary information without putting the audience to sleep.

Conclusion

The tests performed attempted to prove, beyond doubt, that the output from the selected forensic tools, 'ils' and 'icat', is forensically sound. The tests were successful in proving this as they showed that 'ils' correctly displays the low level information (specifically inodes, owners and MAC times for files on the filesystem) and 'icat' correctly retrieves the data from removed files using the inode information retrieved with 'ils'. Both of these tools handled the target file system in a forensically sound manner. That is to say that they accessed it in a read-only manner. Because these tools passed all of the tests performed, there is no reason that they should not be used by an incident responder or in a forensic investigation.

'ils' and 'icat' are able to perform the intended tasks in such a way that there are not any recommendations one can offer to make them more forensically sound. The only issue that could potentially come up or be a problem would be the way that they access the file system. However these tools only access the target file system in a read-only manner. Because of this there are no recommendations that would make the tools more forensically sound.

Additional Information

Brian Carrier, the current maintainer and author of 'The Sleuth Kit', was contacted to see if he would be able to lend assistance in supporting the tools in his kit if it was required. Mr. Carrier mentioned that he would be able to testify regarding the tools, 'ils' and 'icat', in a court of law. In addition to testifying, Mr. Carrier said he would also be able to provide support for individuals who were testifying about the tools. Mr. Carrier can be reached through the contact information located on The Sleuth Kit's contact page, http://www.sleuthkit.org/contact.php

Part 3 - Legal Issues of Incident Handling

Initial Contact With Law Enforcement

During my first contact with the law enforcement officer over the phone I would need to remind myself that since we are an Internet Service Provider who is providing services to the public, we are bound by the provisions in the Electronic Communications Privacy Act, Title 18 United States Code Sections 2701 through 2712. These provisions regulate the release of data to governmental agencies. Without a legal order, we are not allowed to give data to the government unless certain conditions are met. These conditions include; User consent, where consent is given by the user to release information about the user to the government. Consent in this case does not have to be in a written or oral form. It can be in an implied form. In the case of computers, implied consent can be obtained through banners and the terms of service (Eckenwiler). In addition an Internet Service Provider can release information to the government without a court order. They can do this in order to protect the their rights and property, if there is a belief that there is imminent/immediate danger involving death or serious bodily injury as well as disclosing non-content records. There are two categories of non-content records: basic subscriber information and transactional records (Eckenwiler).

Section 2073(c)(2) lists the basic subscriber information:

- (A) name
- (B) address
- (C) local and long distance telephone records, or records of session times and durations
- (D) length of service (including start date) and types of service utilized.
- (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address
- (F) means and source of payment for such service (including any credit card or bank account number)

Transactional records include items that are not content and not basic subscriber information. Such information would be addresses on inbound or outbound email inbound FTP[50] connections and where [the] remote user is logging in from (Eckenwiler).

Preservation of Evidence

If the law enforcement officer wants to ensure that evidence is preserved while they are obtaining the legal authority to require my employer to release the information, they must send a Preservation Request Letter. This letter is

[50] http://dictionary.reference.com/search?q=ftp

specified under § 2703(f) and is also known as a 'F letter' because of the sub section designator. With a F letter, my employer is required to take all necessary steps to preserve records and other evidence as requested pending the law enforcement officer receiving the required legal authority to request the data. Our company is required to hold the data prepared for the F letter for 90 days. This period of time can be extended by the law enforcement officer sending a renewed request (18 USC 2703f).

Legal Authority Required for Disclosure

To require the company to comply with the law enforcement officer's request, we would need to receive a court order § 2073(d). However, this sub paragraph contains a provision that would allow for a company to nullify or modify a court order if the data being requested is unusually large or would cause an undue burden (18 USC 2703d). However, if the consumer has consented to sending this information to the government without the need for a court order, we can send the information to the law enforcement officer without needing a court order.

Permitted Investigative Activity

There are fairly few limitations on other investigative activity that is allowed at this time. The limiting factors would include any company policies that exist regarding looking through the internal details of a customer's accounts. The only federal law that would apply would be the laws regarding wire taps. However, if we are performing a wiretap for the protection of our company, we are well within in our rights.

Disclosure Rules in Break-in

Assuming that the malicious individual used a customer's account to gain access to our system, and then used that account to create new accounts, we would still need to follow the Electronic Communications Privacy Act rules regarding disclosure of information to government. However, if the malicious individual did not use a customer account, but exploited a weakness or flaw present on our computer systems to create a new account for themselves, and then used that new account to break into a government system, we would not be bound by the Electronic Communications Privacy Act rules regarding disclosure to the government. We would be able to disclose information regarding this malicious individual at will to the government.

Bibliography

Active Perl Help - perlport. ActiveState. 25 May 2003 <http://aspn.activestate.com/ASPN/Products/ActivePerl/lib/Pod/perlport.html#files_and_filesystems>

California State. California Computer Crimes. California Codes, Penal Code, Part 1, Title 13, Chapter 5. 1 July 2003 <http://www.davismccownlaw.com/articles/CalCC.htm>

Eckenwiler, Mark. ISPs and Federal Privacy Law: Everything You Need to Know About the Electronic Communications Privacy Act (ECPA). Nanog20, Washington, D.C. 22-24 October 2000. 12 July 2003 <http://www.nanog.org/mtg-0010/ppt/justice.ppt>

Ginski, Richard. Validation of TASK v1.50 fsstat and dstat. 20 July 2003 <http://www.giac.org/practical/GCFA/Richard_Ginski_GCFA.pdf>

Ils Manpage. ils. 20 July 2003 < http://www.sleuthkit.org/sleuthkit/man/ils.html>

Lee, Selgado et al. System Forensics, Investigation and Response, 6 vols. Sans Institute, 2003

Owen, Greg. Analysis and Comparison of Red Hat Linux 6.2 Honeypots With & Without LIDS-enabled Kernels. 20 July 2003 <http://www.giac.org/practical/Greg_Owen_GCFA.zip>

Perlfunc. perlfunc - Perl builtin functions. 20 July 2003 <http://aspn.activestate.com//ASPN/Products/ActivePerl/lib/Pod/perlfunc.html#item_stat>

United States. Department of Justice. Criminal Division. Computer Crime and

Intellectual Property Section. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. July 2002. 15 May 2003 <http://www.cybercrime.gov/s&smanual2002.htm>

United States. United States Code. Chapter 119 - Wire and Electronic Communications Interception and Interception of Oral Communications. 14 July 2003 <http://www.eff.org/Privacy/Email_Internet_Web/ecpa.law>

United States. United States Code. Chapter 121 - Stored Wire and Electronic Communications and Transactional Records Access. 15 July 2003 <http://www4.law.cornell.edu/uscode/18/pIch121.html>

Appendix A - Helpful Strings in target2.exe

Sleep
HeapAlloc
@
GetProcessHeap
TerminateProcess
ReadFile
PeekNamedPipe
CloseHandle
D
CreateProcessA
C
CreatePipe
WriteFile
GetLastError
LocalAlloc
KERNEL32.dll
StartServiceCtrlDispatcherA
SetServiceStatus
RegisterServiceCtrlHandlerA
4
CloseServiceHandle
5
ControlService
U
QueryServiceStatus
G
OpenServiceA
L
CreateServiceA
E
OpenSCManagerA
x
DeleteService
StartServiceA
-
ChangeServiceConfigA
P
QueryServiceConfigA
ADVAPI32.dll
%
WSAIoctl
=
WSASocketA
WS2_32.dll
MFC42.DLL
memmove
I
exit
X
fprintf
_iob
sprintf
perror
strstr
time
printf
MSVCRT.dll
U
__dllonexit
_onexit
_exit
H
_XcptFilter
d
__p___initenv
X
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
j
__p__commode
o
__p__fmode
__set_app_type
_except_handler3
_controlfp
??0Init@ios_base@std@@QAE@X
Z
??1Init@ios_base@std@@QAE@X
Z
??0_Winit@std@@QAE@XZ
??1_Winit@std@@QAE@XZ
MSVCP60.dll
@

@
&@
&@
<
p
`@@
T@@
H@@
ERROR 3
ERROR 2
ERROR 1
impossibile creare raw ICMP socket
%s

RAW ICMP SendTo:
========== Icmp BackDoor V0.1
==========
========= Code by Spoof. Enjoy Yourself!
 Your PassWord:
loki
cmd.exe
 Exit OK!
Local Partners Access
Error UnInstalling Service
Service UnInstalled Sucessfully
0
H
`P
>
H
e
l
l
o

f
r
o
m

M
F
C
!

-d
Error Installing Service
Service Installed Sucessfully
-i
Create Service %s ok!
CreateService failed:%d
Service Stopped
Force Service Stopped Failed%d
The service is running or starting!
Query service status failed!
Open service failed!
Service %s Already exists
Local Printer Manager Service
smsses.exe
Open Service Control Manage failed:%d
%d
Start service successfully!
Starting the service failed!
starting the service <%s>...
Successfully!
Failed!
Try to change the service's start type...
The service is disabled!
Query service config failed!

Appendix B - Filemon Log File When Running 'target2.exe -i test'

```
1       7:19:34 PM   cmd.exe:524 QUERY INFORMATION    C:\target2.exe
        SUCCESS    Attributes: A
2       7:19:34 PM   cmd.exe:524 OPEN C:\      SUCCESS    Options: Open Directory
Access: All
3       7:19:34 PM   cmd.exe:524 DIRECTORY C:\      SUCCESS
        FileBothDirectoryInformation: target2.exe
4       7:19:34 PM   cmd.exe:524 CLOSE        C:\      SUCCESS
5       7:19:34 PM   cmd.exe:524 OPEN C:\target2.exe        SUCCESS    Options: Open
Access: All
6       7:19:34 PM   cmd.exe:524 QUERY INFORMATION    C:\target2.exe
        SUCCESS    Length: 26793
7       7:19:34 PM   cmd.exe:524 OPEN C:\WINDOWS\AppPatch\sysmain.sdb
        SUCCESS    Options: Open  Access: All
8       7:19:34 PM   cmd.exe:524 QUERY INFORMATION
        C:\WINDOWS\AppPatch\sysmain.sdb    SUCCESS    Length: 1026828
9       7:19:34 PM   cmd.exe:524 QUERY INFORMATION
        C:\WINDOWS\AppPatch\sysmain.sdb    SUCCESS    Length: 1026828
10      7:19:34 PM   cmd.exe:524 QUERY INFORMATION
        C:\WINDOWS\AppPatch\sysmain.sdb    SUCCESS    Length: 1026828
11      7:19:34 PM   cmd.exe:524 OPEN C:\WINDOWS\AppPatch\systest.sdb      FILE
NOT FOUNDOptions: Open  Access: All
12      7:19:34 PM   cmd.exe:524 OPEN C:\      SUCCESS    Options: Open Directory
Access: All
13      7:19:34 PM   cmd.exe:524 DIRECTORY C:\      SUCCESS
        FileBothDirectoryInformation: target2.exe
14      7:19:34 PM   cmd.exe:524 CLOSE        C:\      SUCCESS
15      7:19:34 PM   cmd.exe:524 QUERY INFORMATION    C:\target2.exe
        SUCCESS    Attributes: A
16      7:19:34 PM   cmd.exe:524 OPEN C:\      SUCCESS    Options: Open Directory
Access: All
17      7:19:34 PM   cmd.exe:524 DIRECTORY C:\      SUCCESS
        FileBothDirectoryInformation: target2.exe
18      7:19:34 PM   cmd.exe:524 CLOSE        C:\      SUCCESS
19      7:19:34 PM   cmd.exe:524 QUERY INFORMATION    C:\target2.exe
        SUCCESS    Attributes: A
20      7:19:34 PM   cmd.exe:524 OPEN C:\      SUCCESS    Options: Open Directory
Access: All
21      7:19:34 PM   cmd.exe:524 DIRECTORY C:\      SUCCESS
        FileBothDirectoryInformation: target2.exe
22      7:19:34 PM   cmd.exe:524 CLOSE        C:\      SUCCESS
23      7:19:34 PM   cmd.exe:524 QUERY INFORMATION    C:\target2.exe
        SUCCESS    Attributes: A
```

24 7:19:34 PM cmd.exe:524 QUERY INFORMATION C:\target2.exe SUCCESS Length: 26793
25 7:19:34 PM cmd.exe:524 CLOSE C:\WINDOWS\AppPatch\sysmain.sdb SUCCESS
26 7:19:34 PM cmd.exe:524 QUERY INFORMATION C:\target2.exe SUCCESS Attributes: A
27 7:19:34 PM cmd.exe:524 OPEN C:\ SUCCESS Options: Open Directory Access: All
28 7:19:34 PM cmd.exe:524 DIRECTORY C:\ SUCCESS FileBothDirectoryInformation: target2.exe
29 7:19:34 PM cmd.exe:524 CLOSE C:\ SUCCESS
30 7:19:34 PM cmd.exe:524 OPEN C:\target2.exe.Manifest FILE NOT FOUND Options: Open Access: All
31 7:19:34 PM cmd.exe:524 QUERY INFORMATION C:\ SUCCESS Attributes: DHSA
32 7:19:34 PM target2.exe:304 QUERY INFORMATION C:\target2.exe SUCCESS FileNameInformation
33 7:19:34 PM target2.exe:304 OPEN C:\WINDOWS\Prefetch\TARGET2.EXE-08FC3E78.pf FILE NOT FOUND Options: Open Access: All
34 7:19:34 PM target2.exe:304 OPEN C:\ SUCCESS Options: Open Directory Access: Traverse
35 7:19:34 PM target2.exe:304 QUERY INFORMATION C:\target2.exe.Local FILE NOT FOUND Attributes: Error
36 7:19:34 PM cmd.exe:524 CLOSE C:\target2.exe SUCCESS
37 7:19:34 PM target2.exe:304 QUERY INFORMATION C:\WS2_32.dll FILE NOT FOUND Attributes: Error
38 7:19:34 PM target2.exe:304 QUERY INFORMATION C:\WS2_32.dll FILE NOT FOUND Attributes: Error
39 7:19:34 PM target2.exe:304 QUERY INFORMATION C:\WINDOWS\System32\WS2_32.dll SUCCESS Attributes: A
40 7:19:34 PM target2.exe:304 OPEN C:\WINDOWS\System32\WS2_32.dll SUCCESS Options: Open Access: Execute
41 7:19:34 PM target2.exe:304 CLOSE C:\WINDOWS\System32\WS2_32.dll SUCCESS
42 7:19:34 PM target2.exe:304 QUERY INFORMATION C:\WS2HELP.dll FILE NOT FOUND Attributes: Error
43 7:19:34 PM target2.exe:304 QUERY INFORMATION C:\WS2HELP.dll FILE NOT FOUND Attributes: Error
44 7:19:34 PM target2.exe:304 QUERY INFORMATION C:\WINDOWS\System32\WS2HELP.dll SUCCESS Attributes: A
45 7:19:34 PM target2.exe:304 OPEN C:\WINDOWS\System32\WS2HELP.dll SUCCESS Options: Open Access: Execute
46 7:19:34 PM target2.exe:304 CLOSE C:\WINDOWS\System32\WS2HELP.dll SUCCESS
47 7:19:34 PM target2.exe:304 QUERY INFORMATION C:\MFC42.DLL FILE NOT FOUND Attributes: Error

48 7:19:34 PM target2.exe:304 QUERY INFORMATION C:\MFC42.DLL FILE NOT FOUND Attributes: Error
49 7:19:34 PM target2.exe:304 QUERY INFORMATION C:\WINDOWS\System32\MFC42.DLL SUCCESS Attributes: A
50 7:19:34 PM target2.exe:304 OPEN C:\WINDOWS\System32\MFC42.DLL SUCCESS Options: Open Access: Execute
51 7:19:34 PM target2.exe:304 CLOSE C:\WINDOWS\System32\MFC42.DLL SUCCESS
52 7:19:34 PM target2.exe:304 QUERY INFORMATION C:\MSVCP60.dll FILE NOT FOUND Attributes: Error
53 7:19:34 PM target2.exe:304 QUERY INFORMATION C:\MSVCP60.dll FILE NOT FOUND Attributes: Error
54 7:19:34 PM target2.exe:304 QUERY INFORMATION C:\WINDOWS\System32\MSVCP60.dll SUCCESS Attributes: A
55 7:19:34 PM target2.exe:304 OPEN C:\WINDOWS\System32\MSVCP60.dll SUCCESS Options: Open Access: Execute
56 7:19:34 PM target2.exe:304 CLOSE C:\WINDOWS\System32\MSVCP60.dll SUCCESS
57 7:19:34 PM target2.exe:304 QUERY INFORMATION C:\WINDOWS\System32\MFC42LOC.DLL FILE NOT FOUND Attributes: Error

58 7:19:34 PM target2.exe:304 QUERY INFORMATION C:\WINDOWS\System32\MFC42LOC.DLL FILE NOT FOUND Attributes: Error

59 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 8192
60 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 8192
61 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 16384
62 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 20480
63 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 24576
64 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 28672
65 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 32768
66 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 36864
67 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 40960
68 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 40960
69 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system SUCCESS Length: 2097152

70 7:19:34 PM services.exe:664 SET INFORMATION
C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 45056
71 7:19:34 PM services.exe:664 WRITE
C:\WINDOWS\system32\config\system.LOG SUCCESS Offset: 0 Length: 512

72 7:19:34 PM services.exe:664 FLUSH
C:\WINDOWS\system32\config\system.LOG SUCCESS
73 7:19:34 PM services.exe:664 WRITE
C:\WINDOWS\system32\config\system.LOG SUCCESS Offset: 512 Length:
512
74 7:19:34 PM services.exe:664 WRITE
C:\WINDOWS\system32\config\system.LOG SUCCESS Offset: 1024 Length:
4096
75 7:19:34 PM services.exe:664 WRITE
C:\WINDOWS\system32\config\system.LOG SUCCESS Offset: 5120 Length:
4096
76 7:19:34 PM services.exe:664 WRITE
C:\WINDOWS\system32\config\system.LOG SUCCESS Offset: 9216 Length:
4096
77 7:19:34 PM services.exe:664 WRITE
C:\WINDOWS\system32\config\system.LOG SUCCESS Offset: 13312 Length:
8192
78 7:19:34 PM services.exe:664 WRITE
C:\WINDOWS\system32\config\system.LOG SUCCESS Offset: 21504 Length:
4096
79 7:19:34 PM services.exe:664 WRITE
C:\WINDOWS\system32\config\system.LOG SUCCESS Offset: 25600 Length:
4096
80 7:19:34 PM services.exe:664 WRITE
C:\WINDOWS\system32\config\system.LOG SUCCESS Offset: 29696 Length:
4096
81 7:19:34 PM services.exe:664 WRITE
C:\WINDOWS\system32\config\system.LOG SUCCESS Offset: 33792 Length:
4096
82 7:19:34 PM services.exe:664 WRITE
C:\WINDOWS\system32\config\system.LOG SUCCESS Offset: 37888 Length:
4096
83 7:19:34 PM services.exe:664 FLUSH
C:\WINDOWS\system32\config\system.LOG SUCCESS
84 7:19:34 PM services.exe:664 WRITE
C:\WINDOWS\system32\config\system.LOG SUCCESS Offset: 0 Length: 512

85 7:19:34 PM services.exe:664 FLUSH
C:\WINDOWS\system32\config\system.LOG SUCCESS
86 7:19:34 PM explorer.exe:1908 QUERY INFORMATION
C:\WINDOWS\System32\cmd.exe SUCCESS Attributes: A

87 7:19:34 PM services.exe:664 FLUSH C:\WINDOWS\system32\config\system SUCCESS
88 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 1024
89 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 8192
90 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 8192
91 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 16384
92 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 20480
93 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 24576
94 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 28672
95 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 32768
96 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 36864
97 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 40960
98 7:19:34 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 45056
99 7:19:34 PM services.exe:664 QUERY INFORMATION C:\WINDOWS\system32\smsses.exe FILE NOT FOUND Attributes: Error
100 7:19:34 PM services.exe:664 QUERY INFORMATION C:\WINDOWS\system32\smsses.exe FILE NOT FOUND Attributes: Error
101 7:19:34 PM services.exe:664 QUERY INFORMATION C:\WINDOWS\System32\smsses.exe FILE NOT FOUND Attributes: Error
102 7:19:34 PM services.exe:664 QUERY INFORMATION C:\WINDOWS\system\smsses.exe FILE NOT FOUND Attributes: Error
103 7:19:34 PM services.exe:664 QUERY INFORMATION C:\WINDOWS\smsses.exe FILE NOT FOUND Attributes: Error
104 7:19:34 PM services.exe:664 QUERY INFORMATION C:\WINDOWS\system32\smsses.exe FILE NOT FOUND Attributes: Error
105 7:19:34 PM services.exe:664 QUERY INFORMATION C:\WINDOWS\smsses.exe FILE NOT FOUND Attributes: Error
106 7:19:34 PM services.exe:664 QUERY INFORMATION C:\WINDOWS\System32\Wbem\smsses.exe FILE NOT FOUND Attributes: Error

107 7:19:34 PM services.exe:664 OPEN C:\WINDOWS\Debug\UserMode\userenv.log SUCCESS Options: OpenIf Access: All
108 7:19:34 PM services.exe:664 QUERY INFORMATION C:\WINDOWS\Debug\UserMode\userenv.log SUCCESS Length: 6182

109 7:19:34 PM services.exe:664 WRITE C:\WINDOWS\Debug\UserMode\userenv.log SUCCESS Offset: 6182 Length: 60
110 7:19:34 PM services.exe:664 WRITE C:\WINDOWS\Debug\UserMode\userenv.log SUCCESS Offset: 6242 Length: 88
111 7:19:34 PM services.exe:664 WRITE C:\WINDOWS\Debug\UserMode\userenv.log SUCCESS Offset: 6330 Length: 4

112 7:19:34 PM services.exe:664 CLOSE C:\WINDOWS\Debug\UserMode\userenv.log SUCCESS
113 7:19:34 PM target2.exe:304 CLOSE C:\ SUCCESS
114 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\Prefetch\TARGET2.EXE-08FC3E78.pfFILE NOT FOUND Options: Open Access: All
115 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\TARGET2.EXE SUCCESS Attributes: A
116 7:19:35 PM svchost.exe:944 OPEN C:\TARGET2.EXE SUCCESS Options: Open Access: All
117 7:19:35 PM svchost.exe:944 CLOSE C:\TARGET2.EXE SUCCESS

118 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\ADVAPI32.DLL SUCCESS Attributes: A
119 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\ADVAPI32.DLL SUCCESS Options: Open Access: All
120 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\ADVAPI32.DLL SUCCESS
121 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\CTYPE.NLS SUCCESS Attributes: A
122 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\CTYPE.NLS SUCCESS Options: Open Access: All
123 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\CTYPE.NLS SUCCESS
124 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\GDI32.DLL SUCCESS Attributes: A
125 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\GDI32.DLL SUCCESS Options: Open Access: All
126 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\GDI32.DLL SUCCESS
127 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\KERNEL32.DLL SUCCESS Attributes: A
128 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\KERNEL32.DLL SUCCESS Options: Open Access: All
129 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\KERNEL32.DLL SUCCESS

130 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\LOCALE.NLS SUCCESS Attributes: A
131 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\LOCALE.NLS SUCCESS Options: Open Access: All
132 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\LOCALE.NLS SUCCESS
133 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\MFC42.DLL SUCCESS Attributes: A
134 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\MFC42.DLL SUCCESS Options: Open Access: All
135 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\MFC42.DLL SUCCESS
136 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\MSVCP60.DLL SUCCESS Attributes: A
137 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\MSVCP60.DLL SUCCESS Options: Open Access: All
138 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\MSVCP60.DLL SUCCESS
139 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\MSVCRT.DLL SUCCESS Attributes: A
140 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\MSVCRT.DLL SUCCESS Options: Open Access: All
141 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\MSVCRT.DLL SUCCESS
142 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\NTDLL.DLL SUCCESS Attributes: A
143 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\NTDLL.DLL SUCCESS Options: Open Access: All
144 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\NTDLL.DLL SUCCESS
145 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\RPCRT4.DLL SUCCESS Attributes: A
146 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\RPCRT4.DLL SUCCESS Options: Open Access: All
147 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\RPCRT4.DLL SUCCESS
148 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\SORTTBLS.NLS SUCCESS Attributes: A
149 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\SORTTBLS.NLS SUCCESS Options: Open Access: All
150 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\SORTTBLS.NLS SUCCESS
151 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\UNICODE.NLS SUCCESS Attributes: A

152 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\UNICODE.NLS SUCCESS Options: Open Access: All
153 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\UNICODE.NLS SUCCESS
154 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\USER32.DLL SUCCESS Attributes: A
155 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\USER32.DLL SUCCESS Options: Open Access: All
156 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\USER32.DLL SUCCESS
157 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\WS2HELP.DLL SUCCESS Attributes: A
158 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\WS2HELP.DLL SUCCESS Options: Open Access: All
159 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\WS2HELP.DLL SUCCESS
160 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\WS2_32.DLL SUCCESS Attributes: A
161 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\WS2_32.DLL SUCCESS Options: Open Access: All
162 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\WS2_32.DLL SUCCESS
163 7:19:35 PM svchost.exe:944 OPEN C:\ SUCCESS Options: Open Access: All
164 7:19:35 PM svchost.exe:944 CLOSE C:\ SUCCESS
165 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\ SUCCESS Options: Open Access: All
166 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\ SUCCESS

167 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\ SUCCESS Options: Open Access: All
168 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\ SUCCESS
169 7:19:35 PM svchost.exe:944 CREATE C:\WINDOWS\Prefetch\TARGET2.EXE-08FC3E78.pf SUCCESS Options: OverwriteIf Access: All
170 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\Prefetch\ SUCCESS Options: Open Access: 00000000
171 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\Prefetch\ SUCCESS
172 7:19:35 PM winlogon.exe:620 DIRECTORY C:\WINDOWS Change Notify
173 7:19:35 PM svchost.exe:944 WRITE C:\WINDOWS\Prefetch\TARGET2.EXE-08FC3E78.pf SUCCESS Offset: 0 Length: 5512

174 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\Prefetch\TARGET2.EXE-08FC3E78.pf SUCCESS
175 7:19:35 PM svchost.exe:944 READ C:\WINDOWS\system32\wbem\Repository\FS\INDEX.BTR SUCCESS Offset: 679936 Length: 8192
176 7:19:35 PM svchost.exe:944 READ C:\WINDOWS\system32\wbem\Repository\FS\INDEX.BTR SUCCESS Offset: 1105920 Length: 8192
177 7:19:35 PM svchost.exe:944 READ C:\WINDOWS\system32\wbem\Repository\FS\INDEX.BTR SUCCESS Offset: 589824 Length: 8192
178 7:19:35 PM svchost.exe:944 READ C:\WINDOWS\system32\wbem\Repository\FS\OBJECTS.DATA SUCCESS Offset: 4210688 Length: 8192
179 7:19:35 PM svchost.exe:944 READ C:\WINDOWS\system32\wbem\Repository\FS\OBJECTS.DATA SUCCESS Offset: 3072000 Length: 8192
180 7:19:35 PM svchost.exe:944 READ C:\WINDOWS\system32\wbem\Repository\FS\INDEX.BTR SUCCESS Offset: 32768 Length: 8192
181 7:19:35 PM svchost.exe:944 READ C:\WINDOWS\system32\wbem\Repository\FS\OBJECTS.DATA SUCCESS Offset: 0 Length: 8192
182 7:19:35 PM svchost.exe:944 READ C:\WINDOWS\system32\wbem\Repository\FS\OBJECTS.DATA SUCCESS Offset: 73728 Length: 8192
183 7:19:35 PM svchost.exe:944 READ C:\WINDOWS\system32\wbem\Repository\FS\INDEX.BTR SUCCESS Offset: 385024 Length: 8192
184 7:19:35 PM svchost.exe:944 READ C:\WINDOWS\system32\wbem\Repository\FS\OBJECTS.DATA SUCCESS Offset: 3096576 Length: 8192
185 7:19:35 PM explorer.exe:1908 QUERY INFORMATION C:\WINDOWS\System32\cmd.exe SUCCESS Attributes: A
186 7:19:35 PM svchost.exe:944 READ C:\WINDOWS\system32\wbem\Repository\FS\INDEX.BTR SUCCESS Offset: 0 Length: 8192
187 7:19:35 PM svchost.exe:944 READ C:\WINDOWS\system32\wbem\Repository\FS\INDEX.BTR SUCCESS Offset: 65536 Length: 8192
188 7:19:35 PM svchost.exe:944 READ C:\WINDOWS\system32\wbem\Repository\FS\OBJECTS.DATA SUCCESS Offset: 2998272 Length: 8192
189 7:19:35 PM svchost.exe:944 READ C:\WINDOWS\system32\wbem\Repository\FS\INDEX.BTR SUCCESS Offset: 458752 Length: 8192

190 7:19:35 PM svchost.exe:944 READ C:\WINDOWS\system32\wbem\Repository\FS\INDEX.BTR SUCCESS Offset: 671744 Length: 8192
191 7:19:35 PM svchost.exe:944 READ C:\WINDOWS\system32\wbem\Repository\FS\INDEX.BTR SUCCESS Offset: 573440 Length: 8192
192 7:19:35 PM svchost.exe:944 READ C:\WINDOWS\system32\wbem\Repository\FS\OBJECTS.DATA SUCCESS Offset: 2154496 Length: 8192
193 7:19:35 PM svchost.exe:944 READ C:\WINDOWS\system32\wbem\Repository\FS\OBJECTS.DATA SUCCESS Offset: 3014656 Length: 8192
194 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\system32\rpcss.dll SUCCESS Attributes: A
195 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\system32\rpcss.dll SUCCESS Options: Open Access: Execute
196 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\system32\rpcss.dll SUCCESS Length: 259072
197 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\system32\rpcss.dll SUCCESS
198 7:19:35 PM svchost.exe:944 READ C:\WINDOWS\system32\wbem\Repository\FS\INDEX.BTR SUCCESS Offset: 466944 Length: 8192
199 7:19:35 PM svchost.exe:944 READ C:\WINDOWS\system32\wbem\Repository\FS\INDEX.BTR SUCCESS Offset: 851968 Length: 8192
200 7:19:35 PM svchost.exe:944 READ C:\WINDOWS\system32\wbem\Repository\FS\INDEX.BTR SUCCESS Offset: 737280 Length: 8192
201 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\System32\wbem\wbemcons.dll SUCCESS Attributes: A
202 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\System32\wbem\wbemcons.dll SUCCESS Options: Open Access: Execute
203 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\System32\wbem\wbemcons.dll SUCCESS Length: 66048
204 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\System32\wbem\wbemcons.dll SUCCESS
205 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\System32\wbem\wbemcons.dll SUCCESS Attributes: A
206 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\System32\wbem\wbemcons.dll SUCCESS Options: Open Access: Execute
207 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\System32\wbem\wbemcons.dll SUCCESS

208 7:19:35 PM svchost.exe:944 OPEN C:\ SUCCESS Options: Open Directory Access: All
209 7:19:35 PM svchost.exe:944 DIRECTORY C:\ SUCCESS FileBothDirectoryInformation: WINDOWS
210 7:19:35 PM svchost.exe:944 CLOSE C:\ SUCCESS
211 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\ SUCCESS Options: Open Directory Access: All
212 7:19:35 PM svchost.exe:944 DIRECTORY C:\WINDOWS\ SUCCESS FileBothDirectoryInformation: system32
213 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\ SUCCESS

214 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\system32\ SUCCESS Options: Open Directory Access: All
215 7:19:35 PM svchost.exe:944 DIRECTORY C:\WINDOWS\system32\ SUCCESS FileBothDirectoryInformation: WBEM
216 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\system32\ SUCCESS
217 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\system32\WBEM\ SUCCESS Options: Open Directory Access: All
218 7:19:35 PM svchost.exe:944 DIRECTORY C:\WINDOWS\system32\WBEM\ SUCCESS FileBothDirectoryInformation: Logs
219 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\system32\WBEM\ SUCCESS
220 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\system32\rpcss.dll SUCCESS Attributes: A
221 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\system32\rpcss.dll SUCCESS Options: Open Access: Execute
222 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\system32\rpcss.dll SUCCESS Length: 259072
223 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\system32\rpcss.dll SUCCESS
224 7:19:35 PM svchost.exe:944 OPEN C:\WINDOWS\system32\WBEM\Logs\wbemess.log SUCCESS Options: OpenIf Access: All
225 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\system32\WBEM\Logs\wbemess.log SUCCESS Length: 10351

226 7:19:35 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\system32\WBEM\Logs\wbemess.log SUCCESS Length: 10351

227 7:19:35 PM svchost.exe:944 WRITE C:\WINDOWS\system32\WBEM\Logs\wbemess.log SUCCESS Offset: 10351 Length: 96
228 7:19:35 PM svchost.exe:944 CLOSE C:\WINDOWS\system32\WBEM\Logs\wbemess.log SUCCESS

229 7:19:35 PM services.exe:664 WRITE C:\WINDOWS\system32\config\SysEvent.Evt SUCCESS Offset: 12864 Length: 196
230 7:19:35 PM services.exe:664 WRITE C:\WINDOWS\system32\config\SysEvent.Evt SUCCESS Offset: 13060 Length: 40

Appendix C - Filemon Log File When Running 'target2.exe -d test'

255 7:26:16 PM cmd.exe:524 QUERY INFORMATION C:\target2.exe SUCCESS Attributes: A
256 7:26:16 PM cmd.exe:524 OPEN C:\ SUCCESS Options: Open Directory Access: All
257 7:26:16 PM cmd.exe:524 DIRECTORY C:\ SUCCESS FileBothDirectoryInformation: target2.exe
258 7:26:16 PM cmd.exe:524 CLOSE C:\ SUCCESS
259 7:26:16 PM cmd.exe:524 OPEN C:\target2.exe SUCCESS Options: Open Access: All
260 7:26:16 PM cmd.exe:524 QUERY INFORMATION C:\target2.exe SUCCESS Attributes: A
261 7:26:16 PM cmd.exe:524 QUERY INFORMATION C:\target2.exe SUCCESS Length: 26793
262 7:26:16 PM cmd.exe:524 QUERY INFORMATION C:\target2.exe SUCCESS Attributes: A
263 7:26:16 PM cmd.exe:524 OPEN C:\ SUCCESS Options: Open Directory Access: All
264 7:26:16 PM cmd.exe:524 DIRECTORY C:\ SUCCESS FileBothDirectoryInformation: target2.exe
265 7:26:16 PM cmd.exe:524 CLOSE C:\ SUCCESS
266 7:26:16 PM cmd.exe:524 OPEN C:\target2.exe.Manifest FILE NOT FOUND Options: Open Access: All
267 7:26:16 PM cmd.exe:524 QUERY INFORMATION C:\ SUCCESS Attributes: DHSA
268 7:26:16 PM cmd.exe:524 CLOSE C:\target2.exe SUCCESS
269 7:26:16 PM target2.exe:412 QUERY INFORMATION C:\target2.exe SUCCESS FileNameInformation
270 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\Prefetch\TARGET2.EXE-08FC3E78.pfSUCCESS Options: Open Access: All
271 7:26:16 PM target2.exe:412 QUERY INFORMATION C:\WINDOWS\Prefetch\TARGET2.EXE-08FC3E78.pf SUCCESS Length: 5512
272 7:26:16 PM target2.exe:412 READ C:\WINDOWS\Prefetch\TARGET2.EXE-08FC3E78.pf SUCCESS Offset: 0 Length: 5512
273 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\Prefetch\TARGET2.EXE-08FC3E78.pf SUCCESS
274 7:26:16 PM target2.exe:412 OPEN C: SUCCESS Options: Open Access: All
275 7:26:16 PM target2.exe:412 OPEN C:\ SUCCESS Options: Open Directory Access: All
276 7:26:16 PM target2.exe:412 DIRECTORY C:\ SUCCESS FileNamesInformation

277 7:26:16 PM target2.exe:412 DIRECTORY C:\ NO MORE FILES FileNamesInformation
278 7:26:16 PM target2.exe:412 CLOSE C:\ SUCCESS

279 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\ SUCCESS Options: Open Directory Access: All
280 7:26:16 PM target2.exe:412 DIRECTORY C:\WINDOWS\ SUCCESS FileNamesInformation
281 7:26:16 PM target2.exe:412 DIRECTORY C:\WINDOWS\ NO MORE FILES FileNamesInformation
282 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\ SUCCESS

283 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\ SUCCESS Options: Open Directory Access: All
284 7:26:16 PM target2.exe:412 DIRECTORY C:\WINDOWS\SYSTEM32\ SUCCESS FileNamesInformation
285 7:26:16 PM target2.exe:412 DIRECTORY C:\WINDOWS\SYSTEM32\ SUCCESS FileNamesInformation
286 7:26:16 PM target2.exe:412 DIRECTORY C:\WINDOWS\SYSTEM32\ SUCCESS FileNamesInformation
287 7:26:16 PM target2.exe:412 DIRECTORY C:\WINDOWS\SYSTEM32\ SUCCESS FileNamesInformation
288 7:26:16 PM target2.exe:412 DIRECTORY C:\WINDOWS\SYSTEM32\ NO MORE FILES FileNamesInformation
289 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\ SUCCESS
290 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\NTDLL.DLL SUCCESS Options: Open Access: All
291 7:26:16 PM target2.exe:412 QUERY INFORMATION C:\WINDOWS\SYSTEM32\NTDLL.DLL SUCCESS Length: 674304
292 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\KERNEL32.DLL SUCCESS Options: Open Access: All
293 7:26:16 PM target2.exe:412 QUERY INFORMATION C:\WINDOWS\SYSTEM32\KERNEL32.DLL SUCCESS Length: 926720
294 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\UNICODE.NLS SUCCESS Options: Open Access: All
295 7:26:16 PM target2.exe:412 QUERY INFORMATION C:\WINDOWS\SYSTEM32\UNICODE.NLS SUCCESS Length: 89588
296 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\LOCALE.NLS SUCCESS Options: Open Access: All
297 7:26:16 PM target2.exe:412 QUERY INFORMATION C:\WINDOWS\SYSTEM32\LOCALE.NLS SUCCESS Length: 209012
298 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\SORTTBLS.NLS SUCCESS Options: Open Access: All

299 7:26:16 PM target2.exe:412 QUERY INFORMATION C:\WINDOWS\SYSTEM32\SORTTBLS.NLS SUCCESS Length: 21116
300 7:26:16 PM target2.exe:412 OPEN C:\TARGET2.EXE SUCCESS Options: Open Access: All
301 7:26:16 PM target2.exe:412 QUERY INFORMATION C:\TARGET2.EXE SUCCESS Length: 26793
302 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\ADVAPI32.DLL SUCCESS Options: Open Access: All
303 7:26:16 PM target2.exe:412 QUERY INFORMATION C:\WINDOWS\SYSTEM32\ADVAPI32.DLL SUCCESS Length: 549888
304 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\RPCRT4.DLL SUCCESS Options: Open Access: All
305 7:26:16 PM target2.exe:412 QUERY INFORMATION C:\WINDOWS\SYSTEM32\RPCRT4.DLL SUCCESS Length: 463872
306 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\WS2_32.DLL SUCCESS Options: Open Access: All
307 7:26:16 PM target2.exe:412 QUERY INFORMATION C:\WINDOWS\SYSTEM32\WS2_32.DLL SUCCESS Length: 75264
308 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\MSVCRT.DLL SUCCESS Options: Open Access: All
309 7:26:16 PM target2.exe:412 QUERY INFORMATION C:\WINDOWS\SYSTEM32\MSVCRT.DLL SUCCESS Length: 322560
310 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\WS2HELP.DLL SUCCESS Options: Open Access: All
311 7:26:16 PM target2.exe:412 QUERY INFORMATION C:\WINDOWS\SYSTEM32\WS2HELP.DLL SUCCESS Length: 18944
312 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\MFC42.DLL SUCCESS Options: Open Access: All
313 7:26:16 PM target2.exe:412 QUERY INFORMATION C:\WINDOWS\SYSTEM32\MFC42.DLL SUCCESS Length: 995383
314 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\GDI32.DLL SUCCESS Options: Open Access: All
315 7:26:16 PM target2.exe:412 QUERY INFORMATION C:\WINDOWS\SYSTEM32\GDI32.DLL SUCCESS Length: 250880
316 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\USER32.DLL SUCCESS Options: Open Access: All
317 7:26:16 PM target2.exe:412 QUERY INFORMATION C:\WINDOWS\SYSTEM32\USER32.DLL SUCCESS Length: 561152
318 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\MSVCP60.DLL SUCCESS Options: Open Access: All
319 7:26:16 PM target2.exe:412 QUERY INFORMATION C:\WINDOWS\SYSTEM32\MSVCP60.DLL SUCCESS Length: 401462
320 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\CTYPE.NLS SUCCESS Options: Open Access: All
321 7:26:16 PM target2.exe:412 QUERY INFORMATION C:\WINDOWS\SYSTEM32\CTYPE.NLS SUCCESS Length: 8386

322 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\NTDLL.DLL SUCCESS
323 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\KERNEL32.DLL SUCCESS
324 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\UNICODE.NLS SUCCESS
325 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\LOCALE.NLS SUCCESS
326 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\SORTTBLS.NLS SUCCESS
327 7:26:16 PM target2.exe:412 CLOSE C:\TARGET2.EXE SUCCESS

328 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\ADVAPI32.DLL SUCCESS
329 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\RPCRT4.DLL SUCCESS
330 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\WS2_32.DLL SUCCESS
331 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\MSVCRT.DLL SUCCESS
332 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\WS2HELP.DLL SUCCESS
333 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\MFC42.DLL SUCCESS
334 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\GDI32.DLL SUCCESS
335 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\USER32.DLL SUCCESS
336 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\MSVCP60.DLL SUCCESS
337 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\CTYPE.NLS SUCCESS
338 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\NTDLL.DLL SUCCESS Options: Open Access: Execute
339 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\KERNEL32.DLL SUCCESS Options: Open Access: Execute
340 7:26:16 PM target2.exe:412 OPEN C:\TARGET2.EXE SUCCESS Options: Open Access: Execute
341 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\ADVAPI32.DLL SUCCESS Options: Open Access: Execute
342 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\RPCRT4.DLL SUCCESS Options: Open Access: Execute
343 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\WS2_32.DLL SUCCESS Options: Open Access: Execute

344 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\MSVCRT.DLL SUCCESS Options: Open Access: Execute
345 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\WS2HELP.DLL SUCCESS Options: Open Access: Execute
346 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\MFC42.DLL SUCCESS Options: Open Access: Execute
347 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\GDI32.DLL SUCCESS Options: Open Access: Execute
348 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\USER32.DLL SUCCESS Options: Open Access: Execute
349 7:26:16 PM target2.exe:412 OPEN C:\WINDOWS\SYSTEM32\MSVCP60.DLL SUCCESS Options: Open Access: Execute
350 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\NTDLL.DLL SUCCESS
351 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\KERNEL32.DLL SUCCESS
352 7:26:16 PM target2.exe:412 CLOSE C:\TARGET2.EXE SUCCESS

353 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\ADVAPI32.DLL SUCCESS
354 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\RPCRT4.DLL SUCCESS
355 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\WS2_32.DLL SUCCESS
356 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\MSVCRT.DLL SUCCESS
357 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\WS2HELP.DLL SUCCESS
358 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\MFC42.DLL SUCCESS
359 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\GDI32.DLL SUCCESS
360 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\USER32.DLL SUCCESS
361 7:26:16 PM target2.exe:412 CLOSE C:\WINDOWS\SYSTEM32\MSVCP60.DLL SUCCESS
362 7:26:16 PM target2.exe:412 CLOSE C: SUCCESS
363 7:26:16 PM target2.exe:412 OPEN C:\ SUCCESS Options: Open Directory Access: Traverse
364 7:26:16 PM target2.exe:412 QUERY INFORMATION C:\target2.exe.Local FILE NOT FOUND Attributes: Error
365 7:26:16 PM target2.exe:412 QUERY INFORMATION C:\WS2_32.dll FILE NOT FOUND Attributes: Error
366 7:26:16 PM target2.exe:412 QUERY INFORMATION C:\WS2_32.dll FILE NOT FOUND Attributes: Error

```
367  7:26:16 PM  target2.exe:412  QUERY INFORMATION
     C:\WINDOWS\System32\WS2_32.dll  SUCCESS  Attributes: A
368  7:26:16 PM  target2.exe:412  OPEN C:\WINDOWS\System32\WS2_32.dll
     SUCCESS  Options: Open  Access: Execute
369  7:26:16 PM  target2.exe:412  CLOSE
     C:\WINDOWS\System32\WS2_32.dll  SUCCESS
370  7:26:16 PM  target2.exe:412  QUERY INFORMATION  C:\WS2HELP.dll
     FILE NOT FOUND  Attributes: Error
371  7:26:16 PM  target2.exe:412  QUERY INFORMATION  C:\WS2HELP.dll
     FILE NOT FOUND  Attributes: Error
372  7:26:16 PM  target2.exe:412  QUERY INFORMATION
     C:\WINDOWS\System32\WS2HELP.dll  SUCCESS  Attributes: A
373  7:26:16 PM  target2.exe:412  OPEN C:\WINDOWS\System32\WS2HELP.dll
     SUCCESS  Options: Open  Access: Execute
374  7:26:16 PM  target2.exe:412  CLOSE
     C:\WINDOWS\System32\WS2HELP.dll  SUCCESS
375  7:26:16 PM  target2.exe:412  QUERY INFORMATION  C:\MFC42.DLL
     FILE NOT FOUND  Attributes: Error
376  7:26:16 PM  target2.exe:412  QUERY INFORMATION  C:\MFC42.DLL
     FILE NOT FOUND  Attributes: Error
377  7:26:16 PM  target2.exe:412  QUERY INFORMATION
     C:\WINDOWS\System32\MFC42.DLL  SUCCESS  Attributes: A
378  7:26:16 PM  target2.exe:412  OPEN C:\WINDOWS\System32\MFC42.DLL
     SUCCESS  Options: Open  Access: Execute
379  7:26:16 PM  target2.exe:412  CLOSE
     C:\WINDOWS\System32\MFC42.DLL  SUCCESS
380  7:26:16 PM  target2.exe:412  QUERY INFORMATION  C:\MSVCP60.dll
     FILE NOT FOUND  Attributes: Error
381  7:26:16 PM  target2.exe:412  QUERY INFORMATION  C:\MSVCP60.dll
     FILE NOT FOUND  Attributes: Error
382  7:26:16 PM  target2.exe:412  QUERY INFORMATION
     C:\WINDOWS\System32\MSVCP60.dll  SUCCESS  Attributes: A
383  7:26:16 PM  target2.exe:412  OPEN C:\WINDOWS\System32\MSVCP60.dll
     SUCCESS  Options: Open  Access: Execute
384  7:26:16 PM  target2.exe:412  CLOSE
     C:\WINDOWS\System32\MSVCP60.dll  SUCCESS
385  7:26:16 PM  target2.exe:412  QUERY INFORMATION
     C:\WINDOWS\System32\MFC42LOC.DLL  FILE NOT FOUND  Attributes: Error

386  7:26:16 PM  target2.exe:412  QUERY INFORMATION
     C:\WINDOWS\System32\MFC42LOC.DLL  FILE NOT FOUND  Attributes: Error

387  7:26:16 PM  services.exe:664  SET INFORMATION
     C:\WINDOWS\system32\config\system.LOG  SUCCESS  Length: 8192
388  7:26:16 PM  services.exe:664  SET INFORMATION
     C:\WINDOWS\system32\config\system.LOG  SUCCESS  Length: 8192
```

389 7:26:16 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 16384
390 7:26:16 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 20480
391 7:26:16 PM explorer.exe:1908 QUERY INFORMATION C:\WINDOWS\System32\cmd.exe SUCCESS Attributes: A
392 7:26:16 PM target2.exe:412 CLOSE C:\ SUCCESS
393 7:26:16 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 24576
394 7:26:16 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 28672
395 7:26:16 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 32768
396 7:26:16 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 36864
397 7:26:16 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 40960
398 7:26:16 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 45056
399 7:26:16 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 49152
400 7:26:16 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 53248
401 7:26:16 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 57344
402 7:26:16 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 61440
403 7:26:17 PM explorer.exe:1908 QUERY INFORMATION C:\WINDOWS\System32\cmd.exe SUCCESS Attributes: A
404 7:26:17 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 65536
405 7:26:17 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 69632
406 7:26:17 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 73728
407 7:26:17 PM services.exe:664 SET INFORMATION C:\WINDOWS\system32\config\system.LOG SUCCESS Length: 77824
408 7:26:17 PM svchost.exe:944 OPEN C:\WINDOWS\Prefetch\TARGET2.EXE-08FC3E78.pfSUCCESS Options: Open Access: All
409 7:26:17 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\Prefetch\TARGET2.EXE-08FC3E78.pf SUCCESS Length: 5512
410 7:26:17 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\Prefetch\TARGET2.EXE-08FC3E78.pf SUCCESS Length: 5512
411 7:26:17 PM svchost.exe:944 CLOSE C:\WINDOWS\Prefetch\TARGET2.EXE-08FC3E78.pf SUCCESS

412 7:26:17 PM svchost.exe:944 QUERY INFORMATION C:\TARGET2.EXE SUCCESS Attributes: A
413 7:26:17 PM svchost.exe:944 OPEN C:\TARGET2.EXE SUCCESS Options: Open Access: All
414 7:26:17 PM svchost.exe:944 CLOSE C:\TARGET2.EXE SUCCESS

415 7:26:17 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\ADVAPI32.DLL SUCCESS Attributes: A
416 7:26:17 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\ADVAPI32.DLL SUCCESS Options: Open Access: All
417 7:26:17 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\ADVAPI32.DLL SUCCESS
418 7:26:17 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\CTYPE.NLS SUCCESS Attributes: A
419 7:26:17 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\CTYPE.NLS SUCCESS Options: Open Access: All
420 7:26:17 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\CTYPE.NLS SUCCESS
421 7:26:17 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\GDI32.DLL SUCCESS Attributes: A
422 7:26:17 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\GDI32.DLL SUCCESS Options: Open Access: All
423 7:26:17 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\GDI32.DLL SUCCESS
424 7:26:17 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\KERNEL32.DLL SUCCESS Attributes: A
425 7:26:17 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\KERNEL32.DLL SUCCESS Options: Open Access: All
426 7:26:17 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\KERNEL32.DLL SUCCESS
427 7:26:17 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\LOCALE.NLS SUCCESS Attributes: A
428 7:26:17 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\LOCALE.NLS SUCCESS Options: Open Access: All
429 7:26:17 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\LOCALE.NLS SUCCESS
430 7:26:17 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\MFC42.DLL SUCCESS Attributes: A
431 7:26:17 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\MFC42.DLL SUCCESS Options: Open Access: All
432 7:26:17 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\MFC42.DLL SUCCESS
433 7:26:17 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\MSVCP60.DLL SUCCESS Attributes: A

434 7:26:17 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\MSVCP60.DLL SUCCESS Options: Open Access: All
435 7:26:17 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\MSVCP60.DLL SUCCESS
436 7:26:17 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\MSVCRT.DLL SUCCESS Attributes: A
437 7:26:17 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\MSVCRT.DLL SUCCESS Options: Open Access: All
438 7:26:17 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\MSVCRT.DLL SUCCESS
439 7:26:17 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\NTDLL.DLL SUCCESS Attributes: A
440 7:26:17 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\NTDLL.DLL SUCCESS Options: Open Access: All
441 7:26:17 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\NTDLL.DLL SUCCESS
442 7:26:17 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\RPCRT4.DLL SUCCESS Attributes: A
443 7:26:17 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\RPCRT4.DLL SUCCESS Options: Open Access: All
444 7:26:17 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\RPCRT4.DLL SUCCESS
445 7:26:17 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\SORTTBLS.NLS SUCCESS Attributes: A
446 7:26:17 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\SORTTBLS.NLS SUCCESS Options: Open Access: All
447 7:26:17 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\SORTTBLS.NLS SUCCESS
448 7:26:17 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\UNICODE.NLS SUCCESS Attributes: A
449 7:26:17 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\UNICODE.NLS SUCCESS Options: Open Access: All
450 7:26:17 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\UNICODE.NLS SUCCESS
451 7:26:17 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\USER32.DLL SUCCESS Attributes: A
452 7:26:17 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\USER32.DLL SUCCESS Options: Open Access: All
453 7:26:17 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\USER32.DLL SUCCESS
454 7:26:17 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\WS2HELP.DLL SUCCESS Attributes: A
455 7:26:17 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\WS2HELP.DLL SUCCESS Options: Open Access: All

456 7:26:17 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\WS2HELP.DLL SUCCESS
457 7:26:17 PM svchost.exe:944 QUERY INFORMATION C:\WINDOWS\SYSTEM32\WS2_32.DLL SUCCESS Attributes: A
458 7:26:17 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\WS2_32.DLL SUCCESS Options: Open Access: All
459 7:26:17 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\WS2_32.DLL SUCCESS
460 7:26:17 PM svchost.exe:944 OPEN C:\ SUCCESS Options: Open Access: All
461 7:26:17 PM svchost.exe:944 CLOSE C:\ SUCCESS
462 7:26:17 PM svchost.exe:944 OPEN C:\WINDOWS\ SUCCESS Options: Open Access: All
463 7:26:17 PM svchost.exe:944 CLOSE C:\WINDOWS\ SUCCESS

464 7:26:17 PM svchost.exe:944 OPEN C:\WINDOWS\SYSTEM32\ SUCCESS Options: Open Access: All
465 7:26:17 PM svchost.exe:944 CLOSE C:\WINDOWS\SYSTEM32\ SUCCESS
466 7:26:17 PM svchost.exe:944 CREATE C:\WINDOWS\Prefetch\TARGET2.EXE-08FC3E78.pf SUCCESS Options: OverwriteIf Access: All
467 7:26:17 PM svchost.exe:944 OPEN C:\WINDOWS\Prefetch\ SUCCESS Options: Open Access: 00000000
468 7:26:17 PM svchost.exe:944 CLOSE C:\WINDOWS\Prefetch\ SUCCESS
469 7:26:17 PM svchost.exe:944 WRITE C:\WINDOWS\Prefetch\TARGET2.EXE-08FC3E78.pf SUCCESS Offset: 0 Length: 5524
470 7:26:17 PM svchost.exe:944 CLOSE C:\WINDOWS\Prefetch\TARGET2.EXE-08FC3E78.pf SUCCESS

Appendix D - Regmon Log File When Running 'target2.exe -i test'

1 1.93135582 cmd.exe:524 OpenKey HKCU SUCCESS Key: 0xE14F5020
2 1.93145639 cmd.exe:524 OpenKey HKLM\System\CurrentControlSet\Control\Nls\MUILanguages NOTFOUND

3 1.93153769 cmd.exe:524 OpenKey HKCU\Control Panel\Desktop SUCCESS Key: 0xE1441E98
4 1.93159384 cmd.exe:524 QueryValue HKCU\Control Panel\Desktop\MultiUILanguageId NOTFOUND
5 1.93167094 cmd.exe:524 CloseKey HKCU\Control Panel\Desktop SUCCESS Key: 0xE1441E98
6 1.93172710 cmd.exe:524 CloseKey HKCU SUCCESS Key: 0xE14F5020
7 1.93178995 cmd.exe:524 OpenKey HKLM\System\CurrentControlSet\Control\Nls\MUILanguages NOTFOUND

8 1.93706828 cmd.exe:524 OpenKey HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers NOTFOUND
9 1.93712946 cmd.exe:524 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom\target2.exe NOTFOUND
10 1.93840671 cmd.exe:524 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\target2.exeNOTFOUND
11 1.93851818 cmd.exe:524 OpenKey HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers SUCCESS Key: 0xE14F5020
12 1.93865814 cmd.exe:524 QueryValue HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\ExecutableTypes BUFTOOSMALL
13 1.93883666 cmd.exe:524 QueryValue HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\ExecutableTypes SUCCESS "ADE"
14 1.93893388 cmd.exe:524 CloseKey HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers SUCCESS Key: 0xE14F5020
15 1.94020862 cmd.exe:524 OpenKey HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers SUCCESS Key: 0xE14F5020
16 1.94025555 cmd.exe:524 QueryValue HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\LogFileName NOTFOUND
17 1.94032763 cmd.exe:524 CloseKey HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers SUCCESS Key: 0xE14F5020

18 1.96470949 target2.exe:1536 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\target2.exeNOTFOUND
19 1.97256412 target2.exe:1536 OpenKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS Key: 0xE1441E98
20 1.97261692 target2.exe:1536 QueryValue HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat SUCCESS 0x0
21 1.97268732 target2.exe:1536 CloseKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS Key: 0xE1441E98
22 1.98041456 target2.exe:1536 OpenKey HKLM\System\CurrentControlSet\Control\SafeBoot\Option NOTFOUND
23 1.98048831 target2.exe:1536 OpenKey HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers SUCCESS Key: 0xE1441E98
24 1.98053105 target2.exe:1536 QueryValue HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled SUCCESS 0x1
25 1.98060313 target2.exe:1536 CloseKey HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers SUCCESS Key: 0xE1441E98
26 1.98075734 target2.exe:1536 OpenKey HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers NOTFOUND

27 2.00877486 target2.exe:1536 OpenKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS Key: 0xE1441E98
28 2.00882430 target2.exe:1536 QueryValue HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat SUCCESS 0x0
29 2.00889470 target2.exe:1536 CloseKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS Key: 0xE1441E98
30 2.00946377 target2.exe:1536 OpenKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS Key: 0xE1441E98
31 2.00951154 target2.exe:1536 QueryValue HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat SUCCESS 0x0
32 2.00955009 target2.exe:1536 QueryValue HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled SUCCESS 0x0
33 2.00961463 target2.exe:1536 CloseKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS Key: 0xE1441E98

34 2.00972861 target2.exe:1536 OpenKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon SUCCESS Key: 0xE1441E98
35 2.00984007 target2.exe:1536 QueryValue HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LeakTrack NOTFOUND
36 2.00989204 target2.exe:1536 CloseKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon SUCCESS Key: 0xE1441E98
37 2.00994987 target2.exe:1536 OpenKey HKLM SUCCESS Key: 0xE1441E98
38 2.01000183 target2.exe:1536 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics NOTFOUND
39 2.01337600 target2.exe:1536 OpenKey HKLM\System\CurrentControlSet\Control\Error Message Instrument\ NOTFOUND
40 2.02059451 target2.exe:1536 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32 SUCCESS Key: 0xE105F738
41 2.02076967 target2.exe:1536 QueryValue HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32\target2 NOTFOUND
42 2.02090125 target2.exe:1536 CloseKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32 SUCCESS Key: 0xE105F738
43 2.02107306 target2.exe:1536 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility SUCCESS Key: 0xE105F738
44 2.02111748 target2.exe:1536 QueryValue HKLM\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility\target2 NOTFOUND
45 2.02117615 target2.exe:1536 CloseKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility SUCCESS Key: 0xE105F738
46 2.02412289 target2.exe:1536 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows SUCCESS Key: 0xE105F738
47 2.02417234 target2.exe:1536 QueryValue HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs SUCCESS ""
48 2.02424022 target2.exe:1536 CloseKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows SUCCESS Key: 0xE105F738
49 2.03484464 explorer.exe:1908 QueryKey HKCU SUCCESS Name: \REGISTRY\USER\S-1-5-21-1659004503-842925246-839522115-500_CLASSES
50 2.03503238 explorer.exe:1908 OpenKey HKCU\Applications\cmd.exe NOTFOUND
51 2.03508015 explorer.exe:1908 OpenKey HKCR\Applications\cmd.exe NOTFOUND
52 2.04957416 target2.exe:1536 OpenKey HKLM\System\CurrentControlSet\Control\Session Manager SUCCESS Key: 0xE105F738
53 2.04962696 target2.exe:1536 QueryValue HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode NOTFOUND

54 2.04970072 target2.exe:1536 CloseKey HKLM\System\CurrentControlSet\Control\Session Manager SUCCESS Key: 0xE105F738
55 2.07147443 target2.exe:1536 OpenKey HKLM\Software\Microsoft\Rpc\PagedBuffers NOTFOUND
56 2.07156746 target2.exe:1536 OpenKey HKLM\Software\Microsoft\Rpc SUCCESS Key: 0xE105F738
57 2.07160517 target2.exe:1536 QueryValue HKLM\Software\Microsoft\Rpc\MaxRpcSize NOTFOUND
58 2.07167138 target2.exe:1536 CloseKey HKLM\Software\Microsoft\Rpc SUCCESS Key: 0xE105F738
59 2.07173256 target2.exe:1536 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\target2.exe\RpcThreadPoolThrottle NOTFOUND
60 2.07188007 target2.exe:1536 OpenKey HKLM\Software\Policies\Microsoft\Windows NT\Rpc NOTFOUND
61 2.07259831 target2.exe:1536 OpenKey HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key: 0xE105F738
62 2.07265949 target2.exe:1536 OpenKey HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName SUCCESS Key: 0xE17D46B8
63 2.07270224 target2.exe:1536 QueryValue HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\ComputerName SUCCESS "TEXTBOX"
64 2.07276761 target2.exe:1536 CloseKey HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName SUCCESS Key: 0xE17D46B8
65 2.07281873 target2.exe:1536 CloseKey HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key: 0xE105F738
66 2.10025629 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE105F738
67 2.10433949 services.exe:664 CreateKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE17D46B8
68 2.10451549 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE105F738
69 2.10523122 services.exe:664 SetValue HKLM\System\CurrentControlSet\Services\Local Partners Access\Type SUCCESS 0x10
70 2.10577012 services.exe:664 SetValue HKLM\System\CurrentControlSet\Services\Local Partners Access\Start SUCCESS 0x2

71 2.10608943 services.exe:664 SetValue HKLM\System\CurrentControlSet\Services\Local Partners Access\ErrorControl SUCCESS 0x1
72 2.10644562 services.exe:664 SetValue HKLM\System\CurrentControlSet\Services\Local Partners Access\ImagePath SUCCESS "smsses.exe"
73 2.10665263 services.exe:664 SetValue HKLM\System\CurrentControlSet\Services\Local Partners Access\DisplayName SUCCESS "Local Printer Manager Service"
74 2.11637789 services.exe:664 CreateKey HKLM\System\CurrentControlSet\Services\Local Partners Access\Security SUCCESS Key: 0xE1514A70
75 2.11657316 services.exe:664 SetValue HKLM\System\CurrentControlSet\Services\Local Partners Access\Security\Security SUCCESS 01 00 14 80 90 00 00 00 ...
76 2.11670055 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services\Local Partners Access\Security SUCCESS Key: 0xE1514A70
77 2.11726794 services.exe:664 SetValue HKLM\System\CurrentControlSet\Services\Local Partners Access\ObjectName SUCCESS "LocalSystem"
78 2.14647053 services.exe:664 FlushKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE17D46B8
79 2.14660882 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE17D46B8
80 2.15015815 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE17D46B8
81 2.15022268 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE1514A70
82 2.15029308 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE17D46B8
83 2.15036013 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE17D46B8
84 2.15041377 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE105F738
85 2.15045986 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE17D46B8
86 2.15054870 services.exe:664 QueryValue HKLM\System\CurrentControlSet\Services\Local Partners Access\ImagePath BUFOVRFLOW

87 2.15059061 services.exe:664 QueryValue HKLM\System\CurrentControlSet\Services\Local Partners Access\ImagePath SUCCESS "smsses.exe"
88 2.15064173 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE105F738
89 2.15070794 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE105F738
90 2.15076074 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE17D46B8
91 2.15080683 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE105F738
92 2.15084790 services.exe:664 QueryValue HKLM\System\CurrentControlSet\Services\Local Partners Access\Type SUCCESS 0x10
93 2.15088478 services.exe:664 QueryValue HKLM\System\CurrentControlSet\Services\Local Partners Access\Start SUCCESS 0x2
94 2.15092249 services.exe:664 QueryValue HKLM\System\CurrentControlSet\Services\Local Partners Access\ErrorControl SUCCESS 0x1
95 2.15096104 services.exe:664 QueryValue HKLM\System\CurrentControlSet\Services\Local Partners Access\Tag NOTFOUND
96 2.15099876 services.exe:664 QueryValue HKLM\System\CurrentControlSet\Services\Local Partners Access\DependOnService NOTFOUND
97 2.15103563 services.exe:664 QueryValue HKLM\System\CurrentControlSet\Services\Local Partners Access\DependOnGroup NOTFOUND
98 2.15107167 services.exe:664 QueryValue HKLM\System\CurrentControlSet\Services\Local Partners Access\Group NOTFOUND
99 2.15112363 services.exe:664 QueryValue HKLM\System\CurrentControlSet\Services\Local Partners Access\DisplayName BUFOVRFLOW
100 2.15120744 services.exe:664 QueryValue HKLM\System\CurrentControlSet\Services\Local Partners Access\DisplayName SUCCESS "Local Printer Manager Service"
101 2.15125605 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE17D46B8
102 2.15129963 services.exe:664 QueryValue HKLM\System\CurrentControlSet\Services\Local Partners Access\ObjectName BUFOVRFLOW

103 2.15133902 services.exe:664 QueryValue HKLM\System\CurrentControlSet\Services\Local Partners Access\ObjectName SUCCESS "LocalSystem"
104 2.15138847 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE1514A70
105 2.15419525 services.exe:664 OpenKey HKLM\SYSTEM\ControlSet001\Services\Local Partners Access SUCCESS Key: 0xE1514A70
106 2.15424554 services.exe:664 QueryValue HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\PlugPlayServiceType NOTFOUND
107 2.15438131 services.exe:664 OpenKey HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\Enum NOTFOUND
108 2.15449529 services.exe:664 CloseKey HKLM\SYSTEM\ControlSet001\Services\Local Partners Access SUCCESS Key: 0xE1514A70
109 2.15457240 services.exe:664 OpenKey HKLM\SYSTEM\ControlSet001\Services\Local Partners Access SUCCESS Key: 0xE1514A70
110 2.15461011 services.exe:664 QueryValue HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\PlugPlayServiceType NOTFOUND
111 2.15464699 services.exe:664 OpenKey HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\Enum NOTFOUND
112 2.15563426 services.exe:664 OpenKey HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\ROOT SUCCESS Key: 0xE17D46B8
113 2.15710260 services.exe:664 CreateKey HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\ROOT\LEGACY_LOCAL_PARTNERS_ACCESS SUCCESS Key: 0xE105F738
114 2.15724089 services.exe:664 CloseKey HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\ROOT SUCCESS Key: 0xE17D46B8
115 2.15776219 services.exe:664 SetValue HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\ROOT\LEGACY_LOCAL_PARTNERS_ACCESS\NextInstance SUCCESS 0x1
116 2.15810664 services.exe:664 CreateKey HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\ROOT\LEGACY_LOCAL_PARTNERS_ACCESS\0000 SUCCESS Key: 0xE17D46B8
117 2.15820135 services.exe:664 CloseKey HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\ROOT\LEGACY_LOCAL_PARTNERS_ACCESS SUCCESS Key: 0xE105F738

118 2.15872013 services.exe:664 CreateKey
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\ROOT\LEGACY_LOCAL_PART
NERS_ACCESS\0000\Control SUCCESS Key: 0xE105F738
119 2.15881064 services.exe:664 SetValue
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\ROOT\LEGACY_LOCAL_PART
NERS_ACCESS\0000\Control*NewlyCreated* SUCCESS 0x0
120 2.15887601 services.exe:664 CloseKey
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\ROOT\LEGACY_LOCAL_PART
NERS_ACCESS\0000\Control SUCCESS Key: 0xE105F738
121 2.15956996 services.exe:664 SetValue
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\ROOT\LEGACY_LOCAL_PART
NERS_ACCESS\0000\Service SUCCESS "Local Partners Access"
122 2.16017255 services.exe:664 SetValue
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\ROOT\LEGACY_LOCAL_PART
NERS_ACCESS\0000\Legacy SUCCESS 0x1
123 2.16043236 services.exe:664 SetValue
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\ROOT\LEGACY_LOCAL_PART
NERS_ACCESS\0000\ConfigFlags SUCCESS 0x0
124 2.16086230 services.exe:664 SetValue
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\ROOT\LEGACY_LOCAL_PART
NERS_ACCESS\0000\Class SUCCESS "LegacyDriver"
125 2.16111038 services.exe:664 SetValue
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\ROOT\LEGACY_LOCAL_PART
NERS_ACCESS\0000\ClassGUID SUCCESS "{8ECC055D-047F-11D1-A537-
0000F8753ED1}"
126 2.16128135 services.exe:664 OpenKey
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES SUCCESS Key:
0xE105F738
127 2.16137773 services.exe:664 OpenKey
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\Local Partners Access
SUCCESS Key: 0xE186B1F8
128 2.16144813 services.exe:664 CloseKey
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES SUCCESS Key:
0xE105F738
129 2.16172051 services.exe:664 QueryValue
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\Local Partners
Access\DisplayName BUFOVRFLOW
130 2.16187723 services.exe:664 QueryValue
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\Local Partners
Access\DisplayName SUCCESS "Local Printer Manager Service"
131 2.16293742 services.exe:664 SetValue
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\ROOT\LEGACY_LOCAL_PART
NERS_ACCESS\0000\DeviceDesc SUCCESS "Local Printer Manager Service"
132 2.16307403 services.exe:664 CloseKey
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\Local Partners Access
SUCCESS Key: 0xE186B1F8

133 2.16478794 services.exe:664 OpenKey HKLM\SYSTEM\CURRENTCONTROLSET\ENUM SUCCESS Key: 0xE186B1F8
134 2.16489857 services.exe:664 OpenKey HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000 SUCCESS Key: 0xE105F738
135 2.16502596 services.exe:664 CloseKey HKLM\SYSTEM\CURRENTCONTROLSET\ENUM SUCCESS Key: 0xE186B1F8
136 2.16509552 services.exe:664 QueryValue HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000\Service BUFOVRFLOW
137 2.16512820 services.exe:664 QueryValue HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000\Service SUCCESS "Local Partners Access"
138 2.16519190 services.exe:664 CloseKey HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000 SUCCESS Key: 0xE105F738
139 2.16537544 services.exe:664 OpenKey HKLM\SYSTEM\CURRENTCONTROLSET\ENUM SUCCESS Key: 0xE105F738
140 2.16546512 services.exe:664 OpenKey HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000 SUCCESS Key: 0xE186B1F8
141 2.16563190 services.exe:664 CloseKey HKLM\SYSTEM\CURRENTCONTROLSET\ENUM SUCCESS Key: 0xE105F738
142 2.16569978 services.exe:664 QueryValue HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000\ClassGUID BUFOVRFLOW
143 2.16574001 services.exe:664 QueryValue HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000\ClassGUID SUCCESS "{8ECC055D-047F-11D1-A537-0000F8753ED1}"
144 2.16588668 services.exe:664 OpenKey HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\CLASS SUCCESS Key: 0xE105F738
145 2.16598222 services.exe:664 OpenKey HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\CLASS\{8ECC055D-047F-11D1-A537-0000F8753ED1} SUCCESS Key: 0xE14BDFB8
146 2.16604843 services.exe:664 CloseKey HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\CLASS SUCCESS Key: 0xE105F738
147 2.16620516 services.exe:664 QueryValue HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\CLASS\{8ECC055D-047F-11D1-A537-0000F8753ED1}\LowerFilters NOTFOUND

148 2.16629651 services.exe:664 QueryValue
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTN
ERS_ACCESS\0000\LowerFiltersNOTFOUND
149 2.16633506 services.exe:664 QueryValue
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTN
ERS_ACCESS\0000\Service SUCCESS "Local Partners Access"
150 2.16650687 services.exe:664 OpenKey
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES SUCCESS Key:
0xE105F738
151 2.16657224 services.exe:664 OpenKey
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\Local Partners Access
SUCCESS Key: 0xE156B110
152 2.16662253 services.exe:664 CloseKey
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES SUCCESS Key:
0xE105F738
153 2.16688485 services.exe:664 CreateKey
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\Local Partners
Access\Enum SUCCESS Key: 0xE105F738
154 2.16702817 services.exe:664 CloseKey
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\Local Partners Access
SUCCESS Key: 0xE156B110
155 2.16743380 services.exe:664 QueryValue
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\Local Partners
Access\Enum\Count NOTFOUND
156 2.16770199 services.exe:664 SetValue
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\Local Partners
Access\Enum\0 SUCCESS "Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000"

157 2.16780173 services.exe:664 SetValue
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\Local Partners
Access\Enum\Count SUCCESS 0x1
158 2.16787213 services.exe:664 SetValue
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\Local Partners
Access\Enum\NextInstance SUCCESS 0x1
159 2.16806992 services.exe:664 CloseKey
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\Local Partners
Access\Enum SUCCESS Key: 0xE105F738
160 2.16815205 services.exe:664 QueryValue
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTN
ERS_ACCESS\0000\UpperFiltersNOTFOUND
161 2.16823083 services.exe:664 QueryValue
HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\CLASS\{8ECC055D-047F-
11D1-A537-0000F8753ED1}\UpperFilters NOTFOUND
162 2.16830626 services.exe:664 CloseKey
HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\CLASS\{8ECC055D-047F-
11D1-A537-0000F8753ED1} SUCCESS Key: 0xE14BDFB8

163 2.16841940 services.exe:664 CloseKey
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTN
ERS_ACCESS\0000 SUCCESS Key: 0xE186B1F8
164 2.16866832 services.exe:664 CloseKey
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\ROOT\LEGACY_LOCAL_PART
NERS_ACCESS\0000 SUCCESS Key: 0xE17D46B8
165 2.16904295 services.exe:664 CloseKey
HKLM\SYSTEM\ControlSet001\Services\Local Partners Access SUCCESS
Key: 0xE1514A70
166 2.17012660 services.exe:664 OpenKey
HKCC\System\CurrentControlSet\Enum SUCCESS Key: 0xE14BDFB8
167 2.17018527 services.exe:664 OpenKey
HKCC\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACC
ESS\0000 NOTFOUND
168 2.17025399 services.exe:664 CloseKey
HKCC\System\CurrentControlSet\Enum SUCCESS Key: 0xE14BDFB8
169 2.17033194 services.exe:664 OpenKey
HKLM\SYSTEM\ControlSet001\Services\Local Partners Access SUCCESS
Key: 0xE14BDFB8
170 2.17037300 services.exe:664 QueryValue
HKLM\SYSTEM\ControlSet001\Services\Local Partners
Access\PlugPlayServiceType NOTFOUND
171 2.17042664 services.exe:664 OpenKey
HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\Enum
SUCCESS Key: 0xE158E4B0
172 2.17046771 services.exe:664 QueryValue
HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\Enum\Count
SUCCESS 0x1
173 2.17079456 services.exe:664 QueryKey
HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\Enum
SUCCESS Subkeys = 0
174 2.17085155 services.exe:664 CloseKey
HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\Enum
SUCCESS Key: 0xE158E4B0
175 2.17090184 services.exe:664 CloseKey
HKLM\SYSTEM\ControlSet001\Services\Local Partners Access SUCCESS
Key: 0xE14BDFB8
176 2.17116249 services.exe:664 OpenKey
HKLM\SYSTEM\ControlSet001\Services\Local Partners Access SUCCESS
Key: 0xE14BDFB8
177 2.17120858 services.exe:664 QueryValue
HKLM\SYSTEM\ControlSet001\Services\Local Partners
Access\PlugPlayServiceType NOTFOUND
178 2.17126641 services.exe:664 OpenKey
HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\Enum
SUCCESS Key: 0xE158E4B0

179 2.17130413 services.exe:664 QueryValue
HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\Enum\Count
SUCCESS 0x1
180 2.17137453 services.exe:664 QueryValue
HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\Enum\0
SUCCESS "Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000"
181 2.17143319 services.exe:664 CloseKey
HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\Enum
SUCCESS Key: 0xE158E4B0
182 2.17148432 services.exe:664 CloseKey
HKLM\SYSTEM\ControlSet001\Services\Local Partners Access SUCCESS
Key: 0xE14BDFB8
183 2.17174915 services.exe:664 OpenKey
HKCC\System\CurrentControlSet\Enum SUCCESS Key: 0xE14BDFB8
184 2.17179693 services.exe:664 OpenKey
HKCC\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACC
ESS\0000 NOTFOUND
185 2.17184637 services.exe:664 CloseKey
HKCC\System\CurrentControlSet\Enum SUCCESS Key: 0xE14BDFB8
186 2.17192013 services.exe:664 OpenKey
HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE14BDFB8
187 2.17197376 services.exe:664 OpenKey
HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS
Key: 0xE158E4B0
188 2.17202154 services.exe:664 CloseKey
HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE14BDFB8
189 2.17206679 services.exe:664 QueryValue
HKLM\System\CurrentControlSet\Services\Local Partners Access\ObjectName
BUFOVRFLOW
190 2.17210870 services.exe:664 QueryValue
HKLM\System\CurrentControlSet\Services\Local Partners Access\ObjectName
SUCCESS "LocalSystem"
191 2.17221849 services.exe:664 CloseKey
HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS
Key: 0xE158E4B0
192 2.17254283 services.exe:664 OpenKey
HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE158E4B0
193 2.17259731 services.exe:664 OpenKey
HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS
Key: 0xE14BDFB8
194 2.17264675 services.exe:664 CloseKey
HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE158E4B0
195 2.17268866 services.exe:664 QueryValue
HKLM\System\CurrentControlSet\Services\Local Partners Access\ImagePath
BUFOVRFLOW

196 2.17272805 services.exe:664 QueryValue HKLM\System\CurrentControlSet\Services\Local Partners Access\ImagePath SUCCESS "smsses.exe"
197 2.17277834 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE14BDFB8
198 2.17284455 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE14BDFB8
199 2.17289735 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE158E4B0
200 2.17294260 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE14BDFB8
201 2.17298283 services.exe:664 QueryValue HKLM\System\CurrentControlSet\Services\Local Partners Access\Environment NOTFOUND
202 2.17302893 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE158E4B0
203 2.17309514 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE158E4B0
204 2.17314710 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE14BDFB8
205 2.17319235 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE158E4B0
206 2.17323342 services.exe:664 QueryValue HKLM\System\CurrentControlSet\Services\Local Partners Access\ObjectName BUFOVRFLOW
207 2.17327281 services.exe:664 QueryValue HKLM\System\CurrentControlSet\Services\Local Partners Access\ObjectName SUCCESS "LocalSystem"
208 2.17331891 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE14BDFB8
209 2.27465047 cmd.exe:524 OpenKey HKCU SUCCESS Key: 0xE14BDFB8
210 2.27471836 cmd.exe:524 OpenKey HKLM\System\CurrentControlSet\Control\Nls\MUILanguages NOTFOUND

211 2.27478708 cmd.exe:524 OpenKey HKCU\Control Panel\Desktop SUCCESS Key: 0xE158E4B0
212 2.27482982 cmd.exe:524 QueryValue HKCU\Control Panel\Desktop\MultiUILanguageId NOTFOUND
213 2.28480232 cmd.exe:524 CloseKey HKCU\Control Panel\Desktop SUCCESS Key: 0xE158E4B0
214 2.29853199 cmd.exe:524 CloseKey HKCU SUCCESS Key: 0xE14BDFB8

215 2.29925108 cmd.exe:524 OpenKey
HKLM\System\CurrentControlSet\Control\Nls\MUILanguages NOTFOUND

241 2.31856666 svchost.exe:944 OpenKey
HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key:
0xE105F738
242 2.31871751 svchost.exe:944 OpenKey
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
SUCCESS Key: 0xE14BDFB8
243 2.31882814 svchost.exe:944 QueryValue
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\C
omputerName SUCCESS "TEXTBOX"
244 2.32019005 svchost.exe:944 CloseKey
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
SUCCESS Key: 0xE14BDFB8
247 2.32048170 svchost.exe:944 CloseKey
HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key:
0xE105F738
248 2.32256772 svchost.exe:944 OpenKey
HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key:
0xE105F738
252 2.33165435 explorer.exe:1908 QueryKey HKCU SUCCESS Name:
\REGISTRY\USER\S-1-5-21-1659004503-842925246-839522115-500_CLASSES
253 2.33177755 explorer.exe:1908 OpenKey HKCU\Applications\cmd.exe
NOTFOUND
254 2.33182281 explorer.exe:1908 OpenKey HKCR\Applications\cmd.exe
NOTFOUND
255 2.33208429 svchost.exe:944 OpenKey
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
SUCCESS Key: 0xE14BDFB8
256 2.33213709 svchost.exe:944 QueryValue
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\C
omputerName SUCCESS "TEXTBOX"
259 2.33315789 svchost.exe:944 CloseKey
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
SUCCESS Key: 0xE14BDFB8
260 2.33321991 svchost.exe:944 CloseKey
HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key:
0xE105F738
261 2.33515423 svchost.exe:944 OpenKey
HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key:
0xE105F738
266 2.33562357 svchost.exe:944 OpenKey
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
SUCCESS Key: 0xE158E4B0

267 2.33566547 svchost.exe:944 QueryValue
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\C
omputerName SUCCESS "TEXTBOX"
268 2.33571660 svchost.exe:944 CloseKey
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
SUCCESS Key: 0xE158E4B0
273 2.33619682 svchost.exe:944 CloseKey
HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key:
0xE105F738
274 2.33668711 svchost.exe:944 OpenKey
HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key:
0xE105F738
275 2.33683210 svchost.exe:944 OpenKey
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
SUCCESS Key: 0xE156B110
280 2.33714136 svchost.exe:944 QueryValue
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\C
omputerName SUCCESS "TEXTBOX"
281 2.33722098 svchost.exe:944 CloseKey
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
SUCCESS Key: 0xE156B110
282 2.33727294 svchost.exe:944 CloseKey
HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key:
0xE105F738
289 2.39352169 lsass.exe:676 OpenKey HKLM\SECURITY\Policy
SUCCESS Key: 0xE158E4B0
290 2.39357952 lsass.exe:676 OpenKey HKLM\SECURITY\Policy\SecDesc
SUCCESS Key: 0xE14BDFB8
291 2.39362059 lsass.exe:676 QueryValue
HKLM\SECURITY\Policy\SecDesc\(Default) BUFOVRFLOW
292 2.39368344 lsass.exe:676 CloseKey HKLM\SECURITY\Policy\SecDesc
SUCCESS Key: 0xE14BDFB8
293 2.39373876 lsass.exe:676 OpenKey HKLM\SECURITY\Policy\SecDesc
SUCCESS Key: 0xE14BDFB8
294 2.39381922 lsass.exe:676 QueryValue
HKLM\SECURITY\Policy\SecDesc\(Default) SUCCESS NONE
295 2.39386866 lsass.exe:676 CloseKey HKLM\SECURITY\Policy\SecDesc
SUCCESS Key: 0xE14BDFB8
296 2.39495986 lsass.exe:676 CloseKey HKLM\SECURITY\Policy
SUCCESS Key: 0xE158E4B0
297 2.40032116 svchost.exe:944 OpenKey
HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key:
0xE158E4B0
298 2.40038737 svchost.exe:944 OpenKey
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
SUCCESS Key: 0xE14BDFB8

299 2.40043179 svchost.exe:944 QueryValue
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\C
omputerName SUCCESS "TEXTBOX"
300 2.40051643 svchost.exe:944 CloseKey
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
SUCCESS Key: 0xE14BDFB8
301 2.40057007 svchost.exe:944 CloseKey
HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key:
0xE158E4B0
302 2.40213480 svchost.exe:944 OpenKey
HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key:
0xE158E4B0
303 2.40219514 svchost.exe:944 OpenKey
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
SUCCESS Key: 0xE14BDFB8
304 2.40229739 svchost.exe:944 QueryValue
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\C
omputerName SUCCESS "TEXTBOX"
305 2.40235605 svchost.exe:944 CloseKey
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
SUCCESS Key: 0xE14BDFB8
306 2.40240885 svchost.exe:944 CloseKey
HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key:
0xE158E4B0
307 2.40342714 svchost.exe:944 OpenKey
HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key:
0xE158E4B0
308 2.40349251 svchost.exe:944 OpenKey
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
SUCCESS Key: 0xE14BDFB8
309 2.40353525 svchost.exe:944 QueryValue
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\C
omputerName SUCCESS "TEXTBOX"
310 2.40361487 svchost.exe:944 CloseKey
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
SUCCESS Key: 0xE14BDFB8
311 2.40366767 svchost.exe:944 CloseKey
HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key:
0xE158E4B0
312 2.40413784 svchost.exe:944 OpenKey
HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key:
0xE158E4B0
313 2.40419567 svchost.exe:944 OpenKey
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
SUCCESS Key: 0xE14BDFB8

314 2.40423674 svchost.exe:944 QueryValue HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\ComputerName SUCCESS "TEXTBOX"
315 2.40430127 svchost.exe:944 CloseKey HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName SUCCESS Key: 0xE14BDFB8
316 2.40435240 svchost.exe:944 CloseKey HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key: 0xE158E4B0
317 2.40546455 svchost.exe:944 OpenKey HKCR\CLSID\{266c72e6-62e8-11d1-ad89-00c04fd8fdff}\InProcServer32 SUCCESS Key: 0xE158E4B0
318 2.40551902 svchost.exe:944 QueryValue HKCR\CLSID\{266c72e6-62e8-11d1-ad89-00c04fd8fdff}\InProcServer32\ThreadingModel SUCCESS "Both"
319 2.40556177 svchost.exe:944 QueryValue HKCR\CLSID\{266c72e6-62e8-11d1-ad89-00c04fd8fdff}\InProcServer32\Synchronization NOTFOUND
320 2.40560200 svchost.exe:944 QueryValue HKCR\CLSID\{266c72e6-62e8-11d1-ad89-00c04fd8fdff}\InProcServer32\(Default) SUCCESS "C:\WINDOWS\System32\wbem\wbemcons.dll"
321 2.40566318 svchost.exe:944 CloseKey HKCR\CLSID\{266c72e6-62e8-11d1-ad89-00c04fd8fdff}\InProcServer32 SUCCESS Key: 0xE158E4B0
322 2.40580314 svchost.exe:944 OpenKey HKCR\CLSID\{266c72e6-62e8-11d1-ad89-00c04fd8fdff}\LocalServer32 NOTFOUND
323 2.40592382 svchost.exe:944 OpenKey HKCR\CLSID\{266c72e6-62e8-11d1-ad89-00c04fd8fdff} SUCCESS Key: 0xE158E4B0
324 2.40596657 svchost.exe:944 QueryValue HKCR\CLSID\{266c72e6-62e8-11d1-ad89-00c04fd8fdff}\(Default) SUCCESS "Microsoft WBEM NT Event Log Event Consumer Provider"
325 2.40600093 svchost.exe:944 QueryValue HKCR\CLSID\{266c72e6-62e8-11d1-ad89-00c04fd8fdff}\AppId NOTFOUND
326 2.40605038 svchost.exe:944 CloseKey HKCR\CLSID\{266c72e6-62e8-11d1-ad89-00c04fd8fdff} SUCCESS Key: 0xE158E4B0
327 2.42110424 svchost.exe:944 OpenKey HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key: 0xE158E4B0
328 2.42144451 svchost.exe:944 OpenKey HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName SUCCESS Key: 0xE14BDFB8
329 2.42149395 svchost.exe:944 QueryValue HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\ComputerName SUCCESS "TEXTBOX"
330 2.42156855 svchost.exe:944 CloseKey HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName SUCCESS Key: 0xE14BDFB8
331 2.42162386 svchost.exe:944 CloseKey HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key: 0xE158E4B0

332 2.42538607 svchost.exe:944 OpenKey HKCR\CLSID\{266c72e6-62e8-11d1-ad89-00c04fd8fdff}\InProcServer32 SUCCESS Key: 0xE158E4B0
333 2.42544390 svchost.exe:944 QueryValue HKCR\CLSID\{266c72e6-62e8-11d1-ad89-00c04fd8fdff}\InProcServer32\ThreadingModel SUCCESS "Both"
334 2.42551765 svchost.exe:944 QueryValue HKCR\CLSID\{266c72e6-62e8-11d1-ad89-00c04fd8fdff}\InProcServer32\Synchronization NOTFOUND
335 2.42555955 svchost.exe:944 QueryValue HKCR\CLSID\{266c72e6-62e8-11d1-ad89-00c04fd8fdff}\InProcServer32\(Default) SUCCESS "C:\WINDOWS\System32\wbem\wbemcons.dll"
336 2.42562744 svchost.exe:944 CloseKey HKCR\CLSID\{266c72e6-62e8-11d1-ad89-00c04fd8fdff}\InProcServer32 SUCCESS Key: 0xE158E4B0
337 2.42575148 svchost.exe:944 OpenKey HKCR\CLSID\{266c72e6-62e8-11d1-ad89-00c04fd8fdff}\LocalServer32 NOTFOUND
338 2.42586462 svchost.exe:944 OpenKey HKCR\CLSID\{266c72e6-62e8-11d1-ad89-00c04fd8fdff} SUCCESS Key: 0xE158E4B0
339 2.42590653 svchost.exe:944 QueryValue HKCR\CLSID\{266c72e6-62e8-11d1-ad89-00c04fd8fdff}\(Default) SUCCESS "Microsoft WBEM NT Event Log Event Consumer Provider"
340 2.42594005 svchost.exe:944 QueryValue HKCR\CLSID\{266c72e6-62e8-11d1-ad89-00c04fd8fdff}\AppId NOTFOUND
341 2.42599034 svchost.exe:944 CloseKey HKCR\CLSID\{266c72e6-62e8-11d1-ad89-00c04fd8fdff} SUCCESS Key: 0xE158E4B0
342 2.43240260 svchost.exe:944 OpenKey HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key: 0xE158E4B0
343 2.43257441 svchost.exe:944 OpenKey HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName SUCCESS Key: 0xE14BDFB8
344 2.43262134 svchost.exe:944 QueryValue HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\ComputerName SUCCESS "TEXTBOX"
345 2.43270012 svchost.exe:944 CloseKey HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName SUCCESS Key: 0xE14BDFB8
346 2.43275376 svchost.exe:944 CloseKey HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key: 0xE158E4B0
347 2.43407628 svchost.exe:944 OpenKey HKLM\Software\Microsoft\COM3 SUCCESS Key: 0xE158E4B0
348 2.43413243 svchost.exe:944 QueryValue HKLM\Software\Microsoft\COM3\REGDBVersion SUCCESS 07 00 00 00 00 00 00 00
349 2.43459171 svchost.exe:944 CloseKey HKLM\Software\Microsoft\COM3 SUCCESS Key: 0xE158E4B0
350 2.43483894 svchost.exe:944 OpenKey HKLM\Software\Microsoft\COM3 SUCCESS Key: 0xE158E4B0

351 2.43488839 svchost.exe:944 QueryValue HKLM\Software\Microsoft\COM3\REGDBVersion SUCCESS 07 00 00 00 00 00 00 00
352 2.43494622 svchost.exe:944 CloseKey HKLM\Software\Microsoft\COM3 SUCCESS Key: 0xE158E4B0
353 2.43509791 svchost.exe:944 OpenKey HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF} SUCCESS Key: 0xE158E4B0
354 2.43513814 svchost.exe:944 OpenKey HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF}\TreatAs NOTFOUND
355 2.43519094 svchost.exe:944 CloseKey HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF} SUCCESS Key: 0xE158E4B0
356 2.43531163 svchost.exe:944 OpenKey HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF} SUCCESS Key: 0xE158E4B0
357 2.43536862 svchost.exe:944 OpenKey HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF}\InprocServer32 SUCCESS Key: 0xE14BDFB8
358 2.43540969 svchost.exe:944 QueryValue HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF}\InprocServer32\InprocServer32 NOTFOUND
359 2.43545997 svchost.exe:944 CloseKey HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF}\InprocServer32 SUCCESS Key: 0xE14BDFB8
360 2.43575498 svchost.exe:944 OpenKey HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF}\InprocServerX86 NOTFOUND
361 2.43580191 svchost.exe:944 OpenKey HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF}\LocalServer32 NOTFOUND
362 2.43586226 svchost.exe:944 OpenKey HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF}\InprocServer32 SUCCESS Key: 0xE14BDFB8
363 2.43590668 svchost.exe:944 QueryValue HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF}\InprocServer32\(Default) SUCCESS "C:\WINDOWS\System32\wbem\wbemcons.dll"
364 2.43596870 svchost.exe:944 CloseKey HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF}\InprocServer32 SUCCESS Key: 0xE14BDFB8
365 2.43601730 svchost.exe:944 OpenKey HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF}\InprocHandler32NOTFOUND
366 2.43609106 svchost.exe:944 OpenKey HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF}\InprocHandlerX86 NOTFOUND
367 2.43612793 svchost.exe:944 OpenKey HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF}\LocalServer32 NOTFOUND
368 2.43616565 svchost.exe:944 OpenKey HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF}\LocalServer NOTFOUND
369 2.43630645 svchost.exe:944 OpenKey HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF} SUCCESS Key: 0xE14BDFB8
370 2.43634165 svchost.exe:944 QueryValue HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF}\AppID NOTFOUND
371 2.43639193 svchost.exe:944 CloseKey HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF} SUCCESS Key: 0xE14BDFB8
372 2.43644138 svchost.exe:944 CloseKey HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF} SUCCESS Key: 0xE158E4B0

373 2.43659894 svchost.exe:944 OpenKey HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF} SUCCESS Key: 0xE158E4B0
374 2.43665342 svchost.exe:944 OpenKey HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF}\InprocServer32 SUCCESS Key: 0xE14BDFB8
375 2.43669281 svchost.exe:944 QueryValue HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF}\InprocServer32\ThreadingModel SUCCESS "Both"
376 2.43674310 svchost.exe:944 CloseKey HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF}\InprocServer32 SUCCESS Key: 0xE14BDFB8
377 2.43679422 svchost.exe:944 CloseKey HKCR\CLSID\{266C72E6-62E8-11D1-AD89-00C04FD8FDFF} SUCCESS Key: 0xE158E4B0
378 2.43852572 svchost.exe:944 CreateKey HKLM\Software\Microsoft\WBEM\CIMOM SUCCESS Key: 0xE158E4B0
379 2.43872016 svchost.exe:944 QueryValue HKLM\Software\Microsoft\WBEM\CIMOM\Logging Directory SUCCESS "C:\WINDOWS\system32\WBEM\Logs\"
380 2.43902942 svchost.exe:944 QueryValue HKLM\Software\Microsoft\WBEM\CIMOM\Logging Directory SUCCESS "C:\WINDOWS\system32\WBEM\Logs\"
381 2.44002927 svchost.exe:944 CloseKey HKLM\Software\Microsoft\WBEM\CIMOM SUCCESS Key: 0xE158E4B0
382 2.44022706 svchost.exe:944 CreateKey HKLM\Software\Microsoft\WBEM\CIMOM SUCCESS Key: 0xE158E4B0
383 2.44027148 svchost.exe:944 QueryValue HKLM\Software\Microsoft\WBEM\CIMOM\Logging SUCCESS "1"
384 2.44032595 svchost.exe:944 QueryValue HKLM\Software\Microsoft\WBEM\CIMOM\Log File Max Size SUCCESS "65536"

385 2.44037875 svchost.exe:944 CloseKey HKLM\Software\Microsoft\WBEM\CIMOM SUCCESS Key: 0xE158E4B0
386 136.33562860 cmd.exe:524 OpenKey HKCU SUCCESS Key: 0xE14BDFB8

Appendix E - Regmon Log File When Running 'target2.exe -d test'

387 136.33585153 cmd.exe:524 OpenKey HKLM\System\CurrentControlSet\Control\Nls\MUILanguages NOTFOUND

388 136.33593283 cmd.exe:524 OpenKey HKCU\Control Panel\Desktop SUCCESS Key: 0xE1636090
389 136.33603172 cmd.exe:524 QueryValue HKCU\Control Panel\Desktop\MultiUILanguageId NOTFOUND
390 136.33610631 cmd.exe:524 CloseKey HKCU\Control Panel\Desktop SUCCESS Key: 0xE1636090
391 136.33617755 cmd.exe:524 CloseKey HKCU SUCCESS Key: 0xE14BDFB8
392 136.33624208 cmd.exe:524 OpenKey HKLM\System\CurrentControlSet\Control\Nls\MUILanguages NOTFOUND

393 136.33917039 cmd.exe:524 OpenKey HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers NOTFOUND
394 136.33931202 cmd.exe:524 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\target2.exeNOTFOUND
395 136.33941343 cmd.exe:524 OpenKey HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers SUCCESS Key: 0xE14BDFB8
396 136.33945785 cmd.exe:524 QueryValue HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\ExecutableTypes BUFTOOSMALL
397 136.33950060 cmd.exe:524 QueryValue HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\ExecutableTypes SUCCESS "ADE"
398 136.33961961 cmd.exe:524 CloseKey HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers SUCCESS Key: 0xE14BDFB8
399 136.34004284 cmd.exe:524 OpenKey HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers SUCCESS Key: 0xE14BDFB8
400 136.34008391 cmd.exe:524 QueryValue HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\LogFileName NOTFOUND
401 136.34014761 cmd.exe:524 CloseKey HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers SUCCESS Key: 0xE14BDFB8
402 136.36816345 target2.exe:1596 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\target2.exe NOTFOUND

403 136.37127027 target2.exe:1596 OpenKey
HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS Key:
0xE1636090
404 136.37139263 target2.exe:1596 QueryValue
HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat
SUCCESS 0x0
405 136.37161724 target2.exe:1596 CloseKey
HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS Key:
0xE1636090
406 136.37479613 target2.exe:1596 OpenKey
HKLM\System\CurrentControlSet\Control\SafeBoot\Option NOTFOUND
407 136.37486821 target2.exe:1596 OpenKey
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers SUCCESS
Key: 0xE1636090
408 136.37491095 target2.exe:1596 QueryValue
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEna
bled SUCCESS 0x1
409 136.37498554 target2.exe:1596 CloseKey
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers SUCCESS
Key: 0xE1636090
410 136.37514562 target2.exe:1596 OpenKey
HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers NOTFOUND

411 136.37993282 target2.exe:1596 OpenKey
HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS Key:
0xE1636090
412 136.37998646 target2.exe:1596 QueryValue
HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat
SUCCESS 0x0
413 136.38005350 target2.exe:1596 CloseKey
HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS Key:
0xE1636090
414 136.38043568 target2.exe:1596 OpenKey
HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS Key:
0xE1636090
415 136.38047674 target2.exe:1596 QueryValue
HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat
SUCCESS 0x0
416 136.38051613 target2.exe:1596 QueryValue
HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled
SUCCESS 0x0
417 136.38056977 target2.exe:1596 CloseKey
HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS Key:
0xE1636090

418 136.38066112 target2.exe:1596 OpenKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon SUCCESS Key: 0xE1636090
419 136.38071308 target2.exe:1596 QueryValue HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LeakTrack NOTFOUND
420 136.38081617 target2.exe:1596 CloseKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon SUCCESS Key: 0xE1636090
421 136.38087400 target2.exe:1596 OpenKey HKLM SUCCESS Key: 0xE1636090
422 136.38092596 target2.exe:1596 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics NOTFOUND
423 136.38374699 target2.exe:1596 OpenKey HKLM\System\CurrentControlSet\Control\Error Message Instrument\ NOTFOUND
424 136.38478204 target2.exe:1596 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32 SUCCESS Key: 0xE1503C88
425 136.38483987 target2.exe:1596 QueryValue HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32\target2 NOTFOUND
426 136.38492284 target2.exe:1596 CloseKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32 SUCCESS Key: 0xE1503C88
427 136.38502508 target2.exe:1596 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility SUCCESS Key: 0xE1503C88
428 136.38506950 target2.exe:1596 QueryValue HKLM\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility\target2 NOTFOUND
429 136.38512649 target2.exe:1596 CloseKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility SUCCESS Key: 0xE1503C88
430 136.38594699 target2.exe:1596 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows SUCCESS Key: 0xE1503C88
431 136.38599476 target2.exe:1596 QueryValue HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs SUCCESS ""
432 136.38606181 target2.exe:1596 CloseKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows SUCCESS Key: 0xE1503C88

433 136.38683202 target2.exe:1596 OpenKey HKLM\System\CurrentControlSet\Control\Session Manager SUCCESS Key: 0xE1503C88
434 136.38687727 target2.exe:1596 QueryValue HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode NOTFOUND
435 136.38693594 target2.exe:1596 CloseKey HKLM\System\CurrentControlSet\Control\Session Manager SUCCESS Key: 0xE1503C88
436 136.39071072 target2.exe:1596 OpenKey HKLM\Software\Microsoft\Rpc\PagedBuffers NOTFOUND
437 136.39081045 target2.exe:1596 OpenKey HKLM\Software\Microsoft\Rpc SUCCESS Key: 0xE1503C88
438 136.39084733 target2.exe:1596 QueryValue HKLM\Software\Microsoft\Rpc\MaxRpcSize NOTFOUND
439 136.39091270 target2.exe:1596 CloseKey HKLM\Software\Microsoft\Rpc SUCCESS Key: 0xE1503C88
440 136.39097472 target2.exe:1596 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\target2.exe\RpcThreadPoolThrottle NOTFOUND
441 136.39311186 target2.exe:1596 OpenKey HKLM\Software\Policies\Microsoft\Windows NT\Rpc NOTFOUND
442 136.39365244 target2.exe:1596 OpenKey HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key: 0xE1503C88
443 136.39371194 target2.exe:1596 OpenKey HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName SUCCESS Key: 0xE16516B0
444 136.39375636 target2.exe:1596 QueryValue HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\ComputerName SUCCESS "TEXTBOX"
445 136.39382508 target2.exe:1596 CloseKey HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName SUCCESS Key: 0xE16516B0
446 136.39387788 target2.exe:1596 CloseKey HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key: 0xE1503C88
447 136.39902043 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE1503C88
448 136.39908581 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE16516B0
449 136.39915872 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE1503C88

450 136.40025746 services.exe:664 SetValue HKLM\System\CurrentControlSet\Services\Local Partners Access\DeleteFlag SUCCESS 0x1
451 136.40046196 services.exe:664 SetValue HKLM\System\CurrentControlSet\Services\Local Partners Access\Start SUCCESS 0x4
452 136.40050386 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE16516B0
453 136.40146767 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE16516B0
454 136.40532207 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE1503C88
455 136.40540588 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE16516B0
456 136.40548466 services.exe:664 QueryValue HKLM\System\CurrentControlSet\Services\Local Partners Access\ObjectName BUFOVRFLOW
457 136.40552824 services.exe:664 QueryValue HKLM\System\CurrentControlSet\Services\Local Partners Access\ObjectName SUCCESS "LocalSystem"
458 136.40563049 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE1503C88
459 136.40590203 services.exe:664 OpenKey HKLM\SYSTEM\ControlSet001\Services\Local Partners Access SUCCESS Key: 0xE1503C88
460 136.40594226 services.exe:664 QueryValue HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\PlugPlayServiceType NOTFOUND
461 136.40599925 services.exe:664 OpenKey HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\Enum SUCCESS Key: 0xE16516B0
462 136.40603697 services.exe:664 QueryValue HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\Enum\Count SUCCESS 0x1
463 136.40617022 services.exe:664 QueryKey HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\Enum SUCCESS Subkeys = 0
464 136.40622805 services.exe:664 CloseKey HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\Enum SUCCESS Key: 0xE16516B0
465 136.40627834 services.exe:664 CloseKey HKLM\SYSTEM\ControlSet001\Services\Local Partners Access SUCCESS Key: 0xE1503C88

466 136.40649289 services.exe:664 OpenKey HKLM\SYSTEM\ControlSet001\Services\Local Partners Access SUCCESS Key: 0xE1503C88
467 136.40653396 services.exe:664 QueryValue HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\PlugPlayServiceType NOTFOUND
468 136.40658676 services.exe:664 OpenKey HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\Enum SUCCESS Key: 0xE16516B0
469 136.40676024 services.exe:664 QueryValue HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\Enum\Count SUCCESS 0x1
470 136.40686584 services.exe:664 QueryValue HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\Enum\0 SUCCESS "Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000"
471 136.40693038 services.exe:664 CloseKey HKLM\SYSTEM\ControlSet001\Services\Local Partners Access\Enum SUCCESS Key: 0xE16516B0
472 136.40698150 services.exe:664 CloseKey HKLM\SYSTEM\ControlSet001\Services\Local Partners Access SUCCESS Key: 0xE1503C88
473 136.41846843 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Control\IDConfigDB\Hardware Profiles SUCCESS Key: 0xE1636090
474 136.41854889 services.exe:664 EnumerateKey HKLM\System\CurrentControlSet\Control\IDConfigDB\Hardware Profiles SUCCESS Name: 0000
475 136.41892855 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Hardware Profiles\0000\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS NOTFOUND
476 136.41897296 services.exe:664 EnumerateKey HKLM\System\CurrentControlSet\Control\IDConfigDB\Hardware Profiles SUCCESS Name: 0001
477 136.41913723 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Hardware Profiles\0001\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS NOTFOUND
478 136.41917243 services.exe:664 EnumerateKey HKLM\System\CurrentControlSet\Control\IDConfigDB\Hardware Profiles NOMORE
479 136.41924032 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Control\IDConfigDB\Hardware Profiles SUCCESS Key: 0xE1636090

480 136.41932999 services.exe:664 OpenKey
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000 SUCCESS Key: 0xE1636090
481 136.41937106 services.exe:664 QueryValue
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000\Driver NOTFOUND
482 136.41942051 services.exe:664 CloseKey
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000 SUCCESS Key: 0xE1636090
483 136.41966439 services.exe:664 OpenKey
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000 SUCCESS Key: 0xE1636090
484 136.41970378 services.exe:664 QueryValue
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000\Driver NOTFOUND
485 136.41975742 services.exe:664 CloseKey
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000 SUCCESS Key: 0xE1636090
486 136.41982615 services.exe:664 OpenKey
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000 SUCCESS Key: 0xE1636090
487 136.41987140 services.exe:664 QueryValue
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000\ClassGUID SUCCESS "{8ECC055D-047F-11D1-A537-0000F8753ED1}"

488 136.41992001 services.exe:664 CloseKey
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000 SUCCESS Key: 0xE1636090
489 136.42004908 services.exe:664 OpenKey
HKLM\SYSTEM\ControlSet001\Control\Class\{8ECC055D-047F-11D1-A537-0000F8753ED1} SUCCESS Key: 0xE1636090
490 136.42073799 services.exe:664 CreateKey
HKLM\SYSTEM\ControlSet001\Control\Class\{8ECC055D-047F-11D1-A537-0000F8753ED1}\0000 SUCCESS Key: 0xE1503C88
491 136.42081175 services.exe:664 CloseKey
HKLM\SYSTEM\ControlSet001\Control\Class\{8ECC055D-047F-11D1-A537-0000F8753ED1}\0000 SUCCESS Key: 0xE1503C88
492 136.42096679 services.exe:664 OpenKey
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000 SUCCESS Key: 0xE1503C88
493 136.42253403 services.exe:664 SetValue
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000\Driver SUCCESS "{8ECC055D-047F-11D1-A537-0000F8753ED1}\0000"

494 136.42263209 services.exe:664 CloseKey HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000 SUCCESS Key: 0xE1503C88
495 136.42268740 services.exe:664 CloseKey HKLM\SYSTEM\ControlSet001\Control\Class\{8ECC055D-047F-11D1-A537-0000F8753ED1} SUCCESS Key: 0xE1636090
496 136.42283491 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Control\IDConfigDB\Hardware Profiles SUCCESS Key: 0xE1636090
497 136.42287765 services.exe:664 EnumerateKey HKLM\System\CurrentControlSet\Control\IDConfigDB\Hardware Profiles SUCCESS Name: 0000
498 136.42296146 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Hardware Profiles\0000\System\CurrentControlSet\Control\Class\{8ECC055D-047F-11D1-A537-0000F8753ED1} NOTFOUND
499 136.42299917 services.exe:664 EnumerateKey HKLM\System\CurrentControlSet\Control\IDConfigDB\Hardware Profiles SUCCESS Name: 0001
500 136.46290591 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Hardware Profiles\0001\System\CurrentControlSet\Control\Class\{8ECC055D-047F-11D1-A537-0000F8753ED1} NOTFOUND
501 136.46297715 services.exe:664 EnumerateKey HKLM\System\CurrentControlSet\Control\IDConfigDB\Hardware Profiles NOMORE
502 136.46306180 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Control\IDConfigDB\Hardware Profiles SUCCESS Key: 0xE1636090
503 136.46333837 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000 SUCCESS Key: 0xE1636090
504 136.46341715 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000\Device Parameters NOTFOUND
505 136.46345905 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000\Device Parameters NOTFOUND
506 136.46349928 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000\Device Parameters NOTFOUND
507 136.46355292 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000 SUCCESS Key: 0xE1636090

508 136.46363086 services.exe:664 OpenKey HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000 SUCCESS Key: 0xE1636090
509 136.46369037 services.exe:664 QueryValue HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000\Driver SUCCESS "{8ECC055D-047F-11D1-A537-0000F8753ED1}\0000"

510 136.46373982 services.exe:664 CloseKey HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000 SUCCESS Key: 0xE1636090
511 136.46391498 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Control\Class\{8ECC055D-047F-11D1-A537-0000F8753ED1} SUCCESS Key: 0xE1636090
512 136.46397448 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Control\Class\{8ECC055D-047F-11D1-A537-0000F8753ED1}\0000 SUCCESS Key: 0xE16516B0
513 136.46979338 services.exe:664 DeleteKey HKLM\System\CurrentControlSet\Control\Class\{8ECC055D-047F-11D1-A537-0000F8753ED1}\0000 SUCCESS Key: 0xE16516B0
514 136.46992328 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Control\Class\{8ECC055D-047F-11D1-A537-0000F8753ED1}\0000 SUCCESS Key: 0xE16516B0
515 136.47011185 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Control\Class\{8ECC055D-047F-11D1-A537-0000F8753ED1} SUCCESS Key: 0xE1636090
516 136.47062644 cmd.exe:524 OpenKey HKCU SUCCESS Key: 0xE14BDFB8
517 136.47070941 cmd.exe:524 OpenKey HKLM\System\CurrentControlSet\Control\Nls\MUILanguages NOTFOUND

518 136.48171193 cmd.exe:524 OpenKey HKCU\Control Panel\Desktop SUCCESS Key: 0xE1636090
519 136.48175635 services.exe:664 OpenKey HKLM\SYSTEM\CURRENTCONTROLSET\ENUM SUCCESS Key: 0xE1503C88
520 136.48191726 services.exe:664 OpenKey HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000 SUCCESS Key: 0xE16516B0
521 136.48198347 services.exe:664 CloseKey HKLM\SYSTEM\CURRENTCONTROLSET\ENUM SUCCESS Key: 0xE1503C88
522 136.48203376 services.exe:664 QueryValue HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000\Service BUFOVRFLOW

523 136.48207817 services.exe:664 QueryValue
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTN
ERS_ACCESS\0000\Service SUCCESS "Local Partners Access"
524 136.48213600 services.exe:664 CloseKey
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTN
ERS_ACCESS\0000 SUCCESS Key: 0xE16516B0
525 136.48222819 services.exe:664 OpenKey
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM SUCCESS Key:
0xE16516B0
526 136.48230027 services.exe:664 OpenKey
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTN
ERS_ACCESS\0000 SUCCESS Key: 0xE1503C88
527 136.48235139 services.exe:664 CloseKey
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM SUCCESS Key:
0xE16516B0
528 136.48239581 services.exe:664 QueryValue
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTN
ERS_ACCESS\0000\ClassGUID BUFOVRFLOW
529 136.48243436 services.exe:664 QueryValue
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTN
ERS_ACCESS\0000\ClassGUID SUCCESS "{8ECC055D-047F-11D1-A537-
0000F8753ED1}"
530 136.48257097 services.exe:664 OpenKey
HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\CLASS SUCCESS
Key: 0xE16516B0
531 136.48270926 services.exe:664 OpenKey
HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\CLASS\{8ECC055D-047F-
11D1-A537-0000F8753ED1} SUCCESS Key: 0xE13D58C0
532 136.48276709 services.exe:664 CloseKey
HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\CLASS SUCCESS
Key: 0xE16516B0
533 136.48281235 services.exe:664 QueryValue
HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\CLASS\{8ECC055D-047F-
11D1-A537-0000F8753ED1}\LowerFilters NOTFOUND
534 136.48285844 services.exe:664 QueryValue
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTN
ERS_ACCESS\0000\LowerFiltersNOTFOUND
535 136.48289364 services.exe:664 QueryValue
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTN
ERS_ACCESS\0000\Service SUCCESS "Local Partners Access"
536 136.48297996 services.exe:664 OpenKey
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES SUCCESS Key:
0xE16516B0
537 136.48305623 services.exe:664 OpenKey
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\Local Partners Access
SUCCESS Key: 0xE13C08F0

538 136.48310903 services.exe:664 CloseKey
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES SUCCESS Key:
0xE16516B0
539 136.48317775 services.exe:664 CreateKey
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\Local Partners
Access\Enum SUCCESS Key: 0xE16516B0
540 136.48324313 services.exe:664 CloseKey
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\Local Partners Access
SUCCESS Key: 0xE13C08F0
541 136.48329257 services.exe:664 QueryValue
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\Local Partners
Access\Enum\Count SUCCESS 0x1
542 136.48351467 services.exe:664 QueryValue
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\Local Partners
Access\Enum\0 SUCCESS "Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000"

543 136.48524282 services.exe:664 DeleteValueKey
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\Local Partners
Access\Enum\0 SUCCESS
544 136.48540960 services.exe:664 SetValue
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\Local Partners
Access\Enum\Count SUCCESS 0x0
545 136.48545905 services.exe:664 SetValue
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\Local Partners
Access\Enum\NextInstance SUCCESS 0x0
546 136.48557052 services.exe:664 CloseKey
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\Local Partners
Access\Enum SUCCESS Key: 0xE16516B0
547 136.48563337 services.exe:664 QueryValue
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTN
ERS_ACCESS\0000\UpperFiltersNOTFOUND
548 136.48567360 services.exe:664 QueryValue
HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\CLASS\{8ECC055D-047F-
11D1-A537-0000F8753ED1}\UpperFilters NOTFOUND
549 136.48573143 services.exe:664 CloseKey
HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\CLASS\{8ECC055D-047F-
11D1-A537-0000F8753ED1} SUCCESS Key: 0xE13D58C0
550 136.48579010 services.exe:664 CloseKey
HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\Root\LEGACY_LOCAL_PARTN
ERS_ACCESS\0000 SUCCESS Key: 0xE1503C88
556 136.50556244 cmd.exe:524 QueryValue HKCU\Control
Panel\Desktop\MultiUILanguageId NOTFOUND
557 136.50567307 cmd.exe:524 CloseKey HKCU\Control Panel\Desktop
SUCCESS Key: 0xE1636090
558 136.50583314 cmd.exe:524 CloseKey HKCU SUCCESS Key:
0xE14BDFB8

559 136.50598484 cmd.exe:524 OpenKey
HKLM\System\CurrentControlSet\Control\Nls\MUILanguages NOTFOUND

700 136.52508838 explorer.exe:1908 QueryKey HKCU SUCCESS Name:
\REGISTRY\USER\S-1-5-21-1659004503-842925246-839522115-500_CLASSES
701 136.52530209 explorer.exe:1908 OpenKey HKCU\Applications\cmd.exe
NOTFOUND
702 136.52535238 explorer.exe:1908 OpenKey HKCR\Applications\cmd.exe
NOTFOUND
773 136.53066506 services.exe:664 OpenKey
HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACC
ESS SUCCESS Key: 0xE13D58C0
774 136.53072289 services.exe:664 OpenKey
HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACC
ESS\0000 SUCCESS Key: 0xE1547B30
775 136.53100365 services.exe:664 DeleteKey
HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACC
ESS\0000 c0000121 Key: 0xE1547B30
776 136.53103969 services.exe:664 CloseKey
HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACC
ESS\0000 SUCCESS Key: 0xE1547B30
777 136.53110087 services.exe:664 OpenKey
HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACC
ESS\0000 SUCCESS Key: 0xE1547B30
778 136.53114361 services.exe:664 EnumerateKey
HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACC
ESS\0000 SUCCESS Name: Control
779 136.53120060 services.exe:664 OpenKey
HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACC
ESS\0000\Control SUCCESS Key: 0xE16516B0
780 136.53221135 services.exe:664 DeleteKey
HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACC
ESS\0000\Control SUCCESS Key: 0xE16516B0
781 136.53226415 services.exe:664 CloseKey
HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACC
ESS\0000\Control SUCCESS Key: 0xE16516B0
782 136.53232533 services.exe:664 EnumerateKey
HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACC
ESS\0000 NOMORE
783 136.53239824 services.exe:664 CloseKey
HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACC
ESS\0000 SUCCESS Key: 0xE1547B30
784 136.53247200 services.exe:664 OpenKey
HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACC
ESS\0000 SUCCESS Key: 0xE1547B30

785 136.53357660 services.exe:664 DeleteKey HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000 SUCCESS Key: 0xE1547B30
786 136.53362605 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000 SUCCESS Key: 0xE1547B30
787 136.53368556 services.exe:664 QueryKey HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS SUCCESS Subkeys = 0
788 136.53375344 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS SUCCESS Key: 0xE13D58C0
789 136.53398392 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Enum\Root SUCCESS Key: 0xE13D58C0
790 136.53404342 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS SUCCESS Key: 0xE1547B30
791 136.53463260 services.exe:664 DeleteKey HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS SUCCESS Key: 0xE1547B30
792 136.53467954 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS SUCCESS Key: 0xE1547B30
793 136.53475161 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Enum\Root SUCCESS Key: 0xE13D58C0
794 136.53485638 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Control\IDConfigDB\Hardware Profiles SUCCESS Key: 0xE13D58C0
795 136.53489577 services.exe:664 QueryKey HKLM\System\CurrentControlSet\Control\IDConfigDB\Hardware Profiles SUCCESS Subkeys = 2
796 136.53494689 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Control\IDConfigDB\Hardware Profiles SUCCESS Key: 0xE13D58C0
797 136.53503824 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Hardware Profiles\0001\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS NOTFOUND
798 136.53518910 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Hardware Profiles\0002\System\CurrentControlSet\Enum\Root\LEGACY_LOCAL_PARTNERS_ACCESS NOTFOUND
4647 136.76374099 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE1098CA0

4648 136.76436788 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE1547B30
4649 136.76463524 services.exe:664 QueryKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Subkeys = 2
4650 136.76476598 services.exe:664 EnumerateKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Name: Security
4651 136.76486823 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services\Local Partners Access\Security SUCCESS Key: 0xE16516B0
4652 136.76491516 services.exe:664 QueryKey HKLM\System\CurrentControlSet\Services\Local Partners Access\Security SUCCESS Subkeys = 0
4653 136.76497047 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services\Local Partners Access\Security SUCCESS Key: 0xE1090B00
4654 136.78520879 services.exe:664 DeleteKey HKLM\System\CurrentControlSet\Services\Local Partners Access\Security SUCCESS Key: 0xE1090B00
4655 136.78530099 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services\Local Partners Access\Security SUCCESS Key: 0xE1090B00
4656 136.78543592 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services\Local Partners Access\Security SUCCESS Key: 0xE16516B0
4657 136.78548872 services.exe:664 EnumerateKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Name: Enum
4658 136.78556499 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services\Local Partners Access\Enum SUCCESS Key: 0xE16516B0
4659 136.78560521 services.exe:664 QueryKey HKLM\System\CurrentControlSet\Services\Local Partners Access\Enum SUCCESS Subkeys = 0
4660 136.78565885 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services\Local Partners Access\Enum SUCCESS Key: 0xE1090B00
4661 136.78576361 services.exe:664 DeleteKey HKLM\System\CurrentControlSet\Services\Local Partners Access\Enum SUCCESS Key: 0xE1090B00
4662 136.78581641 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services\Local Partners Access\Enum SUCCESS Key: 0xE1090B00

4663 136.78586754 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services\Local Partners Access\Enum SUCCESS Key: 0xE16516B0
4664 136.78593291 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE1547B30
4665 136.78599493 services.exe:664 OpenKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE1547B30
4666 136.78655142 services.exe:664 DeleteKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE1547B30
4667 136.78662434 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services\Local Partners Access SUCCESS Key: 0xE1547B30
4668 136.78667881 services.exe:664 CloseKey HKLM\System\CurrentControlSet\Services SUCCESS Key: 0xE1098CA0

Appendix F - Red Hat 8.0 Installed Packages

4Suite-0.11.1-10
acl-2.0.11-2
alchemist-1.0.24-4
anacron-2.3-23
apmd-3.0.2-12
ash-0.3.8-5
aspell-0.33.7.1-16
at-3.1.8-31
atk-1.0.3-1
attr-2.0.8-3
audiofile-0.2.3-3
authconfig-4.2.12-3
authconfig-gtk-4.2.12-3
autofs-3.1.7-33
basesystem-8.0-1
bash-2.05b-5
bc-1.06-10
bdflush-1.5-21
bind-utils-9.2.1-9
binutils-2.13.90.0.2-2
bitmap-fonts-0.2-2
bonobo-1.0.20-3
bonobo-activation-1.0.3-2
bzip2-1.0.2-5
bzip2-libs-1.0.2-5
chkconfig-1.3.6-3
chkfontpath-1.9.6-3
compat-libstdc7.3-2.96.110
comps-8.0-0.20020910
comps-extras-8.0-3
control-center-2.0.1-8
cpp-3.2-7
cracklib-2.7-18
cracklib-dicts-2.7-18
crontabs-1.10-4
cups-libs-1.1.15-10
curl-7.9.8-1
cyrus-sasl-2.1.7-2
cyrus-sasl-md5-2.1.7-2
cyrus-sasl-plain-2.1.7-2
db4-4.0.14-14
desktop-backgrounds-basic-2.0-10
desktop-backgrounds-extra-2.0-10
desktop-file-utils-0.3-3
dev-3.3.1-2
dhclient-3.0pl1-9
diffutils-2.8.1-3
docbook-dtds-1.0-14
dos2unix-3.1-12
dosfstools-2.8-3
dump-0.4b28-4
e2fsprogs-1.27-9
eel2-2.0.6-1
eject-2.0.12-7
eog-1.0.2-3
esound-0.2.28-1
ethereal-0.9.6-1
ethereal-gnome-0.9.6-1
ethtool-1.6-2
expat-1.95.4-1
fam-2.6.8-4
fbset-2.1-11
file-3.37-8
filesystem-2.1.6-5
fileutils-4.1.9-11
findutils-4.1.7-7
finger-0.17-14
firstboot-1.0.1-10
fontconfig-2.0-3
foomatic-1.9-1.20020617.6
fortune-mod-1.0-24
freetype-2.1.2-7
ftp-0.17-15
gail-0.17-2
gal-0.19.2-4
gawk-3.1.1-4
gcc-3.2-7
gcc-c3.2-7
gcc-g77-3.2-7
gcc-gnat-3.2-7
gcc-java-3.2-7
gcc-objc-3.2-7
GConf-1.0.9-6
GConf2-1.2.1-3
gconf-editor-0.3-1
gd-1.8.4-9

gdbm-1.8.0-18
gdk-pixbuf-0.18.0-4
gdk-pixbuf-gnome-0.18.0-4
gdm-2.4.0.7-13
gedit-2.0.2-5
gftp-2.0.13-5
ghostscript-7.05-20
ghostscript-fonts-5.50-7
gimp-print-4.2.1-5
glib-1.2.10-8
glib2-2.0.6-2
glibc-2.2.93-5
glibc-common-2.2.93-5
glibc-devel-2.2.93-5
glibc-kernheaders-2.4-7.20
Glide3-20010520-19
gmp-4.1-4
gnome-applets-2.0.1-6
gnome-audio-1.4.0-4
gnome-desktop-2.0.6-4
gnome-libs-1.4.1.2.90-22
gnome-media-2.0.0-9
gnome-mime-data-2.0.0-9
gnome-panel-2.0.6-9
gnome-python2-1.99.11-8
gnome-python2-bonobo-1.99.11-8
gnome-python2-canvas-1.99.11-8
gnome-python2-gtkhtml2-1.99.11-8
gnome-session-2.0.5-7
gnome-system-monitor-2.0.0-2
gnome-terminal-2.0.1-5
gnome-user-docs-2.0.0-1
gnome-utils-2.0.2-5
gnome-vfs-1.0.5-6
gnome-vfs2-2.0.2-5
gnome-vfs2-extras-0.99.5-1
gnome-vfs-extras-0.2.0-3
gnupg-1.0.7-6
gpm-1.19.3-23
gqview-1.0.2-2
grep-2.5.1-4
groff-1.18-6
grub-0.92-7
gtk+1.2.10-22
gtk2-2.0.6-8
gtk2-engines-1.9.0-4
gtk-engines-0.11-13
gtkhtml2-2.0.1-2
gzip-1.3.3-5
hdparm-5.2-1
hesiod-3.0.2-21
hotplug-2002_04_01-13
htmlview-2.0.0-6
httpd-2.0.40-8
hwbrowser-0.6-1
hwdata-0.47-1
imlib-1.9.13-9
indexhtml-8.0-1
info-4.2-5
initscripts-6.95-1
intltool-0.22-3
iproute-2.4.7-5
iptables-1.2.6a-2
iputils-20020124-8
irda-utils-0.9.14-6
jfsutils-1.0.17-3
kbd-1.06-26
kbdconfig-1.9.16-1
kernel-2.4.18-14
kernel-pcmcia-cs-3.1.31-9
krb5-libs-1.2.5-6
krbafs-1.1.1-6
ksymoops-2.4.5-1
kudzu-0.99.69-1
less-358-28
lftp-2.5.2-5
lha-1.14i-7
libacl-2.0.11-2
libart_lgpl-2.3.10-1
libattr-2.0.8-3
libbonobo-2.0.0-4
libbonoboui-2.0.1-2
libcap-1.10-12
libelf-0.8.2-2
libf2c-3.2-7
libgal19-0.19.2-4
libgcc-3.2-7
libgcj-3.2-7
libgcj-devel-3.2-7
libglade-0.17-8
libglade2-2.0.0-2
libgnat-3.2-7

libgnome-2.0.2-5
libgnomecanvas-2.0.2-1
libgnomeprint-1.116.0-2
libgnomeprint15-0.35-8
libgnomeprintui-1.116.0-1
libgnomeui-2.0.3-3
libgtop2-2.0.0-3
libIDL-0.8.0-3
libjpeg-6b-21
libmng-1.0.4-1
libobjc-3.2-7
libogg-1.0-1
libpcap-0.6.2-16
libpng10-1.0.13-5
libpng-1.2.2-6
librpm404-4.0.4-8x.27
librsvg2-2.0.1-1
libstdc3.2-7
libstdcdevel-3.2-7
libtermcap-2.0.8-31
libtiff-3.5.7-7
libtool-libs-1.4.2-12
libungif-4.1.0-13
libuser-0.51.1-2
libvorbis-1.0-1
libwnck-0.17-1
libwvstreams-3.70-5
libxml-1.8.17-5
libxml2-2.4.23-1
libxml2-python-2.4.23-1
libxslt-1.0.19-1
lilo-21.4.4-20
linc-0.5.2-2
lockdev-1.0.0-20
logrotate-3.6.5-2
logwatch-2.6-8
lokkit-0.50-18
losetup-2.11r-10
lrzsz-0.12.20-14
lsof-4.63-2
lvm-1.0.3-9
lynx-2.8.5-7
magicdev-1.1.3-1
mailcap-2.1.12-1
mailx-8.1.1-26
make-3.79.1-14
MAKEDEV-3.3.1-2
man-1.5j-11
man-pages-1.53-1
metacity-2.4.0.92-5
mingetty-1.00-3
minicom-2.00.0-6
mkbootdisk-1.4.8-1
mkinitrd-3.4.28-1
mktemp-1.5-16
modutils-2.4.18-2
mount-2.11r-10
mouseconfig-4.26-1
mozilla-1.0.1-24
mozilla-nspr-1.0.1-24
mpage-2.5.2-4
mtools-3.9.8-5
mtr-0.49-7
mtr-gtk-0.49-7
mt-st-0.7-6
nautilus-2.0.6-6
ncurses-5.2-28
netconfig-0.8.12-3
net-snmp-5.0.1-6
net-snmp-utils-5.0.1-6
net-tools-1.60-7
newt-0.51.0-1
nfs-utils-1.0.1-2
nmap-3.00-1
nscd-2.2.93-5
nss_ldap-198-3
ntp-4.1.1a-9
ntsysv-1.3.6-3
oaf-0.6.9-2
Omni-0.7.0-6
Omni-foomatic-0.7.0-6
openjade-1.3.1-9
openldap-2.0.25-1
openssh-3.4p1-2
openssh-askpass-3.4p1-2
openssh-askpass-gnome-3.4p1-2
openssh-clients-3.4p1-2
openssh-server-3.4p1-2
openssl-0.9.6b-29
ORBit-0.5.13-5
ORBit2-2.4.1-1
orbit-python-1.99.0-4

pam-0.75-40
pam_krb5-1.56-1
pam_smb-1.1.6-5
pango-1.1.1-1
parted-1.4.24-6
passwd-0.67-3
patch-2.5.4-14
pax-3.0-4
pciutils-2.1.10-2
pcre-3.9-5
perl-5.8.0-55
perl-CGI-2.81-55
perl-DateManip-5.40-27
perl-Filter-1.28-9
perl-HTML-Parser-3.26-14
perl-HTML-Tagset-3.03-25
perl-libwww-perl-5.65-2
perl-libxml-enno-1.02-25
perl-libxml-perl-0.07-25
perl-Parse-Yapp-1.05-26
perl-URI-1.21-3
perl-XML-Dumper-0.4-22
perl-XML-Encoding-1.01-20
perl-XML-Grove-0.46alpha-21
perl-XML-Parser-2.31-12
perl-XML-Twig-3.05-3
php-4.2.2-8.0.5
pinfo-0.6.4-7
popt-1.7-1.06
portmap-4.0-46
ppp-2.4.1-7
procmail-3.22-7
procps-2.0.7-25
psmisc-20.2-6
pspell-0.12.2-14
psutils-1.17-17
pygtk2-1.99.12-7
pygtk2-libglade-1.99.12-7
pyOpenSSL-0.5.0.91-1
python-2.2.1-17
python-optik-1.3-2
pyxf86config-0.3.1-2
PyXML-0.7.1-6
qt-3.0.5-17
quota-3.06-5
rdate-1.2-5
rdist-6.1.5-24
readline-4.3-3
redhat-artwork-0.47-3
redhat-config-date-1.5.2-10
redhat-config-keyboard-1.0.1-1
redhat-config-language-1.0.1-6
redhat-config-mouse-1.0.1-2
redhat-config-network-1.1.20-1
redhat-config-packages-1.0.1-1
redhat-config-rootpassword-1.0.1-1
redhat-config-securitylevel-1.0.1-1
redhat-config-services-0.8.2-1
redhat-config-soundcard-1.0.1-2
redhat-config-users-1.1.1-2
redhat-config-xfree86-0.6.7-1
redhat-logos-1.1.6-2
redhat-logviewer-0.8.3-2
redhat-menus-0.26-1
redhat-release-8.0-8
redhat-switchmail-0.5.14-1
redhat-switchmail-gnome-0.5.14-1
redhat-switch-printer-0.5.12-1
redhat-switch-printer-gnome-0.5.12-1
reiserfs-utils-3.6.2-2
rhn-applet-2.0.0-28
rhnlib-1.0-1
rhpl-0.51-1
rmt-0.4b28-4
rootfiles-7.2-4
rpm404-python-4.0.4-8x.27
rpm-4.1-1.06
rpm-python-4.1-1.06
rp-pppoe-3.4-7
rsh-0.17-10
rsync-2.5.5-1
scrollkeeper-0.3.10-7
sed-3.02-13
sendmail-8.12.5-7
setserial-2.17-9
setup-2.5.20-1
setuptool-1.10-1
sgml-common-0.6.3-12
shadow-utils-20000902-12
sh-utils-2.0.12-3
slang-1.4.5-11
slocate-2.6-4

sox-12.17.3-7
specspo-8.0-3
star-1.5a04-1
stat-3.3-4
statserial-1.1-30
stunnel-3.22-4
sudo-1.6.6-1
switchdesk-3.9.8-9
switchdesk-gnome-3.9.8-9
sysklogd-1.4.1-10
syslinux-1.75-3
SysVinit-2.84-5
talk-0.17-17

tar-1.13.25-8
tcl-8.3.3-74
tcpdump-3.6.3-3
tcp_wrappers-7.6-23
tcsh-6.12-2
telnet-0.17-23
termcap-11.0.1-13
textutils-2.0.21-5
time-1.7-19
timeconfig-3.2.9-1
tmpwatch-2.8.4-3
traceroute-1.4a12-6
ttfprint-0.9-6
unix2dos-2.2-17
unzip-5.50-5
up2date-3.0.7-1
up2date-gnome-3.0.7-1
urw-fonts-2.0-26
usbutils-0.9-7
usermode-1.63-1
usermode-gtk-1.63-1
utempter-0.5.2-10
util-linux-2.11r-10
VFlib2-2.25.6-8
vim-common-6.1-14
vim-minimal-6.1-14
vixie-cron-3.0.1-69
vte-0.8.19-1
wget-1.8.2-3
which-2.14-1
whois-1.0.10-4
WindowMaker-0.80.1-1
WindowMaker-libs-0.80.1-1
wireless-tools-25-1
words-2-20
wvdial-1.53-7
XFree86-100dpi-fonts-4.2.0-72
XFree86-4.2.0-72
XFree86-75dpi-fonts-4.2.0-72
XFree86-base-fonts-4.2.0-72
XFree86-font-utils-4.2.0-72
XFree86-libs-4.2.0-72
XFree86-Mesa-libGL-4.2.0-72
XFree86-Mesa-libGLU-4.2.0-72
XFree86-tools-4.2.0-72
XFree86-truetype-fonts-4.2.0-72
XFree86-twm-4.2.0-72
XFree86-xauth-4.2.0-72
XFree86-xdm-4.2.0-72
XFree86-xfs-4.2.0-72
Xft-2.0-1
xinetd-2.3.7-2
xinitrc-3.31-1
xml-common-0.6.3-12
xscreensaver-4.05-6
xsri-2.1.0-3
Xtest-2.0-1
yelp-1.0.2-2
ypbind-1.11-2
yp-tools-2.7-3
zip-2.3-14
zlib-1.1.4-4

Appendix G - Floppy Contents

```
.
./lost+found
./dcat
./file
./level1
./level1/md5.c
./level1/md5.h
./level1/level2
./level1/level2/print.c
./level1/level2/patchlevel.h
./level1/level2/level3
./level1/level2/level3/ifind.c
./level1/level2/level3/ffs.c
./level1/level2/level3/ffs.h
./level1d
./level1d/level2d
./level1d/level2d/level3d
./level1d/level2d/level3d/passwd
./level1d/level2d/test
./level1d/dstat.c
./mactime
./sorter
./target2.exe
```

Appendix H - Date Conversion Program epochToDate

```
#!/usr/bin/perl
#by David Gabler, drg-gcfa@gablerfamily.org
#Usage ./epochToDate <epoch time>
use Time::localtime;

$tm = localtime($ARGV[0]);
print $tm->mon+1, "/", $tm->mday, "/", $tm->year+1900, " ", $tm->hour, ":", $tm-
>min, ":", $tm->sec, "\n";
```