
hp
invent

Cyber-Investigation on Cyber-Crime

Ricci Ieong and Vincent Ip,
Security Consultant,

HP e-Security Center, HP Consulting, HK

E-Commerce leads to Cyber Crime

- US$30 billion in 2001 in Internet commerce revenue in 16 Western European countries (ZDNet March 9, 1998)
- US$1.3 trillion by 2003 in Internet Business transaction (Forrester Research)
- Number of Unique Visitors increased in most of the B2C web sites by around 50% (CyberAtlas.internet.com, 8 Jan 2001)
- B2C Internet Commerce Market in 2001 will be US$95 billion (IDC, 4 Jan 2001)

How secure are you?

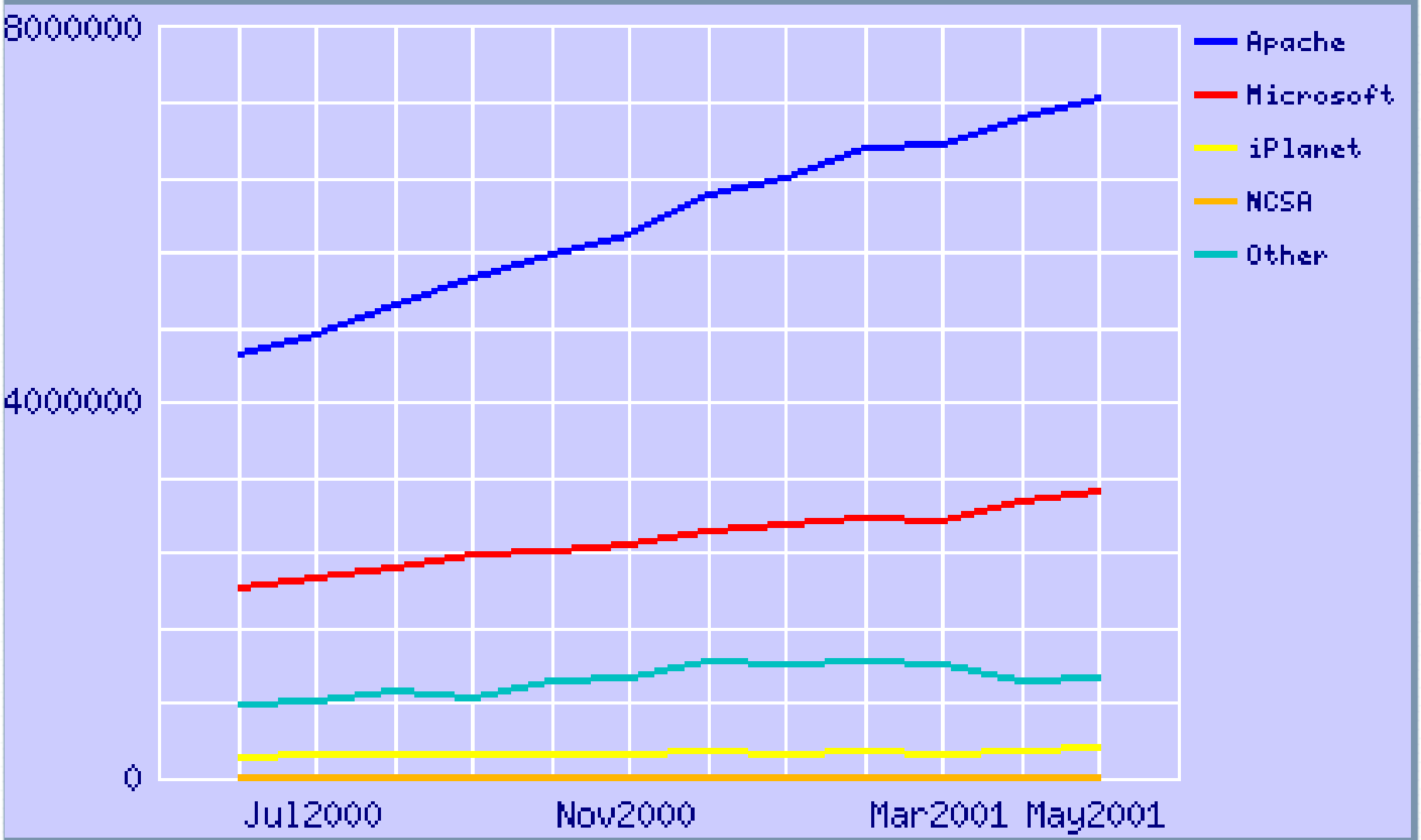
- Internet connection?
- Firewall protection?
- Intrusion Detection System installed?
- Frequently reviewed of security logs? (including firewall logs, router logs, mail server logs, web server logs, etc)
- Encryption of email message?
- Security Risk Assessment performed periodically?
- 24x7 security monitoring?

More potential target for hackers

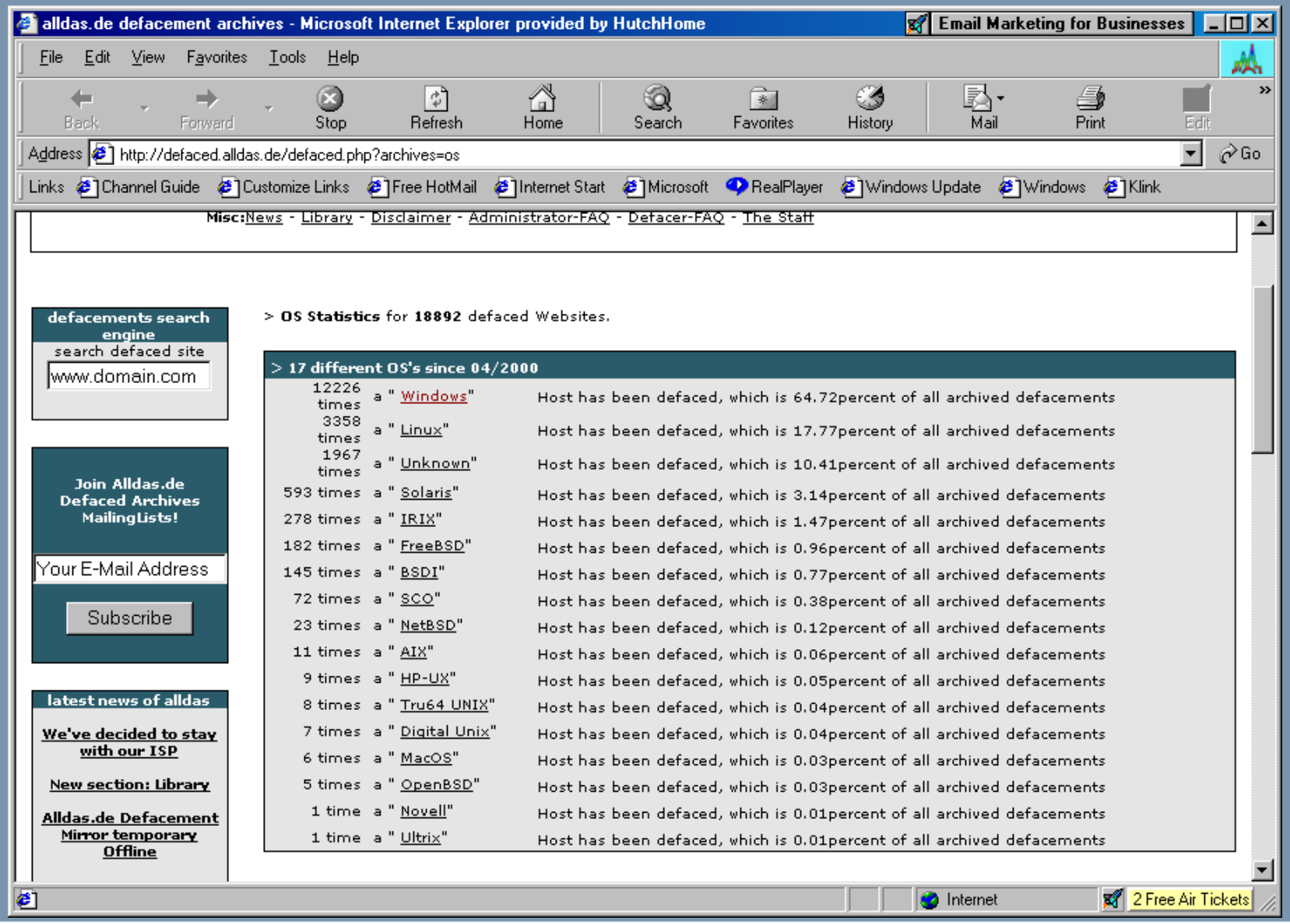
By May 2001

Apache	62.24%
Microsoft IIS	20.52%
iPlanet	6.13%
Zeus	2.75%
Rapidsite	1.40%
AOLserver	1.30%
Thttpd	1.28%
Tigershark	0.74%
WebSitePro	0.41%
ConcentricHost-Ashurbanipal	0.38%

Active Servers – Potential target list



Statistics on Web defacement (from Attrition.org)



Increase in Crime number

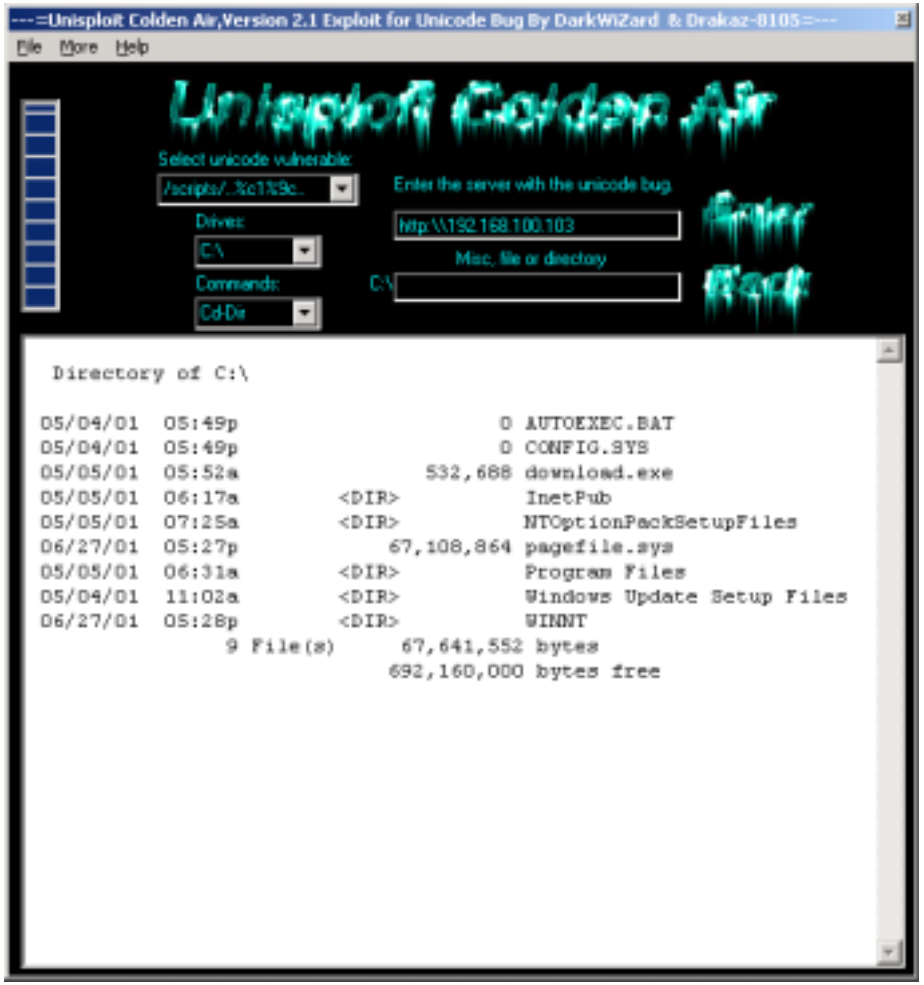
2001 CSI/FBI Computer Crime and Security Survey

- 538 responses
- 64% of respondents detected “unauthorized use of computer systems” in the last 12 months
- 40% detected “system penetration”
  - 95% had 1 firewall
  - 61% had an IDS
- 26% detected “theft of proprietary info”
- 18% detected “sabotage”
- Combined losses from 196 respondents totaled $378 million
  - $151 million from “theft of proprietary info”
  - $19 million from “system penetration”

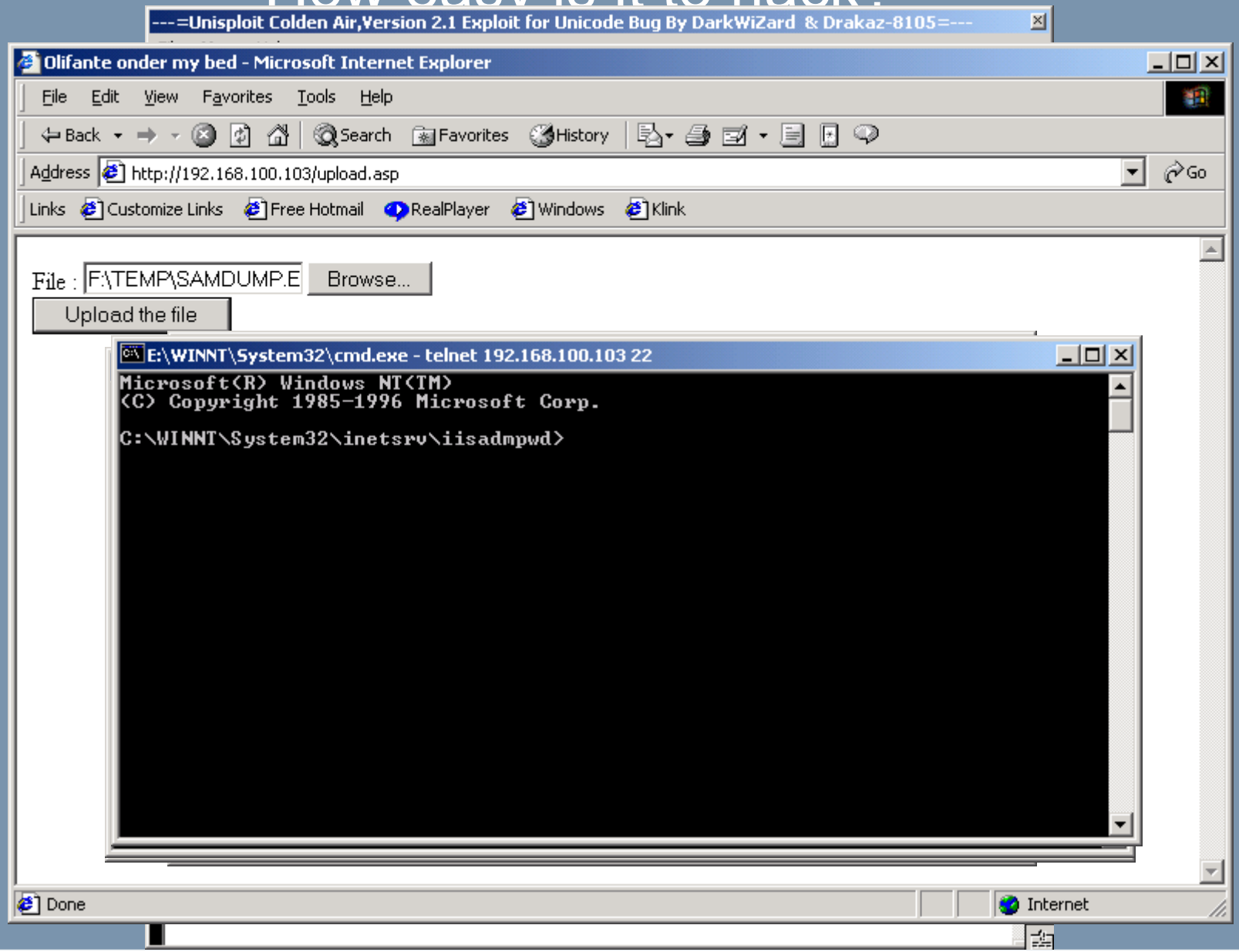
Targeted platform

- Hackers crack four Microsoft sites (22/6/2001)
- Oracle Security Risk On Windows NT (26/6/2001)
  - “This vulnerability causes a Windows NT system to consume 100% of available memory. Access to the server is denied and a full reboot is required”
- Solaris Bug Gives Attackers System-Level Access (21/6/2001)
  - “A newly discovered bug in Solaris could allow attackers to run malicious programs on servers with Sun's operating system installed”
- Apache.org got defaced (30/5/2001)

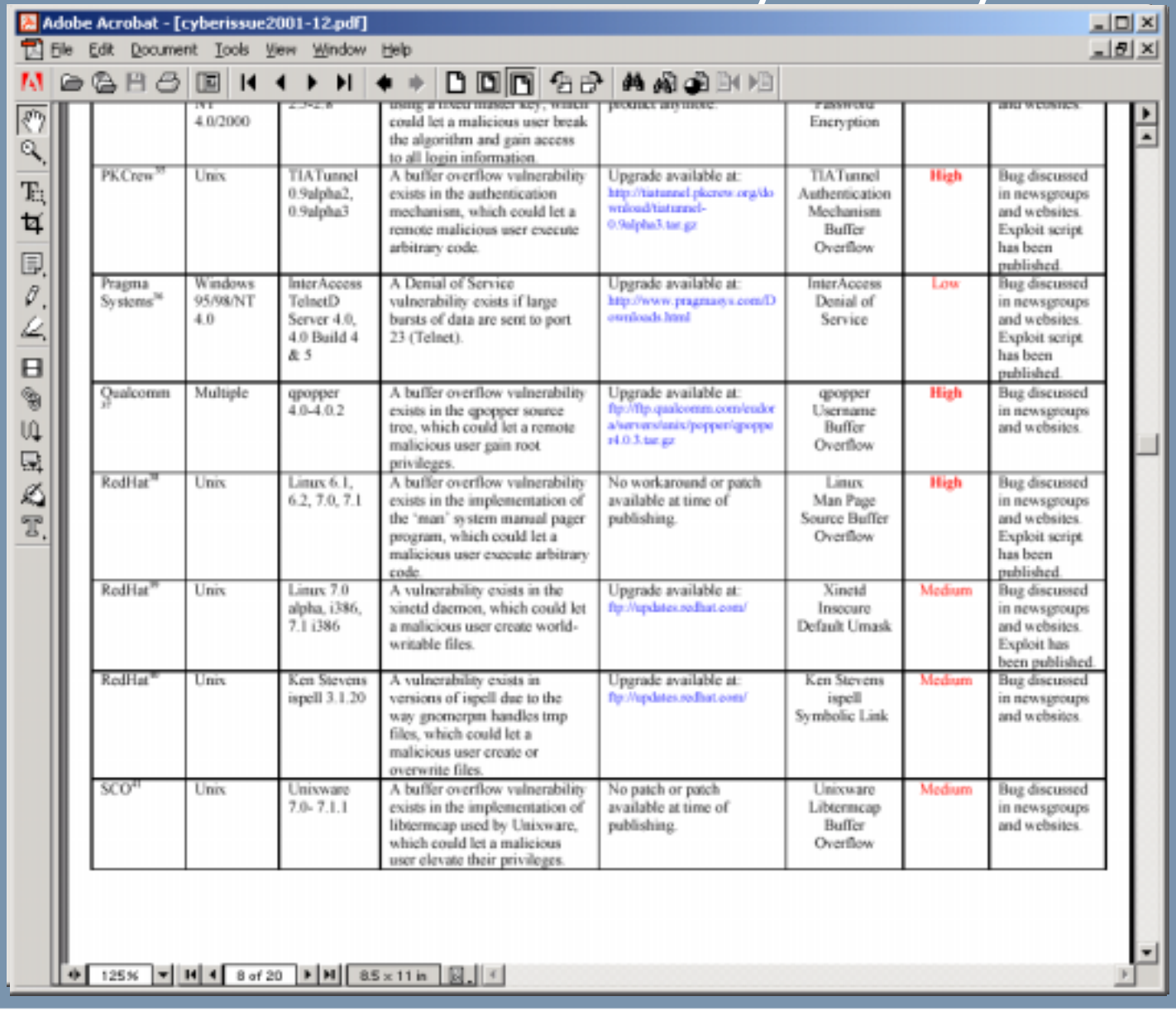
Hacking is as easy as click a button



How easy is it to hack?

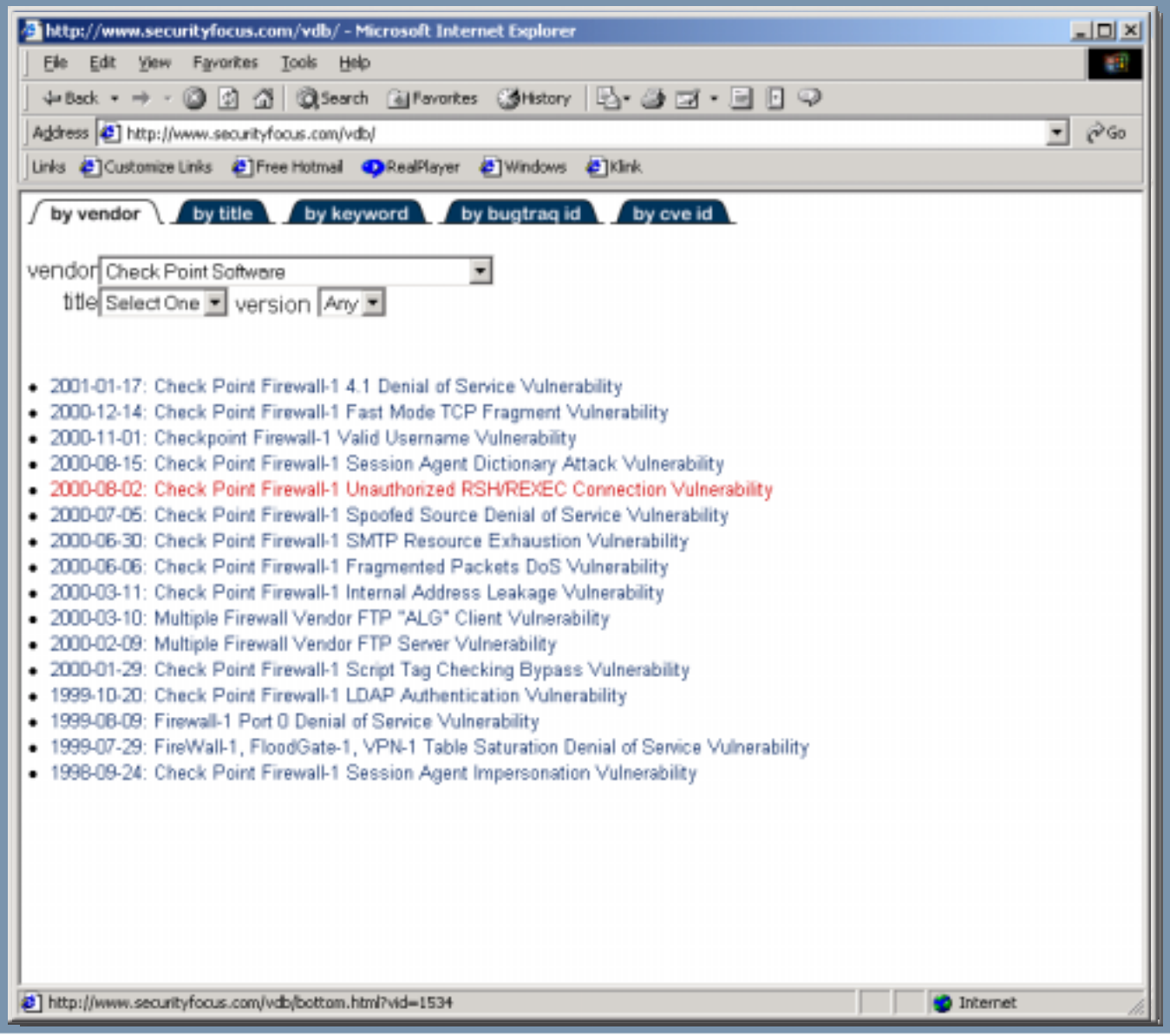


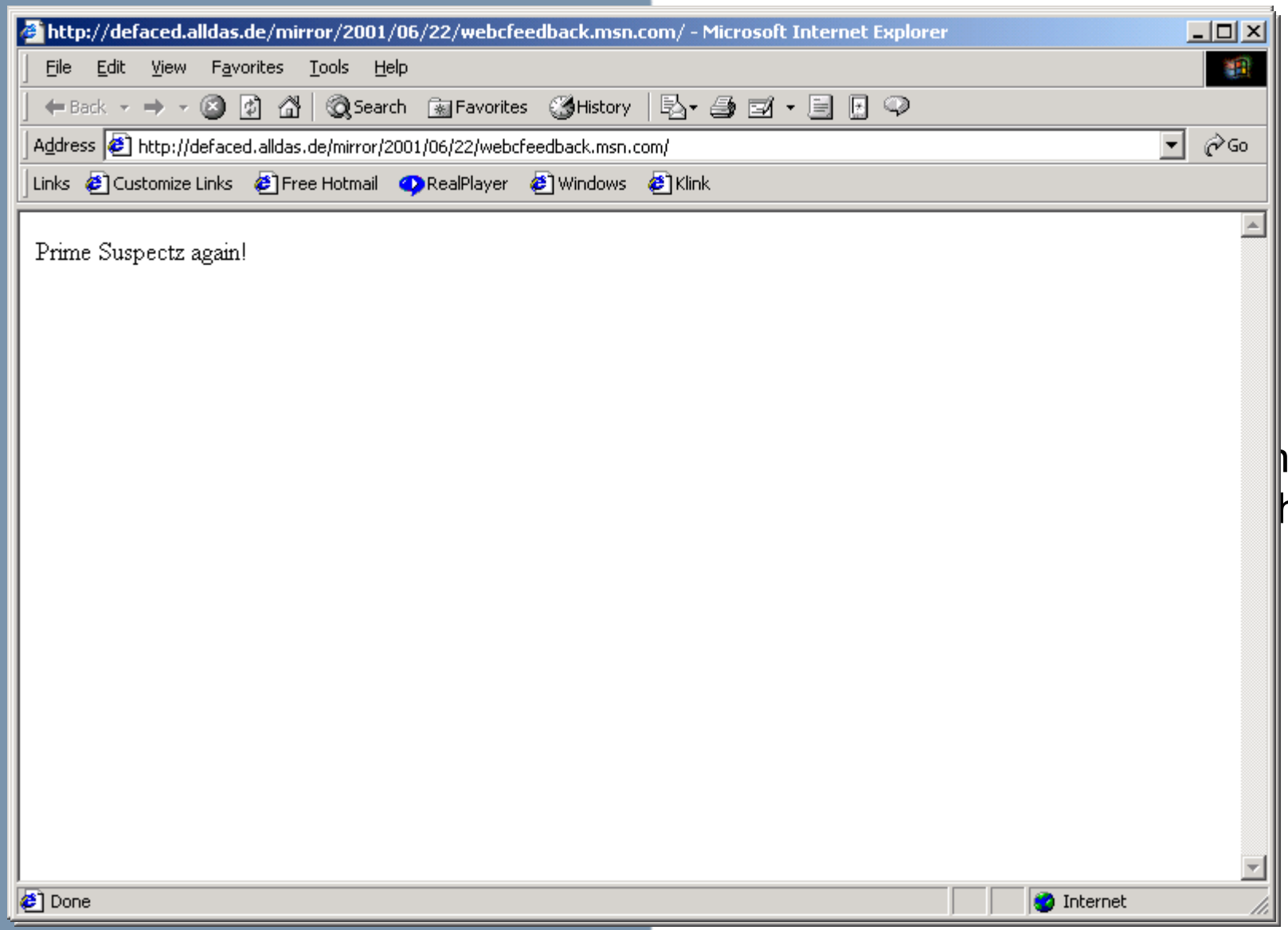
Vulnerabilities are always with you



	4.0/2000		could let a malicious user break the algorithm and gain access to all login information.		Encryption		
PKCrew[39]	Unix	TIATunnel 0.9alpha2, 0.9alpha3	A buffer overflow vulnerability exists in the authentication mechanism, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://tiatunnel.pkcrew.org/download/tiatunnel-0.9alpha3.tar.gz	TIATunnel Authentication Mechanism Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Pragma Systems[36]	Windows 95/98/NT 4.0	InterAccess TelnetD Server 4.0, 4.0 Build 4 & 5	A Denial of Service vulnerability exists if large bursts of data are sent to port 23 (Telnet).	Upgrade available at: http://www.pragmasys.com/Downloads.html	InterAccess Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Qualcomm[37]	Multiple	qpopper 4.0-4.0.2	A buffer overflow vulnerability exists in the qpopper source tree, which could let a remote malicious user gain root privileges.	Upgrade available at: ftp://ftp.qualcomm.com/eudora/servers/unix/popper/qpopper4.0.3.tar.gz	qpopper Username Buffer Overflow	High	Bug discussed in newsgroups and websites.
RedHat[38]	Unix	Linux 6.1, 6.2, 7.0, 7.1	A buffer overflow vulnerability exists in the implementation of the 'man' system manual pager program, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Linux Man Page Source Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
RedHat[39]	Unix	Linux 7.0 alpha, i386, 7.1 i386	A vulnerability exists in the xinetd daemon, which could let a malicious user create world-writable files.	Upgrade available at: ftp://updates.redhat.com/	Xinetd Insecure Default Umask	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
RedHat[40]	Unix	Ken Stevens ispell 3.1.20	A vulnerability exists in versions of ispell due to the way gnomerpm handles tmp files, which could let a malicious user create or overwrite files.	Upgrade available at: ftp://updates.redhat.com/	Ken Stevens ispell Symbolic Link	Medium	Bug discussed in newsgroups and websites.
SCO[41]	Unix	Unixware 7.0- 7.1.1	A buffer overflow vulnerability exists in the implementation of libtermcap used by Unixware, which could let a malicious user elevate their privileges.	No patch or patch available at time of publishing.	Unixware Libtermcap Buffer Overflow	Medium	Bug discussed in newsgroups and websites.

Vulnerabilities are always with you




http://defaced.alldas.de/mirror/2001/06/22/webcfeedback.msn.com/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://defaced.alldas.de/mirror/2001/06/22/webcfeedback.msn.com/
Go
Links Customize Links Free Hotmail RealPlayer Windows Klink
Prime Suspectz again!
Done
Internet

hetpu
hacke

Can we identify the attack?

This is the simplest case in investigation

- From viewing the web directly
- From defacement mailing list
- By external web user

What to do next

Immediate work

- Incident Handling
  - should be meeting the requirements from legal counsel, business, law enforcement and company managers

Afterwards

- Computer Crime and Forensics Investigation
  - usually performed by the 3rd party company, CERT or law enforcement team

Managed Security Services

- On-site Consulting
- Outsource Security Management
  - Remote perimeter management
  - 24x7 Management and monitoring services
- Penetration and vulnerability testing
- Incident Handling and Computer Forensics Investigation
  - Incident Handling
  - **Computer Forensics Investigation**

How to perform Computer Forensics Investigation?

Identify the Incident, then the Evidence

Collect and Preserve the Evidence

Investigation: Extract, process, and interpret

Step 1 - Incident Identification

- Initial Response by the system administrator
  - retrieve information to confirm the incident
  - review from all possible sources of the information
  - identify the scope and size of the affected machines and systems
  - determine the damage caused by the intrusion (if any)
  - identify the possible path of attack
  - Backup all possible evidence

Step 1 - Incident Identification

- Important notes
  - try to prevent modification of the original
  - keep the chain of custody
  - make at least two copies
  - sign and confirm the date of the original
  - check the system clock and time on affected machines

Our Forensics Toolbox

- Traveling forensics lab
  - Boot disks
  - Backup hard disk devices
  - Sniffer machines
  - man pages and manual of different platform
  - Tools for *nix
    - dd, netcat, TCT, TCTUtil, ls, ps, lsof, md5sum, find, netstat, ifconfig, strings, trace, who, w, last, lastlog, tcpdump, unrm, lazarus etc
  - Tools for Windows
    - cmd.exe, date, time, loggedon, IRCR, fport, netstat, listdlls, doskey, uptime, nbtstat, pslist, auditpol, afind, ntlast, dumpel, regdump, pwdump, windump, md5sum, userinfo, sig, getslack, inzider etc

Step 2 - Evidence Collection

Preserving the evidence in Hard disk

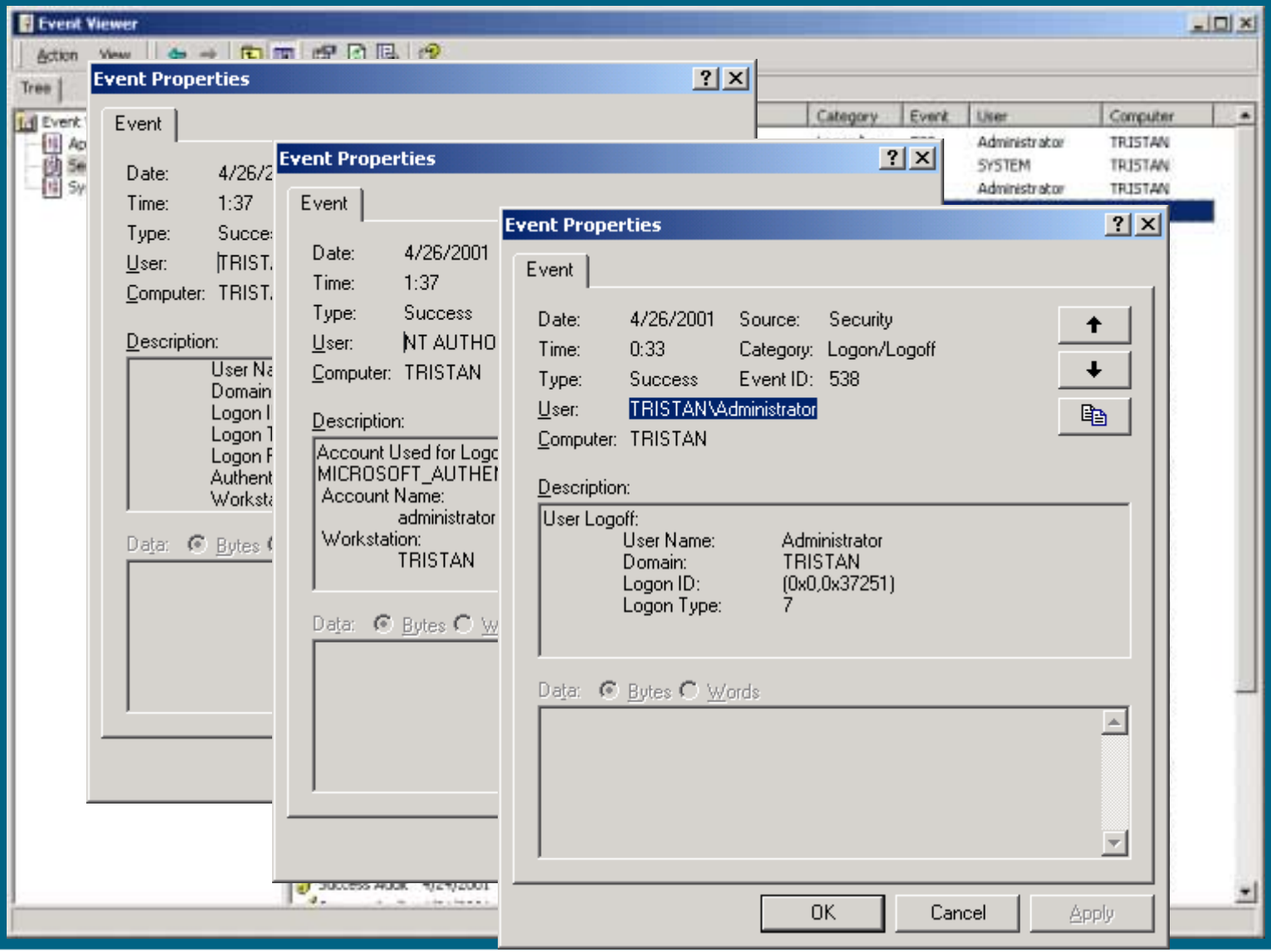
- Cloning of disk based on
  - dd and md5
  - Encase
  - SafeBack
  - Ghost
  - Disk Duplicator
- Near to Exact Copy
  - Back up from backup tape

Step 2 - Evidence Collection

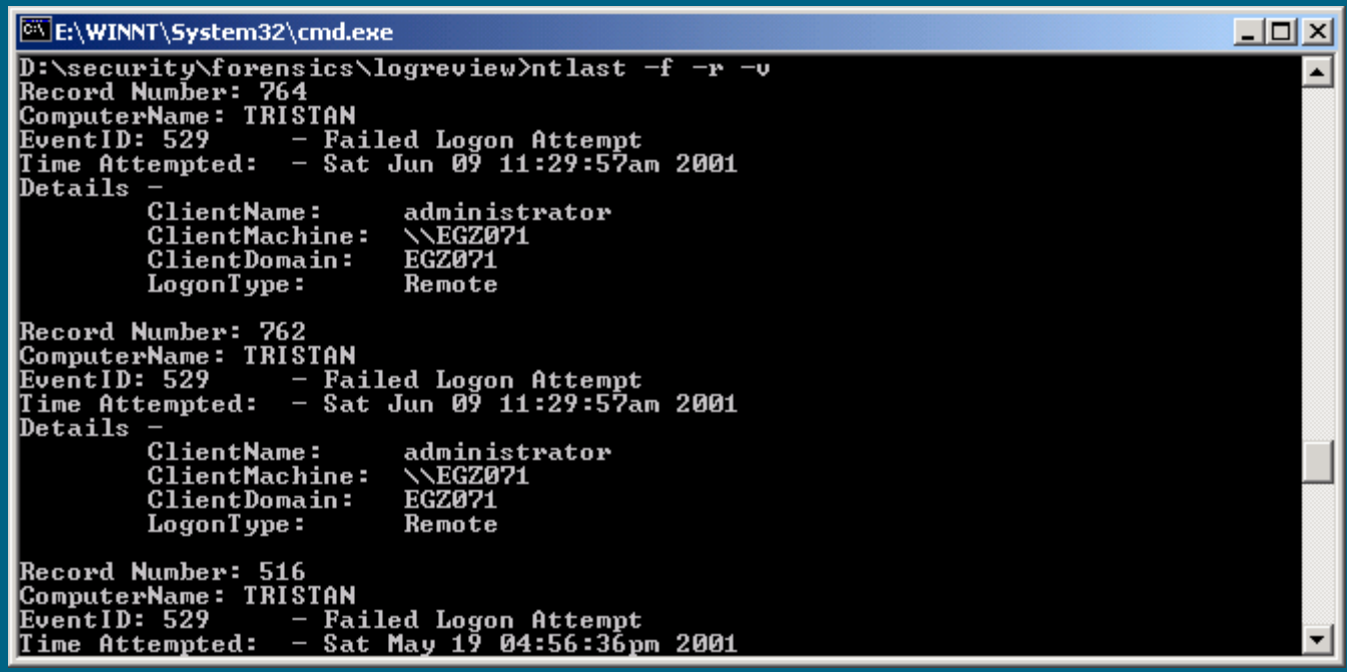
Collect the state of the machine

- Network information
  - netstat, ipconfig, nbtstat, etc.
- Process information
  - ps, pslist, etc
- Open ports and hidden services
  - lsof, fport, inzider, etc
- Log files
  - Phone log, Web server log, mail server log, ftp log, router log, firewall log
  - who, last, lastlog, syslog, event viewer, etc
- Generic Forensics investigation
  - TCT, TCTUtil, IRCR, WinHex, EnCase
- Searching tools

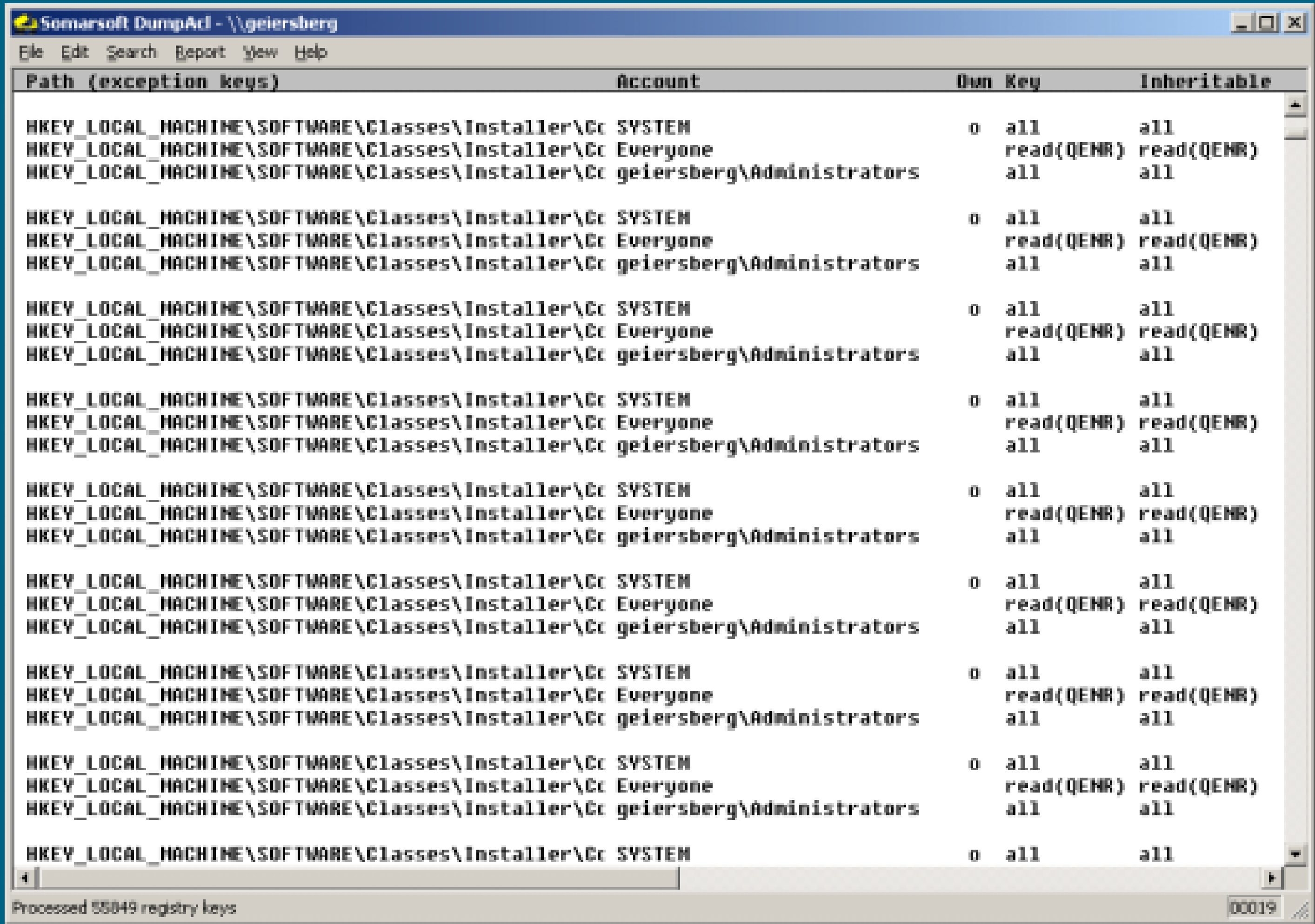
Eventlog


Event Viewer
Action
View
Tree
Category
Event
User
Computer
Administrator
TRISTAN
SYSTEM
TRISTAN
Administrator
TRISTAN
Event Properties
Event
Date:
Time:
Type:
User:
Computer:
Description:
Event Properties
Event
Date: 4/26/2001
Time: 1:37
Type: Success
User: NT AUTHO
Computer: TRISTAN
Description:
Account Used for Logc
MICROSOFT_AUTHEI
Account Name:
administrator
Workstation:
TRISTAN
Data: Bytes
Event Properties
Event
Date: 4/26/2001 Source: Security
Time: 0:33 Category: Logon/Logoff
Type: Success Event ID: 538
User: TRISTAN\Administrator
Computer: TRISTAN
Description:
User Logoff:
User Name: Administrator
Domain: TRISTAN
Logon ID: (0x0,0x37251)
Logon Type: 7
Data: Bytes Words
OK
Cancel
Apply

NTLast


E:\WINNT\System32\cmd.exe
D:\security\forensics\logreview>ntlast -f -r -v
Record Number: 764
ComputerName: TRISTAN
EventID: 529 - Failed Logon Attempt
Time Attempted: - Sat Jun 09 11:29:57am 2001
Details -
ClientName: administrator
ClientMachine: \\EGZ071
ClientDomain: EGZ071
LogonType: Remote
Record Number: 762
ComputerName: TRISTAN
EventID: 529 - Failed Logon Attempt
Time Attempted: - Sat Jun 09 11:29:57am 2001
Details -
ClientName: administrator
ClientMachine: \\EGZ071
ClientDomain: EGZ071
LogonType: Remote
Record Number: 516
ComputerName: TRISTAN
EventID: 529 - Failed Logon Attempt
Time Attempted: - Sat May 19 04:56:36pm 2001

DumpSec – Registry Permission



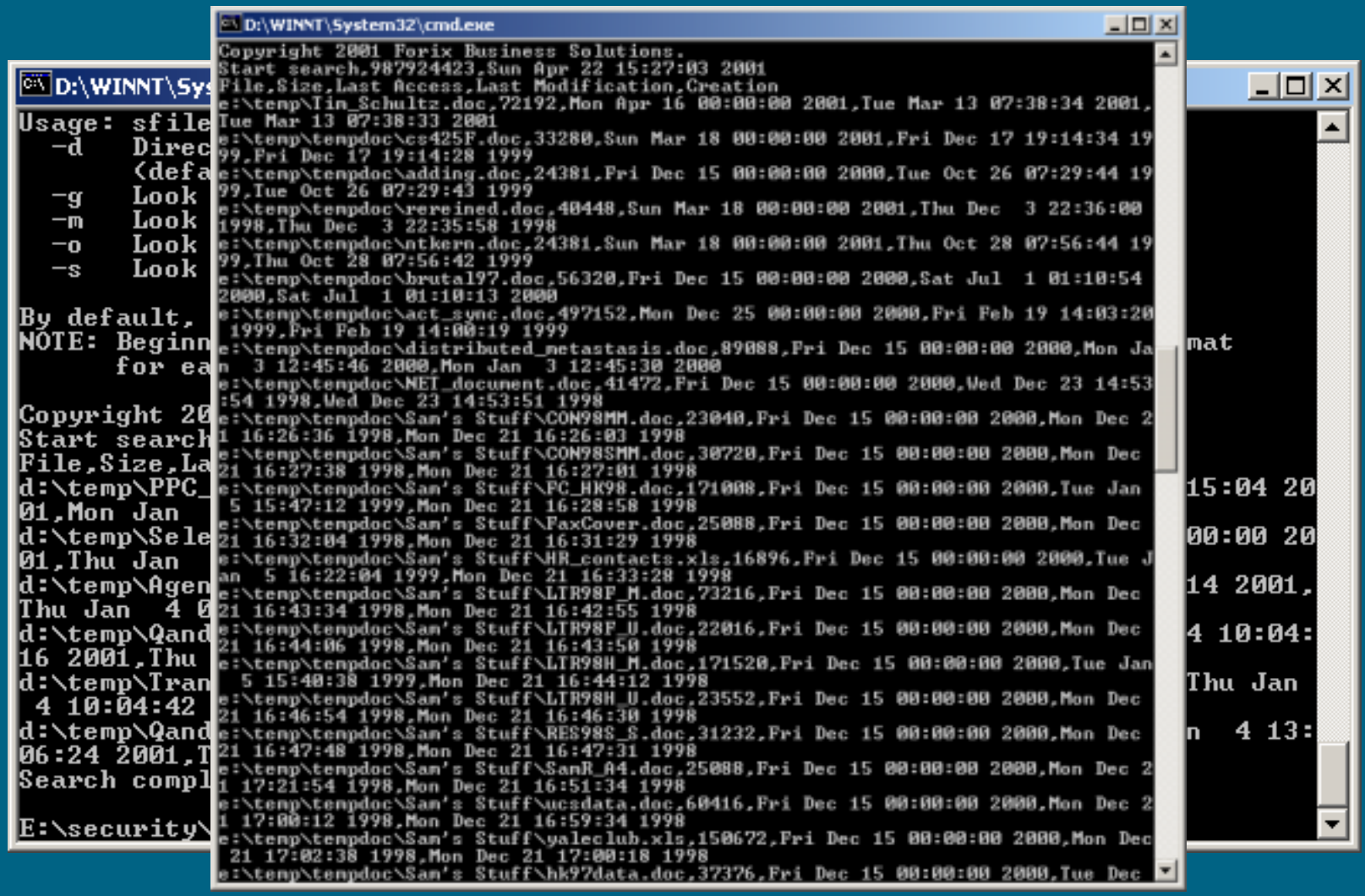
Somarsoft DumpAcl - \\geiersberg

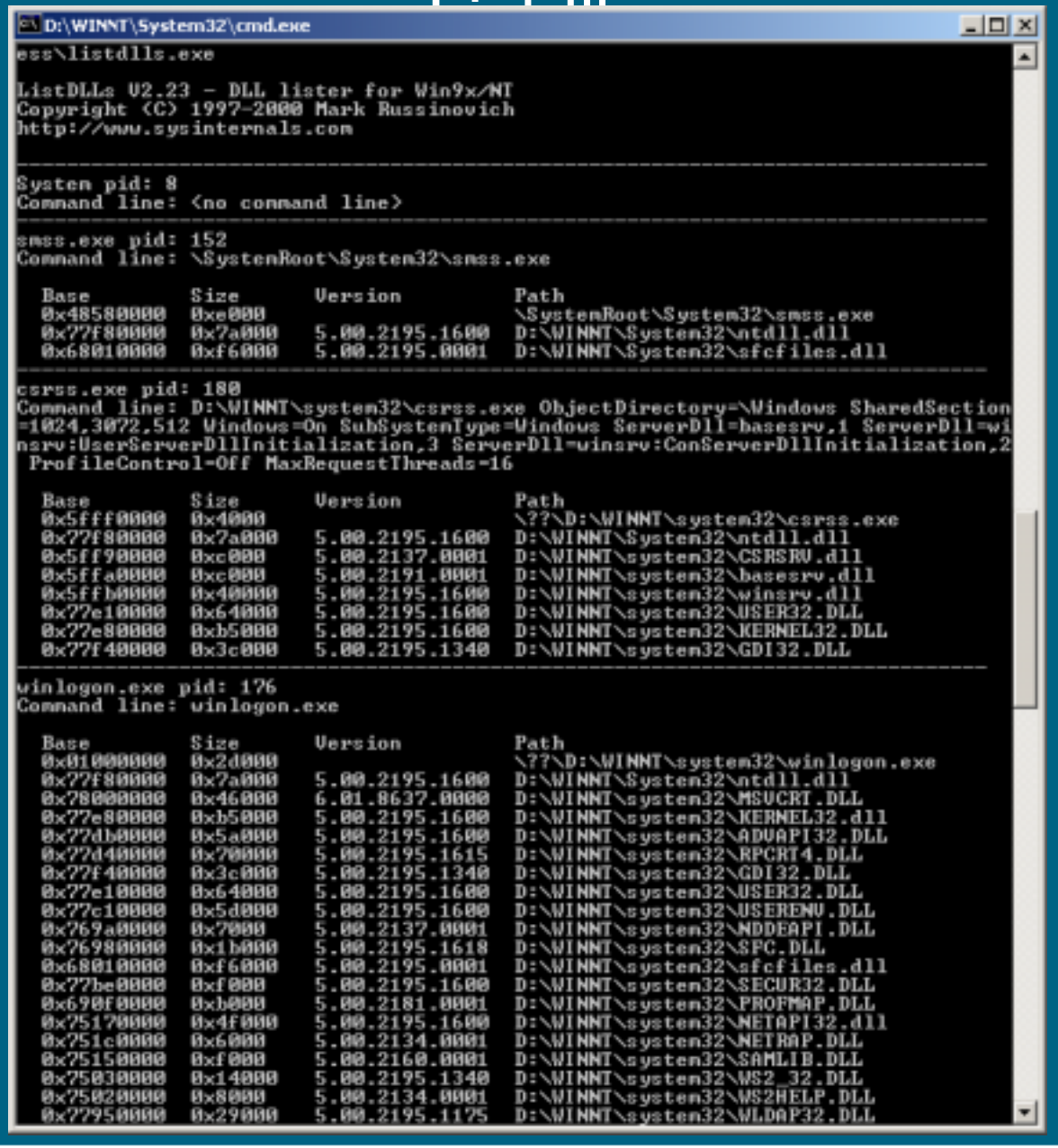
File Edit Search Report View Help

Path (exception keys)	Account	Own	Key	Inheritable
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	SYSTEM	o	all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	Everyone		read(QENR)	read(QENR)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	geiersberg\Administrators		all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	SYSTEM	o	all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	Everyone		read(QENR)	read(QENR)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	geiersberg\Administrators		all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	SYSTEM	o	all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	Everyone		read(QENR)	read(QENR)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	geiersberg\Administrators		all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	SYSTEM	o	all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	Everyone		read(QENR)	read(QENR)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	geiersberg\Administrators		all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	SYSTEM	o	all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	Everyone		read(QENR)	read(QENR)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	geiersberg\Administrators		all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	SYSTEM	o	all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	Everyone		read(QENR)	read(QENR)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	geiersberg\Administrators		all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	SYSTEM	o	all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	Everyone		read(QENR)	read(QENR)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	geiersberg\Administrators		all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	SYSTEM	o	all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	Everyone		read(QENR)	read(QENR)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	geiersberg\Administrators		all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Cc	SYSTEM	o	all	all

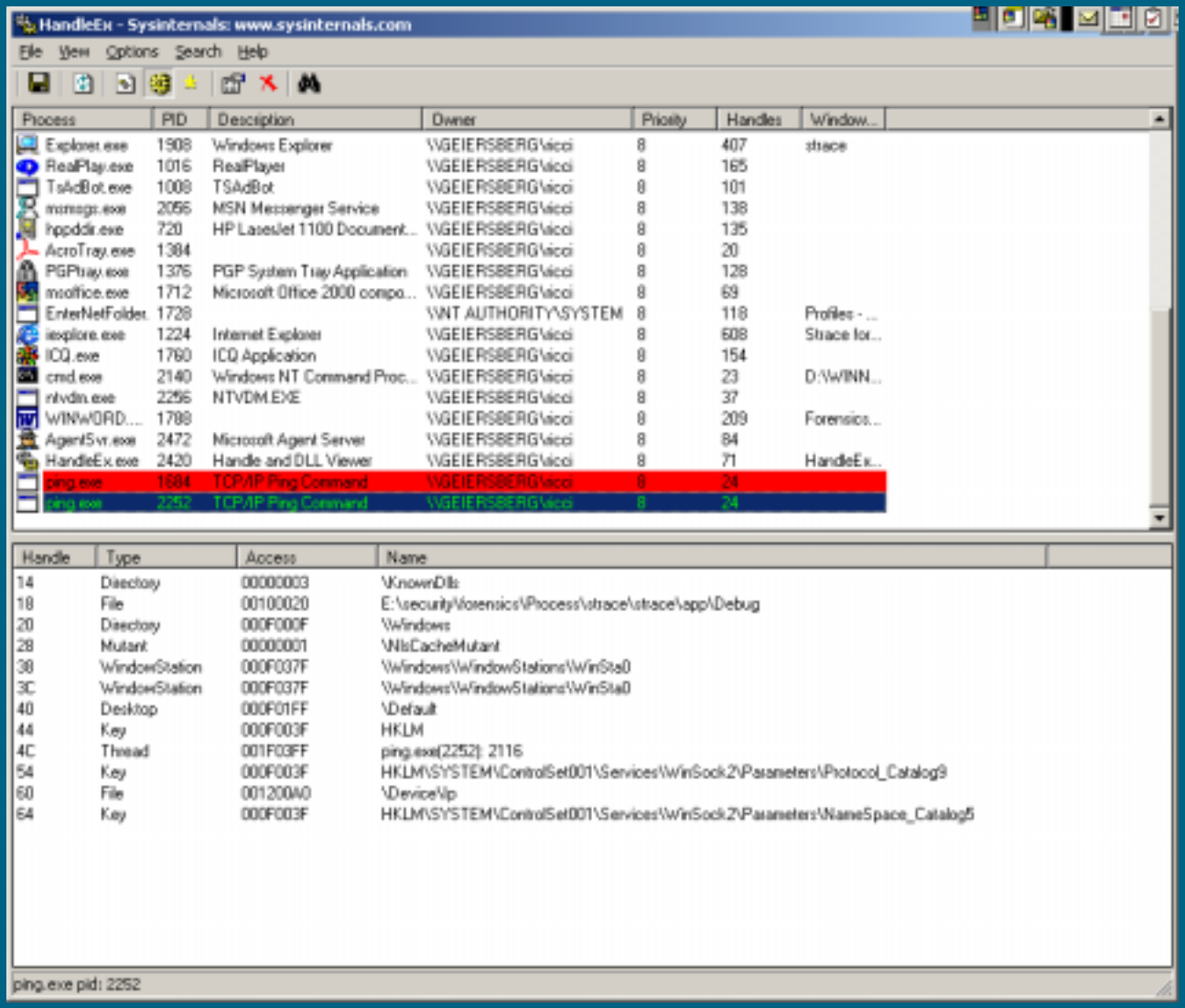
Processed 55849 registry keys 00019

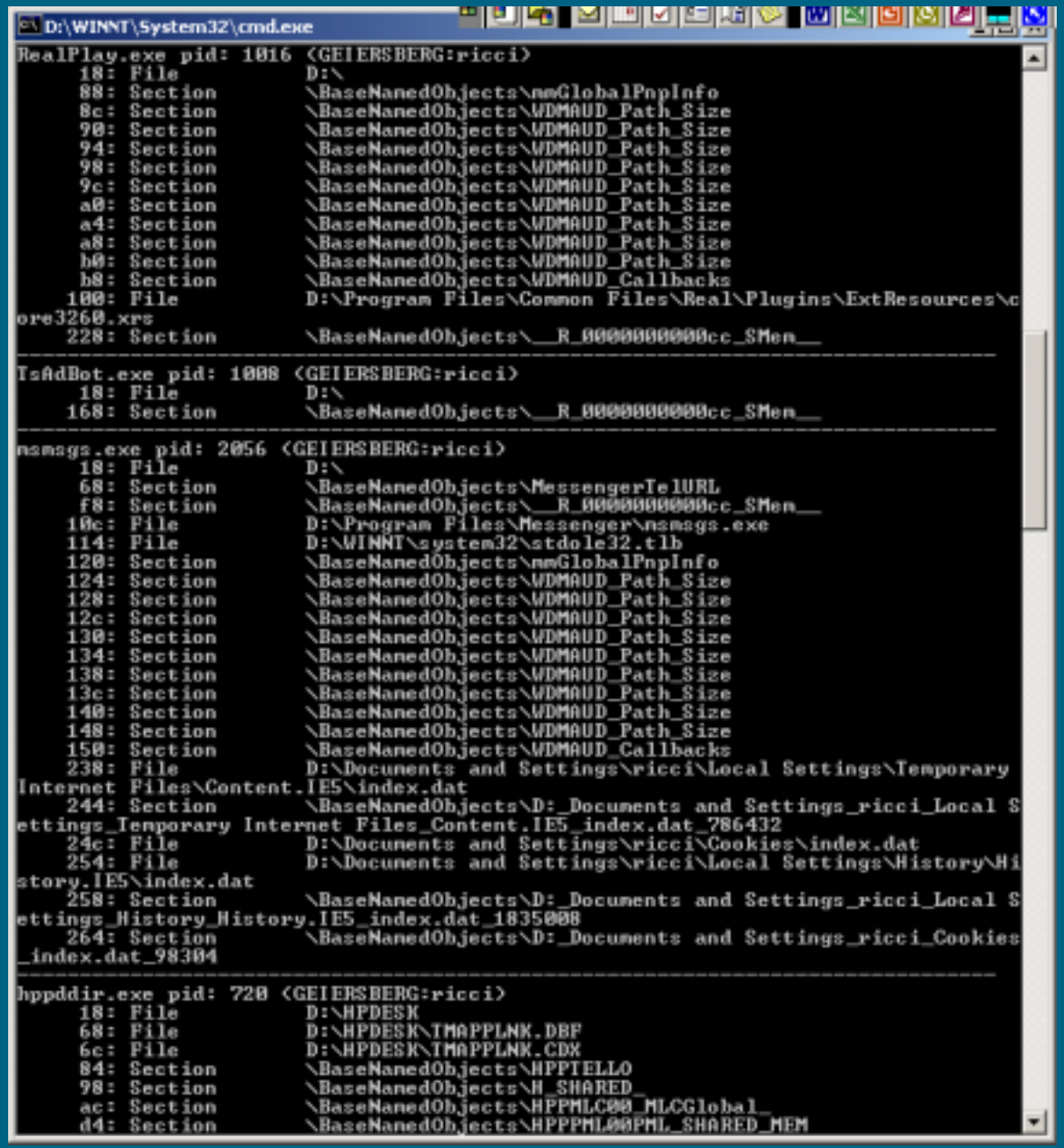
File Access - sfile



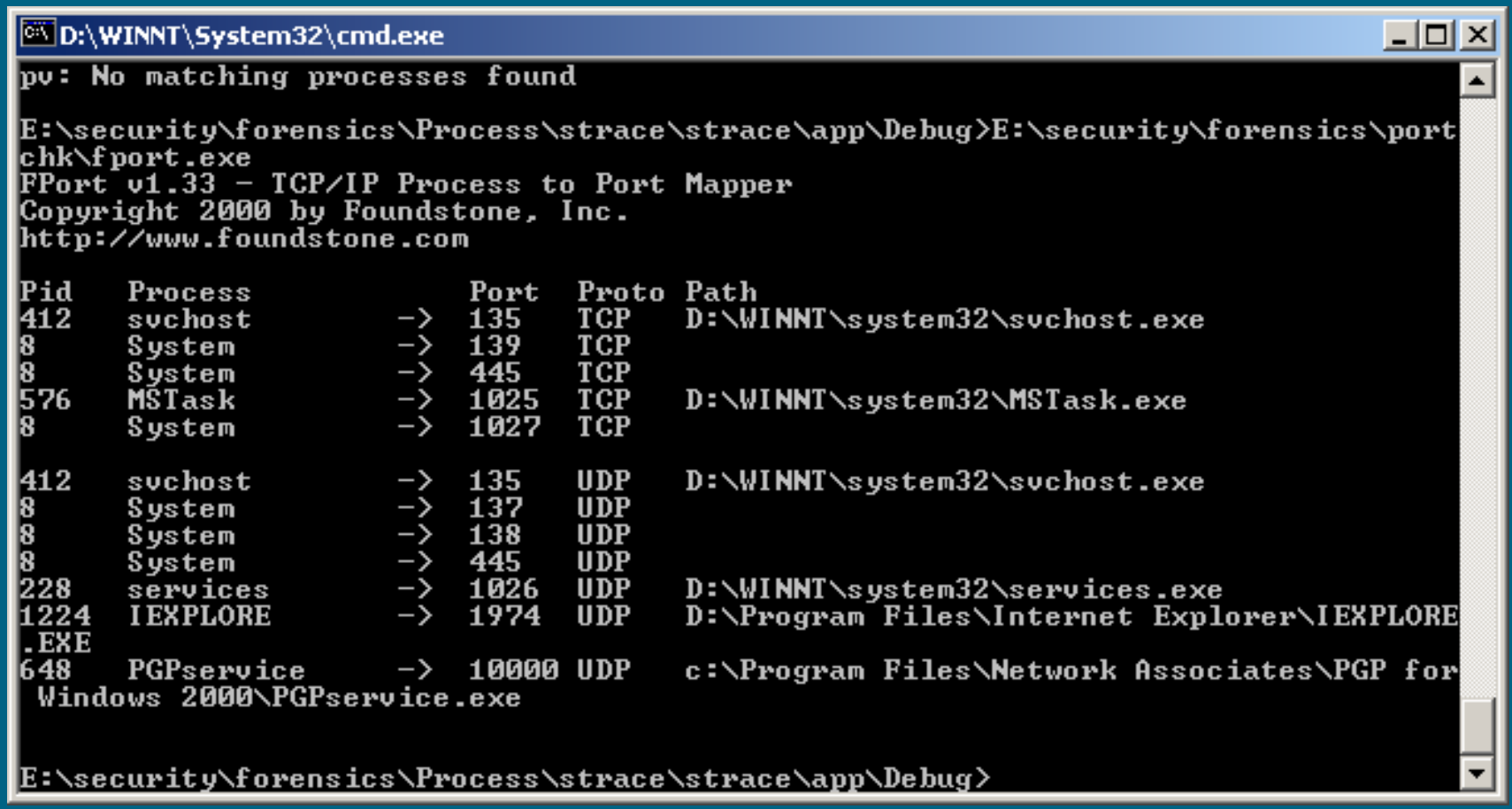

D:\WINNT\System32\cmd.exe
ess\listdlls.exe
ListDLLs V2.23 - DLL lister for Win9x/NT
Copyright (C) 1997-2000 Mark Russinovich
http://www.sysinternals.com
System pid: 8
Command line: <no command line>
smss.exe pid: 152
Command line: \SystemRoot\System32\smss.exe
Base Size Version Path
0x48580000 0xe000 \SystemRoot\System32\smss.exe
0x77f80000 0x7a000 5.00.2195.1600 D:\WINNT\System32\ntdll.dll
0x68010000 0xf6000 5.00.2195.0001 D:\WINNT\System32\sfcfiles.dll
csrss.exe pid: 180
Command line: D:\WINNT\system32\csrss.exe ObjectDirectory=\Windows SharedSection
=1024,3072,512 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=wi
nsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2
ProfileControl=Off MaxRequestThreads=16
Base Size Version Path
0x5fff0000 0x4000 \??\D:\WINNT\system32\csrss.exe
0x77f80000 0x7a000 5.00.2195.1600 D:\WINNT\System32\ntdll.dll
0x5ff90000 0xc000 5.00.2137.0001 D:\WINNT\system32\CSRSRV.dll
0x5ffa0000 0xc000 5.00.2191.0001 D:\WINNT\system32\basesrv.dll
0x5ffb0000 0x40000 5.00.2195.1600 D:\WINNT\system32\winsrv.dll
0x77e10000 0x64000 5.00.2195.1600 D:\WINNT\system32\USER32.DLL
0x77e80000 0xb5000 5.00.2195.1600 D:\WINNT\system32\KERNEL32.DLL
0x77f40000 0x3c000 5.00.2195.1340 D:\WINNT\system32\GDI32.DLL
winlogon.exe pid: 176
Command line: winlogon.exe
Base Size Version Path
0x01000000 0x2d000 \??\D:\WINNT\system32\winlogon.exe
0x77f80000 0x7a000 5.00.2195.1600 D:\WINNT\System32\ntdll.dll
0x78000000 0x46000 6.01.8637.0000 D:\WINNT\system32\MSVCRT.DLL
0x77e80000 0xb5000 5.00.2195.1600 D:\WINNT\system32\KERNEL32.dll
0x77db0000 0x5a000 5.00.2195.1600 D:\WINNT\system32\ADVAPI32.DLL
0x77d40000 0x70000 5.00.2195.1615 D:\WINNT\system32\RPCRT4.DLL
0x77f40000 0x3c000 5.00.2195.1340 D:\WINNT\system32\GDI32.DLL
0x77e10000 0x64000 5.00.2195.1600 D:\WINNT\system32\USER32.DLL
0x77c10000 0x5d000 5.00.2195.1600 D:\WINNT\system32\USERENV.DLL
0x769a0000 0x7000 5.00.2137.0001 D:\WINNT\system32\NDDEAPI.DLL
0x76980000 0x1b000 5.00.2195.1618 D:\WINNT\system32\SFC.DLL
0x68010000 0xf6000 5.00.2195.0001 D:\WINNT\system32\sfcfiles.dll
0x77be0000 0xf000 5.00.2195.1600 D:\WINNT\system32\SECUR32.DLL
0x690f0000 0xb000 5.00.2181.0001 D:\WINNT\system32\PROFMAP.DLL
0x75170000 0x4f000 5.00.2195.1600 D:\WINNT\system32\NETAPI32.dll
0x751c0000 0x6000 5.00.2134.0001 D:\WINNT\system32\NETRAP.DLL
0x75150000 0xf000 5.00.2160.0001 D:\WINNT\system32\SAMLIB.DLL
0x75030000 0x14000 5.00.2195.1340 D:\WINNT\system32\WS2_32.DLL
0x75020000 0x8000 5.00.2134.0001 D:\WINNT\system32\WS2HELP.DLL
0x77950000 0x29000 5.00.2195.1175 D:\WINNT\system32\WLDAP32.DLL

Handleex

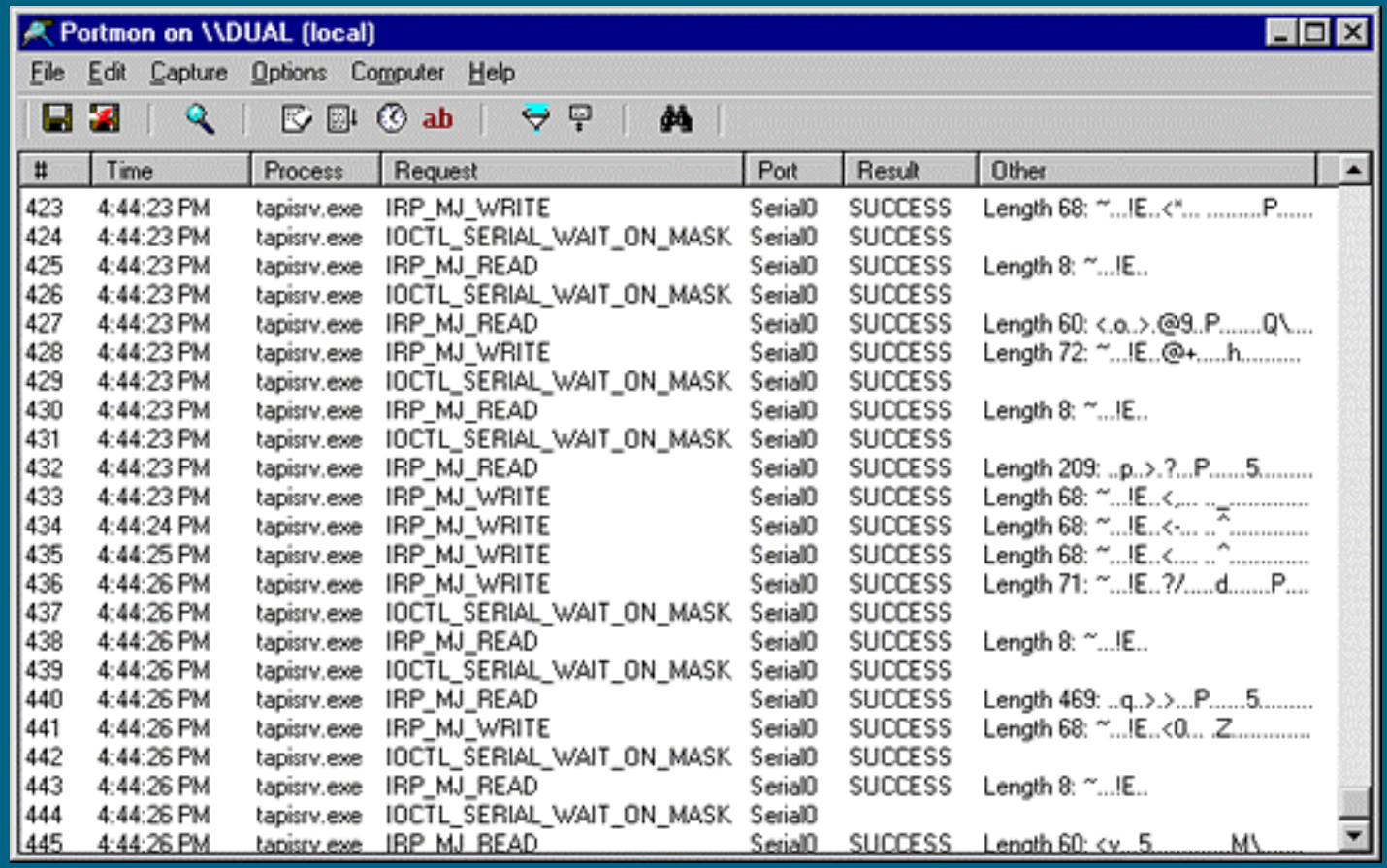

HandleEx - Sysinternals: www.sysinternals.com
File View Options Search Help
Process PID Description Owner Priority Handles Window...
Explorer.exe 1908 Windows Explorer \\GEIERSBERG\icci 8 407 strace
RealPlay.exe 1016 RealPlayer \\GEIERSBERG\icci 8 165
TsAdBot.exe 1008 TSAdBot \\GEIERSBERG\icci 8 101
msmsgs.exe 2056 MSN Messenger Service \\GEIERSBERG\icci 8 138
hppddi.exe 720 HP LaserJet 1100 Document... \\GEIERSBERG\icci 8 135
AcroTray.exe 1384 \\GEIERSBERG\icci 8 20
PGPtray.exe 1376 PGP System Tray Application \\GEIERSBERG\icci 8 128
msoffice.exe 1712 Microsoft Office 2000 compo... \\GEIERSBERG\icci 8 69
EnterNetFolder. 1728 \\NT AUTHORITY\SYSTEM 8 118 Profiles - ...
iexplore.exe 1224 Internet Explorer \\GEIERSBERG\icci 8 608 Strace for...
ICQ.exe 1760 ICQ Application \\GEIERSBERG\icci 8 154
cmd.exe 2140 Windows NT Command Proc... \\GEIERSBERG\icci 8 23 D:\WINN...
ntvdm.exe 2256 NTVDM.EXE \\GEIERSBERG\icci 8 37
WINWORD.... 1788 \\GEIERSBERG\icci 8 209 Forensics...
AgentSvr.exe 2472 Microsoft Agent Server \\GEIERSBERG\icci 8 84
HandleEx.exe 2420 Handle and DLL Viewer \\GEIERSBERG\icci 8 71 HandleEx...
ping.exe 1684 TCP/IP Ping Command \\GEIERSBERG\icci 8 24
ping.exe 2252 TCP/IP Ping Command \\GEIERSBERG\icci 8 24
Handle Type Access Name
14 Directory 00000003 \KnownDlls
18 File 00100020 E:\security\forensics\Process\strace\strace\app\Debug
20 Directory 000F000F \Windows
28 Mutant 00000001 \NlsCacheMutant
38 WindowStation 000F037F \Windows\WindowStations\WinSta0
3C WindowStation 000F037F \Windows\WindowStations\WinSta0
40 Desktop 000F01FF \Default
44 Key 000F003F HKLM
4C Thread 001F03FF ping.exe(2252): 2116
54 Key 000F003F HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\Protocol_Catalog9
60 File 001200A0 \Device\Ip
64 Key 000F003F HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\NameSpace_Catalog5
ping.exe pid: 2252


D:\WINNT\System32\cmd.exe
RealPlay.exe pid: 1016 (GEIERSBERG:ricci)
18: File D:\
88: Section \BaseNanedObjects\nmGlobalPnpInfo
8c: Section \BaseNanedObjects\WDMAUD_Path_Size
90: Section \BaseNanedObjects\WDMAUD_Path_Size
94: Section \BaseNanedObjects\WDMAUD_Path_Size
98: Section \BaseNanedObjects\WDMAUD_Path_Size
9c: Section \BaseNanedObjects\WDMAUD_Path_Size
a0: Section \BaseNanedObjects\WDMAUD_Path_Size
a4: Section \BaseNanedObjects\WDMAUD_Path_Size
a8: Section \BaseNanedObjects\WDMAUD_Path_Size
b0: Section \BaseNanedObjects\WDMAUD_Path_Size
b8: Section \BaseNanedObjects\WDMAUD_Callbacks
100: File D:\Program Files\Common Files\Real\Plugins\ExtResources\core3260.xrs
228: Section \BaseNanedObjects__R_0000000000cc_SMen__
TsAdBot.exe pid: 1008 (GEIERSBERG:ricci)
18: File D:\
168: Section \BaseNanedObjects__R_0000000000cc_SMen__
nsmsgs.exe pid: 2056 (GEIERSBERG:ricci)
18: File D:\
68: Section \BaseNanedObjects\MessengerTelURL
f8: Section \BaseNanedObjects__R_0000000000cc_SMen__
10c: File D:\Program Files\Messenger\nsmsgs.exe
114: File D:\WINNT\system32\stdole32.tlb
120: Section \BaseNanedObjects\nmGlobalPnpInfo
124: Section \BaseNanedObjects\WDMAUD_Path_Size
128: Section \BaseNanedObjects\WDMAUD_Path_Size
12c: Section \BaseNanedObjects\WDMAUD_Path_Size
130: Section \BaseNanedObjects\WDMAUD_Path_Size
134: Section \BaseNanedObjects\WDMAUD_Path_Size
138: Section \BaseNanedObjects\WDMAUD_Path_Size
13c: Section \BaseNanedObjects\WDMAUD_Path_Size
140: Section \BaseNanedObjects\WDMAUD_Path_Size
148: Section \BaseNanedObjects\WDMAUD_Path_Size
150: Section \BaseNanedObjects\WDMAUD_Callbacks
238: File D:\Documents and Settings\ricci\Local Settings\Temporary Internet Files\Content.IE5\index.dat
244: Section \BaseNanedObjects\D:_Documents and Settings_ricci_Local Settings_Temporary Internet Files_Content.IE5_index.dat_786432
24c: File D:\Documents and Settings\ricci\Cookies\index.dat
254: File D:\Documents and Settings\ricci\Local Settings\History\History.IE5\index.dat
258: Section \BaseNanedObjects\D:_Documents and Settings_ricci_Local Settings_History_History.IE5_index.dat_1835008
264: Section \BaseNanedObjects\D:_Documents and Settings_ricci_Cookies_index.dat_98304
hppddir.exe pid: 720 (GEIERSBERG:ricci)
18: File D:\HPDESK
68: File D:\HPDESK\TMAPPLNK.DBF
6c: File D:\HPDESK\TMAPPLNK.CDX
84: Section \BaseNanedObjects\HPPTELLO
98: Section \BaseNanedObjects\H_SHARED_
ac: Section \BaseNanedObjects\HPPMLC00_MLCGlobal_
d4: Section \BaseNanedObjects\HPPPML00PML_SHARED_MEM

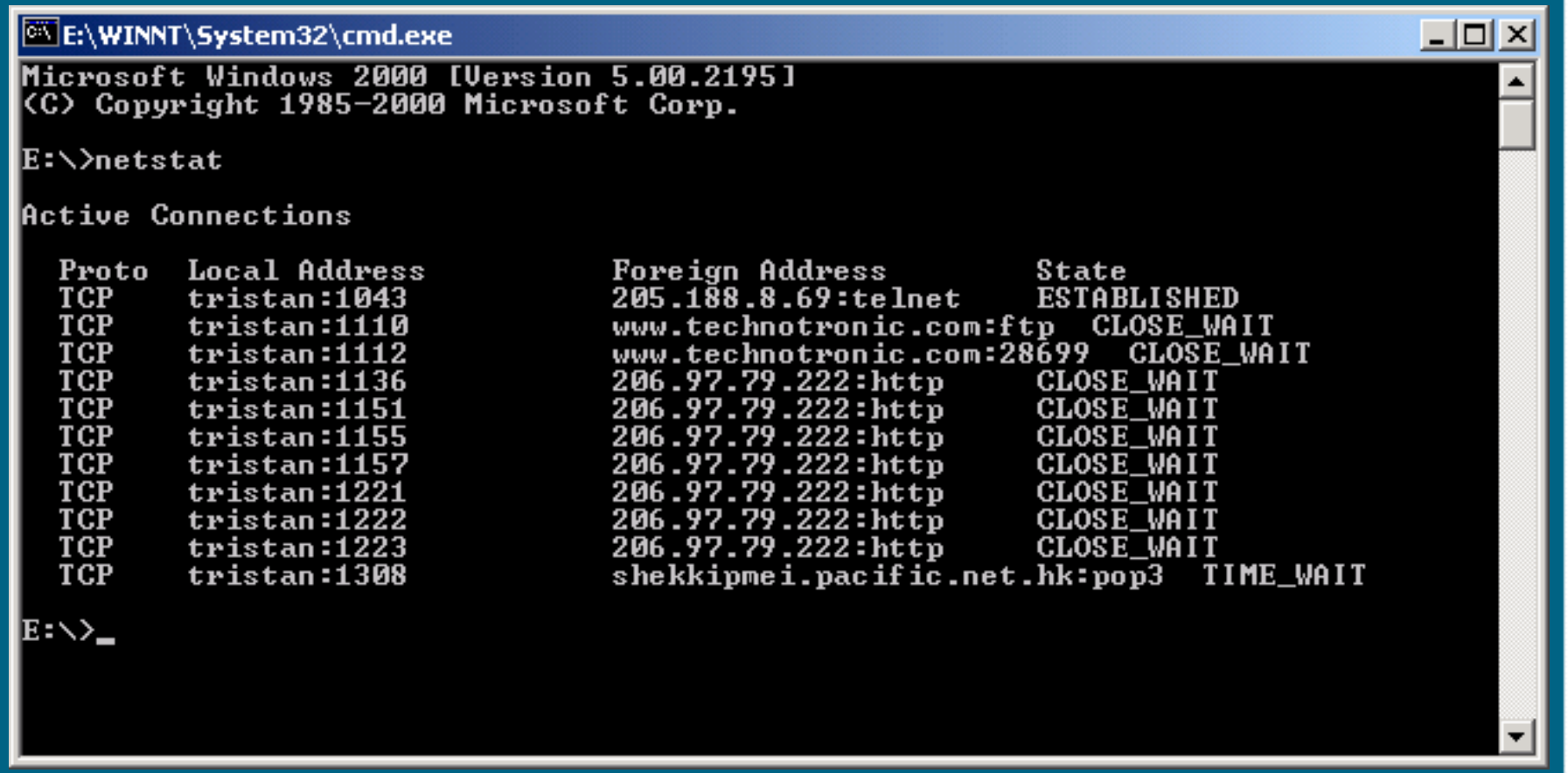
Fport


D:\WINNT\System32\cmd.exe
pv: No matching processes found
E:\security\forensics\Process\strace\strace\app\Debug>E:\security\forensics\portchk\fport.exe
FPort v1.33 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com
Pid Process Port Proto Path
412 svchost -> 135 TCP D:\WINNT\system32\svchost.exe
8 System -> 139 TCP
8 System -> 445 TCP
576 MSTask -> 1025 TCP D:\WINNT\system32\MSTask.exe
8 System -> 1027 TCP
412 svchost -> 135 UDP D:\WINNT\system32\svchost.exe
8 System -> 137 UDP
8 System -> 138 UDP
8 System -> 445 UDP
228 services -> 1026 UDP D:\WINNT\system32\services.exe
1224 IEXPLORE -> 1974 UDP D:\Program Files\Internet Explorer\IEXPLORE.EXE
648 PGPservice -> 10000 UDP c:\Program Files\Network Associates\PGP for Windows 2000\PGPservice.exe
E:\security\forensics\Process\strace\strace\app\Debug>

PortMon


Portmon on \\DUAL (local)
File Edit Capture Options Computer Help
Time Process Request Port Result Other
423 4:44:23 PM tapisrv.exe IRP_MJ_WRITE Serial0 SUCCESS Length 68: ~...!E..<"... .....P.....
424 4:44:23 PM tapisrv.exe IOCTL_SERIAL_WAIT_ON_MASK Serial0 SUCCESS
425 4:44:23 PM tapisrv.exe IRP_MJ_READ Serial0 SUCCESS Length 8: ~...!E..
426 4:44:23 PM tapisrv.exe IOCTL_SERIAL_WAIT_ON_MASK Serial0 SUCCESS
427 4:44:23 PM tapisrv.exe IRP_MJ_READ Serial0 SUCCESS Length 60: <.o..>.@9..P.....Q\...
428 4:44:23 PM tapisrv.exe IRP_MJ_WRITE Serial0 SUCCESS Length 72: ~...!E..@+.....h.....
429 4:44:23 PM tapisrv.exe IOCTL_SERIAL_WAIT_ON_MASK Serial0 SUCCESS
430 4:44:23 PM tapisrv.exe IRP_MJ_READ Serial0 SUCCESS Length 8: ~...!E..
431 4:44:23 PM tapisrv.exe IOCTL_SERIAL_WAIT_ON_MASK Serial0 SUCCESS
432 4:44:23 PM tapisrv.exe IRP_MJ_READ Serial0 SUCCESS Length 209: ..p..>.?...P.....5.....
433 4:44:23 PM tapisrv.exe IRP_MJ_WRITE Serial0 SUCCESS Length 68: ~...!E..<,... ..._.....
434 4:44:24 PM tapisrv.exe IRP_MJ_WRITE Serial0 SUCCESS Length 68: ~...!E..<-... ..^.....
435 4:44:25 PM tapisrv.exe IRP_MJ_WRITE Serial0 SUCCESS Length 68: ~...!E..<.... ..^.....
436 4:44:26 PM tapisrv.exe IRP_MJ_WRITE Serial0 SUCCESS Length 71: ~...!E..?/.....d.....P....
437 4:44:26 PM tapisrv.exe IOCTL_SERIAL_WAIT_ON_MASK Serial0 SUCCESS
438 4:44:26 PM tapisrv.exe IRP_MJ_READ Serial0 SUCCESS Length 8: ~...!E..
439 4:44:26 PM tapisrv.exe IOCTL_SERIAL_WAIT_ON_MASK Serial0 SUCCESS
440 4:44:26 PM tapisrv.exe IRP_MJ_READ Serial0 SUCCESS Length 469: ..q..>.>...P.....5.....
441 4:44:26 PM tapisrv.exe IRP_MJ_WRITE Serial0 SUCCESS Length 68: ~...!E..<0... .Z.....
442 4:44:26 PM tapisrv.exe IOCTL_SERIAL_WAIT_ON_MASK Serial0 SUCCESS
443 4:44:26 PM tapisrv.exe IRP_MJ_READ Serial0 SUCCESS Length 8: ~...!E..
444 4:44:26 PM tapisrv.exe IOCTL_SERIAL_WAIT_ON_MASK Serial0
445 4:44:26 PM tapisrv.exe IRP_MJ_READ Serial0 SUCCESS Length 60: <v...5.....M\.....

Network status check



Step 3 - Investigation

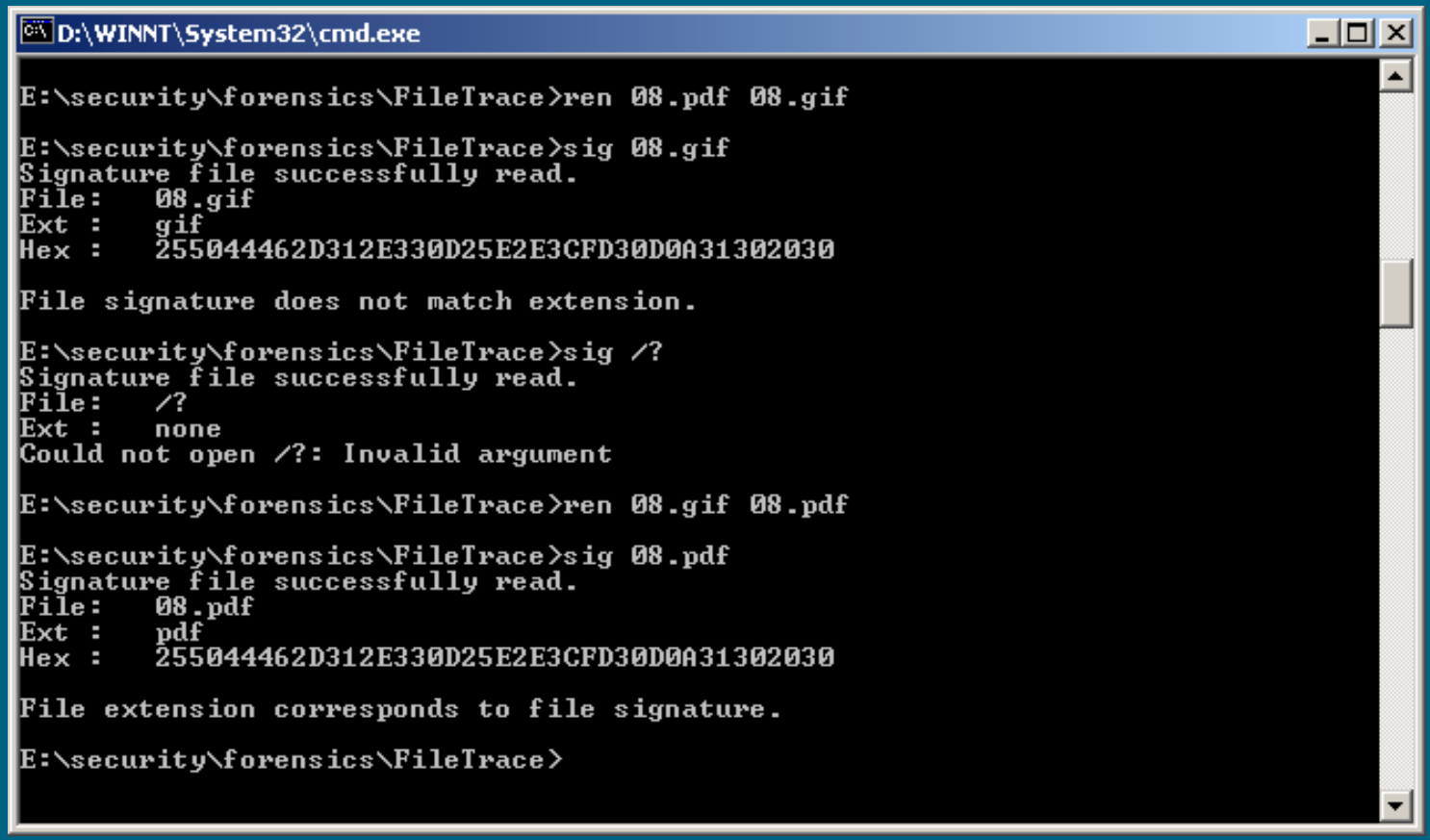
- Identify the “first handle” of the case
- Obtain volatile data
- Review logs, system setting files
- Determine the possible source of evidence
  - Network connection in router, firewall
  - Sniffer and IDS packet captured
  - System, Web and FTP log files
  - Trace of CPU usage, process running on the machine
  - Possible hidden files, deleted files and updated files
  - Open ports, services, files
  - Email message header
  - Possible installation of root kits

Step 3 - Further Investigation

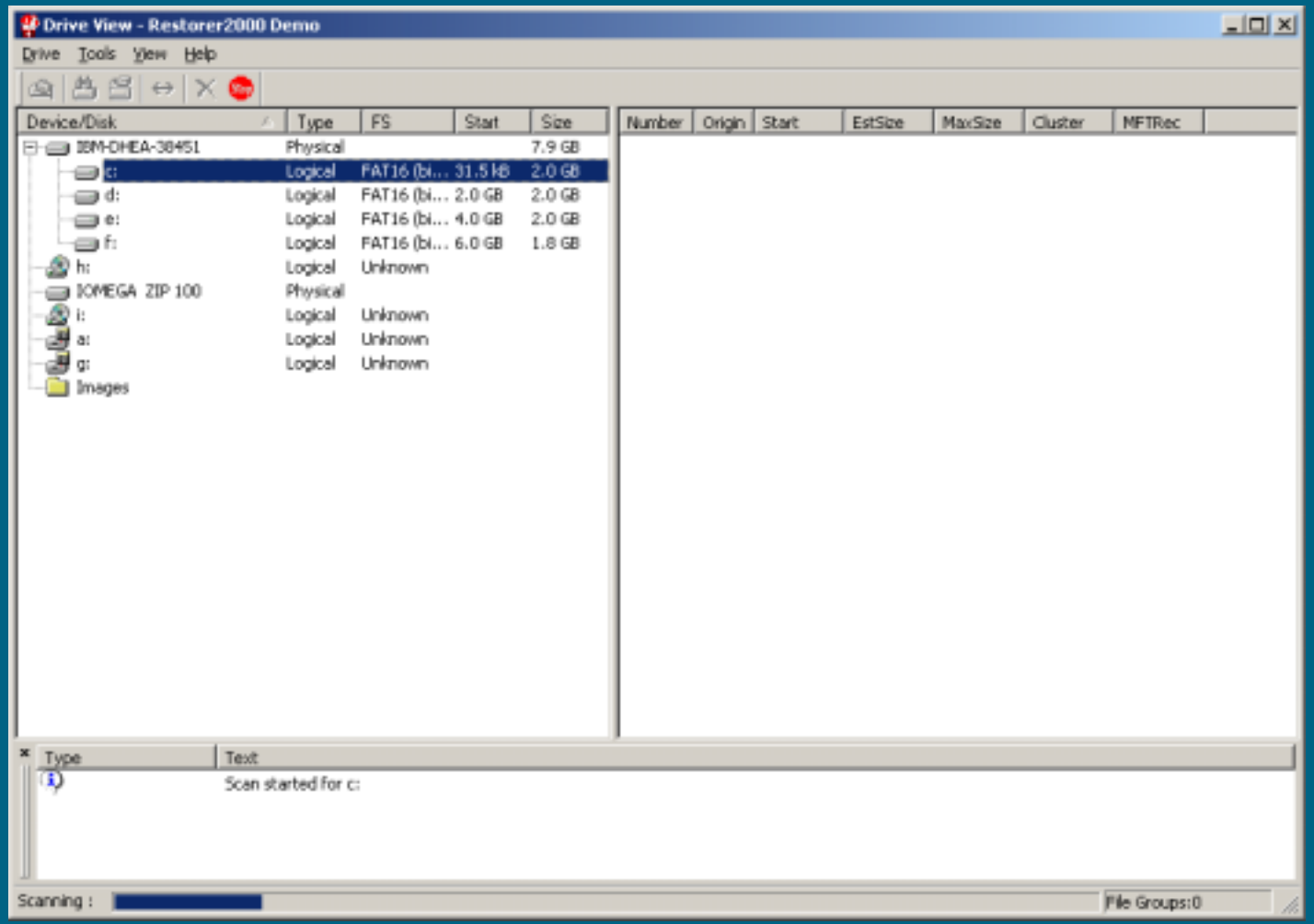
Further Investigation

- Check where is the attack from
- Determine the suspected process using ps, lsof
- Capturing process memory using core dump (in Unix, gcore PID)
- Capture Process information
- Examine the core using strings
- Determine backdoor
- Watching process action
- Undelete files
- Search the slack space
- Review pagefiles.sys, Recycle Bin, Printer spool
- Search hidden information in picture and document

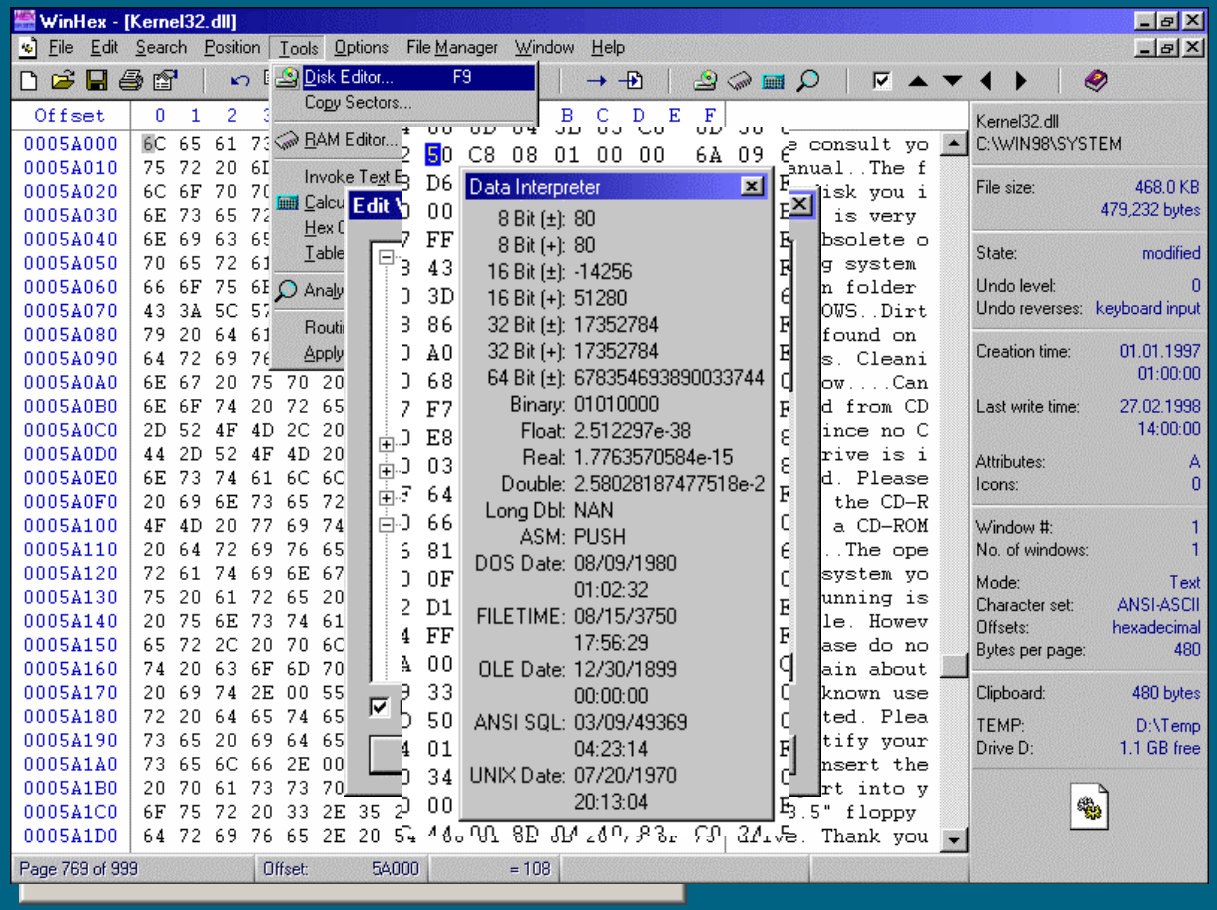
File handling tools - sig



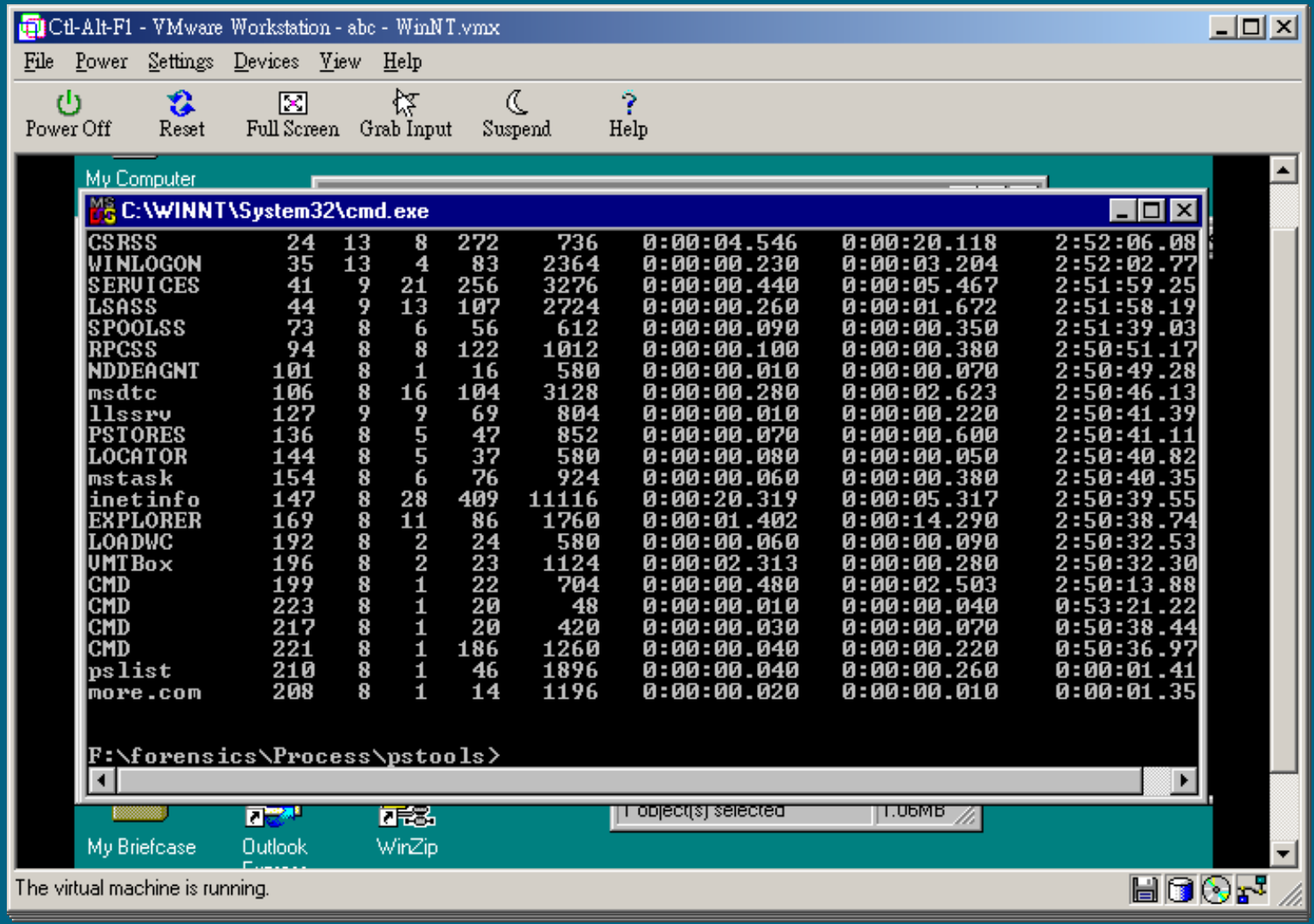
Undelete


Drive View - Restorer2000 Demo
Drive Tools View Help
Device/Disk Type FS Start Size
IBM-DHEA-38451 Physical 7.9 GB
c: Logical FAT16 (bi... 31.5 kB 2.0 GB
d: Logical FAT16 (bi... 2.0 GB 2.0 GB
e: Logical FAT16 (bi... 4.0 GB 2.0 GB
f: Logical FAT16 (bi... 6.0 GB 1.8 GB
h: Logical Unknown
IOMEGA ZIP 100 Physical
i: Logical Unknown
a: Logical Unknown
g: Logical Unknown
Images
Number Origin Start EstSize MaxSize Cluster MFTRec
Type Text
Scan started for c:
Scanning :
File Groups:0

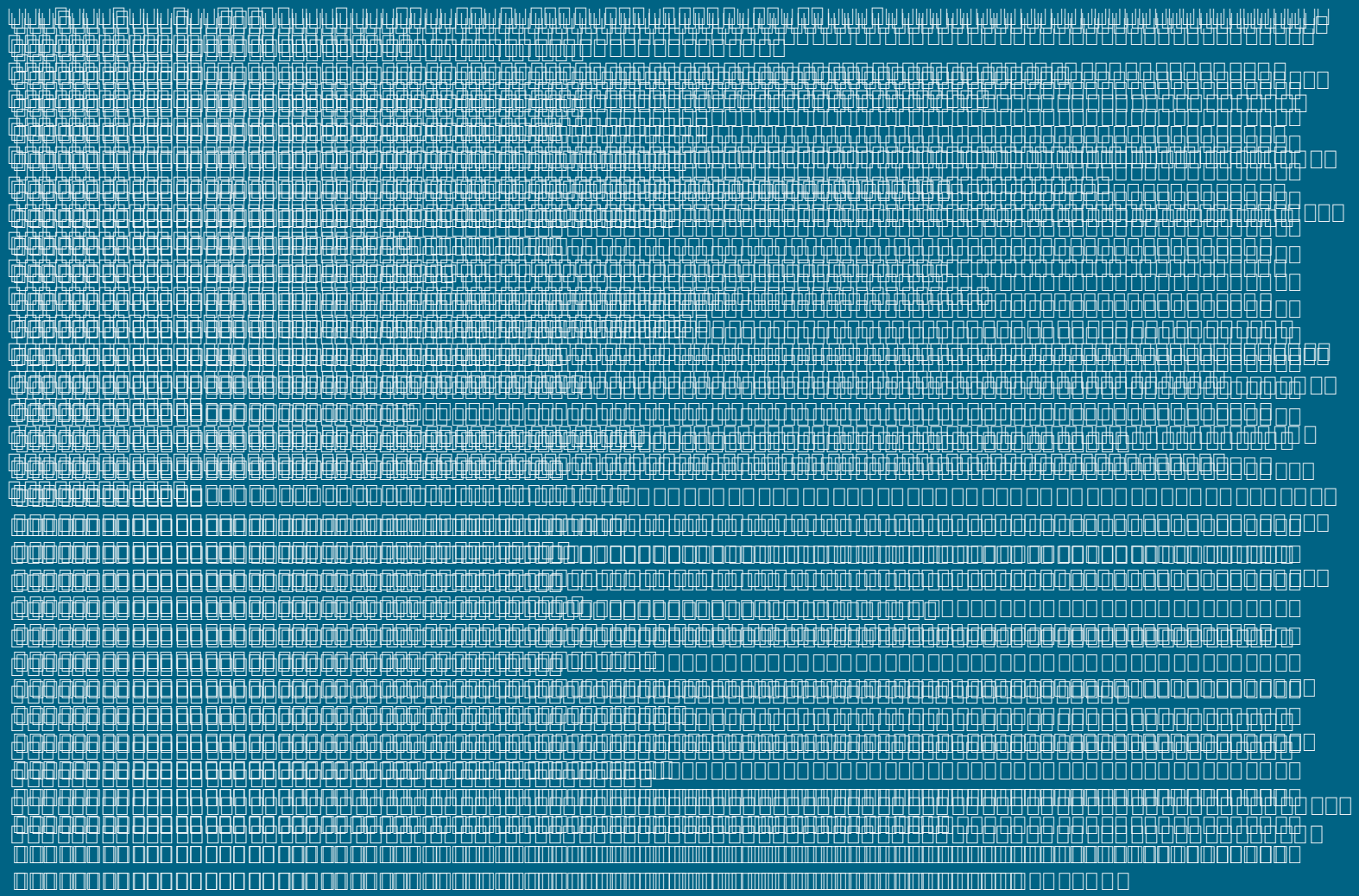
WinHex


WinHex - [Kernel32.dll]
File Edit Search Position Tools Options File Manager Window Help
Disk Editor... F9
Copy Sectors...
RAM Editor...
Invoke Text E
Calcu
Hex
Table
Analy
Routi
Apply
Edit
Data Interpreter
8 Bit (±): 80
8 Bit (+): 80
16 Bit (±): -14256
16 Bit (+): 51280
32 Bit (±): 17352784
32 Bit (+): 17352784
64 Bit (±): 678354693890033744
Binary: 01010000
Float: 2.512297e-38
Real: 1.7763570584e-15
Double: 2.58028187477518e-2
Long Dbl: NAN
ASM: PUSH
DOS Date: 08/09/1980 01:02:32
FILETIME: 08/15/3750 17:56:29
OLE Date: 12/30/1899 00:00:00
ANSI SQL: 03/09/49369 04:23:14
UNIX Date: 07/20/1970 20:13:04
Kernel32.dll
C:\WIN98\SYSTEM
File size: 468.0 KB 479,232 bytes
State: modified
Undo level: 0
Undo reverses: keyboard input
Creation time: 01.01.1997 01:00:00
Last write time: 27.02.1998 14:00:00
Attributes: A
Icons: 0
Window #: 1
No. of windows: 1
Mode: Text
Character set: ANSI-ASCII
Offsets: hexadecimal
Bytes per page: 480
Clipboard: 480 bytes
TEMP: D:\Temp
Drive D: 1.1 GB free
Page 769 of 999
Offset: 5A000
= 108

Investigation of victim machine



Investigation of log files

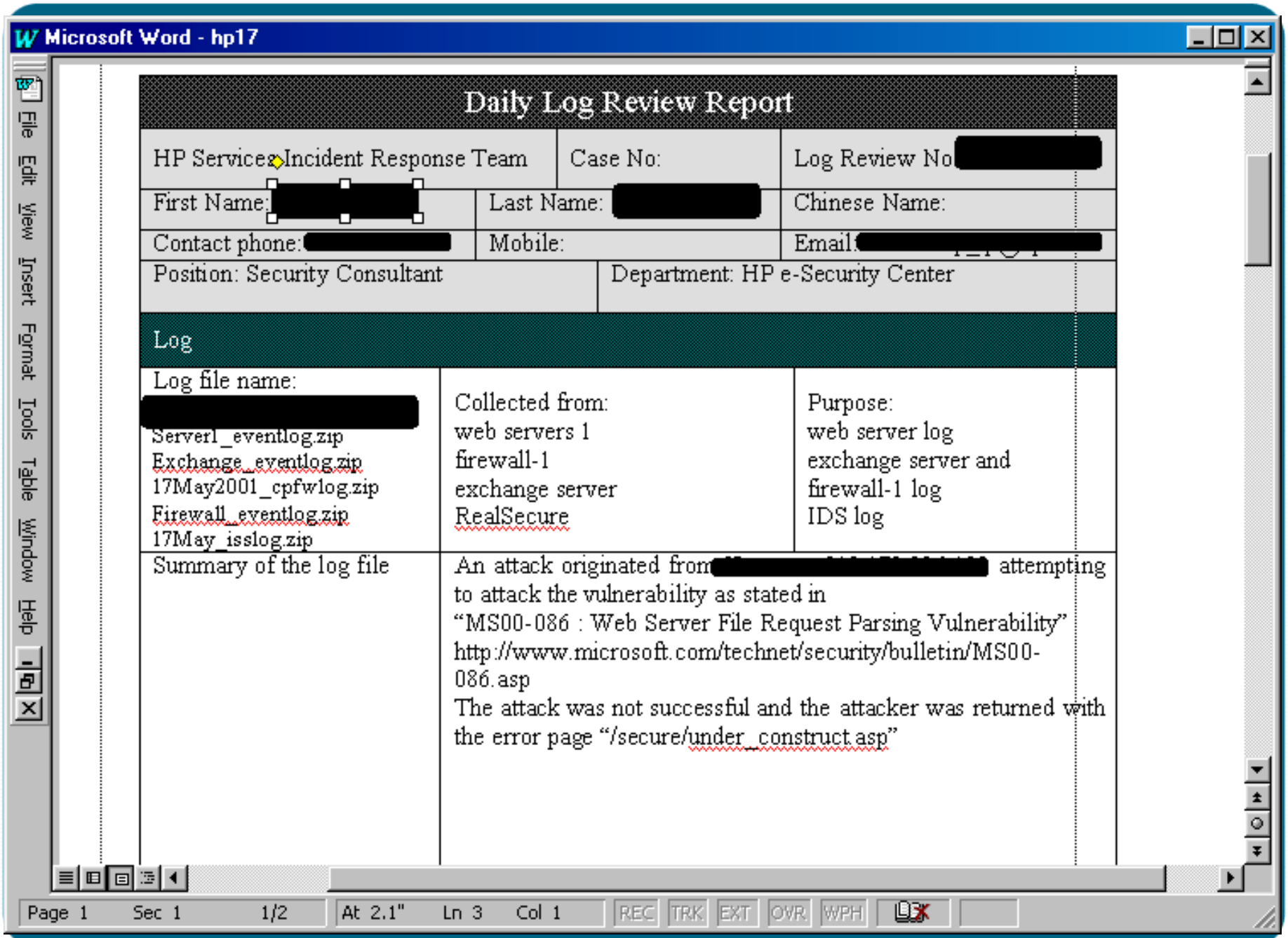


Step 4 - Summarize and Presentation

- Summarize the cause and source of the incident
- Construct the chronological map of the events
- Presentation of the investigation procedures and findings
- Determine the explanations of the case

Sample Logs from real case

```
sp 404;http://10.2.1.2/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -
sp 404;http://10.2.1.2/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -
sp 404;http://10.2.1.2/scripts/..%c1%pc../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -
sp 404;http://10.2.1.2/scripts/..%c0%9v../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -
sp 404;http://10.2.1.2/scripts/..%c0%qf../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -
sp 404;http://10.2.1.2/scripts/..%c1%8s../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -
sp 404;http://10.2.1.2/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -
sp 404;http://10.2.1.2/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -
sp 404;http://10.2.1.2/scripts/..%c1%af../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -
sp 404;http://10.2.1.2/scripts/..%e0%80%af../winnt/system32/cmd.exe?/c+dir 200 0 0 69 80 HTTP/1.0 -
sp 404;http://10.2.1.2/scripts/..%f0%80%80%af../winnt/system32/cmd.exe?/c+dir 200 0 0 72 80 HTTP/1
sp 404;http://10.2.1.2/scripts/..%f8%80%80%80%af../winnt/system32/cmd.exe?/c+dir 200 0 0 75 80 HT
sp 404;http://10.2.1.2/scripts/..%fc%80%80%80%80%af../winnt/system32/cmd.exe?/c+dir 200 0 0 78 8
sp 404;http://10.2.1.2/msadc/..%e0%80%af../..%e0%80%af../..%e0%80%af../winnt/system32/cmd.exe?/
```


Microsoft Word - hp17
File Edit View Insert Format Tools Table Window Help
Daily Log Review Report
HP Services Incident Response Team
Case No:
Log Review No
First Name:
Last Name:
Chinese Name:
Contact phone:
Mobile:
Email:
Position: Security Consultant
Department: HP e-Security Center
Log
Log file name:
Server1_eventlog.zip
Exchange_eventlog.zip
17May2001_cpfw1log.zip
Firewall_eventlog.zip
17May_isslog.zip
Collected from:
web servers 1
firewall-1
exchange server
RealSecure
Purpose:
web server log
exchange server and
firewall-1 log
IDS log
Summary of the log file
An attack originated from attempting to attack the vulnerability as stated in
"MS00-086 : Web Server File Request Parsing Vulnerability"
http://www.microsoft.com/technet/security/bulletin/MS00-086.asp
The attack was not successful and the attacker was returned with the error page "/secure/under_construct.asp"
Page 1 Sec 1 1/2 At 2.1" Ln 3 Col 1 REC TRK EXT OVR WPH

Conclusion

- Vulnerabilities and bugs are always with you
- No security vendors can eliminate them all
- Incident Handling and Forensics Investigation Service is one of the key Solutions in Security Risk Management
- Everyone can participate in Cyber-Investigation
- Early identification and containment of cyber-crime is helpful to the Cyber Crime Investigation

Thank you.

HP e-Security Center

- Tel: 25997126

Ricci Ieong

- Tel: 25994717
  Fax: 25069259
  email: ricci-sc_ieong@hp.com

Vincent Ip

- Tel: 25994224
  Fax: 25069259
  email: vincent-tp_ip@hp.com