Analysis of Unknown Binary, Forensic Tool Validation, and Legal Issues of Incident Handling for GIAC Certified Forensic Analyst Certification, Version 1.3

Abstract:
The investigator: analyzes an unknown binary using several Linux and Windows forensic tools revealing an ICMP Backdoor; Tests Dependency Walker as a forensic tool for analyzing unknown Windows binaries; Explores the legal issues of a system administrator of an imaginary ISP sharing possible forensic evidence with a government agent acting under color of law.

Christopher Vera
SANS GCFA
Practical v.1.3

Table of Contents

Table of Contents 2
PART ONE - Analysis of Unknown Binary 4
  Background 4
    Preparing the Lab 4
      Linux Forensics Workstation Preparation 4
      Windows 2000 Forensics Workstation Preparation 5
  Binary Details 8
    Linux Forensics Analysis 8
    Windows 2000 Forensics Analysis 10
    Binary Analysis Summary 12
  Program Description 12
    Windows Analysis Workstation 12
    Windows Network Capture Workstation 13
    Winalysis Snapshot 13
    Running the Specimen 14
    Filemon Results 15
    Regmon Results 16
    Network-related system changes 17
    Program Description Summary 17
  Forensic Details 17
    Dependency Walker Passive Results 17
    Dependency Walker Profile Mode 18
    Winalysis Results 19
    Network Capture Results 19
  Program Identification 20
    Program Identification Summary 21
  Legal Implications 21
    18 U.S.C. § 1029 Fraud and Related Activity in Connection with Access Devices 22
    18 U.S.C. § 1030. Fraud and Related Activity in Connection with Computers 22
    18 USC § 2701-11 The Electronic Communications Privacy Act 23
  Interview Questions 23
  Additional Info 24
PART TWO - Option Two, Forensic Tool Validation 25
  Background 25
  Scope 25
  Tool Description 25
  Test Apparatus 28
    Hardware 28
    Software 29
    Windows Services 29
    Page File 30
  Environmental Conditions 30
  Description of Procedures 30
    Step 1-Prepare Software Tools CD 30

Step 2-Prepare the Test System....31
Step 3-Baseline the Test System....32
Step 4-Examine the specimen passively in DW....33
Step 5-Check for System Modifications by DW....34
Step 6-New Baseline Snapshot Taken....34
Step 7-Examine Specimen in DW Runtime Mode....34
Step 8-Check for System Modifications by DW....35
Step 9- Accuracy Checks....35
Step 10-Sanitize Test System....35
Criteria for approval....36
Data and results....36
Compare Baseline vs. Post Snapshot....36
TEST DATA - Dependency Walker Passive....38
TEST DATA - Dependency Walker in Profile Mode....40
TEST DATA – Accuracy....44
Analysis....46
DW Information....46
DW Accuracy....47
PE EXPLORER COMPARE....48
DLL REPLACEMENT....49
Presentation....49
Conclusion....51
PART THREE - Legal Issues of Incident Handling....52
Background....52
What Information Can Be Provided at Initial Contact....52
Law Enforcement Obligations to Require ISP to Preserve Evidence....54
Legal Authority Required for Law Enforcement to Obtain Logs....55
Other Investigative Activity That Can Be Performed by ISP....55
Other Possibilities....57
References....59
Appendices....60
Appendix 1-A SANS Linux Workstation Script....60
Appendix 1-B Specimen Zip File Info....60
Appendix 1-C Specimen Strings Output....61
Appendix 1-D Specimen Filestat Output....64
Appendix 2-A Dependency Walker Output....65
Appendix 2-B Winalysis HKU results- Dependency Walker Passive Mode....76
Appendix 2-C Winalysis HKU results- Dependency Walker Profiler Mode....79
Appendix 2-D Dependency Walker Profile of Specimen....82
Appendix 3-A Modified EPCA Quick Reference Guide....91

PART ONE - Analysis of Unknown Binary

Background

A binary of unknown origin, hereafter called the specimen, was provided to the investigator. No information was provided to the investigator by the original collector of the specimen as to what kind of computer the specimen was captured from, or the circumstances that lead the collector to discover the existence of the specimen in the first place. It would be the job of the investigator to learn whatever additional information could be learned by analyzing the specimen in a controlled environment.

Preparing the Lab

Two forensics analysis computers were used to investigate the specimen; A Linux workstation first, and, as it became apparent the binary was a Win32 executable, a Windows 2000 Professional workstation.

The file was first examined in Linux because this operating system provides several tools that allow the investigator to quickly inspect the binary.

The following procedures were used to prepare the analysis computers.

Linux Forensics Workstation Preparation

The "Analysis of Unknown Binary" by Greg Owen SANS GCFA provides an excellent resource for preparing a Linux workstation to examine an unknown binary (http://www.giac.org/GCFA.php, number 0023). Rather than reinvent the wheel, the investigator adopted some steps of this preparation method, with some minor modifications.

1. The hard disk was wiped using a Linux boot disk with dd to overwrite the disk.
2. Linux RedHat version 8.0 was installed from CD.
3. The OS is boot and the investigator logs in.
4. The SANS script for Linux forensics workstations, provided by the instructor Rob Lee in the March 2003 class, was run. Among other things, the script installed some forensic tools. The actual script is included in Appendix 1-A.

The following commands in step 5 were taken from Greg Owen's paper, with some explanation by the investigator.

5. To create a lab to examine the specimen, the investigator used **dd**. Here, **dd** allowed the investigator to create a file of a specified size, in this case

50 MB.

```
# dd if=/dev/zero of=/forensics/petridish.fs bs=1024k count=50
```

losetup allowed the investigator to use this new file as a loopback device.

```
#losetup /dev/loop5 /forensics/petridish.fs
# mkfs.ext3 /dev/loop5
# losetup –d /dev/loop5
```

Having created the new file system, the investigator mounted it with options designed to prevent accidental execution or access timestamp modification of the specimen.

```
# mkdir /forensics/lab
# mount –t ext3 –o loop,noatime,noexec /forensics/petridish.fs
/forensics/lab
```

6. The lab environment, safely mounted, allowed the specimen to be copied into it as any other file system.

Windows 2000 Forensics Workstation Preparation

Although the Windows workstation was not required until some investigation was done on the Linux workstation, it was prepared in the following fashion after it became apparent that its services would be required.

1. A clean installation was done of Windows 2000 Server from the Microsoft Software Developer Network (MSDN) CD.
2. The latest service packs and hotfixes were applied from CD.
3. The local audit policy was configured to audit all events for success and failure.
4. The SANS Windows forensics tools were copied from CD and those that required installation were installed.
5. Norton Anti-Virus Corporate Edition Scanned specimen with Norton Anti-Virus Corporate Edition v.7.51.847, Scan Engine 4.1.0.6, was installed with real-time scanning turned off.
6. Windows offers an interesting tool called **Cipher.exe** that is normally used with the Windows Encrypting File System (EFS). However, **Cipher.exe** offers the ability to "zero out" or wipe slack space that may have been modified by the installation of Windows and other programs. **Cipher.exe** with the **/w** switch will fill clean out slack space and fill it with random numbers.

```
C:\Forensics\Tools> cipher /w:c:\

To remove as much data as possible, please close all other applications
while
running CIPHER /W.
Writing 0x00
.....................................................................
.........
....................
```

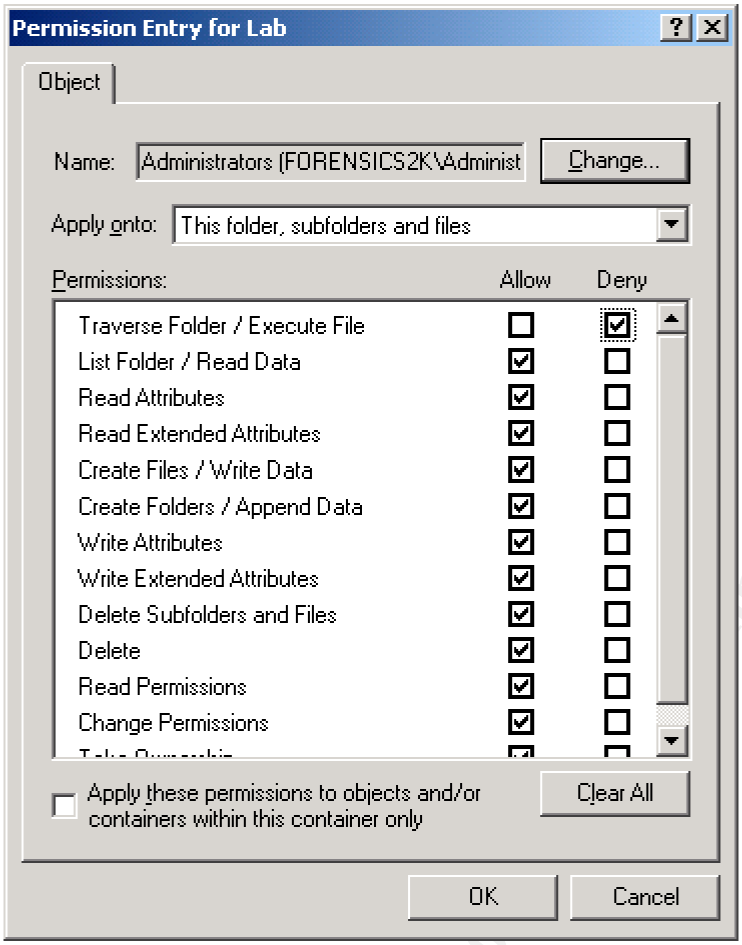
```
Writing OxFF
.....................................................................
.........
..................
Writing Random Numbers
.....................................................................
.........
..................

C:\Forensics\Tools>
```

Note that **Cipher.exe** overwrites the unallocated space three times: First with all zero's, then with all ones (FF in hex equals 255 in decimal, or 11111111 in binary), and finally in a random fashion. This is in accordance with the Department of Defense (DoD) standard for non-classified data (http://www.dss.mil/isec/chapter8.htm, 8-306). Note that disks containing classified data must be destroyed according to the standard. Wiping alone is not acceptable.

Cipher.exe is available in Windows 2000 service pack 3 and above. It is also available via the Windows 2000 Security Rollup Package 1 (SRP1), (http://support.microsoft.com/?kbid=298009)

7. Windows does not offer the loopback non-executable file system tools that Linux does for preventing the accidental execution of specimens or access time modification. But there are still precautions that can be taken. A folder was created in c:\forensics called Lab. All inherited permissions to this folder were removed and Administrators were assigned full control with one caveat: The ability to execute code was removed. Folder Properties > Security tab > Advanced button > View/Edit button. Deny Traverse folder/Execute File permissions.

See Figure 1-a below.



Permission Entry for Lab

Object

Name: Administrators (FORENSICS2K\Administ

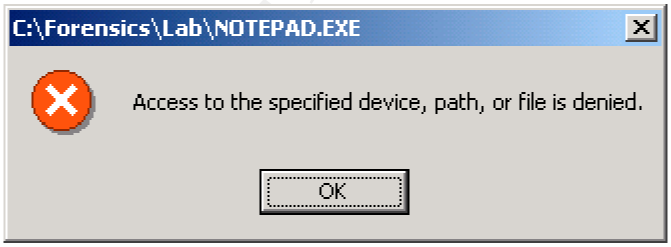
Apply onto: This folder, subfolders and files

Permissions:	Allow	Deny
Traverse Folder / Execute File	□	☑
List Folder / Read Data	☑	□
Read Attributes	☑	□
Read Extended Attributes	☑	□
Create Files / Write Data	☑	□
Create Folders / Append Data	☑	□
Write Attributes	☑	□
Write Extended Attributes	☑	□
Delete Subfolders and Files	☑	□
Delete	☑	□
Read Permissions	☑	□
Change Permissions	☑	□
Take Ownership	☑	□

□ Apply these permissions to objects and/or containers within this container only

Figure 1-a Permission of Lab folder.

A simple test by copying a known executable, in this case a copy of Notepad.exe, into the Lab folder and attempting to execute it confirmed that this file type will not run. Figure 1-b shows the error received.



C:\Forensics\Lab\NOTEPAD.EXE

Access to the specified device, path, or file is denied.

Figure 1-b Error received when attempting to execute

The specimen could then be copied into the Lab folder. After the examination of the specimen on the Linux workstation, the specimen was unzipped to the Lab folder for further analysis.

Note that this permission change will prevent the investigator from changing into the directory (cd) from the command line.

For example,

```
C:\Forensics> cd lab
Access is denied.
```

However, the investigator can still view and manipulate files within the folder.

```
>dir c:\forensics\lab
 Volume in drive C has no label.
 Volume Serial Number is FC44-247D

 Directory of c:\forensics\lab

04/13/2003  07:01p      <DIR>          .
04/13/2003  07:01p      <DIR>          ..
02/20/2003  12:45p              26,793 target2.exe
               1 File(s)         26,793 bytes
               2 Dir(s)   5,028,806,656 bytes free

>
```

It was time to get to work.

Binary Details

Linux Forensics Analysis

The specimen was first examined on the Linux workstation. It was copied from CD to the /forensics/lab mount point. The first order of business was to see what was in the zip file and learn a little about what the investigator was up against.

Zipinfo in verbose mode can tell the investigator much about the contents of the zip file. The output below has been truncated to show interesting information. The entire output of the command can be found in Appendix 1-B.

```
# zipinfo –v /forensics/lab/binary_v1.3.zip

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

 target2.exe

 file system of operating system of origin:     MS-DOS, OS/2 or NT FAT
 minimum file system compatibility required:    MS-DOS, OS/2 or NT FAT
 file security status:                          not encrypted
 file last modified on (DOS date/time):         2003 Feb 20 12:45:48
 uncompressed size:                             26793 bytes
 MS-DOS file attributes (20 hex):               arc
```

From this information the investigator had learned much.

The name of specimen was **target2.exe**. It was a DOS, Windows or OS/2-based file. It was not encrypted inside the zipped file.

It was last modified on February 20, 2003 around 12:45 pm. This is possibly misleading and it is more likely that this is when the file was captured, copied and zipped by the person who initially discovered the specimen rather than the last time the file was modified. It was not clear yet as to what time zone the computer was in when the specimen was captured.

The file size was 26,793 bytes, or just about 26.7 Kb.

There was no way to determine the original owner of the file from this information.

Next, the investigator unzipped the file.

```
# pwd
/forensics/lab
# unzip –X binary_v1.3.zip
 inflating: target2.exe
# ls – l
total 46
-r-xr-xr-x  1 root      root   5687     Apr  3 20:55 binary_v1.3.zip
drwx------  2 root      root  12288     Apr  3 20:53 lost+found
-rw-r–r--   1 root      root  26793     Feb 20 12:45 target2.exe
```

Note that no execute permissions had been assigned to the specimen.

An MD5 hash was performed on the specimen, a copy of which was stored in a text file as evidence. No MD5 hash was provided with the specimen to verify it against for authenticity.

```
# md5sum target2.exe > /forensics/evidence/target2.md5
# cat /forensics/evidence/target2.md5
848903a92843895f3ba7fb77f02f9bf1 target2.exe
```

From the **zipinfo** data collected, it appeared the specimen was a Windows or DOS file. The investigator used the **file** command to further verify this.

```
# file target2.exe
target2.exe: MS-DOS executable (EXE), OS/2 or MS Windows
#
```

The results of the **file** command also supported the conclusion that the specimen was most likely a Windows file.

Next, the investigator ran the **strings** command against the file, again stored in a text file for use as evidence. The output below is sorted for a sample of interesting content. The entire output can be viewed in Appendix 1-C.

```
# strings target2.exe > /forensics/evidence/target2.strings
```

Files	Possible Commands	Output or Other Strings
KERNEL32.dll ADVAPI32.dll WS2_32.dll MFC42.DLL MSVCRT.dll MSVCP60.dll cmd.exe smsses.exe	StartServiceCtrlDispatcherA SetServiceStatus RegisterServiceCtrlHandlerA CloseServiceHandle Memmove Sucessfully	Exit OK! Impossibile creare raw ICMP socket RAW ICMP SendTo: ======= Icmp BackDoor V0.1 ======== Code by Spoof. Enjoy Youself! Your PassWord: loki Local Partners Access Error UnInstalling Service Service UnInstalled Sucessfully Error Installing Service Service Installed

Confident that the specimen was Windows-based, the investigator continued the analysis on the Windows 2000 forensics workstation.

Windows 2000 Forensics Analysis

After the specimen was unzipped into the c:\forensics\lab folder, the investigator ran **md5sum.exe** against it to verify the same binary was being analyzed.

```
C:\Forensics\Tools>md5sum c:\forensics\lab\target2.exe >
c:\forensics\evidence\target2.md5
Results: 848903a92843895f3ba7fb77f02f9bf1
```

The investigator scanned the specimen with Norton Anti-Virus Corporate Edition v.7.51.847, Scan Engine 4.1.0.6, Virus Definition file 50402t dated 04-02-03. The results were clean. The specimen did not register to the anti-virus software as a virus or Trojan.

Although the specimen's time stamps were examined under Linux, this was a good opportunity to compare these results against a tool in Windows known as **filestat.exe** (by JD Glaser, available at www.foundstone.com). This tool dumps security attributes of a given file. The truncated results are shown here.

```
> filestat c:\forensics\lab\target2.exe

Creation Time - 08/04/2003  21:40:05
Last Mod Time - 20/02/2003  12:45:48
Last Access Time - 13/04/2003  20:46:05
Main File Size - 26793
File Attrib Mask - Arch
Dump complete...Dumping c:\forensics\lab\target2.exe...
```

The entire output of Filestat can be viewed in Appendix 1-D. Note the creation time shows the date and time the investigator first unzipped the specimen. The last mod time coincides with the date and time observed from the zipinfo information gathered from the Linux workstation. The last access time shows the limitations of the operating system to protect the file against time stamp modification.

Then it was time to look at the strings in the file again, this time using a tool from Foundstone called BinText v3.0. The investigator's version came from the SANS CD. However, the current version can always be obtained directly from Foundstone at http://www.foundstone.com.

BinText Results

In addition to the strings noted from the Linux workstation analysis, BinText also uncovered some previously undetected strings. The results have been truncated to show only the unique new strings of interest.

```
!This program cannot be run in DOS mode.
Hello from MFC!
\winnt\system32\smsses.exe
\\199.107.97.191\C$
\winnt\system32\reg.exe
```

Note the IP address 199.107.97.191. A search at the American Registry for Internet Numbers (http://www.arin.net) revealed the IP's owner:

Search results for: 199.107.97.191

```
CERFnet NETBLK-CERFNET-CBLK2 (NET-199-105-0-0-1)
                                  199.105.0.0 - 199.108.255.255
CERFnet customer - Azusa Pacific University CERF-AZUSA (NET-199-107-96-
0-1)
                                  199.107.96.0 - 199.107.99.255
```

Azusa University is a Christian university in Azusa, California (http://www.apu.edu). The investigator now had a lead on where to continue the investigation should it become necessary to find the specimen's author or at least another computer the author might have compromised.

The IP address was **ping**ed and found to be alive on the Internet during the investigation. **Nslookup** also provided results.

```
> ping 199.107.97.191

Pinging 199.107.97.191 with 32 bytes of data:

Reply from 199.107.97.191: bytes=32 time=70ms TTL=114
Reply from 199.107.97.191: bytes=32 time=41ms TTL=114
Reply from 199.107.97.191: bytes=32 time=40ms TTL=114
Reply from 199.107.97.191: bytes=32 time=40ms TTL=114

Ping statistics for 199.107.97.191:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 70ms, Average = 47ms

> nslookup 199.107.97.191
*** Can't find server name for address 192.168.0.1: Non-existent domain
*** Default servers are not available
Server: Unknown
```

```
Address: 192.168.0.1

Name: sbm191.dtc.apu.edu
Address: 199.107.97.191
```

Just because the investigator had this information did not grant him the right to port scan or otherwise further interrogate the box owning the IP address. It was filed as evidence for future use.

Binary Analysis Summary

Even without executing the specimen, the investigator was able to discover many things about it.

- The MD5 checksum.
- The last modified date of Feb 20 2003.
- The specimen was a Windows file, perhaps not compatible with Windows 98 or earlier.
- Keywords in the specimen, especially the Italian language and some similar string structures pointed to multiple likely sources of original code.
- The specimen did not register to Norton Anti-Virus as malicious code.
- An IP address found in the strings of the specimen pointed to an active and Internet-connected computer that may have been used or exploited by the specimen's author.

Program Description

The next stage of the analysis process required the execution of the specimen in an isolated environment. Two Windows workstations, any analysis workstation for executing the specimen and the other for capturing network traffic, were connected to a Linksys hub with no other network connectivity.

From searches on the Internet for similar code, it appeared the specimen was an ICMP backdoor of some kind. It made sense to determine some common characteristics of ICMP tools compare their functionality against the specimen. From the readme file of Peter Eluks' ICMP shell (http://peter.eluks.com/code/Unix/C/ICMP-Shell/ISH-src/README), the investigator found some probable switches to use with the specimen.

Windows Analysis Workstation

The Windows Analysis Workstation was created with a default installation of Windows 2000 Server and service pack 3. No other patches or hotfixes were installed on this workstation.

The Windows 2000 Support Tools, available on the Windows 2000 installation

CD, were installed on the Windows Analysis workstation.

Winalysis 3.0 was installed on the Windows Analysis workstation (www.winalysis.com). Winalysis allows for a snapshot to be taken of the system to look for changes in files or the registry. The Application, Security and System event logs were cleared. A snapshot was taken in Winalysis for all files in c:\ including security descriptors and sub-directories), the registry, services, shares, volumes, system, scheduler, rights, users and groups. Doing a snapshot of all files on the drive will produce a warning because not all files can be accessed (i.e., the pagefile).

Regmon v4.32, Filemon v6.02, and TDImon v1.0 were downloaded on the Windows Analysis workstation. All these tools are from www.sysinternals.com.

Regmon is used to monitor registry activity and capture changes.

Filemon is used to monitor file level activity and capture changes.

TDImon is used to monitor Transport Driver Interface (TCP and UDP) activity and capture changes.

Windows Network Capture Workstation

The Windows Network Capture workstation was installed with Ethereal for Windows version 0.9.7 and left running with its network card in promiscuous mode.

Finally, permissions were reset on the c:\forensics\lab folder to allow execution of the specimen.

Winalysis Snapshot

Winalysis was used to take a snapshot of the system to discover changes.

The snapshot was taken with the following options:

- Files
- Registry
- Services
- Shares
- Volumes
- System
- Scheduler
- Rights
- Users
- Groups

The following filter options were used:

- C:\ drive
- Include subfolders
- Track security descriptors
- Track file version numbers
- Track digital signature numbers (SHA-1)

- The entire registry was selected.

Running the Specimen

Filemon, Regmon were started as was Ethereal on the Network Capture workstation. Then the specimen was executed with the following command

```
> target2.exe –i 666

Create Service Local Partners Access ok!
starting the service (Local Partners Access)…
Starting the service failed!

Error Installing Service
```

The "-i" switch was added after some trial and error. The specimen had been apparently unresponsive before with switch was added. However, either the investigator had incorrectly started the specimen or it had failed for an unknown reason.

After reviewing some of the Filemon and Regmon output (see below), the investigator made some changes to help the specimen along. First, Dependency Walker was used to determine what DLLs were required by the specimen (see Forensic Details section for full information). According to MS DLL Help database, Mfc42loc.dll is an MFC Language Specific Resource that ships with Windows 98 Plus Pack (http://support.microsoft.com/default.aspx?scid=/servicedesks/fileversion/dllinfo.asp&SD=MSDN&FR=0).

Microsoft states that "you should never install an Mfc42loc.dll on an English system. English resources are built into Mfc42.dll, and it is faster to load them from that DLL instead of searching (and loading) an MFC localization DLL first." (Redistributing Microsoft Visual C++ 6.0 Applications, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnvc60/html/redistribvc6.asp). However, the specimen appeared to require mfc42loc.dll.

After subsequent runs, the specimen also appeared to require **msvcp60.dll**. Per Microsoft's DLL Help database, this file is a C++ runtime file. Several products include this DLL, including some Office products such as Access and Outlook, and some server products such as Exchange Server 2000 and SQL Server 2000.

To see if the investigator could get the specimen to load and run normally, the following changes were made to the system:

- A copy of the local **mfc42.dll** was made, renamed to **mfc42loc.dll** and placed in the c:\winnt\system32 folder.

- A copy of **msvcp60.dll** was copied from another Windows 2000 server via floppy disk to the c:\winnt\system32 folder.

- A copy of the specimen was copied, renamed to **smsses.exe** and put in the c:\forensics\lab and c:\winnt\system32 folders.

- The image path registry entry for the failed Local Printer Manager Service was changed to c:\forensics\lab\smsses.exe.

Then the specimen was rerun.

```
> smsses.exe –i 666
Service Local Partners Access Already exists
starting the service (Local Partners Access)…
Start service successfully!

Service Installed Sucessfully
```

However, the “666” could be any string and start the service the same way.

Also, the “–d” switch with any string uninstalled the specimen by stopping the smsses.exe process and disabling the Local Printer Manager Service.

No other switches tried, (i.e., -a, -b, -c,…,-aa, -bb, -cc, etc.) , or combinations of port numbers or IP addresses as the last string (i.e, smsses.exe –x 127.0.0.1) appeared to have any effect on the specimen or invoke the suspect service.

PINGing the host with packets of 666 bytes failed to produce a result other than successful pings.

Filemon and Regmon provided the following results. These have been edited for brevity.

Filemon Results

The specimen took action on the following unique files in this order.

Process	Request	Path	Action
Smsses.exe	Query, Open	C:\ws2_32.dll	Open, Execute
Smsses.exe	Query, Open	C:\ws2help.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\mfc42.dll	Open, Execute

Smsses.exe	Query, Open	C:\program files\support tools\msvcp60.dll	Open, Execute
Smsses.exe	Query	C:\forensics\lab\smsses.exe.Local	FILE NOT FOUND (subsequently the investigator renamed target2.exe to smsses.exe as stated above)
Smsses.exe	Query, Open	C:\winnt\system32\mfc42loc.dll	Open, Execute Note: This file, copied from mfc42.dll, was placed by the investigator.
Services.exe	Query, Open	C:\forensics\lab\smsses.exe	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\msafd.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\wshtcpip.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\rnr20.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\dnsapi.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\wsock32.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\iphlpapi.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\icmp.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\mprapi.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\samlib.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\netapi32.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\secur32.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\netrap.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\activeds.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\adsldpc.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\rtutils.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\setupapi.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\userenv.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\rasapi.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\tapi32.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\dhcpcsvc.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\winrnr.dll	Open, Execute
Smsses.exe	Query, Open	C:\winnt\system32\rasadhlp.dll	Open, Execute

Regmon Results

The specimen touched far too many unique registry keys to list here. However, there were some items that should be noted from the Regmon results:

- The specimen created a service called “Local Printer Manager”.
- It set the service image to “smsses.exe”
- It then queried several network-related registry entries, including, tcp/ip data such as the IP address, telephony, RAS, and WINSOCK parameters, user settings such as personal (i.e., “My Documents” in the default setting) and local settings.
- It queried the computer name.
- It queried OS and service pack file locations.

Network-related system changes

Neither “NETSTAT –an” nor “NBTSTAT –an” showed any difference in listening ports or connections after the specimen was successfully run which was not entirely unexpected from an ICMP backdoor.

```
>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3372           0.0.0.0:0              LISTENING
```

All these ports are used by Microsoft protocols. Port 135 is used by Windows RPC. Port 445 is used by Server Message Block (SMB). Port 1025 and 3372 are used by Microsoft Distributed Transaction Coordinator.

Other network activity captured by the network sniffer is noted in Forensics Details below.

Program Description Summary

Review of similar source code and limited documentation of those tools indicated that the specimen appeared to be an ICMP backdoor pieced together with code from multiple sources. Because of the data gathered, it appeared the specimen was installed as a Windows service and allowed an attacker with the client to

a) Enumerate Windows services and TCP/IP data about the victim host and,
b) Obtain a command shell.

Forensic Details

The specimen touched very few parts of the operating system and file system. However, what it did touch would be enough to uniquely identify it.

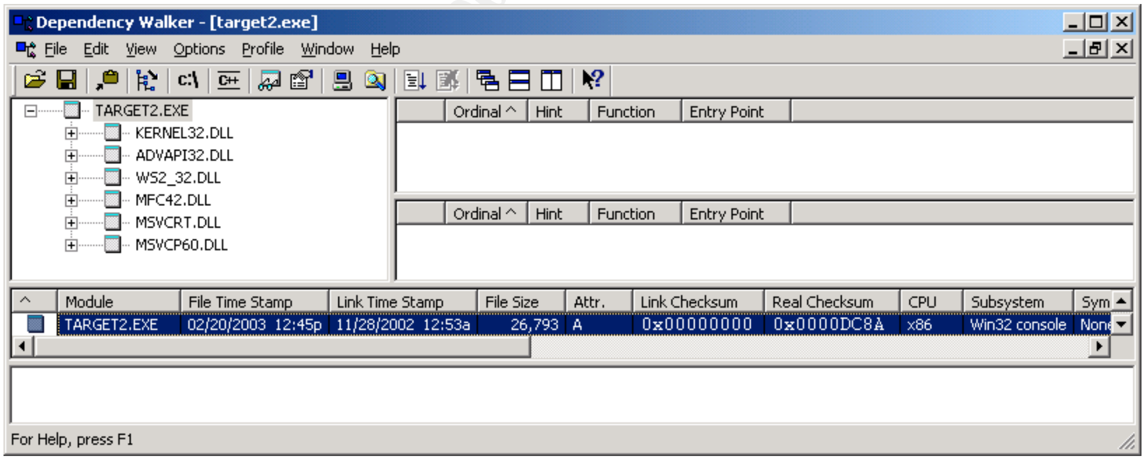
Dependency Walker Passive Results

Dependency Walker version 2.0 Beta 5 was required for learning more about the specimen’s dependencies on Windows DLLs. Version 2.0 beta 5 was used because it ships with the Windows 2000 Resource Kit. Newer versions are available at the Dependency Walker website (http://www.dependencywalker.com). Dependency Walker allowed the investigator to view DLL dependencies without executing the code. An option called runtime profiling allowed the investigator to step through the specimen as it ran although this option was not initiated during the passive phase.

Dependency Walker showed that the specimen required the following modules

Required Module	Location on Disk	Notes
Kernel32.dll	C:\winnt\system32	Also in c:\winnt\ServicePackFiles\i386
Advapi32.dll	C:\winnt\system32	Also in c:\winnt\ServicePackFiles\i386
Ws2_32.dll	C:\winnt\system32	Also in c:\winnt\ServicePackFiles\i386
Mfc42.dll	C:\winnt\system32	Also in c:\winnt\system32\dllcache, meaning this file is protected by the Windows File Protection system.
Msvcrt.dll	C:\winnt\system32	Also in c:\winnt\ServicePackFiles\i386
Msvcp60.dll	C:\Program Files\Support Tools	It is interesting to note that this dll does not exist on a default installation of Windows 2000 server English version.

Dependency Walker showed the specimen had a file time stamp of 02-20-2003 12:45p, which corresponded with what the investigator had already learned. In addition, the specimen had a link time stamp of 11-28-2002 12:53a, which told the investigator when the file was built. This evidence may be useful in the event the specimen's author was discovered and their computer investigated. Figure 1-c shows a snapshot of the results.



TARGET2.EXE
- KERNEL32.DLL
- ADVAPI32.DLL
- WS2_32.DLL
- MFC42.DLL
- MSVCRT.DLL
- MSVCP60.DLL

^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Sym
	TARGET2.EXE	02/20/2003 12:45p	11/28/2002 12:53a	26,793	A	0x00000000	0x0000DC8A	x86	Win32 console	None

Figure 1-c Specimen target2.exe in Dependency Walker

The specimen was designed to work in a Win32 console and appeared to be made to run on OS version 4.0, most likely Windows NT 4.0.

Dependency Walker Profile Mode

When the specimen was first executed, Dependency Walker in Profile mode showed that the specimen had attempted and failed to load **c:\winnt\system32\mfc42loc.dll**. According to the Dependency Walker FAQ this dll is a localized module for language-specific resource (http://www.dependencywalker.com/faq.html),. The file was modified for use on Windows 2000 as described in the Program Description section above.

Winalysis Results

Winalysis showed exactly where the specimen left its footprints.

The specimen did not create any new files. Nor did it create or modify any users, groups, or rights.

It did, however, modify the registry by creating a new service.

Registry
New key: HKLM\system\CurrentControlSet\Services\Local Partners Access
New values under this key:
Type: 16
Start: 2 (automatic)
ErrorControl: 1
ImagePath: smsses.exe
DisplayName: Local Printer Manager Service
ObjectName: LocalSystem

Several subkeys were also created under this key. Note tha the executable “smsses.exe” was probably chosen to closely resemble “smss.exe”, a real Windows system file.

Network Capture Results

No unusual network traffic was noted upon executing the specimen. However, TDImon, a TCP and UDP monitoring application from SysInternals, did capture data from the Transport Driver Interface. The results below have been modified for brevity.

```
IRP_MJ_CREATE
IRP_MJ_CLEANUP
IRP_MJ_CLOSE
IRP_MJ_DEVICE_CONTROL > IOCTL_TCP_QUERY_INFORMATION_EX
```

IRP stands for I/O Request Packet.

IRP_MJ_CREATE is used by a driver to create a request a handle for a device in Windows Kernel-mode architecture.

(http://msdn.microsoft.com/library/default.asp?url=/library/en-us/kmarch/hh/kmarch/k113_02lu.asp).

IRP_MJ_Cleanup is serviced by the DispatchCleanup routine. Cleanups are sent when the last handle on a file object associated with a device has been closed, but might not have been released. (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/kmarch/hh/kmarch/k113_6vg2.asp).

IRP_MJ_CLOSEs are sent when the last handle has been closed AND released (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/kmarch/hh/kmarch/k113_3naq.asp).

The last entry was repeated several times. The "IOCTL_TCP…" control code is used to retrieve information about the TCP/IP driver (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/devnotes/winprog/ioctl_tcp_query_information_ex.asp)

This information can be used to determine that a network input/output driver had been accessed, and that TCP/IP information was queried, but does not by itself provide more detail.

Program Identification

Many of the command string patterns were used to match against source code found on the Internet. Of interest are the misspellings of the string "sucessfully". The investigator noted the name "Spoof" in the code, apparently the author of the specimen. Also of interest was the apparent use of a non-English language, in the string "Impossibile creare…". Finally, there were several files mentioned, such as **ADVAPI32.dll**, which does not exist in a default install of Windows 98 or older. This dll is used to call functions that among other things, allow the enumeration and control of Windows NT-based services and to determine or log out the current user, or even to shut down or restart the computer. (http://www.andreavb.com/API_ADVAPI32.html). Also, **smsses.exe** is not a Microsoft Windows file and no reference to it could be found on Google. The author of the specimen may be using this file name to closely resemble the smss.exe file in Windows 2000.

The unusual phrase "impossibile creare raw ICMP socket" appeared to be Italian. A possible example of the source was found at http://www.s0ftpj.org/bfi/online/bfi7/bfi07-13.html. Similar source code with similar text was found on a Chinese website here: http://www.20cn.net/ns/wz/comp/data/20020819052905.htm. However, the strings from neither the Italian nor the Chinese code exactly matched that of the specimen. Perhaps the specimen was the child of cut-and-paste from others' hard work?

Another source on a Chinese site found here, http://mcking.8u8.com/hkwz18.htm, provided strong evidence of part of the original stolen source code with this phrase

```
"======================== Ping BackDoor V0.1
========================\r\n========= Code by Lion. Welcome to
Http://www.cnhonker.net =========".
```

The author of the specimen appears to have modified this phrase only slightly. See below for the author's text.

```
"======================== Icmp BackDoor V0.1 ========================
========= Code by Spoof. Enjoy Yourself!"
```

It is typical for malicious hackers to claim credit for code they did not write.

A visit to http://www.cnhonker.net produced a Windows Ping Backdoor. http://www.cnhonker.net/Files/show.php?id=189. A comparison of strings in this source showed some similarities, but it was clear they were not exactly the same.

Last, another Chinese website revealed several similar unique strings in the same order in a small program called Service Application (Serviceapp.exe) by a programmer called "refdom" designed to enumerate Windows services on local and remote computers.
http://www.20cn.net/ns/wz/comp/data/20020819052905.htm

It was unlikely that compiling any of this code would result in the same program as the specimen because the specimen appeared to have been pieced together from multiple sources. Also, each code used many words in characters in either Italian or Chinese in the comments that were not found in the specimen. Therefore, no MD5 hashes were compared.

Program Identification Summary

The investigator was unsuccessful in getting the specimen to function end-to-end as the author probably intended or to compile a similar client from elsewhere. However, based on other evidence, the specimen appeared to be an ICMP backdoor installed as a Windows service that allowed a client to do one or more of the following:

- enumerate TCP/IP information;
- enumerate Windows services;
- provide a command shell to the remote client.

Legal Implications

The specimen can be shown to have been executed by

a) the presence of the "Local Printer Manager" service on the victim host,
b) the presence of this service in the registry, or
c) the presence of smsses.exe running as an active process.

The investigator was never informed as to whether any of these conditions were found on the victim host and no data gathered provides evidence either.

But assuming it can be shown the specimen had been executed, what laws would have been broken?

The evidence shows that the tool used would provide its user with information about the victim host and a tool for accessing and controlling the system remotely. Such control could expose any data residing on the system to the attacker.

For purposes of discussion, this paper will assume the victim host was an Internet facing web server owned and operated by a private global telecommunications company located in the United States, and subject to U.S. laws, that provided Internet access only to its employees.

18 U.S.C. § 1029 Fraud and Related Activity in Connection with Access Devices

18 U.S.C. § 1029(a)(7) requires that the attacker "knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services". (http://www.cybercrime.gov/usc1029.htm).

If the ability to remotely control the web server gives the attacker the ability to grant his or herself unauthorized use of telecom services (perhaps in the form of creating an account or setting up an unauthorized phone number), this law will apply.

For a first offense the penalty would be a fine or imprisonment of not more than 10 years.

18 U.S.C. § 1030. Fraud and Related Activity in Connection with Computers

The Computer Fraud and Abuse Act may be able to be brought to bear because it can be argued that:

- The victim host was a protected computer, meaning a computer "used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States" (http://www4.law.cornell.edu/uscode/18/1030.html). In this case, because the victim host belonged to a telecommunications company and is probably used by the federal government.

- The attacker "knowingly accessed a computer without authorization or exceeding authorized access" and "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer" (http://www4.law.cornell.edu/uscode/18/1030.html).

The company will need to be able to prove the attack caused at least $5000 in accumulated losses.

Assuming a first offense, the penalty for the attacker would have been a felony resulting in a minimum of one year imprisonment or a fine.

18 USC § 2701-11 The Electronic Communications Privacy Act

Because the attacker would be granted a command shell upon successful connection to the victim host, and therefore have access to all data stored on the victim, the Electronic Communications Privacy act may apply because "whoever intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section." (http://www4.law.cornell.edu/uscode/18/2701.html)

Assuming a first offense, the attacker could expect to be charged with a felony resulting in a minimum of one year imprisonment or a fine.

Interview Questions

Interviewing a suspect is a sensitive process. Interviewing suspects is best left to professionals who specialize in interrogation. After all, what computer forensics investigator would want a poorly trained individual to attempt to collect electronic evidence? However, a professional interrogator would need to know what kind of information to obtain from the suspect. Due to the nature of the specimen, the suspect would have required a desire to use it since it is unlikely the specimen could be executed and configured accidentally. Below is a list of questions that a professional interrogator may massage into an interview, although the questions may not be worded in this exact manner.

1. *How did you obtain the backdoor?* The suspect may be able to tell us more about how the backdoor was created, or at least where to go to get

more information.

2. *Is there a reason you could not use one of the company-approved remote control tools*? This question may open up the possibility in the suspect's mind that there was a logical reason for installing it and convince them to explain.
3. *Do you have any relationship with Azusa University or know someone from there?* This is the investigator's opportunity to find a possible link to the Azusa-owned IP address found in the binary strings.
4. *Did you install the backdoor on any other systems?* It is important to find out where else the backdoor may exist. Although the investigator will use other means to determine this, it would be helpful if the suspect confessed and detrimental to the suspect if it was discovered they were lying.
5. *Do you or anyone you know anyone go by the name, "Spoof"?* If the suspect is not the author of the code, perhaps they know more about who claimed to be the author in the binary strings.

Additional Info

References can be found in the References section of this paper.

PART TWO - Option Two, Forensic Tool Validation

Background

Examination of unknown binaries requires the use of forensic tools that have measurable or no impact on the specimen to be examined. A captured unknown binary (hereafter called the specimen) was used as the basis for testing the value of a Microsoft Windows module diagramming tool called Dependency Walker. Dependency Walker provides the forensic investigator a tool to determine software dependencies in Microsoft Windows binary which can be used to provide clues as to the function of an unknown binary.

Software dependencies are module, or pieces of code, which an application requires in order to load and run correctly. Such dependencies are often found in the operating environment and not included in the application in order to save space and time.

By determining an unknown binary's dependencies, an investigator can learn more about what the binary is and how it works.

Scope

Dependency Walker is described by its author, Steve P. Miller, as "a free utility that scans any 32-bit or 64-bit Windows module (exe, dll, ocx, sys, etc.) and builds a hierarchical tree diagram of all dependent modules." (http://www.dependencywalker.com)

The goal of this test will be to determine

1. Whether Dependency Walker can be run from a forensic toolkit CD
2. Dependency Walker's forensic footprint on a inspected system
3. How accurate Dependency Walker is at finding dependencies.

In a forensic laboratory, the specimen could be copied to CD and analyzed using Dependency Walker without fear of modifying the original specimen. However, in order to understand Dependency Walker as a forensic tool it was important to perform this analysis.

Tool Description

The current version as of this writing of Dependency Walker is 2.1.3623 which was the version tested. It can be executed on all x86 versions of Windows 9x, Me, NT, 2000 and XP. The same version will also run on IA64 architecture. Older versions, no longer supported, will run on Alpha, AXP64, MIPS and PowerPC.

Dependency Walker was written by Steve P. Miller and is copyrighted by Microsoft Corporation.

The latest version of the tool is maintained at www.dependencywalker.com. Version 2.0 beta 5 can be found in the Windows Support Tools section of the Microsoft Windows 2000 Server CD although newer versions include some enhancements and bug fixes.

Version 2.1.3623 from the website is contained with several required files in a zipped file. No source code was available to review or compile from.

For purposes of identification, MD5 hashes were taken of the Dependency Walker core files (version 2.1.3623):

```
\0975f419562bdf2ae8fac583b008b368 * c:\\lab\\dw\\depends.cnt
\1d66a3cd8e401f38a1880319c0b14506 * c:\\lab\\dw\\depends.dll
\b6b2db895399c6bdd6a9b26dc9b4a063 * c:\\lab\\dw\\depends.exe
\cf78be8fbfc69f3eeeabb031a053dd78 *c:\\lab\\dw\\depends.hlp
```

Note that these core files can be copied to and run from an incident response CD.

According to its website, Dependency Walker produces diagrams of dependent modules, provides full paths to files, base addresses, version numbers, machine type, and debug information. For poorly written specimens, Dependency Walker can also be used to troubleshoot system errors caused by the loading or executing of modules. It is helpful in discovering missing or invalid modules, import/export mismatches, circular dependencies and other module-related problems. (www.dependencywalker.com).

This information is invaluable to the forensic investigator attempting to learn how an unknown binary works and what it relies on to function properly in a Windows environment.

Dependency Walker can help the investigator learn the following:

- The minimum set of files required for the specimen to load and run.
- What functions are exposed by the specimen.
- What functions are being called by other modules.
- The complete path to modules loaded by the specimen.

The easiest way to determine which system files Dependency Walker depends on is to access it with a software dependency checker. Two checkers were used: Dependency Walker and PE Explorer by Heaventools (www.pe-explorer.com).

A copy of depends.exe and depends.dll were examined using Dependency Walker and PE Explorer using the test environment described in the section, Test Apparatus using the procedures described in the Description of Procedures section.

First the examined modules were loaded into Dependency Walker in its passive mode to determine implicit, delay-load and forward dependencies. Then, runtime profiling was conducted on depends.exe to determine explicit and system hook dependencies.

Dependency Walker Results

Depends.exe	
Passive (Implicit)	**Runtime (Explicit)**
Advapi32.dll	Kernel32.dll
Kernel32.dll	Ntdll.dll
Gdi32.dll	Imagehlp.dll
User32.dll	Riched32.dll
Winspool.drv	Comctl32.dll
Comdlg32.dll	
Comctl32.dll	
Shell32.dll	

PE Explorer Results

Depends.exe	
Passive (Implicit)	**Runtime (Explicit)**
Advapi32.dll	Dynamically loaded libraries are not yet supported in PE Explorer
Kernel32.dll	
Gdi32.dll	
User32.dll	
Winspool.drv	
Comdlg32.dll	
Comctl32.dll	
Shell32.dll	

Note the results for implicit modules were the same.

Dependency Walker relies on several files with the extension of dll. DLLs, also known as Dynamic Link Libraries, are files used to store data or functions in Windows applications.

Passive, or implicit dependencies are load time dependencies that must be called at load time before the target file can be successfully loaded and run.

Runtime, explicit, or dynamic dependencies may be called at runtime and may not be reported in the target file's import tables. Runtime modules may be loaded by the target file without any notification to the operating system.

Implicit and explicit modules may also have dependencies of their own. These dependencies are not listed in the table. There may be other explicit dependencies that were not called during the running of the program if Dependency Walker did not invoke the necessary calls to the explicit dependency. This is important because one can never be certain DW, or any other dependency checker, is aware of all explicit dependencies.

All files listed in the tables are located in the c:\winnt\system32 directory.

The entire report of dependencies for depends.exe is provided in appendix 2-A.

Depends.dll had only a single implicit dependency on kernel32.dll. Depends.dll could not be profiled because it is not an executable file.

Implicit dependency modules are required for the examined module to load correctly, also known as a load-time dependency. This information is stored in the module's import table.

Explicit dependency modules, or dynamic modules, are loaded when called, as needed, while the program is running. It is necessary for Dependency Walker to run the program to determine its explicit dependencies.

Test Apparatus

The test was conducted on a computer with the following characteristics. The computer was configured to run with a few applications and services as possible in order to reduce the number of variables that would affect the testing of Dependency Walker.

Hardware

Model:	Compaq Deskpro
Processor:	x86 Family 6 Model 5 Stepping 2, GenuineIntel
RAM:	512 MB
Hard drive:	6 GB IDE drive
Sound card:	None
Network Cards:	3Com Etherlink XL 10/100 PCI (3C905C-TX) Compaq NC3121 Fast Ethernet
CD-ROM:	Compaq CRD-8322B
Disk Drives:	Fujitsu MPC3064AT
Display Adapter:	ATI Technologies Inc. 3D Rage Pro AGP 2X
Monitor:	CTX Color monitor using default plug and play driver

Software

Windows 2000 Server
Windows 2000 Service Pack 3
No other patches or hotfixes were installed.
All Windows components were removed, including Accessories and Utilities, Indexing Service, Internet Information Server, and Script Debugger.

Windows Services

The following services were shut down and disabled in an effort to reduce the number of applications that may inadvertently influence the system and affect the test:

- Alerter
- Automatic Updates
- Background Intelligent Transfer Service
- Computer Browser
- Distributed File System
- IPSec Policy Agent
- License Logging Service
- Messenger
- Network Connections
- Print Spooler
- Remote Registry Service
- RunAs Service
- Server
- Task Scheduler
- TCP/IP NetBIOS Helper Service
- Telephony
- Workstation

This left the following services remaining in a running state:

- DHCP Client
- Distributed Link Tracking Client
- Distributed Link Transaction Coordinator
- DNS Client
- Event Log
- Logical Disk Manager
- Plug and Play
- Protected Storage
- Remote Procedure Call
- Removable Storage
- Security Accounts Manager
- Server

- System Event Notification
- Windows Management Instrumentation

Page File

The paging file was set to a static size of 800 MB.

Environmental Conditions

The test system was located in a laboratory environment that was open only to authorized individuals. To reduce the possibility of contamination, the test system was locked with a password known only to the tester when not in use.

Testing was completed in a non-networked lab environment. The test system was not connected to a network of any kind in order to isolate the test system as much as possible.

Description of Procedures

The procedures can be summarized as follows and are explained in more detail below.

1. Prepare the Software Tools CD.
2. Prepare the Test System.
3. Baseline the Test System.
4. Examine the Specimen Passively in DW.
5. Check for System Modifications by DW.
6. New Baseline Taken
7. Examine the Specimen in DW Runtime Mode.
8. Check for System Modifications by DW.
9. Examine specimen with another Dependency Checking tool.
10. Sanitize Test System.

Step 1-Prepare Software Tools CD

Since the specimen may adversely affect system files on the test system, it was necessary to copy all essential tools that will be needed for the testing to a CD.

Several tools were copied to the CD.

Windows System Tools
cmd.exe

Dependency Walker
Depends.exe
Depends.dll
Depends.cnt

Depends.hlp

MD5sum (from SANS Track 8 Course CD v1.7)
Md5sum.exe
Md5lib.dll
Getopt.dll
Msvcr70.dll

Other Tools
Winalysis 3.0 install file
WinZip 8.0 install file
Binary_v1.3.zip – This file contains the specimen to be examined using Dependency Walker.
PE Explorer 1.93 eval version.

Step 2-Prepare the Test System

The test system was prepared as follows.

1. Windows 2000 Server was installed from the Microsoft Software Developer Network (MSDN) CD to a single partition formatted in NTFS.
2. Windows 2000 Service Pack 3 was installed from the MSDN CD.
3. The Windows components described in the Test Apparatus section were removed.
4. The Windows services described in the Test Apparatus section were shut down and disabled.
5. The page file was set to 800 MB, lower and upper range.
6. Winzip 8.1 was installed from the Tools CD using default settings with the Classic interface (www.winzip.com).
7. Winalysis 3.0 trial version was installed from the Tools CD using default settings (www.winalysis.com). Winalysis is used to take a "snapshot" of a system state so that any changes can be observed in the file system and registry.
8. Cipher.exe (local version on hard disk) was executed from the command prompt with the "wipe" switch (/w) in order to wipe the remaining slack space from root of the partition.

```
> cipher.exe /w c:\
```

9. A folder structure was created to contain the specimen and a copy of Dependency Walker for examination.

```
> mkdir c:\lab
> mkdir c:\lab\specimen
```
– the specimen will be placed here. Changes in this folder will be noted.

```
> mkdir c:\lab\dw
```

`> mkdir c:\lab\evidence` – logs and other evidence will be stored here. Changes discovered in this folder during the test will be ignored.

10. The specimen was copied to c:\lab\specimen from the Tools CD and unzipped. This revealed a file called target2.exe. An MD5 checksum was computed on target2.exe.

```
> md5sum.exe c:\lab\specimen\target2.exe
 \848903a92843895f3ba7fb77f02f9bf1
*c:\\lab\\specimen\\target2.exe
```

11. A copy of Dependency Walker and its core files were copied to c:\lab\dw from the Tools CD. The purpose of copying Dependency Walker to the hard disk was to examine it using PE Explorer and Dependency Walker.
12. The system was then rebooted.

Step 3-Baseline the Test System

In order to determine how Dependency Walker modifies the test system, a baseline of its virgin state was required.

1. DIR commands provided a complete list of all directories and files in the filesystem according to time created, the time last accessed and the time last modified. This information was saved in the form of text files in the c:\lab\devidence folder.

```
> dir /t:c /a /s /o:d c:\ > c:\lab\evidence\01-dir-created.txt
> dir /t:a /a /s /o:d c:\ > c:\lab\evidence\01-dir-lastaccess.txt
> dir /t:w /a /s /o:d c:\ > c:\lab\evidence\01-dir-lastwrite.txt
```

2. Winalysis
   A snapshot of the test system was taken. This snapshot provided the baseline for determining which parts of the file system, registry, or other parts of the system would be modified by Dependency Walker, if any.

   The snapshot was taken with the following options:
   - Files
   - Registry
   - Services
   - Shares
   - Volumes
   - System
   - Scheduler
   - Rights
   - Users
   - Groups

The following filter options were used:

- C:\ drive
- Include subfolders
- Track security descriptors
- Track file version numbers
- Track digital signature numbers (SHA-1)

The entire registry was selected.

Winalysis labeled the snapshot as “03/06/20 17:21:22”

An “access denied” error was detected in the Shares section. This was probably due to the fact that the Server service was shutdown and no shares are possible.

The pagefile also produces an error in that Winalysis cannot access it as a file to determine changes.

3. DIR commands (Again)

Why run the DIR commands again? A diff will be done of the first set of DIRs and this one to see what files Winalysis added, accessed or modified, if any. This is necessary to maintain a controlled environment that shows only deltas created by Dependency Walker.

```
> dir /t:c /a /s /o:d c:\ > c:\lab\evidence\02-dir-created.txt
> dir /t:a /a /s /o:d c:\ > c:\lab\evidence\02-dir-lastaccess.txt
> dir /t:w /a /s /o:d c:\ > c:\lab\evidence\02-dir-lastwrite.txt
```

Step 4-Examine the specimen passively in DW

1. Dependency Walker GUI was started.

2. Target2.exe was loaded in DW.

   An error occurred. “Error: At least one required implicit or forwarded dependency was not found.” (MSVCP60.dll). This error is expected from the Analysis of an Unknown Binary (Part One). Because the goal is to test Dependency Walker and not the specimen itself, the specimen must not be allowed to change the environment. Therefore, the required DLL will not be added to the environment in order to allow the specimen to load for the Runtime Profile.

3. DW was shut down.

Step 5-Check for System Modifications by DW

1. Performed Winalysis comparison.
   The 03/06/20 17:21:22 snapshot was compared against the live system data. The results were saved in c:\lab\evidence.

2. Executed DIR commands
```
> dir /t:c /a /s /o:d c:\ > c:\lab\evidence\03-dir-created.txt
> dir /t:a /a /s /o:d c:\ > c:\lab\evidence\03-dir-lastaccess.txt
> dir /t:w /a /s /o:d c:\ > c:\lab\evidence\03-dir-lastwrite.txt
```

Step 6-New Baseline Snapshot Taken

This snapshot will capture all the changes from the passive test in order to provide a fresh baseline for comparing against the Dependency Walker Run Time Profiler.

New snapshot name: 03/06/20 17:55:11

Step 7-Examine Specimen in DW Runtime Mode

1. Dependency Walker GUI was started.

2. The specimen, **Target2.exe**, was loaded.

   Received expected error regarding the missing DLL.

3. Chose Profile > Start Profiling
   Default options
   - Simulate ShellExecute by inserting app path directories into the path environment variables
   - Log DllMain calls for process attach and process detach messages
   - Hook the process to gather more detailed dependency information
   - Log LoadLibrary function calls
   - Log GetProcAddress function calls
   - Log debug output messages
   - Automatically open and profile child processes

   Received expected error during attempt to load and execute: unable to locate dll MSVCP60.dll

4. Saved DW log to c:\lab\evidence.

5. DW was shut down.

Step 8-Check for System Modifications by DW

1. A Winalysis comparison was performed.
   Compared 03/06/20 17:55:11 image against live data. Results were stored in c:\lab\evidence.

2. Executed DIR commands
```
> dir /t:c /a /s /o:d c:\ > c:\lab\evidence\04-dir-created.txt
> dir /t:a /a /s /o:d c:\ > c:\lab\evidence\04-dir-lastaccess.txt
> dir /t:w /a /s /o:d c:\ > c:\lab\evidence\04-dir-lastwrite.txt
```

Step 9- Accuracy Checks

In order to test the accuracy of Dependency Walker in determining the dependencies of the specimen, it was compared against PE explorer version 1.93, by HeavenTools (http://www.pe-explorer.com). The evaluation version of PE Explorer used was the full version with no limitations, with a 30-day expiration.

1. To get the specimen to function normally in this test, a copy of the local **mfc42.dll** was made, renamed to **mfc42loc.dll** and placed in the c:\winnt\system32 folder.

2. A copy of **msvcp60.dll** was copied from another Windows 2000 server via floppy disk to the c:\winnt\system32 folder.

3. PE Explorer was installed on the test system from a CD. Default install options were selected.

4. After installation, the specimen was loaded in PE Explorer and results were recorded in c:\lab\evidence.

5. MSVCP60.DLL, an implicit dependency was renamed to MSVCP60.DLL.old.

6. DW was run and the specimen was loaded. Results were recorded and DW was shut down.

7. PE Explorer was run and the specimen was loaded. Dependency Scanner was initiated. Results were recorded and PE Explorer was shut down.

Step 10-Sanitize Test System

Before the evidence folder and specimen folders were moved off the test system, they were zipped and an MD5sum taken of the zipped files to ensure the data was unmodified during transit on a floppy disk.

An MD5sum was taken of the specimen to determine if the executable had been modified during testing.

```
> md5sum.exe c:\lab\specimen\target2.exe
 \848903a92843895f3ba7fb77f02f9bf1 *c:\\lab\\specimen\\target2.exe
```

It had not.

After the zipped file containing the evidence and specimen folders was copied to a floppy disk, the system was wiped to prevent any possibility of releasing the specimen outside the lab.

Criteria for approval

It is expected that Dependency Walker will modify time stamps of the system files it has dependencies on. Time stamps of the specimen may also be modified. However, since Dependency Walker can be run against a copy of the specimen, there is no concern of overwriting the original timestamps.

More importantly is the type of information that can be collected from Dependency Walker about the specimen. When examining a binary of unknown origin, the investigator requires a tool that can preferably be run from CD and that is self-contained as possible in order to reduce the possibility of calling system modules that may be contaminated by malicious code being inspected in Dependency Walkers Runtime Profiling mode. This will be discussed in detail in the section, “Data and results”.

Data and results

After the baseline of the virgin system was established, a comparison of the DIR results was required to determine what, if any, changes that Winalysis had on the system before running Dependency Walker.

Windiff version 5 (build 2195), a tool available in the Windows 2000 Support Tools, is a tool used to compare the content differences in files or folders. Windiff was used to compare the results of the DIRs on an independent system outside the test environment.

Compare Baseline vs. Post Snapshot

The first data comparison of DIRs between the baseline of the virgin system and after the first snapshot was necessary to eliminate Winalysis as a potential contaminant of the test data. This compare established a more accurate baseline.

<u>Identifier</u> <u>File Name</u>

Baseline: 01-dir-xxxxx.txt
Deltas: 02-dir-xxxxx.txt

CREATED FILES
The following differences in the 01-dir-created.txt and 02-dir-created.txt file were noted. These differences represent the file and folder timestamp changes between the baseline and the post-Winalysis snapshot.

New files in the following folders were expected and ignored:

- c:\lab\evidence
- c:\program files\winalysis folder and its subdirectories

No unexpected files were created after the snapshot.

LAST ACCESSED FILES
Some forensics investigators warn that the “last accessed” time stamp of Windows files is easily modified and not to be trusted.

This certainly held true in this test. Countless files, from fonts to .ini files to help files, showed modified “last accessed” time stamps in the Windiff compare.

It was clear that “last accessed” data would be of little use for further testing.

LAST WRITE FILES
The following files were written to after the snapshot had been taken.

Modified files in the following folders were expected and ignored:

- c:\lab\evidence
- c:\program files\winalysis folder and its subdirectories

```
Directory of c:\Documents and Settings\Administrator
Baseline:         06/20/2003  05:18p           192,512 NTUSER.DAT
Delta:            06/20/2003  05:20p           196,608 NTUSER.DAT
Baseline:         06/20/2003  05:18p             1,024 ntuser.dat.LOG
Delta:            06/20/2003  05:20p             1,024 ntuser.dat.LOG

Directory of c:\Documents and Settings\Administrator\Cookies
Baseline:         06/19/2003  06:03p           16,384 index.dat
Delta:            06/20/2003  05:19p           16,384 index.dat

Directory of c:\Documents and Settings\Administrator\Local
Settings\History\History.IE5
Baseline:         06/19/2003  06:03p           32,768 index.dat
Delta:            06/20/2003  05:19p           32,768 index.dat

Directory of c:\Documents and Settings\Administrator\Local
Settings\Temporary Internet Files\Content.IE5
Baseline:         06/19/2003  06:03p           32,768 index.dat
Delta:            06/20/2003  05:19p           32,768 index.dat
Directory of c:\WINNT
```

```
Baseline:          06/20/2003  05:16p      <DIR>         system32
Delta:             06/20/2003  05:21p      <DIR>         system32

Directory of c:\WINNT\system32\config
Baseline:          06/20/2003  05:17p            6,291,456 software
Delta:             06/20/2003  05:41p            6,299,648 software
Baseline:          06/20/2003  05:17p            1,024 software.LOG
Delta:             06/20/2003  05:41p            1,024 software.LOG

Directory of c:\WINNT\system32\wbem\Logs
Baseline:          06/20/2003  05:14p            21,845 wbemcore.log
Delta:             06/20/2003  05:28p            21,901 wbemcore.log
```

Armed with an understanding of the files created or modified by Winalysis, a more accurate baseline had been established. The files of this compare would be ignored in further comparisons in order to remove Winalysis as a data contaminant.

TEST DATA - Dependency Walker Passive

The next compare was between the newly established baseline that accounted for Winalysis and the results of the DIR after the first run of Dependency Walker in passive mode.

Identifier	File
Baseline	02-dir-xxxxx.txt
Delta	03-dir-xxxxx.txt

CREATED FILES
The results of the created files compare showed nothing unusual or that was not expected. No new files had been created by Dependency Walker.

Files created in the following folders were expected and ignored:

- c:\lab\evidence
- c:\program files\winalysis folder and its subdirectories

```
Directory of c:\Documents and Settings\Administrator\Recent
06/20/2003  05:53p                 509 01-Winalysis-Diff.txt.lnk
06/20/2003  05:53p                 374 evidence.lnk
```

LAST ACCESSED FILES
Results were not investigated due to volume of data.

LAST WRITTEN FILES
No files or folders were written to that were not expected from the first compare.

WINALYSIS SNAPSHOT
The Winalysis snapshot showed the following changes after the Dependency Walker passive mode run.

Files

The snapshot showed results similar to the DIR compares for files created or written to. Winalysis does not show files that have only their “Last Accessed” time stamp modified.

Registry

Two parts of the registry showed modification.

HKLM

The Hive Key Local Machine showed the following results.

```
             Changes on \\IP-TEST
                      (All Changes -- No Severity Filters)

Changes from Snapshot Summary for Registry
Snapshot:Tested:   06/20/03 17:55:11

Name

HKLM\
HKU\

Changes from Snapshot Details for Registry -- HKLM\
Snapshot:
Tested:

Name

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Reliability
          Key Last Modified Date
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Reliability\LastAliveSta
mp
          Value Changed
HKLM\SOFTWARE\Microsoft\Cryptography\RNG
          Key Last Modified Date
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed
          Value Changed
HKLM\SOFTWARE\Classes
          Number of Subkeys
HKLM\SOFTWARE\Classes\.dwi
          New Key
HKLM\SOFTWARE\Classes\.dwp
          New Key
HKLM\SOFTWARE\Classes\dwifile
          New Key
HKLM\SOFTWARE\Classes\dwpfile
          New Key
```

HKU

The Hive Key User showed several modifications pertaining to Dependency Walker. For brevity, expected results in Winalysis and Explorer subkeys were left out. This indicates that Dependency Walker modified the registry in passive mode. The entire output can be found in Appendix 2-B.

```
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Dependency Walker
          New Key
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Dependency Walker\Settings
          New Key
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Dependency Walker\Settings\ScreenWidth
          New Value
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Dependency Walker\Settings\ScreenHeight
          New Value
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Dependency Walker\Settings\WindowLeft
          New Value
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Dependency Walker\Settings\WindowTop
          New Value
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Dependency Walker\Settings\WindowRight
          New Value
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Dependency Walker\Settings\WindowBottom
          New Value
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Dependency Walker\Recent File List
          New Key
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Dependency Walker\Recent File List\File1
          New Value
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Dependency Walker\External Viewer
          New Key
```

It was clear that the GUI version of Dependency Walker maintained information about open windows in the registry. It also maintained a “recent files list”. The changes show to be measurable and predictable since they fall under the …\Microsoft\Dependency Walker subkey.

TEST DATA - Dependency Walker in Profile Mode

After running Dependency Walker in Profile mode against the specimen, the following results were recorded.

CREATED FILES
No new files or folders were created.

LAST ACCESSED FILES
Results were not investigated due to volume of data.

LAST WRITTEN FILES
No unexpected files or folders were written to.

WINALYSIS SNAPSHOT

Files
No unexpected files showed modification.

The following registry keys showed modification.

HKLM

```
                              Changes on \\IP-TEST
                      (All Changes -- No Severity Filters)

Changes from Snapshot Summary for Registry
Snapshot:Tested:   06/20/03 18:04:05

Name

HKLM\
HKU\

Changes from Snapshot Details for Registry -- HKLM\
Snapshot:
Tested:

Name

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Reliability
          Key Last Modified Date å
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Reliability\LastAliveSta
mp
          Value Changed
HKLM\SOFTWARE\Microsoft\Cryptography\RNG
          Key Last Modified Date
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed
          Value Changed
```

HKU

The HKU hive showed new values in registry keys for Dependency Walker, indicating that Dependency Walker modified the registry in Profiling mode. The full output is in Appendix 2-C.

```
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings
          Number of Values            20                    6
          Key Last Modified Date      6/20/2003 6:00:34 PM 6/20/2003 5:45:38 PM
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileLogClear
          New Value                   0
```

```
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileSimulateShellExecute
          New Value                   1
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileLogDllMainProcessMsgs
          New Value                   1
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileLogDllMainOtherMsgs
          New Value                   0
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileHookProcess
          New Value                   1
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileLogLoadLibraryCalls
          New Value                   1
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileLogGetProcAddressCalls
          New Value                   1
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileLogThreads
          New Value                   0
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileUseThreadIndexes
          New Value                   1
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileLogExceptions
          New Value                   0
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileLogDebugOutput
          New Value                   1
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileUseFullPaths
          New Value                   0
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileLogTimeStamps
          New Value                   0
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileChildren
          New Value                   1
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Recent File List
          Key Last Modified Date      6/20/2003 6:03:10 PM 6/20/2003 5:45:38 PM
```

DEPENDENCY WALKER LOG

The Dependency Walker log contained the following data of interest about the specimen and the system it was tested on. The full dependencies portion of the output can be found in Appendix 2-D.

```
*****************************| System Information
|*****************************

Dependency Walker:       2.1.3623 (32-bit)
Operating System:        Microsoft Windows 2000 Server (32-bit)
OS Version:              5.00.2195 Service Pack 3
Processor:               x86 Family 6 Model 5 Stepping 2, GenuineIntel, ~398MHz
Number of Processors:    1
Computer Name:           IP-TEST
User Name:               Administrator
Local Date:              Friday, June 20, 2003
Local Time:              6:02:18 PM Pacific Daylight Time (GMT-07:00)
OS Language:             0x0409: English (United States)
```

```
Memory Load:             17%
Physical Memory Total:   536,399,872 (512 MB)
Physical Memory Used:    93,863,936
Physical Memory Free:    442,535,936
Page File Memory Total:  1,342,713,856
Page File Memory Used:   63,909,888
Page File Memory Free:   1,278,803,968
Virtual Memory Total:    2,147,352,576
Virtual Memory Used:     36,618,240
Virtual Memory Free:     2,110,734,336
Page Size:               0x00001000 (4,096)
Allocation Granularity:  0x00010000 (65,536)
Min. App. Address:       0x00010000 (65,536)
Max. App. Address:       0x7FFEFFFF (2,147,418,111)

********************************| Search Order
|********************************
*
*
* Legend: F  File                     E  Error (path not valid)
*
*
*
*******************************************************************************
*

The system's "KnownDLLs" list
   [F ] c:\winnt\system32\ADVAPI32.DLL
   [F ] c:\winnt\system32\COMCTL32.DLL
   [F ] c:\winnt\system32\COMDLG32.DLL
   [F ] c:\winnt\system32\GDI32.DLL
   [F ] c:\winnt\system32\IMAGEHLP.DLL
   [F ] c:\winnt\system32\KERNEL32.DLL
   [F ] c:\winnt\system32\LZ32.DLL
   [F ] c:\winnt\system32\MPR.DLL
   [F ] c:\winnt\system32\MSVCRT.DLL
   [F ] c:\winnt\system32\NTDLL.DLL
   [F ] c:\winnt\system32\OLE32.DLL
   [F ] c:\winnt\system32\OLEAUT32.DLL
   [F ] c:\winnt\system32\OLECLI32.DLL
   [F ] c:\winnt\system32\OLECNV32.DLL
   [F ] c:\winnt\system32\OLESVR32.DLL
   [F ] c:\winnt\system32\OLETHK32.DLL
   [F ] c:\winnt\system32\RPCRT4.DLL
   [F ] c:\winnt\system32\SHELL32.DLL
   [F ] c:\winnt\system32\SHLWAPI.DLL
   [F ] c:\winnt\system32\URL.DLL
   [F ] c:\winnt\system32\URLMON.DLL
   [F ] c:\winnt\system32\USER32.DLL
   [F ] c:\winnt\system32\VERSION.DLL
   [F ] c:\winnt\system32\WININET.DLL
   [F ] c:\winnt\system32\WLDAP32.DLL
   [F ] c:\winnt\system32\WOW32.DLL
The application directory
   [  ] C:\lab\specimen\
The 32-bit system directory
   [  ] C:\WINNT\System32\
The 16-bit system directory (Windows NT/2000/XP only)
   [  ] C:\WINNT\system\
The system's root OS directory
   [  ] C:\WINNT\
The application's registered "App Paths" directories
The system's "PATH" environment variable directories
```

```
   [  ] C:\WINNT\system32\
   [  ] C:\WINNT\
   [  ] C:\WINNT\System32\Wbem\

(dependencies removed-see Appendix 2-D for full report)


************************************| Log
|************************************

Error: At least one required implicit or forwarded dependency was not found.

--------------------------------------------------------------------------------
-
Starting profile on 6/20/2003 at 6:00:34 PM

Operating System: Microsoft Windows 2000 Server (32-bit), version 5.00.2195
Service Pack 3
Program Executable: c:\lab\specimen\TARGET2.EXE
Program Arguments:
Starting Directory: C:\lab\specimen\
Search Path: C:\WINNT\system32;C:\WINNT;C:\WINNT\System32\Wbem

Options Selected:
     Simulate ShellExecute by inserting any App Paths directories into the PATH
environment variable.
     Log DllMain calls for process attach and process detach messages.
     Hook the process to gather more detailed dependency information.
     Log LoadLibrary function calls.
     Log GetProcAddress function calls.
     Log debug output messages.
     Automatically open and profile child processes.
--------------------------------------------------------------------------------
-

Started "TARGET2.EXE" (process 0x6C) at address 0x00400000.  Cannot hook
module.
Loaded "NTDLL.DLL" at address 0x77F80000.  Cannot hook module.
Loaded "KERNEL32.DLL" at address 0x77E80000.  Cannot hook module.
Loaded "ADVAPI32.DLL" at address 0x77DB0000.  Cannot hook module.
Loaded "RPCRT4.DLL" at address 0x77D30000.  Cannot hook module.
Loaded "WS2_32.DLL" at address 0x75030000.  Cannot hook module.
Loaded "MSVCRT.DLL" at address 0x78000000.  Cannot hook module.
Loaded "WS2HELP.DLL" at address 0x75020000.  Cannot hook module.
Loaded "MFC42.DLL" at address 0x6C370000.  Cannot hook module.
Loaded "GDI32.DLL" at address 0x77F40000.  Cannot hook module.
Loaded "USER32.DLL" at address 0x77E10000.  Cannot hook module.
Second chance exception 0xC0000135 (DLL Not Found) occurred in "NTDLL.DLL" at
address 0x77FB120C.
Exited "TARGET2.EXE" (process 0x6C) with code 128 (0x80).
```

TEST DATA – Accuracy

PE EXPLORER LOG

PE Explorer does not provide the detailed reporting of Dependency Walker. However, the following information was captured about the specimen.

```
// File name: C:\lab\specimen\target2.exe
// Created  : 06:08:2003 19:27
// Type     : Dependencies


activeds.dll      c:\winnt\system32\activeds.dll
adsldpc.dll       c:\winnt\system32\adsldpc.dll
advapi32.dll      c:\winnt\system32\advapi32.dll
comctl32.dll      c:\winnt\system32\comctl32.dll
comdlg32.dll      c:\winnt\system32\comdlg32.dll
crypt32.dll       c:\winnt\system32\crypt32.dll
dnsapi.dll        c:\winnt\system32\dnsapi.dll
gdi32.dll         c:\winnt\system32\gdi32.dll
kernel32.dll      c:\winnt\system32\kernel32.dll
lz32.dll          c:\winnt\system32\lz32.dll
mfc42.dll         c:\winnt\system32\mfc42.dll
mpr.dll           c:\winnt\system32\mpr.dll
msasn1.dll        c:\winnt\system32\msasn1.dll
msvcp60.dll       c:\winnt\system32\msvcp60.dll
msvcrt.dll        c:\winnt\system32\msvcrt.dll
netapi32.dll      c:\winnt\system32\netapi32.dll
netrap.dll        c:\winnt\system32\netrap.dll
ntdll.dll         c:\winnt\system32\ntdll.dll
ntdsapi.dll       c:\winnt\system32\ntdsapi.dll
odbc32.dll        c:\winnt\system32\odbc32.dll
ole32.dll         c:\winnt\system32\ole32.dll
oleaut32.dll      c:\winnt\system32\oleaut32.dll
oledlg.dll        c:\winnt\system32\oledlg.dll
olepro32.dll      c:\winnt\system32\olepro32.dll
rpcrt4.dll        c:\winnt\system32\rpcrt4.dll
samlib.dll        c:\winnt\system32\samlib.dll
secur32.dll       c:\winnt\system32\secur32.dll
shell32.dll       c:\winnt\system32\shell32.dll
shlwapi.dll       c:\winnt\system32\shlwapi.dll
urlmon.dll        c:\winnt\system32\urlmon.dll
user32.dll        c:\winnt\system32\user32.dll
version.dll       c:\winnt\system32\version.dll
w32topl.dll       c:\winnt\system32\w32topl.dll
wininet.dll       c:\winnt\system32\wininet.dll
winspool.drv      c:\winnt\system32\winspool.drv
wldap32.dll       c:\winnt\system32\wldap32.dll
ws2_32.dll        c:\winnt\system32\ws2_32.dll
ws2help.dll       c:\winnt\system32\ws2help.dll
wsock32.dll       c:\winnt\system32\wsock32.dll
```

MSVCP60.DLL RENAME

DW detected the missing implicit dependency. The dependency tree view showed a question mark (?) next to msvcp60.dll, indicating a missing module. The log contained the text: “Error: At least one required implicit or forwarded dependency was not found.”

PE Explorer did not detect the missing module until the Dependency Scanner was activated.

MFC42LOC.DLL RENAME

On reboot, Windows indicated that a service failed to start. The service was Local Printer Manager, the service created by the specimen on install.

Analysis

DW Information

Dependency Walker gathered a lot of interesting information about the specimen.

Several file dependencies. Dependency Walker was able to show that the specimen would not load correctly without MSVCP60.DLL even without executing the specimen.

- File Time Stamps.
  Dependency Walker showed the File Time Stamp, or when the file was last saved (02-20-2003 12:45) as well as the Link Time Stamp, when the file was built (11-28-2002 0:53). This evidence could be used to correlate data gathered from a suspect's computer.

- File size and attributes.
  The specimen was 26793 bytes and had the archive bit set (A). The significance of the archive bit is that the file is scheduled to be backed up during a normal (i.e., full) or incremental backup. Since we are confident the specimen was not modified, this means the file has never been backed up using normal or incremental methods. This also indicates the file was not hidden, read-only, encrypted or compressed.

- Real Checksum.
  A checksum is a simple way of detecting errors or differences in a file. The real checksum is calculated by DW. When compared against the checksum calculated by the linker when the file was built, these checksums should be the same. This could be useful if the suspect's computer is investigated. The specimen's real checksum as calculated by DW was 0x0000DC8A.

- Subsystem.
  Subsystems define how the operating system will execute the file. Dependency Walker showed the specimen was meant to run in a console subsystem, meaning Win32 character mode. So the specimen was designed to be interacted with from a command line. Other possible subsystems include GUI (Windows mode), native (generally for device drivers) or POSIX (for POSIX apps).

- The Preferred and Actual base.

The investigator can use this information to determine whether the author set a preferred base load address for the specimen and the actual base address the module was loaded into (using runtime profiler). The specimen loaded in 0x00400000. Knowing where the specimen loads in memory can be used to help find traces of it on other victim hosts.

- The load order.
  Dependency Walker showed the order the specimen called its dependent modules. The following was the load order of the specimen.

Load Order	Module
1	TARGET2.EXE
*	MSVCP60.DLL
2	NTDLL.DLL
3	KERNEL32.DLL
4	ADVAPI32.DLL
5	RPCRT4.DLL
6	WS2_32.DLL
7	MSVCRT.DLL
8	WS2HELP.DLL
9	MFC42.DLL
10	GDI32.DLL
11	USER32.DLL

* There was an error during load because the file did not exist. From previous tests in Part One, it is known this module would have loaded here.

- Versions.
  Although Dependency Walker can show the file and product version information, it cannot always be trusted since these parameters are set by the author. However, the linker, OS and subsystem versions may provide some data to correlate with a suspect's computer. The specimen had a

  - linker version of 6,
  - OS version 4, and a
  - subsystem version of 4.

However, Dependency Walker also modified the registry of the system it ran on. Particularly, new keys, containing several new values, were created for Dependency Walker settings in HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency Walker.

DW Accuracy

An essential requirement from Dependency Walker is that it can be relied on by an investigator to provide reliable information about an unknown binary.

First, it should be noted that the makers of Dependency Walker state in their help files that DW may not catch every dynamically-loaded dependency. This is because not every dynamic dependency may be called by DW during the profiling process.

This comparison would help to determine if any were missed by DW.

Accuracy was tested in two ways.

PE EXPLORER COMPARE

PE Explorer was used to examine the specimen and provide data to test the accuracy of Dependency Walker. PE Explorer uses passive checks similar to Dependency Walker to look for dependencies. PE Explorer includes a dependency scanner that checks delay-load dependencies as well. PE Explorer does not check for dynamically loaded dependencies in the version used in this test.

PE Explorer noted the following dependant modules, known as imports in PE Explorer.

Kernal32.dll
Advapi32.dll
Ws2_32.dll
Mfc42.dll
Msvcrt.dll
Msvcp60.dll

This list corresponds one-for-one with the list of DLLs discovered by Dependency Walker in passive mode.

PE Explorer's help file indicated that its "scanner" mode was not as accurate as DW since it would not check for dynamically loaded dependencies so no comparison was attempted.

PE Explorer also verified the following data as the same in DW.

Machine:	i386
Time Stamp Date:	28/11/2002 7:53:13am
Linker Version:	6.0
Operating System version:	4.0
Subsystem version:	4.0
Subsystem:	Win32 console

PE Explorer showed the file size to be different however.

Dependency Walker	
Size:	26793 bytes
PE Explorer	
Size:	24576 bytes

In Part One, Analysis of an Unknown Binary, it was determined by multiple Linux and Windows tools that the file size was 26793 bytes. This leads one to believe that Dependency Walker's size estimate is probably the more accurate.

DLL REPLACEMENT

DW accurately noted the missing MSVCP60.DLL after it was renamed with a '.old" extension.

However, DW called the renamed MFC42.DLL by its new name: MFC42LOC.DLL. DW did not make any attempt to indicate that this was the incorrect DLL. However, DW did correctly report the properties of the renamed DLL. The properties showed to be the same in every respect except for the load order, which was expected.

	MFC42.DLL	**MFC42LOC.DLL (renamed from MFC42.DLL)**
File Time Stamp	12/07/1999 1:00pm	12/07/1999 1:00pm
Link Time Stamp	11/30/1999 2:33am	11/30/1999 2:33am
File Size	995,383	995,383
Link Checksum	0x000FE3F3	0x000FE3F3
Real Checksum	0x000FE3F3	0x000FE3F3
Load Order	**9**	**13**
File Version	6.0.8665.0	6.0.8665.0
Product Version	6.0.4.0	6.0.4.0

For brevity, not all properties are shown.

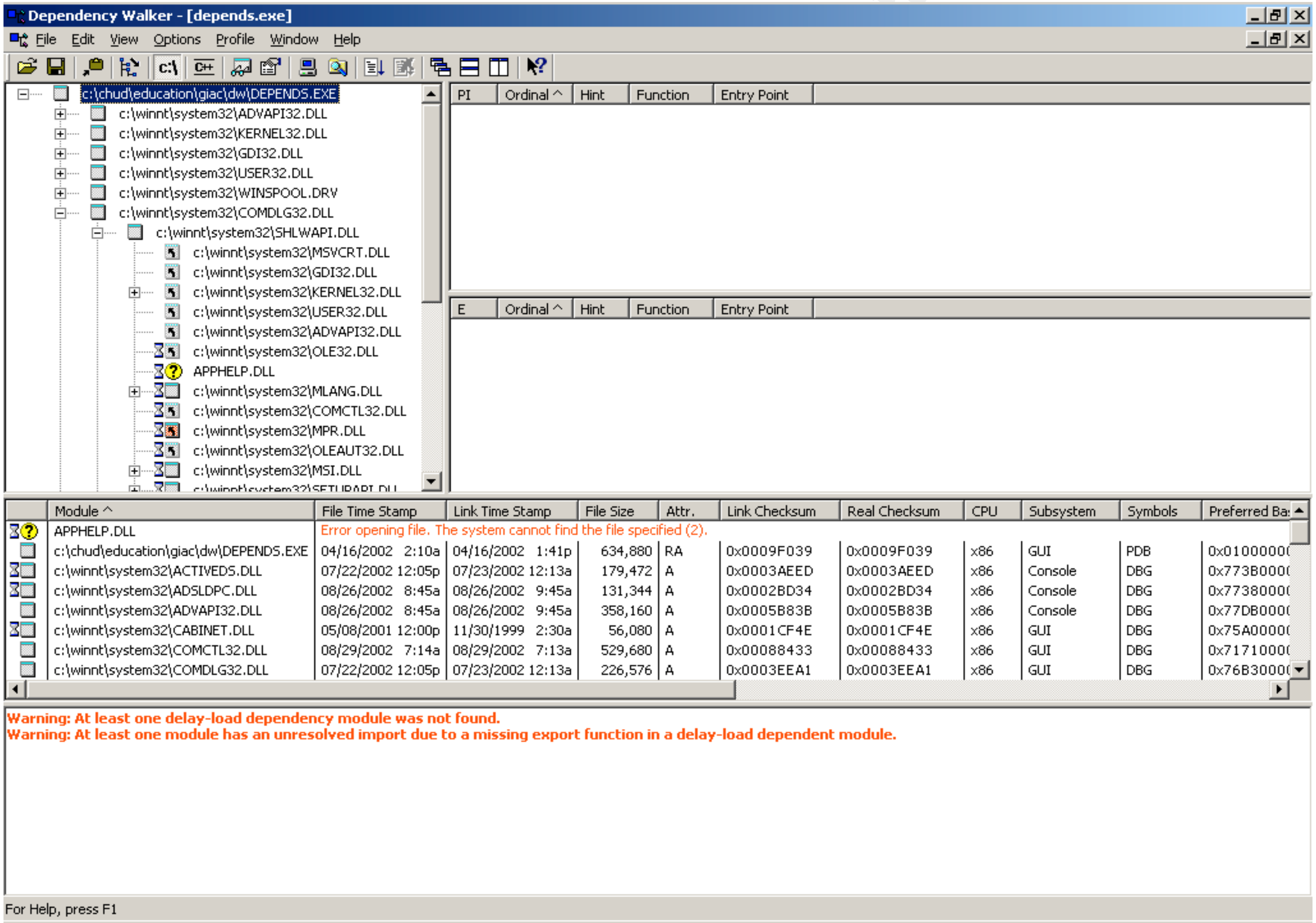
Presentation

Dependency Walker can be used as a GUI and in command line. The output of both can be saved into the text format used throughout this report. Dependency Walker can also save output into comma-delimited format for use in spreadsheets.

However, for presentation in court, the text output can be confusing to a jury that has no technical background. Even with appropriate use of MD5 hashes of the output, the text files could be argued to have been modified by the investigator before the hash was taken.

Screenshots of the GUI may provide better evidence in a courtroom setting because the output is easier to read. However, the screenshots may not capture all of the relevant data because dependency lists can be extremely long. Fortunately, Dependency Walker shows the dependencies in trees that can be expanded or closed as needed.

A screenshot of Dependency Walker in passive mode is shown below in figure 2-a. The dependencies of the depends.exe (Dependency Walker's executable) can be seen and warnings and errors noted.


Dependency Walker - [depends.exe]
File Edit View Options Profile Window Help
PI Ordinal ^ Hint Function Entry Point
E Ordinal ^ Hint Function Entry Point
For Help, press F1

```
⊟ c:\chud\education\giac\dw\DEPENDS.EXE
    ⊞ c:\winnt\system32\ADVAPI32.DLL
    ⊞ c:\winnt\system32\KERNEL32.DLL
    ⊞ c:\winnt\system32\GDI32.DLL
    ⊞ c:\winnt\system32\USER32.DLL
    ⊞ c:\winnt\system32\WINSPOOL.DRV
    ⊟ c:\winnt\system32\COMDLG32.DLL
        ⊟ c:\winnt\system32\SHLWAPI.DLL
              c:\winnt\system32\MSVCRT.DLL
              c:\winnt\system32\GDI32.DLL
            ⊞ c:\winnt\system32\KERNEL32.DLL
              c:\winnt\system32\USER32.DLL
              c:\winnt\system32\ADVAPI32.DLL
              c:\winnt\system32\OLE32.DLL
              APPHELP.DLL
            ⊞ c:\winnt\system32\MLANG.DLL
              c:\winnt\system32\COMCTL32.DLL
              c:\winnt\system32\MPR.DLL
              c:\winnt\system32\OLEAUT32.DLL
            ⊞ c:\winnt\system32\MSI.DLL
            ⊞ c:\winnt\system32\SETUPAPI.DLL
```

Module ^	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Ba:
APPHELP.DLL	Error opening file. The system cannot find the file specified (2).									
c:\chud\education\giac\dw\DEPENDS.EXE	04/16/2002 2:10a	04/16/2002 1:41p	634,880	RA	0x0009F039	0x0009F039	x86	GUI	PDB	0x0100000
c:\winnt\system32\ACTIVEDS.DLL	07/22/2002 12:05p	07/23/2002 12:13a	179,472	A	0x0003AEED	0x0003AEED	x86	Console	DBG	0x773B000
c:\winnt\system32\ADSLDPC.DLL	08/26/2002 8:45a	08/26/2002 9:45a	131,344	A	0x0002BD34	0x0002BD34	x86	Console	DBG	0x7738000
c:\winnt\system32\ADVAPI32.DLL	08/26/2002 8:45a	08/26/2002 9:45a	358,160	A	0x0005B83B	0x0005B83B	x86	Console	DBG	0x77DB000
c:\winnt\system32\CABINET.DLL	05/08/2001 12:00p	11/30/1999 2:30a	56,080	A	0x0001CF4E	0x0001CF4E	x86	GUI	DBG	0x75A0000
c:\winnt\system32\COMCTL32.DLL	08/29/2002 7:14a	08/29/2002 7:13a	529,680	A	0x00088433	0x00088433	x86	GUI	DBG	0x7171000
c:\winnt\system32\COMDLG32.DLL	07/22/2002 12:05p	07/23/2002 12:13a	226,576	A	0x0003EEA1	0x0003EEA1	x86	GUI	DBG	0x76B3000

Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.

Figure 2-a Dependency Walker Screen Capture

Note that this screenshot not taken from the test system and is shown only for display purposes.

The screen is divided into five sections.

The top left window, the Module Dependency Tree View, shows all the dependencies and sub-dependencies of the target file. It also shows whether a dependency is a delay load module, a duplicate module (called already by another dependency) and related information.

Of the two top right windows, the Parent Import Function List View shows imported functions of the selected module (none are currently selected in Figure 2-a above so the window is empty). These are the functions that the file is calling upon.

The Export Function List View beneath the Parent Import window shows those functions that may be called upon by other modules. In other words, these functions are what the file is making available to other programs to call upon.

In the middle, the Module List View shows all modules necessary to load and execute the file. This window also shows which dependencies could not be found on the system, were invalid, or had errors.

Finally, at the very bottom, the Log View window shows warnings, errors, and other log data when a file is examined in Profile mode. This information can be useful to troubleshoot why an unknown binary will not execute.

Conclusion

Dependency Walker proves itself to be invaluable to the forensics investigator for the study of unknown Windows binaries. The tool makes minor and predictable changes to the system it is run on, most particularly in the registry, even if it is run from CD.

Ideally, Dependency Walker would not modify the system in any way, including the registry, although this would impart some loss of functionality in the way of user convenience. However, it was shown that DW does indeed make some modifications to the registry.

Most importantly, Dependency Walker provides important information about the makeup and system dependencies of an unknown binary. Implicit dependencies are displayed with great accuracy. Explicit dependencies displayed are accurate with the caveat that DW will not say with certainty that all explicit dependencies have been reported.

Although the modifications made by Dependency Walker are documented here, the cautious investigator would do well to study any unknown binary in an isolated lab environment rather than on a system under investigation. Because of the detailed information it can provide about an unknown binary Dependency Walker should be a part of every Windows forensics toolkit.

PART THREE - Legal Issues of Incident Handling

Background

This paper discusses the legal issues involved with a scenario presented in the GIAC Certified Forensic Analyst certification version 1.3.

Version 1.3 of the GCFA assignment provided a scenario in which a system administrator of an Internet Service Provider (ISP) that provides access to paying customers is contacted by a law enforcement officer to inform the ISP that an account of the ISP was used to hack into a government computer. The officer has requested that the ISP review their logs to determine whether the attack initiated with the ISP or from somewhere else. A review of the logs by the ISP sysadmin shows that a valid user account logged in to the ISP via a dial-up connection during the time the suspicious activity took place. (paraphrased from http://www.giac.org/GCFA_assignment_print.php)

Furthermore, the scenario requires that the assumption be made that the law enforcement officer is really who he says he is and this is not an attempt at social engineering.

Finally, the scenario will assume the ISP is located in the state of California, United States of America.

What Information Can Be Provided at Initial Contact

Without a court order or warrant, any information divulged by the ISP to law enforcement entities must be considered voluntary.

The Electronic Communications Privacy Act (ECPA), 18 USC §§ 2701-2712, was written, in part, to plug some of the holes in the 4th Amendment by defining how law enforcement entities can obtain stored data from electronic communications service providers. According to the SSCOEECI, "any attempt to obtain the consent of the [ISP] [to divulge evidence]…must comply with the ECPA". This is because the ISP, according to the ECPA, represents an entity that provides an electronic communications service. (18 USC § 2701(c)(1), http://www4.law.cornell.edu/uscode/18/2701.html). Appendix 3-A shows how under what category the data in this scenario will be treated with respect to the ECPA.

USC § 2702, Voluntary Disclosure provides rules under which an electronic communication provider may provide evidence voluntarily to law enforcement (http://www4.law.cornell.edu/uscode/18/2702.html).

In this scenario, the law enforcement entity is not after communication data, such as the contents of an e-mail, but rather log data that about the session that took place. Under the ECPA, transactional records, such as log files, are not allowed to be disclosed voluntarily to any government entity unless one of the following exceptions can be met:

1. A court order or warrant is obtained by the government entity as per section 2703 (18 USC § 2702(c)(1)). Argument: Since the law enforcement entity does not yet have a warrant, this option clearly does not apply.

2. The ISP has obtained the "lawful consent of the customer or subscriber". (18 USC § 2702(c)(2)). Argument: Because it is not clear yet whether the account owner is, in fact, the perpetrator of the security incident, the law enforcement entity may not yet wish to let the account owner know that the incident was detected. Therefore, it is unlikely that the ISP will be asked to obtain the permission of the customer to divulge the information.

3. Voluntary disclosure "may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider" (18 USC § 2702(c)(3)). Argument: Although it may be difficult to argue that the ISP's ability to render services is adversely affected, it is more plausible that the ISP's rights, in the form of its usage policy, has been abused and therefore subject to section 2702(c)(3). However, without more information, it would be risky to use this as the basis of the argument.

4. The provider believes that voluntary disclosure is justified because the provider "reasonably believes that an emergency involving immediate danger or death or serious physical injury to any person" exists. 18 USC § 2702(c)(4)). Argument: There is also no evidence (yet) for the ISP to reasonably believe that an individual is in danger or may be physically harmed by the events that have occurred.

Therefore, no information should be provided to the law enforcement entity at this time and it is in the interest of the law enforcement entity to seek and obtain a warrant or court order before attempting to request the log file data from the ISP. It may also be in the interest of the ISP to request the warrant from law enforcement in order to protect itself from lawsuits and loss of reputation by sharing customer account information unlawfully.

Note that section 2702 does allow for the ISP to voluntarily share this information with non-government entities. For example, had the upstream service provider in the scenario contacted the ISP to ask whether the log files showed anomalous usage, it may have been acceptable for the ISP to share this information under 2702. (18 USC § 2702(c)(5)).

Also note that the situation would have been dramatically different had the account been created for, and used by, an employee of the ISP for purposes of conducting ISP business. In such a case, the ISP becomes a non-public provider of services. If the ISP had a sound policy regarding Internet and systems usage, it could have been argued that the account owner had given up his or her 4th Amendment rights when the ISP's usage policy was violated by the misuse of the account to attack a government system. For example, logon banners can be used to inform an employee accessing the ISP system that they must waive certain rights in order to use the system. The SSCOEECI states that "individuals who retain a reasonable expectation of privacy in stored electronic information under their control may lose Fourth Amendment protections when they relinquish that control to third parties." (Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (SSCOEECI), http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm).
In this case, the ISP would have been justified in sharing the information voluntarily with the law enforcement entity if the ISP had contacted law enforcement first.

Law Enforcement Obligations to Require ISP to Preserve Evidence

Having concluded that the evidence the law enforcement entity requires cannot be obtained without a warrant or court order, what can be done to ensure the evidence remains intact when they return with one?

Depending on the ISP's backup and data retention policies, the log file data may be overwritten or destroyed after a given period of time. If a warrant or court order is required by law enforcement, USC § 2703, Required disclosure of customer communications or records, provides the rules law enforcement and the ISP must follow in order to preserve evidence until a legal search can be conducted.

At the request of the law enforcement agency or other government entity, "[the ISP]…shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process." (USC § 2703(f)(1), http://www4.law.cornell.edu/uscode/18/2703.html). This evidence must be maintained by the ISP for up to 90 days, after which the government entity must request another 90 extension to the ISP to continue to preserve the evidence. (USC § 2703(f)(2)).

Interestingly, the law does not require a particular format for the request. Although law enforcement can make the initial request to the ISP to preserve the logs verbally, it's a good idea for the law enforcement agent to follow such a request immediately with a written one in the form of a fax or e-mail to preserve a log of communications between the law enforcement entity and the ISP. (SSCOEECI, approx. pg. 49)

Legal Authority Required for Law Enforcement to Obtain Logs

The law enforcement entity requires the ISP to send them all logs which may contain suspicious activity regarding the security incident. Such logs will certainly contain log entries of unrelated innocent activity as well as that of the criminal activity. What authority does the law enforcement entity have to ask for such data?

The real question that will be asked by the court in a legal case regarding search and seizure of electronic evidence is whether the search "violate[ed] a reasonable expectation of privacy" according to the 4th Amendment? (SSCOEECI)

The requirement for the law enforcement entity to obtain the log data is a warrant or court order (USC § 2703(d)). The warrant can and should be crafted such that, if possible, a minimal amount of innocent data is extracted along with the required suspicious activity. "When agents have a factual basis for believing that they can locate the evidence using a specific set of techniques, the affidavit should explain the techniques that the agents plan to use to distinguish incriminating [data] from commingled [data]." (SSCOEECI, approx. pg. 35).
But are innocent ISP customers' 4th Amendment rights being abused by section 2703? The question of may be dependant upon the published privacy policy of the ISP and the relationship of the account owner to the ISP. A privacy policy should clearly state that the ISP may be required to share information with government agencies to comply with legal obligations

For example, the court found in United States v. Miller, 425 U.S. 435, 443 (1976), that "By placing information under the control of a third party…[the customer] assumes the risk that the information will be conveyed to the government." Or again, as noted in Smith v. Maryland, 442 U.S. 735, 743-44 (1979) which found "no reasonable expectation of privacy in phone numbers dialed by owner of a telephone because act of dialing the number effectively tells the number to the phone company." (Both quoted examples from SSCOEECI, approx. pg. 8)

Therefore, it can be argued that ISP customers relinquish access time stamps and identification data to the ISP via log files maintained by the ISP whenever they access the ISP's systems. Since the log files are the property of the ISP, employees or customers of the ISP cannot reasonably expect that these access-related data are private. Following the ECPA, law enforcement can exercise 18 USC § 2703(d) to compel the ISP to provide commingled log evidence while maintaining compliance with the 4th Amendment.

Other Investigative Activity That Can Be Performed by ISP

In order to protect its rights and property, the ISP may wish to conduct its own internal investigation. There are two things the ISP may do immediately.

1. Detect a crime in progress. The perpetrator (whether human or malicious software) may still be performing attacks against the government systems or other systems, including the ISP's own internal systems. The ISP may wish to determine what kinds of attacks are being launched and from what system(s). Any log capability of the ISP's systems that was not enabled already will now be enabled in order to collect as much information as possible. Additionally, one or more network sniffers may be deployed to capture network traffic.

2. Root Cause Analysis. The ISP will certainly want to determine in more details how the attacker gained access to its systems, what methods were used to attack the government system, and preserve any evidence left behind. The primary means of capturing this information will be through log files and other evidence, such as hacker tools, left on victim system within the ISP.

The ISP will certainly want to capture network traffic in order to learn which ISP systems are being used to attack the government computer, as well as to determine whether any other computers are being attacked. Capturing network traffic may also tell the ISP what tools are being used to perform the attack. Network traffic may also give the ISP more clues as to the identity of the suspect.

It is in the ISP's best interest to have a solid security policy that describes when logs will be enabled and monitoring will occur. This enables the ISP to show a court that it was following a normal and approved company procedure.

18 USC § 2511, part of the Wiretap Act, prohibits the interception and disclosure of electronic communications, including the contents of network traffic Specifically, 2511(a) makes it a crime for anyone who "intentionally intercepts, endeavors to intercept…any wire, oral, or electronic communication." (http://www4.law.cornell.edu/uscode/18/2511.html).

Worse in this case for the ISP, section 2511(e)(ii) adds that anyone who "knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation" is also subject to punishment. Since the ISP was contacted by a law enforcement entity, the ISP is now aware that the evidence they collect is in connection with a criminal investigation.

This sounds like bad news for the ISP. However, lawmakers provided some exceptions for service providers like the ISP for just this kind of scenario.

Section 2511(2)(a)(i) states that "it shall not be unlawful…for [an] agent of [the ISP], whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity…to the protection of the rights or property of the [ISP]". This section allows the ISP to act in self-defense to monitor electronic communications across its own systems if it suspects unauthorized use. It is important to note that the ISP must make every attempt collect only the evidence necessary to the investigation. Further, the evidence collected under this subsection can only apply to damage done directly to the ISP. This subsection cannot be used to gather evidence of an unrelated crime (Frameworks and Best Practices: Managerial and Legal Issues, pg. 30, SANS Track 8).

Section 2511(2)(a)(i) is important to the ISP because the ISP is interested in the contents of the network traffic, not just addressing information in the traffic headers. However, the ISP has broader rights if its intent is to gather only addressing information. Section 2511(2)(h)(ii) permits the ISP to use a pen register or trap and trace device to "record the fact that…electronic communication was initiated or completed in order to protect [the ISP or its customers] from fraudulent, unlawful, or abusive use of such service." While such information might not be useful to determine details about the attacker, the type of attack, or to replay the attack, it can be very useful in recording dates, times, sources and destinations of the attack.

If the ISP's systems were properly bannered, and the attacker accessed the systems in such a way that the logon banners could be proven to have been viewed, section 2511(2)(c)-(d) may also apply. The attacker may have implicitly given his or her consent to be monitored when they accessed the ISP's systems, thereby allowing the collection of electronic communications evidence by the ISP.

Since it was a government system that was attacked (a "protected computer" under 18 USC § 1030), section 2511(2)(i) allows for the interception of electronic communications of a computer trespasser if the following requirements are met:

a) The ISP, as the system owner, agrees to allow the interception,
b) The interception is done by a law enforcement entity,
c) The law enforcement entity has "reasonable grounds" for suspecting the communications are relevant to the investigation, and
d) The interception captures ONLY the attacker's communications. This last requirement may be met in this scenario if the network traffic can be filtered by the destination IP address of the victim government computer.

Of course, once the law enforcement entity obtains the necessary court order, section 2511(2)(a)(ii) permits the ISP to work with the law enforcement entity to collect all allowable evidence in the form of electronic communication under section 2703, Required disclosure of customer communications or records.

Other Possibilities

If the ISP's investigation showed that the attacker had gained unauthorized access to the ISP's systems and created a user account to attack the government system, then the ISP would have certain rights to collect evidence to defend its rights and property.

Section 2702(b)(5) and (c)(3) allow the ISP to voluntarily disclose communications "to the protection of the rights or property of the provider".

Section 2511(2)(a)(i) allows for the ISP to capture electronic communications in order to protect its "rights or property" as long as the evidence collection was not the result of random monitoring.

The bad news for this California ISP is that, beginning July 01, 2003, California State law SB 1386 requires any "person or business that conducts business in California, that owns or licenses computerized data that includes personal information…to disclose…any breach of the security of the data…to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" (http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html).

If the ISP has any reasonable belief that the attacker had access to any system holding customer data, possibly the system used to create the unauthorized user account, the ISP would be required to report this fact to the affected customers. Under SB 1386, personal information is defined a customer's first name or initial, tand their last name combined with one or more of the following:

- Social security number,
- Driver's license number, or
- Account or credit card numbers in combination with password or passcodes required to access the customer's financial account.

References

- 20cn, http://20cn.net
- American Registry for Internet Numbers, http://www.arin.net
- "Analysis of Unknown Binary" by Greg Owen SANS GCFA, http://www.giac.org/GCFA.php.
- Andrea VB programming and Downloads, http://www.andreavb.com
- Azusa University, http://www.apu.edu
- California State Senate website, http://www.sen.ca.gov
- Cnhonker website, http://www.cnhonker.net
- Defense Security Service, http://www.dss.mil/isec/chapter8.htm.
- Dependency Walker, http://www.dependencywalker.com
- Eluks, Peter-ICMP Shell, http://peter.eluks.com
- Foundstone, Inc., http://foundstone.com
- Frameworks and Best Practices: Managerial and Legal Issues, SANS Track 8, GCFA, version 1.3.
- Global Information Assurance Certification, http://www.giac.org
- Legal Information Institute, Cornell University, http://www4.law.cornell.edu
- U.S. Department of Justice, Computer Crime and Intellectual Property Division, http://www.cybercrime.gov
- McKing, http://www.mcking.8u8.com
- Microsoft Developers Network, http://msdn.mocrosoft.com
- Microsoft Corporation Support, http://support.microsoft.com
- Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (SSCOEECI), http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm
- Soft Project 2003, http://www.s0ftpj.org
- Sysinternals, http://www.sysinternals.com
- Winalysis Software, http://www.winalysis.com
- Winzip Software, http://www.winzip.com

Appendices

Appendix 1-A SANS Linux Workstation Script

SANS Linux Forensics Workstation script
Created by Rob Lee (rob_t_lee@yahoo.com)

```
#!/bin/bash
echo "MOUNTING CDROM IN CASE IT IS NOT MOUNTED"
/bin/mount /dev/cdrom /mnt/cdrom
echo "COPYING FORENSIC SKELETON FILES TO FORENSIC WORKSTATION"
/bin/cp /mnt/cdrom/forensic.tgz /
echo "UNARCHIVING SKELETON FILES"
/bin/sleep 10
cd /
/bin/tar -zxvf forensic.tgz
echo "Finished with SKELETON DIRECTORIES"
/bin/rm -f /forensic.tgz
/bin/sleep 10
/bin/sleep 10
echo "Reconfiguring your networking"
/sbin/ifconfig eth0 192.168.2.1 netmask 255.255.255.0
echo "Adding UNCOMMENTED (for now) entries into /etc/fstab"
/bin/cat /tmp/fstab_add >> /etc/fstab
echo "Adding Windows Forensic Server Mount Point into rc.local"
/bin/cat /tmp/SMBFS_MOUNT >> /etc/rc.d/rc.local
echo "Starting SAMBA SERVER"
/etc/rc.d/init.d/smb restart
```

Appendix 1-B Specimen Zip File Info

Specimen zip file ZIPINFO –V (Verbose mode)

```
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.
```

Appendix 1-C Specimen Strings Output

Specimen target2.exe STRINGS results

```
hl@@
SUVW
D$,QPR
|4,3
D$ j'P
T$,j'RP
L$,j
T$,VRS
D$ j'P
T$,j'RP
|$ h
L$0h
L$ j'Q
D$"j
D$,j'PQ
SUVW
D$0QPR
D$$j'P
T$0j'RP
L$0j
T$0URV
D$$j'P
T$0j'RP
_^][
T$$h
D$ j'PQ
D$(h
L$(Q
h(@@
T$$QRj
D$$PW
5 @@
5,@@
5 @@
5,@@
5 @@
5,@@
 h0A@
VPPP
5 @@
5,@@
IRQh
5H0@
SPhxD@
h|D@
```

```
SQhpD@
htD@
|$,h`D@
D$|j
D$@SPS
D$TD
=d0@
5P0@
-T0@
T$|h
T$|RP
USSSP3
- @@
-,@@
_^]3
SUVW
D$(PQ
5d0@
- @@
-,@@
;eui
x!xu\
x"iuV
x#tuP
IQh@A@
- @@
-,@@
_^]3
_^][
u Wj
hhA@
hPA@
5LD@
5PD@
5TD@
5XD@
t1h@D@
5TD@
5XD@
Ht Ht
h@D@
5LD@
5TD@
5XD@
5D@@
VWh?
hPA@
=@0@
hPA@
hPA@
u@h`B@
Ph<B@
h(B@
T$(QR
hPA@
L$0PQ
=$0@
hPA@
Ph0C@
5$0@
hPA@
hxC@
hXC@
h8C@
%|0@
%x0@
h '@
%p0@
%l0@
h(1@
 SVW
= D@
```

```
Sleep
HeapAlloc
GetProcessHeap
TerminateProcess
ReadFile
PeekNamedPipe
CloseHandle
CreateProcessA
CreatePipe
WriteFile
GetLastError
LocalAlloc
KERNEL32.dll
StartServiceCtrlDispatcherA
SetServiceStatus
RegisterServiceCtrlHandlerA
CloseServiceHandle
ControlService
QueryServiceStatus
OpenServiceA
CreateServiceA
OpenSCManagerA
DeleteService
StartServiceA
ChangeServiceConfigA
QueryServiceConfigA
ADVAPI32.dll
WSAIoctl
WSASocketA
WS2_32.dll
MFC42.DLL
memmove
exit
fprintf
_iob
sprintf
perror
strstr
time
printf
MSVCRT.dll
__dllonexit
_onexit
_exit
_XcptFilter
__p___initenv
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode
__set_app_type
_except_handler3
_controlfp
??0Init@ios_base@std@@QAE@XZ
??1Init@ios_base@std@@QAE@XZ
??0_Winit@std@@QAE@XZ
??1_Winit@std@@QAE@XZ
MSVCP60.dll
ERROR 3
ERROR 2
ERROR 1
impossibile creare raw ICMP socket
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
Error Installing Service
Service Installed Sucessfully
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
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 1-D Specimen Filestat Output

Filestat of Target2.exe

```
Creation Time - 08/04/2003  21:40:05
Last Mod Time - 20/02/2003  12:45:48
Last Access Time - 13/04/2003  20:46:05
Main File Size - 26793
File Attrib Mask - Arch
Dump complete...Dumping c:\forensics\lab\target2.exe...
SD is valid.
SD is 120 bytes long.
SD revision is 1 == SECURITY_DESCRIPTOR_REVISION1
SD's Owner is Not NULL
SD's Owner-Defaulted flag is FALSE
  SID = BUILTIN/Administrators   S-1-5-32-544
SD's Group-Defaulted flag is FALSE
  SID = FORENSICS2K/None   S-1-5-21-1801674531-1580818891-1343024091-513
SD's DACL is Present
SD's DACL-Defaulted flag is FALSE
    ACL has 2 ACE(s), 56 bytes used, 0 bytes free
    ACL revision is 2 == ACL_REVISION2
  SID = BUILTIN/Administrators   S-1-5-32-544
    ACE 0 is an ACCESS_DENIED_ACE_TYPE
    ACE 0 size = 24
    ACE 0 flags = 0x10
    ACE 0 mask = 0x00000020
  SID = BUILTIN/Administrators   S-1-5-32-544
    ACE 1 is an ACCESS_ALLOWED_ACE_TYPE
    ACE 1 size = 24
    ACE 1 flags = 0x10
    ACE 1 mask = 0x001f01df -R -W -D -DEL_CHILD -CHANGE_PERMS -TAKE_OWN
SD's SACL is Not Present
Stream 1:
  Type: Security
  Stream name = a Size: 120

Stream 2:
  Type: Data
  Stream name = a Size: 26793

Stream 3:
  Type: Unknown
  Stream name = a Size: 64
```

Appendix 2-A Dependency Walker Output

Full Dependency Walker report on depends.exe. Note that this output was not gathered from the test system in order to reduce possible contamination. It is for information only.

```
*****************************| System Information
|*****************************

Dependency Walker:        2.1.3623 (32-bit)
Operating System:         Microsoft Windows 2000 Professional (32-bit)
OS Version:               5.00.2195 Service Pack 3
Processor:                x86 Family 15 Model 2 Stepping 4,
GenuineIntel, ~1196MHz
Number of Processors:     1
Computer Name:            xxxxxx
User Name:                Vera
Local Date:               Sunday, July 13, 2003
Local Time:               5:19:51 PM Pacific Daylight Time (GMT-07:00)
OS Language:              0x0409: English (United States)
Memory Load:              40%
Physical Memory Total:    535,740,416 (511 MB)
Physical Memory Used:     219,308,032
Physical Memory Free:     316,432,384
Page File Memory Total:   1,236,750,336
Page File Memory Used:    190,713,856
Page File Memory Free:    1,046,036,480
Virtual Memory Total:     2,147,352,576
Virtual Memory Used:      41,271,296
Virtual Memory Free:      2,106,081,280
Page Size:                0x00001000 (4,096)
Allocation Granularity:   0x00010000 (65,536)
Min. App. Address:        0x00010000 (65,536)
Max. App. Address:        0x7FFEFFFF (2,147,418,111)

********************************| Search Order
|********************************
*
*
* Legend: F  File                     E  Error (path not valid)
*
*
*
***********************************************************************
*********

The system's "KnownDLLs" list
   [F ] c:\winnt\system32\ADVAPI32.DLL
   [F ] c:\winnt\system32\COMCTL32.DLL
   [F ] c:\winnt\system32\COMDLG32.DLL
   [F ] c:\winnt\system32\CRYPT32.DLL
   [F ] c:\winnt\system32\GDI32.DLL
   [F ] c:\winnt\system32\IMAGEHLP.DLL
   [F ] c:\winnt\system32\IMM32.DLL
   [F ] c:\winnt\system32\KERNEL32.DLL
   [F ] c:\winnt\system32\LZ32.DLL
   [F ] c:\winnt\system32\MPR.DLL
   [F ] c:\winnt\system32\MSASN1.DLL
   [F ] c:\winnt\system32\MSVCRT.DLL
   [F ] c:\winnt\system32\NTDLL.DLL
   [F ] c:\winnt\system32\OLE32.DLL
   [F ] c:\winnt\system32\OLEAUT32.DLL
   [F ] c:\winnt\system32\OLECLI32.DLL
   [F ] c:\winnt\system32\OLECNV32.DLL
   [F ] c:\winnt\system32\OLESVR32.DLL
   [F ] c:\winnt\system32\OLETHK32.DLL
   [F ] c:\winnt\system32\PGPCLIENTLIB.DLL
   [F ] c:\winnt\system32\PGPHK.DLL
   [F ] c:\winnt\system32\PGPSC.DLL
   [F ] c:\winnt\system32\PGPSDK.DLL
   [F ] c:\winnt\system32\PGPSDKNL.DLL
   [F ] c:\winnt\system32\PGPSDKUI.DLL
   [F ] c:\winnt\system32\RPCRT4.DLL
   [F ] c:\winnt\system32\SHELL32.DLL
   [F ] c:\winnt\system32\SHLWAPI.DLL
   [F ] c:\winnt\system32\URL.DLL
   [F ] c:\winnt\system32\URLMON.DLL
   [F ] c:\winnt\system32\USER32.DLL
   [F ] c:\winnt\system32\VERSION.DLL
   [F ] c:\winnt\system32\WININET.DLL
   [F ] c:\winnt\system32\WINMM.DLL
   [F ] c:\winnt\system32\WLDAP32.DLL
   [F ] c:\winnt\system32\WOW32.DLL
   [F ] c:\winnt\system32\WS2_32.DLL
   [F ] c:\winnt\system32\WS2HELP.DLL
   [F ] c:\winnt\system32\WSOCK32.DLL
The application directory
   [  ] C:\chud\Education\GIAC\DW\
The 32-bit system directory
   [  ] C:\WINNT\System32\
The 16-bit system directory (Windows NT/2000/XP only)
   [  ] C:\WINNT\system\
The system's root OS directory
   [  ] C:\WINNT\
The application's registered "App Paths" directories
The system's "PATH" environment variable directories
   [  ] C:\WINNT\system32\
   [  ] C:\WINNT\
   [  ] C:\WINNT\System32\Wbem\
   [  ] C:\SYSMGT\TNGSD\BIN\
   [  ] C:\Program Files\Common Files\Adaptec Shared\System\
   [  ] C:\WINNT\system32\nls\
   [  ] C:\WINNT\system32\nls\ENGLISH\
   [  ] C:\Program Files\Resource Kit\
   [  ] C:\Program Files\Support Tools\
   [  ] C:\chud\Apps\Forensic Toolkits\w2k\

**************************| Module Dependency Tree
|**************************
*
*
* Legend: F  Forwarded Module   ?  Missing Module        6  64-bit
Module      *
*         D  Delay Load Module  !  Invalid Module
*
```

```
*         *  Dynamic Module     E  Import/Export Mismatch or Load
Failure      *
*                               ^  Duplicate Module
*
*
*
************************************************************************
*********

[   ] c:\chud\education\giac\dw\DEPENDS.EXE
     [   ] c:\winnt\system32\ADVAPI32.DLL
          [   ] c:\winnt\system32\NTDLL.DLL
          [ ^ ] c:\winnt\system32\KERNEL32.DLL
               [F^ ] c:\winnt\system32\NTDLL.DLL
          [   ] c:\winnt\system32\RPCRT4.DLL
               [ ^ ] c:\winnt\system32\NTDLL.DLL
               [ ^ ] c:\winnt\system32\KERNEL32.DLL
                    [F^ ] c:\winnt\system32\NTDLL.DLL
               [ ^ ] c:\winnt\system32\ADVAPI32.DLL
     [   ] c:\winnt\system32\KERNEL32.DLL
          [ ^ ] c:\winnt\system32\NTDLL.DLL
          [F^ ] c:\winnt\system32\NTDLL.DLL
     [   ] c:\winnt\system32\GDI32.DLL
          [ ^ ] c:\winnt\system32\NTDLL.DLL
          [ ^ ] c:\winnt\system32\KERNEL32.DLL
               [F^ ] c:\winnt\system32\NTDLL.DLL
          [ ^ ] c:\winnt\system32\USER32.DLL
     [   ] c:\winnt\system32\USER32.DLL
          [ ^ ] c:\winnt\system32\NTDLL.DLL
          [ ^ ] c:\winnt\system32\KERNEL32.DLL
               [F^ ] c:\winnt\system32\NTDLL.DLL
          [ ^ ] c:\winnt\system32\GDI32.DLL
     [   ] c:\winnt\system32\WINSPOOL.DRV
          [ ^ ] c:\winnt\system32\NTDLL.DLL
          [ ^ ] c:\winnt\system32\KERNEL32.DLL
               [F^ ] c:\winnt\system32\NTDLL.DLL
          [ ^ ] c:\winnt\system32\RPCRT4.DLL
          [ ^ ] c:\winnt\system32\ADVAPI32.DLL
          [ ^ ] c:\winnt\system32\GDI32.DLL
          [ ^ ] c:\winnt\system32\USER32.DLL
          [   ] c:\winnt\system32\MPR.DLL
               [ ^ ] c:\winnt\system32\NTDLL.DLL
               [ ^ ] c:\winnt\system32\KERNEL32.DLL
                    [F^ ] c:\winnt\system32\NTDLL.DLL
               [ ^ ] c:\winnt\system32\ADVAPI32.DLL
               [ ^ ] c:\winnt\system32\USER32.DLL
          [D  ] c:\winnt\system32\OLE32.DLL
               [ ^ ] c:\winnt\system32\RPCRT4.DLL
               [ ^ ] c:\winnt\system32\GDI32.DLL
               [ ^ ] c:\winnt\system32\KERNEL32.DLL
                    [F^ ] c:\winnt\system32\NTDLL.DLL
               [ ^ ] c:\winnt\system32\USER32.DLL
               [ ^ ] c:\winnt\system32\ADVAPI32.DLL
               [ ^ ] c:\winnt\system32\NTDLL.DLL
          [D  ] c:\winnt\system32\OLEAUT32.DLL
               [ ^ ] c:\winnt\system32\OLE32.DLL
               [ ^ ] c:\winnt\system32\USER32.DLL
               [ ^ ] c:\winnt\system32\GDI32.DLL
               [ ^ ] c:\winnt\system32\KERNEL32.DLL
                    [F^ ] c:\winnt\system32\NTDLL.DLL
               [ ^ ] c:\winnt\system32\ADVAPI32.DLL
          [D  ] c:\winnt\system32\ACTIVEDS.DLL
               [   ] c:\winnt\system32\ADSLDPC.DLL
                    [ ^ ] c:\winnt\system32\MSVCRT.DLL
                    [ ^ ] c:\winnt\system32\NTDLL.DLL
                    [ ^ ] c:\winnt\system32\NETAPI32.DLL
                    [   ] c:\winnt\system32\WLDAP32.DLL
                         [ ^ ] c:\winnt\system32\MSVCRT.DLL
                         [ ^ ] c:\winnt\system32\KERNEL32.DLL
                              [F^ ] c:\winnt\system32\NTDLL.DLL
                         [ ^ ] c:\winnt\system32\ADVAPI32.DLL
                         [D  ] c:\winnt\system32\CRYPT32.DLL
                              [ ^ ] c:\winnt\system32\MSVCRT.DLL
                              [   ] c:\winnt\system32\MSASN1.DLL
                                   [ ^ ] c:\winnt\system32\MSVCRT.DLL
                                   [ ^ ] c:\winnt\system32\KERNEL32.DLL
                                   [ ^ ] c:\winnt\system32\USER32.DLL
                              [ ^ ] c:\winnt\system32\RPCRT4.DLL
                              [ ^ ] c:\winnt\system32\ADVAPI32.DLL
                              [ ^ ] c:\winnt\system32\KERNEL32.DLL
                                   [F^ ] c:\winnt\system32\NTDLL.DLL
                              [ ^ ] c:\winnt\system32\USER32.DLL
                              [D  ] c:\winnt\system32\VERSION.DLL
                                   [ ^ ] c:\winnt\system32\KERNEL32.DLL
                                   [ ^ ] c:\winnt\system32\NTDLL.DLL
                                   [   ] c:\winnt\system32\LZ32.DLL
                                        [ ^ ]
c:\winnt\system32\NTDLL.DLL
                                        [ ^ ]
c:\winnt\system32\KERNEL32.DLL
                                        [ ^ ]
c:\winnt\system32\USER32.DLL
                                   [ ^ ] c:\winnt\system32\USER32.DLL
                    [ ^ ] c:\winnt\system32\ADVAPI32.DLL
                    [ ^ ] c:\winnt\system32\USER32.DLL
                    [ ^ ] c:\winnt\system32\KERNEL32.DLL
                         [F^ ] c:\winnt\system32\NTDLL.DLL
               [   ] c:\winnt\system32\MSVCRT.DLL
                    [ ^ ] c:\winnt\system32\KERNEL32.DLL
                         [F^ ] c:\winnt\system32\NTDLL.DLL
               [ ^ ] c:\winnt\system32\NTDLL.DLL
               [ ^ ] c:\winnt\system32\OLE32.DLL
               [ ^ ] c:\winnt\system32\ADVAPI32.DLL
               [ ^ ] c:\winnt\system32\KERNEL32.DLL
                    [F^ ] c:\winnt\system32\NTDLL.DLL
               [ ^ ] c:\winnt\system32\USER32.DLL
               [ ^ ] c:\winnt\system32\OLEAUT32.DLL
          [D  ] c:\winnt\system32\NETAPI32.DLL
               [ ^ ] c:\winnt\system32\MSVCRT.DLL
               [ ^ ] c:\winnt\system32\NTDLL.DLL
               [   ] c:\winnt\system32\SECUR32.DLL
                    [ ^ ] c:\winnt\system32\NTDLL.DLL
                    [ ^ ] c:\winnt\system32\KERNEL32.DLL
                    [ ^ ] c:\winnt\system32\ADVAPI32.DLL
               [ ^ ] c:\winnt\system32\ADVAPI32.DLL
               [   ] c:\winnt\system32\NETRAP.DLL
                    [ ^ ] c:\winnt\system32\MSVCRT.DLL
                    [ ^ ] c:\winnt\system32\NTDLL.DLL
                    [ ^ ] c:\winnt\system32\KERNEL32.DLL
               [ ^ ] c:\winnt\system32\RPCRT4.DLL
               [ ^ ] c:\winnt\system32\KERNEL32.DLL
                    [F^ ] c:\winnt\system32\NTDLL.DLL
               [   ] c:\winnt\system32\SAMLIB.DLL
                    [ ^ ] c:\winnt\system32\NTDLL.DLL
                    [ ^ ] c:\winnt\system32\ADVAPI32.DLL
                    [ ^ ] c:\winnt\system32\RPCRT4.DLL
                    [ ^ ] c:\winnt\system32\KERNEL32.DLL
                         [F^ ] c:\winnt\system32\NTDLL.DLL
               [   ] c:\winnt\system32\WS2_32.DLL
                    [ ^ ] c:\winnt\system32\MSVCRT.DLL
                    [ ^ ] c:\winnt\system32\KERNEL32.DLL
                         [F^ ] c:\winnt\system32\NTDLL.DLL
                    [ ^ ] c:\winnt\system32\ADVAPI32.DLL
                    [   ] c:\winnt\system32\WS2HELP.DLL
                         [ ^ ] c:\winnt\system32\NTDLL.DLL
                         [ ^ ] c:\winnt\system32\ADVAPI32.DLL
                         [ ^ ] c:\winnt\system32\KERNEL32.DLL
                              [F^ ] c:\winnt\system32\NTDLL.DLL
                         [D^ ] c:\winnt\system32\USER32.DLL
                    [D^ ] c:\winnt\system32\USER32.DLL
               [ ^ ] c:\winnt\system32\WLDAP32.DLL
               [ ^ ] c:\winnt\system32\DNSAPI.DLL
          [D  ] c:\winnt\system32\NTDSAPI.DLL
               [ ^ ] c:\winnt\system32\MSVCRT.DLL
               [ ^ ] c:\winnt\system32\NTDLL.DLL
               [ ^ ] c:\winnt\system32\DNSAPI.DLL
               [ ^ ] c:\winnt\system32\RPCRT4.DLL
               [ ^ ] c:\winnt\system32\WLDAP32.DLL
               [ ^ ] c:\winnt\system32\NETAPI32.DLL
               [ ^ ] c:\winnt\system32\KERNEL32.DLL
                    [F^ ] c:\winnt\system32\NTDLL.DLL
               [ ^ ] c:\winnt\system32\SECUR32.DLL
               [ ^ ] c:\winnt\system32\WS2_32.DLL
               [D  ] c:\winnt\system32\W32TOPL.DLL
                    [ ^ ] c:\winnt\system32\NTDLL.DLL
                    [ ^ ] c:\winnt\system32\KERNEL32.DLL
          [D  ] c:\winnt\system32\DNSAPI.DLL
               [ ^ ] c:\winnt\system32\MSVCRT.DLL
               [ ^ ] c:\winnt\system32\ADVAPI32.DLL
               [ ^ ] c:\winnt\system32\KERNEL32.DLL
                    [F^ ] c:\winnt\system32\NTDLL.DLL
               [   ] c:\winnt\system32\WSOCK32.DLL
                    [ ^ ] c:\winnt\system32\KERNEL32.DLL
                    [ ^ ] c:\winnt\system32\WS2_32.DLL
                    [F^ ] c:\winnt\system32\WS2_32.DLL
               [ ^ ] c:\winnt\system32\RPCRT4.DLL
     [   ] c:\winnt\system32\COMDLG32.DLL
          [   ] c:\winnt\system32\SHLWAPI.DLL
               [ ^ ] c:\winnt\system32\MSVCRT.DLL
               [ ^ ] c:\winnt\system32\GDI32.DLL
               [ ^ ] c:\winnt\system32\KERNEL32.DLL
                    [F^ ] c:\winnt\system32\NTDLL.DLL
               [ ^ ] c:\winnt\system32\USER32.DLL
               [ ^ ] c:\winnt\system32\ADVAPI32.DLL
               [D^ ] c:\winnt\system32\OLE32.DLL
               [D? ] APPHELP.DLL
               [D  ] c:\winnt\system32\MLANG.DLL
                    [ ^ ] c:\winnt\system32\ADVAPI32.DLL
                    [ ^ ] c:\winnt\system32\GDI32.DLL
                    [ ^ ] c:\winnt\system32\KERNEL32.DLL
                         [F^ ] c:\winnt\system32\NTDLL.DLL
                    [ ^ ] c:\winnt\system32\MSVCRT.DLL
                    [ ^ ] c:\winnt\system32\OLE32.DLL
                    [ ^ ] c:\winnt\system32\SHLWAPI.DLL
                    [ ^ ] c:\winnt\system32\USER32.DLL
                    [ ^ ] c:\winnt\system32\VERSION.DLL
               [D^ ] c:\winnt\system32\COMCTL32.DLL
               [DE ] c:\winnt\system32\MPR.DLL
               [D^ ] c:\winnt\system32\OLEAUT32.DLL
               [D  ] c:\winnt\system32\MSI.DLL
                    [ ^ ] c:\winnt\system32\NTDLL.DLL
                    [ ^ ] c:\winnt\system32\ADVAPI32.DLL
                    [ ^ ] c:\winnt\system32\KERNEL32.DLL
                         [F^ ] c:\winnt\system32\NTDLL.DLL
                    [ ^ ] c:\winnt\system32\USER32.DLL
                    [ ^ ] c:\winnt\system32\GDI32.DLL
                    [ ^ ] c:\winnt\system32\RPCRT4.DLL
               [D  ] c:\winnt\system32\SETUPAPI.DLL
                    [ ^ ] c:\winnt\system32\MSVCRT.DLL
                    [ ^ ] c:\winnt\system32\NTDLL.DLL
                    [ ^ ] c:\winnt\system32\ADVAPI32.DLL
                    [ ^ ] c:\winnt\system32\GDI32.DLL
                    [ ^ ] c:\winnt\system32\KERNEL32.DLL
                         [F^ ] c:\winnt\system32\NTDLL.DLL
                    [ ^ ] c:\winnt\system32\RPCRT4.DLL
                    [ ^ ] c:\winnt\system32\USER32.DLL
                    [ ^ ] c:\winnt\system32\USERENV.DLL
                    [D  ] c:\winnt\system32\CABINET.DLL
                         [ ^ ] c:\winnt\system32\KERNEL32.DLL
                              [F^ ] c:\winnt\system32\NTDLL.DLL
                         [ ^ ] c:\winnt\system32\OLE32.DLL
                    [D^ ] c:\winnt\system32\COMCTL32.DLL
                    [D^ ] c:\winnt\system32\COMDLG32.DLL
                    [D^ ] c:\winnt\system32\CRYPT32.DLL
                    [D^ ] c:\winnt\system32\LZ32.DLL
                    [D^ ] c:\winnt\system32\MPR.DLL
                    [D^ ] c:\winnt\system32\OLE32.DLL
                    [D  ] c:\winnt\system32\SFC.DLL
                         [ ^ ] c:\winnt\system32\MSVCRT.DLL
                         [ ^ ] c:\winnt\system32\NTDLL.DLL
                         [ ^ ] c:\winnt\system32\USER32.DLL
                         [ ^ ] c:\winnt\system32\KERNEL32.DLL
                              [F^ ] c:\winnt\system32\NTDLL.DLL
                         [ ^ ] c:\winnt\system32\RPCRT4.DLL
                         [ ^ ] c:\winnt\system32\ADVAPI32.DLL
                         [   ] c:\winnt\system32\SFCFILES.DLL
                              [ ^ ] c:\winnt\system32\NTDLL.DLL
                         [D^ ] c:\winnt\system32\SETUPAPI.DLL
```

```
                         [D^ ] c:\winnt\system32\VERSION.DLL
                         [D^ ] c:\winnt\system32\MPR.DLL
                    [D^ ] c:\winnt\system32\SHELL32.DLL
                    [D^ ] c:\winnt\system32\VERSION.DLL
                    [D^ ] c:\winnt\system32\WINSPOOL.DRV
                    [D  ] c:\winnt\system32\WINTRUST.DLL
                         [ ^ ] c:\winnt\system32\MSVCRT.DLL
                         [ ^ ] c:\winnt\system32\CRYPT32.DLL
                         [ ^ ] c:\winnt\system32\MSASN1.DLL
                         [ ^ ] c:\winnt\system32\USER32.DLL
                         [ ^ ] c:\winnt\system32\KERNEL32.DLL
                              [F^ ] c:\winnt\system32\NTDLL.DLL
                         [ ^ ] c:\winnt\system32\ADVAPI32.DLL
                         [   ] c:\winnt\system32\IMAGEHLP.DLL
                              [ ^ ] c:\winnt\system32\MSVCRT.DLL
                              [ ^ ] c:\winnt\system32\KERNEL32.DLL
                                   [F^ ] c:\winnt\system32\NTDLL.DLL
                              [D  ] c:\winnt\system32\DBGHELP.DLL
                                   [ ^ ] c:\winnt\system32\MSVCRT.DLL
                                   [ ^ ] c:\winnt\system32\KERNEL32.DLL
                                        [F^ ]
c:\winnt\system32\NTDLL.DLL
                         [ ^ ] c:\winnt\system32\OLE32.DLL
                         [D^ ] c:\winnt\system32\COMCTL32.DLL
               [D  ] c:\winnt\system32\USERENV.DLL
                    [ ^ ] c:\winnt\system32\MSVCRT.DLL
                    [ ^ ] c:\winnt\system32\NTDLL.DLL
                    [ ^ ] c:\winnt\system32\KERNEL32.DLL
                         [F^ ] c:\winnt\system32\NTDLL.DLL
                    [ ^ ] c:\winnt\system32\ADVAPI32.DLL
                    [ ^ ] c:\winnt\system32\USER32.DLL
               [D^ ] c:\winnt\system32\SHELL32.DLL
               [D  ] c:\winnt\system32\WINMM.DLL
                    [ ^ ] c:\winnt\system32\NTDLL.DLL
                    [ ^ ] c:\winnt\system32\USER32.DLL
                    [ ^ ] c:\winnt\system32\GDI32.DLL
                    [ ^ ] c:\winnt\system32\ADVAPI32.DLL
                    [ ^ ] c:\winnt\system32\KERNEL32.DLL
                         [F^ ] c:\winnt\system32\NTDLL.DLL
               [D^ ] c:\winnt\system32\VERSION.DLL
               [D^ ] c:\winnt\system32\COMDLG32.DLL
          [ ^ ] c:\winnt\system32\KERNEL32.DLL
               [F^ ] c:\winnt\system32\NTDLL.DLL
          [ ^ ] c:\winnt\system32\USER32.DLL
          [ ^ ] c:\winnt\system32\GDI32.DLL
          [ ^ ] c:\winnt\system32\ADVAPI32.DLL
          [ ^ ] c:\winnt\system32\COMCTL32.DLL
          [ ^ ] c:\winnt\system32\SHELL32.DLL
          [ ^ ] c:\winnt\system32\MSVCRT.DLL
          [ ^ ] c:\winnt\system32\NTDLL.DLL
          [D^ ] c:\winnt\system32\WINSPOOL.DRV
     [   ] c:\winnt\system32\COMCTL32.DLL
          [ ^ ] c:\winnt\system32\NTDLL.DLL
          [ ^ ] c:\winnt\system32\GDI32.DLL
          [ ^ ] c:\winnt\system32\KERNEL32.DLL
               [F^ ] c:\winnt\system32\NTDLL.DLL
          [ ^ ] c:\winnt\system32\USER32.DLL
          [ ^ ] c:\winnt\system32\ADVAPI32.DLL
     [   ] c:\winnt\system32\SHELL32.DLL
          [ ^ ] c:\winnt\system32\NTDLL.DLL
          [ ^ ] c:\winnt\system32\GDI32.DLL
          [ ^ ] c:\winnt\system32\USER32.DLL
          [ ^ ] c:\winnt\system32\KERNEL32.DLL
               [F^ ] c:\winnt\system32\NTDLL.DLL
          [ ^ ] c:\winnt\system32\ADVAPI32.DLL
          [ ^ ] c:\winnt\system32\SHLWAPI.DLL
          [ ^ ] c:\winnt\system32\COMCTL32.DLL
          [D^ ] c:\winnt\system32\RPCRT4.DLL

********************************| Module List
|********************************
*
*
* Legend: D  Delay Load Module   ?  Missing Module          6  64-bit
Module  *
*         *  Dynamic Module      !  Invalid Module
*
*                                E  Import/Export Mismatch or Load
Failure     *
*
*
**********************************************************************
*********

       Module                                 File Time Stamp    Link
Time Stamp    File Size  Attr.  Link Checksum  Real Checksum  CPU
Subsystem  Symbols  Preferred Base  Actual Base  Virtual Size  Load
Order  File Ver         Product Ver      Image Ver  Linker Ver  OS Ver
Subsystem Ver
-----  ------------------------------------  ----------------  ------
-----------  ---------  -----  -------------  -------------  ---  -----
----  -------  --------------  -----------  ------------  ----------  -
-------------  --------------  ---------  ----------  ------  -------
------
[D? ]  APPHELP.DLL                            Error opening file. The
system cannot find the file specified (2).
[   ]  c:\chud\education\giac\dw\DEPENDS.EXE  04/16/2002  2:10a
04/16/2002  1:41p    634,880  RA     0x0009F039     0x0009F039     x86
GUI        PDB      0x01000000      Unknown      0x000A2000    Not
Loaded  2.1.3623.0       2.1.3623.0       2.1        7.1         5.1
4.0
[D  ]  c:\winnt\system32\ACTIVEDS.DLL         07/22/2002 12:05p
07/23/2002 12:13a    179,472  A      0x0003AEED     0x0003AEED     x86
Console    DBG      0x773B0000      Unknown      0x0002E000    Not
Loaded  5.0.2195.5312    5.0.2195.5312    5.0        5.12        5.0
4.0
[D  ]  c:\winnt\system32\ADSLDPC.DLL          08/26/2002  8:45a
08/26/2002  9:45a    131,344  A      0x0002BD34     0x0002BD34     x86
Console    DBG      0x77380000      Unknown      0x00022000    Not
Loaded  5.0.2195.5781    5.0.2195.5781    5.0        5.12        5.0
4.0
[   ]  c:\winnt\system32\ADVAPI32.DLL         08/26/2002  8:45a
08/26/2002  9:45a    358,160  A      0x0005B83B     0x0005B83B     x86
Console    DBG      0x77DB0000      Unknown      0x0005B000    Not
```

```
Loaded  5.0.2195.5992    5.0.2195.5992    5.0        5.12        5.0
4.0
[D  ]  c:\winnt\system32\CABINET.DLL          05/08/2001 12:00p
11/30/1999  2:30a     56,080  A      0x0001CF4E     0x0001CF4E     x86
GUI        DBG      0x75A00000      Unknown      0x00013000    Not
Loaded  5.0.2147.1       5.0.2147.1       5.0        5.12        5.0
4.0
[   ]  c:\winnt\system32\COMCTL32.DLL         08/29/2002  7:14a
08/29/2002  7:13a    529,680  A      0x00088433     0x00088433     x86
GUI        DBG      0x71710000      Unknown      0x00084000    Not
Loaded  5.81.4916.400    5.50.4916.400    5.0        5.12        5.0
4.0
[   ]  c:\winnt\system32\COMDLG32.DLL         07/22/2002 12:05p
07/23/2002 12:13a    226,576  A      0x0003EEA1     0x0003EEA1     x86
GUI        DBG      0x76B30000      Unknown      0x0003D000    Not
Loaded  5.0.3315.3727    5.0.3315.3727    5.0        5.12        5.0
4.0
[D  ]  c:\winnt\system32\CRYPT32.DLL          09/25/2002 12:36p
09/25/2002  1:36p    469,776  A      0x00079F29     0x00079F29     x86
GUI        DBG      0x77440000      Unknown      0x00076000    Not
Loaded  5.131.2195.6072  5.131.2195.6072  5.0        5.12        5.0
4.0
[D  ]  c:\winnt\system32\DBGHELP.DLL          07/22/2002 12:05p
07/23/2002 12:13a    163,088  A      0x0002870F     0x0002870F     x86
Console    DBG      0x72A00000      Unknown      0x0002D000    Not
Loaded  5.0.2195.5242    5.0.2195.5242    5.0        5.12        5.0
4.0
[D  ]  c:\winnt\system32\DNSAPI.DLL           08/26/2002  8:45a
08/26/2002  9:45a    135,952  A      0x000220DC     0x000220DC     x86
Console    DBG      0x77980000      Unknown      0x00024000    Not
Loaded  5.0.2195.6012    5.0.2195.6012    5.0        5.12        5.0
4.0
[   ]  c:\winnt\system32\GDI32.DLL            08/26/2002  8:45a
08/26/2002  9:45a    222,992  A      0x0003F788     0x0003F788     x86
Console    DBG      0x77F40000      Unknown      0x00039000    Not
Loaded  5.0.2195.5907    5.0.2195.5907    5.0        5.12        5.0
4.10
[D  ]  c:\winnt\system32\IMAGEHLP.DLL         07/22/2002 12:05p
07/23/2002 12:13a    128,784  A      0x00029654     0x00029654     x86
Console    DBG      0x77920000      Unknown      0x00023000    Not
Loaded  5.0.2195.5242    5.0.2195.5242    5.0        5.12        5.0
4.0
[   ]  c:\winnt\system32\KERNEL32.DLL         11/01/2002  4:33p
11/01/2002  5:33p    708,880  A      0x000B7998     0x000B7998     x86
Console    DBG      0x77E80000      Unknown      0x000B1000    Not
Loaded  5.0.2195.6079    5.0.2195.6079    5.0        5.12        5.0
4.0
[D  ]  c:\winnt\system32\LZ32.DLL             05/08/2001 12:00p
11/30/1999  2:30a     10,000  A      0x0000A8D0     0x0000A8D0     x86
Console    DBG      0x759B0000      Unknown      0x00006000    Not
Loaded  5.0.2134.1       5.0.2134.1       5.0        5.12        5.0
4.10
[D  ]  c:\winnt\system32\MLANG.DLL            08/29/2002  7:14a
08/29/2002  7:13a    574,976  A      0x00095F06     0x00095F06     x86
GUI        PDB      0x70440000      Unknown      0x0008F000    Not
Loaded  6.0.2800.1106    6.0.2800.1106    5.1        7.0         5.1
4.0
```

```
[   ]  c:\winnt\system32\MPR.DLL              07/22/2002 12:05p
07/23/2002 12:14a     55,056  A      0x00012F0A     0x00012F0A     x86
Console    DBG      0x76620000      Unknown      0x00010000    Not
Loaded  5.0.2195.3649    5.0.2195.3649    5.0        5.12        5.0
4.0
[D  ]  c:\winnt\system32\MSASN1.DLL           07/22/2002 12:05p
07/23/2002 12:13a     52,496  A      0x0001011D     0x0001011D     x86
GUI        DBG      0x77430000      Unknown      0x00010000    Not
Loaded  5.0.2195.4067    5.0.2195.4067    5.0        5.12        5.0
4.0
[D  ]  c:\winnt\system32\MSI.DLL              01/26/2002  2:16a
01/26/2002  3:16a  1,994,240  A      0x001F66C3     0x001F66C3     x86
Console    PDB      0x770F0000      Unknown      0x001FD000    Not
Loaded  2.0.2600.2       2.0.2600.2       5.1        7.0         5.1
4.10
[   ]  c:\winnt\system32\MSVCRT.DLL           07/22/2002 12:05p
09/20/2001  2:52p    290,869  A      0x00048405     0x00048405     x86
GUI        PDB      0x78000000      Unknown      0x00046000    Not
Loaded  6.1.9359.0       6.1.9359.0       0.0        6.0         4.0
4.0
[D  ]  c:\winnt\system32\NETAPI32.DLL         08/26/2002  8:45a
08/26/2002  9:45a    307,472  A      0x00057334     0x00057334     x86
Console    DBG      0x75170000      Unknown      0x0004F000    Not
Loaded  5.0.2195.5979    5.0.2195.5979    5.0        5.12        5.0
4.0
[D  ]  c:\winnt\system32\NETRAP.DLL           05/08/2001 12:00p
11/30/1999  2:31a     11,536  A      0x0000D1DD     0x0000D1DD     x86
Console    DBG      0x751C0000      Unknown      0x00006000    Not
Loaded  5.0.2134.1       5.0.2134.1       5.0        5.12        5.0
4.10
[   ]  c:\winnt\system32\NTDLL.DLL            03/14/2003  8:23p
03/14/2003  9:23p    476,944  A      0x00083F58     0x00083F58     x86
Console    DBG      0x77F80000      Unknown      0x0007A000    Not
Loaded  5.0.2195.6685    5.0.2195.6685    5.0        5.12        5.0
4.0
[D  ]  c:\winnt\system32\NTDSAPI.DLL          07/22/2002 12:05p
07/23/2002 12:13a     57,616  A      0x000123C1     0x000123C1     x86
Console    DBG      0x77BF0000      Unknown      0x00011000    Not
Loaded  5.0.2195.4827    5.0.2195.4827    5.0        5.12        5.0
4.10
[D  ]  c:\winnt\system32\OLE32.DLL            10/25/2002  5:07p
10/25/2002  6:07p    943,376  A      0x000EE7DE     0x000EE7DE     x86
Console    DBG      0x77A50000      Unknown      0x000EC000    Not
Loaded  5.0.2195.6089    5.0.2195.6089    5.0        5.12        5.0
4.0
[D  ]  c:\winnt\system32\OLEAUT32.DLL         07/22/2002 12:05p
07/23/2002 12:13a    626,960         0x0009F6F0     0x0009F6F0     x86
GUI        DBG      0x779B0000      Unknown      0x0009B000    Not
Loaded  2.40.4518.0      2.40.4518.0      0.0        5.12        4.0
4.0
[   ]  c:\winnt\system32\RPCRT4.DLL           10/25/2002  5:07p
10/25/2002  6:07p    429,840  A      0x000748A1     0x000748A1     x86
Console    DBG      0x77D30000      Unknown      0x0006D000    Not
Loaded  5.0.2195.6106    5.0.2195.6106    5.0        5.12        5.0
4.10
[D  ]  c:\winnt\system32\SAMLIB.DLL           07/22/2002 12:05p
07/23/2002 12:14a     50,960  A      0x0001208B     0x0001208B     x86
```

```
Console    DBG      0x75150000     Unknown      0x00010000    Not
Loaded  5.0.2195.4827    5.0.2195.4827    5.0        5.12        5.0
4.0
[D  ]  c:\winnt\system32\SECUR32.DLL          07/22/2002 12:05p
07/23/2002 12:13a     48,400  A      0x00018014     0x00018014     x86
Console    DBG      0x77BE0000     Unknown      0x0000F000    Not
Loaded  5.0.2195.4587    5.0.2195.4587    5.0        5.12        5.0
4.0
[D  ]  c:\winnt\system32\SETUPAPI.DLL         07/22/2002 12:05p
07/23/2002 12:13a    567,056  A      0x00092385     0x00092385     x86
GUI        DBG      0x77880000     Unknown      0x0008D000    Not
Loaded  5.0.2195.5400    5.0.2195.5400    5.0        5.12        5.0
4.0
[D  ]  c:\winnt\system32\SFC.DLL              07/22/2002 12:05p
07/23/2002 12:13a     94,320  A      0x00018BEB     0x00018BEB     x86
Console    DBG      0x76980000     Unknown      0x0001B000    Not
Loaded  5.0.2195.3649    5.0.2195.3649    5.0        5.12        5.0
4.10
[D  ]  c:\winnt\system32\SFCFILES.DLL         07/22/2002 12:05p
07/23/2002 12:14a    974,096  A      0x000F7403     0x000F7403     x86
Console    DBG      0x68010000     Unknown      0x000F1000    Not
Loaded  5.0.2195.5426    5.0.2195.5426    5.0        5.12        5.0
4.10
[   ]  c:\winnt\system32\SHELL32.DLL          12/10/2002  5:37p
12/10/2002  6:37p  2,354,448  A      0x0024EBDD     0x0024EBDD     x86
GUI        DBG      0x782F0000     Unknown      0x00244000    Not
Loaded  5.0.3502.6144    5.0.3502.6144    5.0        5.12        5.0
4.0
[   ]  c:\winnt\system32\SHLWAPI.DLL          08/29/2002  7:14a
08/29/2002  7:13a    395,264  A      0x0006CCB4     0x0006CCB4     x86
GUI        PDB      0x70BD0000     Unknown      0x00065000    Not
Loaded  6.0.2800.1106    6.0.2800.1106    5.1        7.0         5.1
4.0
[   ]  c:\winnt\system32\USER32.DLL           11/01/2002  4:33p
11/01/2002  5:33p    379,664         0x0006648E     0x0006648E     x86
GUI        DBG      0x77E10000     Unknown      0x0005F000    Not
Loaded  5.0.2195.6097    5.0.2195.6097    5.0        5.12        5.0
4.0
[D  ]  c:\winnt\system32\USERENV.DLL          11/01/2002  4:33p
11/01/2002  5:33p    370,448         0x0005D654     0x0005D654     x86
GUI        DBG      0x77C10000     Unknown      0x0005D000    Not
Loaded  5.0.2195.6085    5.0.2195.6085    5.0        5.12        5.0
4.0
[D  ]  c:\winnt\system32\VERSION.DLL          05/08/2001 12:00p
12/01/1999 12:37a     16,144  A      0x0000C983     0x0000C983     x86
GUI        DBG      0x77820000     Unknown      0x00007000    Not
Loaded  5.0.2134.1       5.0.2134.1       5.0        5.12        5.0
4.0
[D  ]  c:\winnt\system32\W32TOPL.DLL          05/08/2001 12:00p
11/30/1999  2:31a     12,560  A      0x00006E3B     0x00006E3B     x86
Console    DBG      0x754A0000     Unknown      0x00007000    Not
Loaded  5.0.2160.1       5.0.2160.1       5.0        5.12        5.0
4.10
[D  ]  c:\winnt\system32\WINMM.DLL            05/08/2001 12:00p
12/01/1999 12:37a    189,200  A      0x0002E779     0x0002E779     x86
GUI        DBG      0x77570000     Unknown      0x00030000    Not
```

```
Loaded  5.0.2161.1       5.0.2161.1       5.0        5.12        5.0
4.0
[   ]  c:\winnt\system32\WINSPOOL.DRV         11/01/2002 11:55a
11/01/2002 12:55p    114,448  A      0x0002B86B     0x0002B86B     x86
GUI        DBG      0x77800000      Unknown      0x0001E000    Not
Loaded  5.0.2195.6032    5.0.2195.6032    5.0        5.12        5.0
4.0
[D  ]  c:\winnt\system32\WINTRUST.DLL         07/22/2002 12:05p
07/23/2002 12:13a    166,160  A      0x0002C30A     0x0002C30A     x86
GUI        DBG      0x76930000      Unknown      0x0002B000    Not
Loaded  5.131.2195.3775  5.131.2195.3775  5.0        5.12        5.0
4.0
[D  ]  c:\winnt\system32\WLDAP32.DLL          08/26/2002  8:45a
08/26/2002  9:45a    125,712  A      0x0001EE78     0x0001EE78     x86
GUI        DBG      0x77950000      Unknown      0x00028000    Not
Loaded  5.0.2195.5944    5.0.2195.5944    5.0        5.12        5.0
4.0
[D  ]  c:\winnt\system32\WS2_32.DLL           07/22/2002 12:05p
07/23/2002 12:14a     68,368  A      0x0001A8F4     0x0001A8F4     x86
Console    DBG      0x75030000      Unknown      0x00013000    Not
Loaded  5.0.2195.4874    5.0.2195.4874    5.0        5.12        5.0
4.10
[D  ]  c:\winnt\system32\WS2HELP.DLL          05/08/2001 12:00p
11/30/1999  2:31a     18,192  A      0x000087D1     0x000087D1     x86
Console    DBG      0x75020000      Unknown      0x00008000    Not
Loaded  5.0.2134.1       5.0.2134.1       5.0        5.12        5.0
4.0
[D  ]  c:\winnt\system32\WSOCK32.DLL          07/22/2002 12:05p
07/23/2002 12:14a     21,776  A      0x00012632     0x00012632     x86
Console    DBG      0x75050000      Unknown      0x00008000    Not
Loaded  5.0.2195.4874    5.0.2195.4874    5.0        5.12        5.0
4.10

************************************| Log
|************************************

Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing
export function in a delay-load dependent module.
```

Appendix 2-B Winalysis HKU results- Dependency Walker Passive Mode

```
                          Changes on \\IP-TEST
                    (All Changes -- No Severity Filters)

Changes from Snapshot Summary for Registry
Snapshot:Tested:   06/20/03 17:55:11

Name

HKLM\
HKU\

Changes from Snapshot Details for Registry -- HKU\
Snapshot:
Tested:
```

```
Name

HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft
          Number of Subkeys
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker
          New Key
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings
          New Key
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ScreenWidth
          New Value
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ScreenHeight
          New Value
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\WindowLeft
          New Value
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\WindowTop
          New Value
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\WindowRight
          New Value
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\WindowBottom
          New Value
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Recent File List
          New Key
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Recent File List\File1
          New Value
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\External Viewer
          New Key
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-
EF1F-11D0-9888-006097DEACF9}\Count

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-
EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-
EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:Q:\qrcraqf.rkr

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU\MRUList
```

```
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU\d

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\MRUList

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\e

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\f

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder\MRULis
t

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder\c

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\Version

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_GVI

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_GVI\LastU
pdate

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_GFA

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_GFA\LastU
pdate

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_GFA\Cache

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_GFA\Versi
on

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_DriveFlag
s

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_DriveFlag
s\LastUpdate
```

```
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_DriveFlag
s\Cache
          Deleted Value                                    00 04 00 00
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_DriveFlag
s\Version
          Deleted Value                                    1
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_DIL
          Key Last Modified Date      6/20/2003 5:53:48 PM 6/20/2003 5:17:31 PM
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_DIL\Versi
on
          Value Changed               1                    9
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_DIL\LastU
pdate
          Value Changed               2310822              133832
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_Autorun
          Key Last Modified Date      6/20/2003 5:53:48 PM 6/20/2003 5:14:21 PM
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_Autorun\V
ersion
          Value Changed               1                    5
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_Autorun\L
astUpdate
          Value Changed               2310822              84759868
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts
          Number of Subkeys           3                    1
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.tab
          New Key
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.txt
          New Key
```

Appendix 2-C Winalysis HKU results- Dependency Walker Profiler Mode

```
                              Changes on \\IP-TEST
                      (All Changes -- No Severity Filters)

Changes from Snapshot Summary for Registry
Snapshot:Tested:   06/20/03 18:04:05

Name

HKLM\
HKU\

Changes from Snapshot Details for Registry -- HKU\
Snapshot:
Tested:

Name
```

```
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-
EF1F-11D0-9888-006097DEACF9}\Count

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-
EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-
EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:Q:\qrcraqf.rkr

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\MRUList

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\g

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt\MRUList

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt\b

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\Version

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_GVI

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_GVI\LastU
pdate

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_DIL

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_DIL\LastU
pdate

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_Autorun

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints\C\_Autorun\L
astUpdate

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.csv
```

```
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.csv\OpenWithLi
st

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\csv

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\csv
\a

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\csv
\MRUList

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\txt


HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\txt
\MRUList

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\txt
\b

HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\*
          Number of Values            6                    4
          Key Last Modified Date      6/20/2003 6:03:03 PM 6/20/2003 5:54:05 PM
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\*\M
RUList
          Value Changed               edacb                cba
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\*\d
          New Value                   C:\lab\evidence\DW-ta get2.txt
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\*\e
          New Value                   C:\lab\evidence\DW-ta get2.csv
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
          Key Last Modified Date      6/20/2003 6:02:17 PM 6/20/2003 5:53:32 PM
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU\
a
          Value Changed               64 00 65 00 70 00 65 64 00 65 00 70 00 65
00 6e 00 64 00 73 00 2e 00 65 00 78 00 65 00 00 00 43 00 3a 00 5c 00 6c 00 ...
HKU\S-1-5-21-1482476501-789336058-1202660629-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU\
MRUList
          Value Changed               ab                   ba
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings
          Number of Values            20                   6
          Key Last Modified Date      6/20/2003 6:00:34 PM 6/20/2003 5:45:38 PM
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileLogClear
          New Value                   0
```

```
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileSimulateShellExecute
          New Value                   1
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileLogDllMainProcessMsgs
          New Value                   1
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileLogDllMainOtherMsgs
          New Value                   0
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileHookProcess
          New Value                   1
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileLogLoadLibraryCalls
          New Value                   1
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileLogGetProcAddressCalls
          New Value                   1
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileLogThreads
          New Value                   0
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileUseThreadIndexes
          New Value                   1
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileLogExceptions
          New Value                   0
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileLogDebugOutput
          New Value                   1
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileUseFullPaths
          New Value                   0
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileLogTimeStamps
          New Value                   0
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Settings\ProfileChildren
          New Value                   1
HKU\S-1-5-21-1482476501-789336058-1202660629-500\Software\Microsoft\Dependency
Walker\Recent File List
          Key Last Modified Date      6/20/2003 6:03:10 PM 6/20/2003 5:45:38 PM
```

Appendix 2-D Dependency Walker Profile of Specimen

Runtime Profiling log of Dependency Walker on specimen target2.exe.

```
****************************| System Information
|****************************

Dependency Walker:       2.1.3623 (32-bit)
Operating System:        Microsoft Windows 2000 Server (32-bit)
OS Version:              5.00.2195 Service Pack 3
Processor:               x86 Family 6 Model 5 Stepping 2, GenuineIntel, ~398MHz
Number of Processors:    1
Computer Name:           IP-TEST
User Name:               Administrator
Local Date:              Friday, June 20, 2003
Local Time:              6:02:18 PM Pacific Daylight Time (GMT-07:00)
OS Language:             0x0409: English (United States)
```

```
Memory Load:             17%
Physical Memory Total:   536,399,872 (512 MB)
Physical Memory Used:    93,863,936
Physical Memory Free:    442,535,936
Page File Memory Total:  1,342,713,856
Page File Memory Used:   63,909,888
Page File Memory Free:   1,278,803,968
Virtual Memory Total:    2,147,352,576
Virtual Memory Used:     36,618,240
Virtual Memory Free:     2,110,734,336
Page Size:               0x00001000 (4,096)
Allocation Granularity:  0x00010000 (65,536)
Min. App. Address:       0x00010000 (65,536)
Max. App. Address:       0x7FFEFFFF (2,147,418,111)

********************************| Search Order
|********************************
*
*
* Legend: F  File                     E  Error (path not valid)
*
*
*
*******************************************************************************
*

The system's "KnownDLLs" list
   [F ] c:\winnt\system32\ADVAPI32.DLL
   [F ] c:\winnt\system32\COMCTL32.DLL
   [F ] c:\winnt\system32\COMDLG32.DLL
   [F ] c:\winnt\system32\GDI32.DLL
   [F ] c:\winnt\system32\IMAGEHLP.DLL
   [F ] c:\winnt\system32\KERNEL32.DLL
   [F ] c:\winnt\system32\LZ32.DLL
   [F ] c:\winnt\system32\MPR.DLL
   [F ] c:\winnt\system32\MSVCRT.DLL
   [F ] c:\winnt\system32\NTDLL.DLL
   [F ] c:\winnt\system32\OLE32.DLL
   [F ] c:\winnt\system32\OLEAUT32.DLL
   [F ] c:\winnt\system32\OLECLI32.DLL
   [F ] c:\winnt\system32\OLECNV32.DLL
   [F ] c:\winnt\system32\OLESVR32.DLL
   [F ] c:\winnt\system32\OLETHK32.DLL
   [F ] c:\winnt\system32\RPCRT4.DLL
   [F ] c:\winnt\system32\SHELL32.DLL
   [F ] c:\winnt\system32\SHLWAPI.DLL
   [F ] c:\winnt\system32\URL.DLL
   [F ] c:\winnt\system32\URLMON.DLL
   [F ] c:\winnt\system32\USER32.DLL
   [F ] c:\winnt\system32\VERSION.DLL
   [F ] c:\winnt\system32\WININET.DLL
   [F ] c:\winnt\system32\WLDAP32.DLL
   [F ] c:\winnt\system32\WOW32.DLL
The application directory
   [  ] C:\lab\specimen\
The 32-bit system directory
   [  ] C:\WINNT\System32\
The 16-bit system directory (Windows NT/2000/XP only)
   [  ] C:\WINNT\system\
The system's root OS directory
   [  ] C:\WINNT\
The application's registered "App Paths" directories
The system's "PATH" environment variable directories
```

```
   [  ] C:\WINNT\system32\
   [  ] C:\WINNT\
   [  ] C:\WINNT\System32\Wbem\

**************************| Module Dependency Tree
|**************************
*
*
* Legend: F  Forwarded Module   ?  Missing Module        6  64-bit Module
*
*         D  Delay Load Module  !  Invalid Module
*
*         *  Dynamic Module     E  Import/Export Mismatch or Load Failure
*
*                               ^  Duplicate Module
*
*
*
*******************************************************************************
*

[   ] TARGET2.EXE
     [   ] KERNEL32.DLL
          [   ] NTDLL.DLL
          [F^ ] NTDLL.DLL
     [   ] ADVAPI32.DLL
          [ ^ ] NTDLL.DLL
          [ ^ ] KERNEL32.DLL
               [F^ ] NTDLL.DLL
          [   ] RPCRT4.DLL
               [ ^ ] NTDLL.DLL
               [ ^ ] KERNEL32.DLL
                    [F^ ] NTDLL.DLL
               [ ^ ] ADVAPI32.DLL
     [   ] WS2_32.DLL
          [ ^ ] MSVCRT.DLL
          [ ^ ] KERNEL32.DLL
               [F^ ] NTDLL.DLL
          [ ^ ] ADVAPI32.DLL
          [   ] WS2HELP.DLL
               [ ^ ] NTDLL.DLL
               [ ^ ] ADVAPI32.DLL
               [ ^ ] KERNEL32.DLL
                    [F^ ] NTDLL.DLL
               [D^ ] USER32.DLL
          [D  ] USER32.DLL
               [ ^ ] NTDLL.DLL
               [ ^ ] KERNEL32.DLL
                    [F^ ] NTDLL.DLL
               [   ] GDI32.DLL
                    [ ^ ] NTDLL.DLL
                    [ ^ ] KERNEL32.DLL
                         [F^ ] NTDLL.DLL
                    [ ^ ] USER32.DLL
     [   ] MFC42.DLL
          [ ^ ] MSVCRT.DLL
          [ ^ ] KERNEL32.DLL
               [F^ ] NTDLL.DLL
          [ ^ ] GDI32.DLL
          [ ^ ] USER32.DLL
          [D  ] OLEPRO32.DLL
               [ ^ ] KERNEL32.DLL
                    [F^ ] NTDLL.DLL
               [ ^ ] USER32.DLL
               [ ^ ] GDI32.DLL
               [ ^ ] OLE32.DLL
               [ ^ ] ADVAPI32.DLL
               [ ^ ] OLEAUT32.DLL
          [D^ ] ADVAPI32.DLL
          [D  ] OLE32.DLL
               [ ^ ] RPCRT4.DLL
               [ ^ ] GDI32.DLL
               [ ^ ] KERNEL32.DLL
                    [F^ ] NTDLL.DLL
               [ ^ ] USER32.DLL
               [ ^ ] ADVAPI32.DLL
               [ ^ ] NTDLL.DLL
          [D  ] OLEAUT32.DLL
               [ ^ ] OLE32.DLL
               [ ^ ] USER32.DLL
               [ ^ ] GDI32.DLL
               [ ^ ] KERNEL32.DLL
                    [F^ ] NTDLL.DLL
               [ ^ ] ADVAPI32.DLL
          [D  ] COMCTL32.DLL
               [ ^ ] NTDLL.DLL
               [ ^ ] GDI32.DLL
               [ ^ ] KERNEL32.DLL
                    [F^ ] NTDLL.DLL
               [ ^ ] USER32.DLL
               [ ^ ] ADVAPI32.DLL
          [D  ] SHELL32.DLL
               [ ^ ] NTDLL.DLL
               [ ^ ] GDI32.DLL
               [ ^ ] USER32.DLL
               [ ^ ] KERNEL32.DLL
                    [F^ ] NTDLL.DLL
               [ ^ ] ADVAPI32.DLL
               [   ] SHLWAPI.DLL
                    [ ^ ] GDI32.DLL
                    [ ^ ] KERNEL32.DLL
                         [F^ ] NTDLL.DLL
                    [ ^ ] USER32.DLL
                    [ ^ ] ADVAPI32.DLL
               [ ^ ] COMCTL32.DLL
               [D^ ] RPCRT4.DLL
          [D  ] COMDLG32.DLL
               [ ^ ] SHLWAPI.DLL
               [ ^ ] KERNEL32.DLL
                    [F^ ] NTDLL.DLL
               [ ^ ] USER32.DLL
               [ ^ ] GDI32.DLL
               [ ^ ] ADVAPI32.DLL
               [ ^ ] COMCTL32.DLL
               [ ^ ] SHELL32.DLL
               [ ^ ] MSVCRT.DLL
               [ ^ ] NTDLL.DLL
               [D^ ] WINSPOOL.DRV
          [D  ] WINSPOOL.DRV
               [ ^ ] NTDLL.DLL
               [ ^ ] KERNEL32.DLL
                    [F^ ] NTDLL.DLL
               [ ^ ] RPCRT4.DLL
               [ ^ ] ADVAPI32.DLL
               [ ^ ] GDI32.DLL
               [ ^ ] USER32.DLL
               [   ] MPR.DLL
                    [ ^ ] NTDLL.DLL
                    [ ^ ] KERNEL32.DLL
                         [F^ ] NTDLL.DLL
                    [ ^ ] ADVAPI32.DLL
                    [ ^ ] USER32.DLL
               [D^ ] OLE32.DLL
               [D^ ] OLEAUT32.DLL
               [D  ] ACTIVEDS.DLL
                    [   ] ADSLDPC.DLL
                         [ ^ ] MSVCRT.DLL
                         [ ^ ] NTDLL.DLL
                         [ ^ ] NETAPI32.DLL
                         [   ] WLDAP32.DLL
                              [ ^ ] MSVCRT.DLL
                              [ ^ ] KERNEL32.DLL
                                   [F^ ] NTDLL.DLL
                              [ ^ ] ADVAPI32.DLL
                              [D  ] CRYPT32.DLL
                                   [ ^ ] MSVCRT.DLL
                                   [   ] MSASN1.DLL
                                        [ ^ ] MSVCRT.DLL
                                        [ ^ ] KERNEL32.DLL
                                        [ ^ ] USER32.DLL
                                   [ ^ ] RPCRT4.DLL
                                   [ ^ ] ADVAPI32.DLL
                                   [ ^ ] KERNEL32.DLL
                                        [F^ ] NTDLL.DLL
                                   [ ^ ] USER32.DLL
                                   [D  ] VERSION.DLL
                                        [ ^ ] KERNEL32.DLL
                                        [ ^ ] NTDLL.DLL
                                        [   ] LZ32.DLL
                                             [ ^ ] NTDLL.DLL
                                             [ ^ ] KERNEL32.DLL
                                             [ ^ ] USER32.DLL
                                        [ ^ ] USER32.DLL
                         [ ^ ] ADVAPI32.DLL
                         [ ^ ] USER32.DLL
                         [ ^ ] KERNEL32.DLL
                              [F^ ] NTDLL.DLL
                    [ ^ ] MSVCRT.DLL
                    [ ^ ] NTDLL.DLL
                    [ ^ ] OLE32.DLL
                    [ ^ ] ADVAPI32.DLL
                    [ ^ ] KERNEL32.DLL
                         [F^ ] NTDLL.DLL
                    [ ^ ] USER32.DLL
                    [ ^ ] OLEAUT32.DLL
               [D  ] NETAPI32.DLL
                    [ ^ ] MSVCRT.DLL
                    [ ^ ] NTDLL.DLL
                    [   ] SECUR32.DLL
                         [ ^ ] NTDLL.DLL
                         [ ^ ] KERNEL32.DLL
                         [ ^ ] ADVAPI32.DLL
                    [ ^ ] ADVAPI32.DLL
                    [   ] NETRAP.DLL
                         [ ^ ] MSVCRT.DLL
                         [ ^ ] NTDLL.DLL
                         [ ^ ] KERNEL32.DLL
                    [ ^ ] RPCRT4.DLL
                    [ ^ ] KERNEL32.DLL
```

```
               [F^ ] NTDLL.DLL
          [   ] SAMLIB.DLL
               [ ^ ] NTDLL.DLL
               [ ^ ] ADVAPI32.DLL
               [ ^ ] RPCRT4.DLL
               [ ^ ] KERNEL32.DLL
                    [F^ ] NTDLL.DLL
          [ ^ ] WS2_32.DLL
          [ ^ ] WLDAP32.DLL
          [ ^ ] DNSAPI.DLL
     [D  ] NTDSAPI.DLL
          [ ^ ] MSVCRT.DLL
          [ ^ ] NTDLL.DLL
          [ ^ ] DNSAPI.DLL
          [ ^ ] RPCRT4.DLL
          [ ^ ] WLDAP32.DLL
          [ ^ ] NETAPI32.DLL
          [ ^ ] KERNEL32.DLL
               [F^ ] NTDLL.DLL
          [ ^ ] SECUR32.DLL
          [ ^ ] WS2_32.DLL
          [D  ] W32TOPL.DLL
               [ ^ ] NTDLL.DLL
               [ ^ ] KERNEL32.DLL
     [D  ] DNSAPI.DLL
          [ ^ ] MSVCRT.DLL
          [ ^ ] ADVAPI32.DLL
          [ ^ ] KERNEL32.DLL
               [F^ ] NTDLL.DLL
          [ ^ ] WSOCK32.DLL
               [F^ ] WS2_32.DLL
          [ ^ ] RPCRT4.DLL
[D  ] WININET.DLL
     [ ^ ] SHLWAPI.DLL
     [ ^ ] ADVAPI32.DLL
     [ ^ ] KERNEL32.DLL
          [F^ ] NTDLL.DLL
     [ ^ ] USER32.DLL
     [D^ ] CRYPT32.DLL
     [D^ ] OLE32.DLL
     [D^ ] VERSION.DLL
[D  ] WSOCK32.DLL
     [ ^ ] KERNEL32.DLL
     [ ^ ] WS2_32.DLL
     [F^ ] WS2_32.DLL
[D  ] OLEDLG.DLL
     [ ^ ] MSVCRT.DLL
     [ ^ ] KERNEL32.DLL
     [ ^ ] USER32.DLL
     [ ^ ] GDI32.DLL
     [ ^ ] ADVAPI32.DLL
     [ ^ ] OLE32.DLL
[D  ] URLMON.DLL
     [ ^ ] OLE32.DLL
     [ ^ ] SHLWAPI.DLL
     [ ^ ] USER32.DLL
     [ ^ ] GDI32.DLL
     [ ^ ] ADVAPI32.DLL
     [ ^ ] KERNEL32.DLL
          [F^ ] NTDLL.DLL
     [ ^ ] VERSION.DLL
     [D^ ] WININET.DLL
     [D^ ] RPCRT4.DLL
```

```
               [D^ ] SHELL32.DLL
               [D^ ] MPR.DLL
          [D  ] ODBC32.DLL
               [ ^ ] MSVCRT.DLL
               [ ^ ] KERNEL32.DLL
                    [F^ ] NTDLL.DLL
               [ ^ ] ADVAPI32.DLL
               [ ^ ] USER32.DLL
               [ ^ ] COMDLG32.DLL
               [ ^ ] COMCTL32.DLL
               [ ^ ] SHELL32.DLL
     [   ] MSVCRT.DLL
          [ ^ ] KERNEL32.DLL
               [F^ ] NTDLL.DLL
     [ ? ] MSVCP60.DLL

********************************| Module List
|*********************************
*
*
* Legend: D  Delay Load Module   ?  Missing Module           6  64-bit Module
*
*         *  Dynamic Module      !  Invalid Module
*
*                                E  Import/Export Mismatch or Load Failure
*
*
*
*******************************************************************************
*

       Module        File Time Stamp    Link Time Stamp    File Size  Attr.
Link Checksum  Real Checksum  CPU  Subsystem  Symbols  Preferred Base  Actual
Base  Virtual Size  Load Order  File Ver         Product Ver      Image Ver
Linker Ver  OS Ver  Subsystem Ver
-----  ------------  -----------------  -----------------  ---------  -----  --
-----------  -------------  ---  ---------  -------  --------------  ----------
-  ------------  ----------  ---------------  ---------------  ---------  -----
-----  ------  -------------
[ ? ]  MSVCP60.DLL   Error opening file. The system cannot find the file
specified (2).
[   ]  ADVAPI32.DLL  07/22/2002 12:05p  07/23/2002 12:13a    367,376  A
0x00065640     0x00065640     x86  Console    DBG      0x77DB0000
0x77DB0000   0x0005D000    4           5.0.2195.5385    5.0.2195.5385    5.0
5.12        5.0    4.0
[   ]  GDI32.DLL     07/22/2002 12:05p  07/23/2002 12:13a    234,256  A
0x00048894     0x00048894     x86  Console    DBG      0x77F40000
0x77F40000   0x0003C000    10          5.0.2195.5252    5.0.2195.5252    5.0
5.12        5.0    4.10
[   ]  KERNEL32.DLL  07/22/2002 12:05p  07/23/2002 12:13a    733,968  A
0x000B5326     0x000B5326     x86  Console    DBG      0x77E80000
0x77E80000   0x000B6000    3           5.0.2195.5400    5.0.2195.5400    5.0
5.12        5.0    4.0
[   ]  MFC42.DLL     12/07/1999  1:00p  11/30/1999  2:33a    995,383  A
0x000FE3F3     0x000FE3F3     x86  GUI        PDB      0x6C370000
0x6C370000   0x000F2000    9           6.0.8665.0       6.0.4.0          6.0
6.0         4.0    4.0
[   ]  MSVCRT.DLL    07/22/2002 12:05p  09/20/2001  2:52p    290,869  A
0x00048405     0x00048405     x86  GUI        PDB      0x78000000
0x78000000   0x00046000    7           6.1.9359.0       6.1.9359.0       0.0
6.0         4.0    4.0
[   ]  NTDLL.DLL     07/22/2002 12:05p  07/23/2002 12:13a    490,768  A
0x0007B14B     0x0007B14B     x86  Console    DBG      0x77F80000
```

```
0x77F80000   0x0007B000    2           5.0.2195.5400    5.0.2195.5400    5.0
5.12         5.0     4.0
[   ] RPCRT4.DLL    07/22/2002 12:05p  07/23/2002 12:13a    450,832  A
0x0007B599     0x0007B599     x86  Console    DBG      0x77D30000
0x77D30000   0x00071000    5           5.0.2195.5419    5.0.2195.5419    5.0
5.12         5.0     4.10
[   ] TARGET2.EXE   02/20/2003 12:45p  11/28/2002 12:53a     26,793  A
0x00000000     0x0000DC8A     x86  Console    None     0x00400000
0x00400000   0x00006000    1           N/A              N/A              0.0
6.0          4.0     4.0
[   ] USER32.DLL    07/22/2002 12:05p  07/23/2002 12:13a    405,264  A
0x00067389     0x00067389     x86  GUI        DBG      0x77E10000
0x77E10000   0x00065000    11          5.0.2195.4314    5.0.2195.4314    5.0
5.12         5.0     4.0
[   ] WS2_32.DLL    07/22/2002 12:05p  07/23/2002 12:14a     68,368  A
0x0001A8F4     0x0001A8F4     x86  Console    DBG      0x75030000
0x75030000   0x00013000    6           5.0.2195.4874    5.0.2195.4874    5.0
5.12         5.0     4.10
[   ] WS2HELP.DLL   12/07/1999  1:00p  11/30/1999  2:31a     18,192  A
0x000087D1     0x000087D1     x86  Console    DBG      0x75020000
0x75020000   0x00008000    8           5.0.2134.1       5.0.2134.1       5.0
5.12         5.0     4.0
[D  ] ACTIVEDS.DLL  07/22/2002 12:05p  07/23/2002 12:13a    179,472  A
0x0003AEED     0x0003AEED     x86  Console    DBG      0x773B0000      Unknown
0x0002E000    Not Loaded  5.0.2195.5312    5.0.2195.5312    5.0        5.12
5.0     4.0
[D  ] ADSLDPC.DLL   07/22/2002 12:05p  07/23/2002 12:13a    130,832  A
0x000297D6     0x000297D6     x86  Console    DBG      0x77380000      Unknown
0x00022000    Not Loaded  5.0.2195.5400    5.0.2195.5400    5.0        5.12
5.0     4.0
[D  ] COMCTL32.DLL  07/22/2002 12:05p  07/23/2002 12:13a    552,208  A
0x0008CC1D     0x0008CC1D     x86  GUI        DBG      0x77B50000      Unknown
0x00089000    Not Loaded  5.81.3315.3727   5.0.3315.3727    5.0        5.12
5.0     4.0
[D  ] COMDLG32.DLL  07/22/2002 12:05p  07/23/2002 12:13a    226,576  A
0x0003EEA1     0x0003EEA1     x86  GUI        DBG      0x76B30000      Unknown
0x0003D000    Not Loaded  5.0.3315.3727    5.0.3315.3727    5.0        5.12
5.0     4.0
[D  ] CRYPT32.DLL   07/22/2002 12:05p  07/23/2002 12:13a    475,408  A
0x00078DCF     0x00078DCF     x86  GUI        DBG      0x77440000      Unknown
0x00077000    Not Loaded  5.131.2195.4558  5.131.2195.4558  5.0        5.12
5.0     4.0
[D  ] DNSAPI.DLL    07/22/2002 12:05p  07/23/2002 12:13a    134,416  A
0x0002D9AB     0x0002D9AB     x86  Console    DBG      0x77980000      Unknown
0x00024000    Not Loaded  5.0.2195.5354    5.0.2195.5354    5.0        5.12
5.0     4.0
[D  ] LZ32.DLL      12/07/1999  1:00p  11/30/1999  2:30a     10,000  A
0x0000A8D0     0x0000A8D0     x86  Console    DBG      0x759B0000      Unknown
0x00006000    Not Loaded  5.0.2134.1       5.0.2134.1       5.0        5.12
5.0     4.10
[D  ] MPR.DLL       07/22/2002 12:05p  07/23/2002 12:14a     55,056  A
0x00012F0A     0x00012F0A     x86  Console    DBG      0x76620000      Unknown
0x00010000    Not Loaded  5.0.2195.3649    5.0.2195.3649    5.0        5.12
5.0     4.0
[D  ] MSASN1.DLL    07/22/2002 12:05p  07/23/2002 12:13a     52,496  A
0x0001011D     0x0001011D     x86  GUI        DBG      0x77430000      Unknown
0x00010000    Not Loaded  5.0.2195.4067    5.0.2195.4067    5.0        5.12
5.0     4.0
[D  ] NETAPI32.DLL  07/22/2002 12:05p  07/23/2002 12:14a    312,592  A
0x00052F82     0x00052F82     x86  Console    DBG      0x75170000      Unknown
0x0004F000    Not Loaded  5.0.2195.5427    5.0.2195.5427    5.0        5.12
5.0     4.0
```

```
[D  ]  NETRAP.DLL    12/07/1999  1:00p  11/30/1999  2:31a     11,536  A
0x0000D1DD     0x0000D1DD     x86  Console    DBG      0x751C0000      Unknown
0x00006000    Not Loaded  5.0.2134.1       5.0.2134.1       5.0        5.12
5.0     4.10
[D  ]  NTDSAPI.DLL   07/22/2002 12:05p  07/23/2002 12:13a     57,616  A
0x000123C1     0x000123C1     x86  Console    DBG      0x77BF0000      Unknown
0x00011000    Not Loaded  5.0.2195.4827    5.0.2195.4827    5.0        5.12
5.0     4.10
[D  ]  ODBC32.DLL    07/22/2002 12:05p  03/25/2002  3:40p    217,360  A
0x00042E91     0x00042E91     x86  GUI        DBG      0x1F7D0000      Unknown
0x00034000    Not Loaded  3.520.6200.0     3.520.6200.0     5.0        5.12
5.0     4.0
[D  ]  OLE32.DLL     07/22/2002 12:05p  07/23/2002 12:13a    991,504  A
0x000F9027     0x000F9027     x86  Console    DBG      0x77A50000      Unknown
0x000F5000    Not Loaded  5.0.2195.5400    5.0.2195.5400    5.0        5.12
5.0     4.0
[D  ]  OLEAUT32.DLL  07/22/2002 12:05p  07/23/2002 12:13a    626,960  A
0x0009F6F0     0x0009F6F0     x86  GUI        DBG      0x779B0000      Unknown
0x0009B000    Not Loaded  2.40.4518.0      2.40.4518.0      0.0        5.12
4.0     4.0
[D  ]  OLEDLG.DLL    12/07/1999  1:00p  12/07/1999  5:42p    118,032  A
0x0002A26A     0x0002A26A     x86  GUI        DBG      0x752F0000      Unknown
0x0001F000    Not Loaded  5.0.2134.1       5.0.2134.1       5.0        5.12
5.0     4.0
[D  ]  OLEPRO32.DLL  07/22/2002 12:05p  07/23/2002 12:14a    164,112  A
0x0002F005     0x0002F005     x86  GUI        DBG      0x695E0000      Unknown
0x00029000    Not Loaded  5.0.4518.0       2.40.4518.0      0.0        5.12
4.0     4.0
[D  ]  SAMLIB.DLL    07/22/2002 12:05p  07/23/2002 12:14a     50,960  A
0x0001208B     0x0001208B     x86  Console    DBG      0x75150000      Unknown
0x00010000    Not Loaded  5.0.2195.4827    5.0.2195.4827    5.0        5.12
5.0     4.0
[D  ]  SECUR32.DLL   07/22/2002 12:05p  07/23/2002 12:13a     48,400  A
0x00018014     0x00018014     x86  Console    DBG      0x77BE0000      Unknown
0x0000F000    Not Loaded  5.0.2195.4587    5.0.2195.4587    5.0        5.12
5.0     4.0
[D  ]  SHELL32.DLL   07/22/2002 12:05p  07/23/2002 12:13a  2,374,416  A
0x00250F59     0x00250F59     x86  GUI        DBG      0x782F0000      Unknown
0x00246000    Not Loaded  5.0.3502.5436    5.0.3502.5436    5.0        5.12
5.0     4.0
[D  ]  SHLWAPI.DLL   07/22/2002 12:05p  07/23/2002 12:13a    290,064  A
0x00051018     0x00051018     x86  GUI        DBG      0x77C70000      Unknown
0x0004A000    Not Loaded  5.0.3502.5332    5.0.3502.5332    5.0        5.12
5.0     4.0
[D  ]  URLMON.DLL    07/22/2002 12:05p  07/23/2002 12:13a    452,880  A
0x000739D4     0x000739D4     x86  GUI        DBG      0x77640000      Unknown
0x00072000    Not Loaded  5.0.3502.5400    5.0.3502.5400    5.0        5.12
5.0     4.0
[D  ]  VERSION.DLL   12/07/1999  1:00p  12/01/1999 12:37a     16,144  A
0x0000C983     0x0000C983     x86  GUI        DBG      0x77820000      Unknown
0x00007000    Not Loaded  5.0.2134.1       5.0.2134.1       5.0        5.12
5.0     4.0
[D  ]  W32TOPL.DLL   12/07/1999  1:00p  11/30/1999  2:31a     12,560  A
0x00006E3B     0x00006E3B     x86  Console    DBG      0x754A0000      Unknown
0x00007000    Not Loaded  5.0.2160.1       5.0.2160.1       5.0        5.12
5.0     4.10
[D  ]  WININET.DLL   07/22/2002 12:05p  07/23/2002 12:13a    461,584  A
0x00073F00     0x00073F00     x86  GUI        DBG      0x76C00000      Unknown
0x00073000    Not Loaded  5.0.3502.4619    5.0.3502.4619    5.0        5.12
5.0     4.0
[D  ]  WINSPOOL.DRV  07/22/2002 12:05p  07/23/2002 12:13a    113,936  A
0x00027317     0x00027317     x86  GUI        DBG      0x77800000      Unknown
```

```
0x0001E000    Not Loaded  5.0.2195.5225    5.0.2195.5225    5.0        5.12
5.0     4.0
[D  ]  WLDAP32.DLL   07/22/2002 12:05p  07/23/2002 12:13a    162,576  A
0x00034EEE     0x00034EEE     x86  GUI        DBG      0x77950000      Unknown
0x0002A000    Not Loaded  5.0.2195.5400    5.0.2195.5400    5.0        5.12
5.0     4.0
[D  ]  WSOCK32.DLL   07/22/2002 12:05p  07/23/2002 12:14a     21,776  A
0x00012632     0x00012632     x86  Console    DBG      0x75050000      Unknown
0x00008000    Not Loaded  5.0.2195.4874    5.0.2195.4874    5.0        5.12
5.0     4.10

***********************************| Log
|************************************

Error: At least one required implicit or forwarded dependency was not found.

------------------------------------------------------------------------------
-
Starting profile on 6/20/2003 at 6:00:34 PM

Operating System: Microsoft Windows 2000 Server (32-bit), version 5.00.2195
Service Pack 3
Program Executable: c:\lab\specimen\TARGET2.EXE
Program Arguments:
Starting Directory: C:\lab\specimen\
Search Path: C:\WINNT\system32;C:\WINNT;C:\WINNT\System32\Wbem

Options Selected:
     Simulate ShellExecute by inserting any App Paths directories into the PATH
environment variable.
     Log DllMain calls for process attach and process detach messages.
     Hook the process to gather more detailed dependency information.
     Log LoadLibrary function calls.
     Log GetProcAddress function calls.
     Log debug output messages.
     Automatically open and profile child processes.
------------------------------------------------------------------------------
-

Started "TARGET2.EXE" (process 0x6C) at address 0x00400000.  Cannot hook
module.
Loaded "NTDLL.DLL" at address 0x77F80000.  Cannot hook module.
Loaded "KERNEL32.DLL" at address 0x77E80000.  Cannot hook module.
Loaded "ADVAPI32.DLL" at address 0x77DB0000.  Cannot hook module.
Loaded "RPCRT4.DLL" at address 0x77D30000.  Cannot hook module.
Loaded "WS2_32.DLL" at address 0x75030000.  Cannot hook module.
Loaded "MSVCRT.DLL" at address 0x78000000.  Cannot hook module.
Loaded "WS2HELP.DLL" at address 0x75020000.  Cannot hook module.
Loaded "MFC42.DLL" at address 0x6C370000.  Cannot hook module.
Loaded "GDI32.DLL" at address 0x77F40000.  Cannot hook module.
Loaded "USER32.DLL" at address 0x77E10000.  Cannot hook module.
Second chance exception 0xC0000135 (DLL Not Found) occurred in "NTDLL.DLL" at
address 0x77FB120C.
Exited "TARGET2.EXE" (process 0x6C) with code 128 (0x80).
```

Appendix 3-A Modified EPCA Quick Reference Guide

Quick Reference Guide for Use of EPCA.
Modified from http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm, approx. pg. 47-48, to correct formatting problems in that document.

The highlighted section in bold denotes the portion of the EPCA that applied to this scenario.

	Voluntary Disclosure Allowed?		Mechanisms to Compel Disclosure	
Type of Data	**Public Provider**	**Non-Public Provider**	**Public Provider**	**Non-Public Provider**
Basic subscriber, session, and billing information	Not to government, unless § 2702(c) exception applies [§ 2702(a)(3)]	Yes [§ 2702(a)(3)]	Subpoena; 2703(d) order; or search warrant [§ 2703(c)(2)]	Subpoena; 2703(d) order; or search warrant [§ 2703(c)(2)]
Other transactional and account records	**Not to government, unless § 2702(c) exception applies [§ 2702(a)(3)]**	**Yes [§ 2702(a)(3)]**	**2703(d) order or search warrant [§ 2703(c)(1)]**	**2703(d) order or search warrant [§ 2703(c)(1)]**
Accessed communications (opened e-mail and voice mail) left with provider and other stored files	No, unless § 2702(b) exception applies [§ 2702(a)(2)]	Yes [§ 2702(a)(2)]	Subpoena with notice; 2703(d) order with notice; or search warrant [§ 2703(b)]	Subpoena; ECPA doesn't apply [§ 2711(2)]
Unretrieved communication, including e-mail and voice mail (in electronic storage more than 180 days)	No, unless § 2702(b) exception applies [§ 2702(a)(1)]	Yes [§ 2702(a)(1)]	Subpoena with notice; 2703(d) order with notice; or search warrant [§ 2703(a,b)]	Subpoena with notice; 2703(d) order with notice; or search warrant [§ 2703(a,b)]
Unretrieved communication, including e-mail and voice mail (in electronic storage 180 days or less)	No, unless § 2702(b) exception applies [§ 2702(a)(1)]	Yes [§ 2702(a)(1)]	Search warrant [§ 2703(a)]	Search warrant [§ 2703(a)]