Linux and the 6 W's of Computer Forensics

James G. McIntyre

Senior Consultant
McIntyre & Associates, Inc.
jim@mcintyresecurity.com

Overview

- Forensics
- Computer Forensics
- Why would I use it ?
- Legal vs Non-Legal
  (Court of Law)
- Tools

Forensics Defined

- **Dictionary.com -**
  - The art or study of formal debate; argumentation.
  - The use of science and technology to investigate and establish facts in criminal or civil courts of law.

- **Library.Thinkquest.org -**
  - Forensic science is any science used for the purposes of the law, and therefore provides impartial scientific evidence for use in the courts of law, and in a criminal investigation and trial.
  - Forensic science is a multidisciplinary subject, drawing principally from chemistry and biology, but also from physics, geology, psychology, social science, etc.

“**Computer forensics** involves the **preservation, identification, extraction,** and **documentation** of computer evidence stored in the form of magnetically encoded information.”

Warren Kruse III

Computer Forensic Services, LLC

“The application of computer investigation and analysis techniques in the interest of determining potential *legal evidence*.”

Judd Robbins

CIO, ABC Company

Forensic Analysis Framework

- Identification
- Preservation
  - Approach strategy *
  - Preparation *
- Collection
- Examination
- Analysis
- Presentation
  - Action *

* Proposed change

Forensic Analysis Framework

- Identification – That a problem exists.
  - “Houston, we have a problem”
  - Tripwire
  - End User
  - Customer
  - Sys-Admin 12 time zones away

Forensic Analysis Framework

- Preservation of crime scene
  - Do not allow to be further modified
  - 100 users on production system
  - 3 Terabyte SANS
  - Start “Chain of Custody”

Forensic Analysis Framework

- Approach Strategy – Outcome based analysis ?
  - Legal vs Non-legal
  - Corporate
  - Government
  - International

Proposed

Forensic Analysis Framework

- Preparation
  - Forensics work station built
  - Hard drives pre-formatted
  - Tools loaded
  - Trained on use of tools & process

Proposed

Forensic Analysis Framework

- Identification
- Preservation
  - Approach strategy *
  - Preparation *
- Collection
- Examination
- Analysis
- Presentation
  - Action *

* Proposed change

WWW.DFRWS.ORG

HP WORLD 2004
Solutions and Technology Conference & Expo

Forensic Analysis Framework

- Collection of evidence
  - Hard drives, memory drives, diskettes, tapes
  - Cell phones, smart phones, digital cameras
  - Xbox
  - Hard copy reports, notes
  - Computers
  - Bag & Tag

Forensic Analysis Framework

- Examination of all the evidence
  - Use established forensic tools
  - Document everything

Forensic Analysis Framework

- Analysis
  - Given all the collected data what does it mean ?
  - Who did what where when how and why?

Forensic Analysis Framework

- Identification
- Preservation
  - Approach strategy *
  - Preparation *
- Collection
- Examination
- Analysis
- Presentation
  - Action *

* Proposed change

Forensic Analysis Framework

- Presentation - Final analysis of collected evidence
  - Intended audience ?
  - Hope you documented everything !

Forensic Analysis Framework

- Action – What do you do with the results ?
  - Corporate – fire the bastard !
  - Government – make him disappear !
  - Law Enforcement – fry him !

Proposed

Overview

- Forensics
- Computer Forensics
- What is it ?
- Why would I use it ?
- Legal vs Non-Legal
- Tools

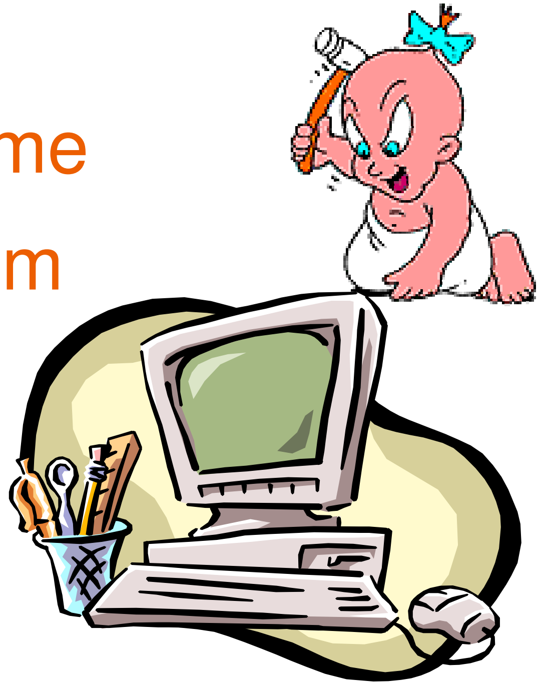
Possible uses for Forensics ?

- Questionable computer use by an employee
- Fraud
- Espionage
- Harassment
- Porn
- Law Enforcement

HP WORLD 2004
Solutions and Technology Conference & Expo

Possible uses for Forensics ?

- Embezzlement
- Terrorism
- Divorce
- Unexplained system down time
- Possible compromised system



Overview

- Forensics
- Computer Forensics
- What is it ?
- Why would I use it ?
- Legal vs Non-Legal
- Tools

HP WORLD 2004
Solutions and Technology Conference & Expo

Determine outcome of Examination

- Legal
  (Court of Law)

- Non-legal

Acquiring Evidence for a Court of Law

- Involve corporate attorneys immediately
- Talk with a Professional Forensics Company
- Get assistance as soon as possible
- Try to leave all equipment untouched
- Restrict Access to all equipment
- Start the documentation for the Chain of Custody.

“6 W’s – Chain of Custody”

- What equipment (evidence) is involved ?
- Why was the machine in use ?
- When did they have access to the equipment ?
- Who has had access to the equipment ?
- Where did it come from and where has it been stored ?
- Woh - How did they do that ?

Forensics Expert Should Provide

- Utilize accepted forensic computer tools
- Perform an examination that is capable of scrutiny in a court room
- Chain of custody
- Reproducible results
- Speaking ability to testify in court of law

Computer evidence provided for more than 30 years in a court of law

- US Federal Rules of Evidence
- Economic Espionage Act
- Electronic Communications Privacy Act
- Computer Security Act
- Federal Guidelines for Search & Seizing Computers
- US Patriot Act
- Sarbanes-Oxley Act
- Rules for the Collection of Evidence
- Federal Computer Fraud and Abuse Act

Parts is Parts-
A Forensic Examination/Analysis

- Protect the crime scene
- Timely analysis
- Recover deleted files
- Provide access to hidden files, temp & swap files, encrypted or password protected
- Analyze all storage media
- Locate files stored in unusual locations
- Build a time line of what happened
- Document the examination process & results

HP WORLD 2004
Solutions and Technology Conference & Expo

A Forensic Analysis Workstation

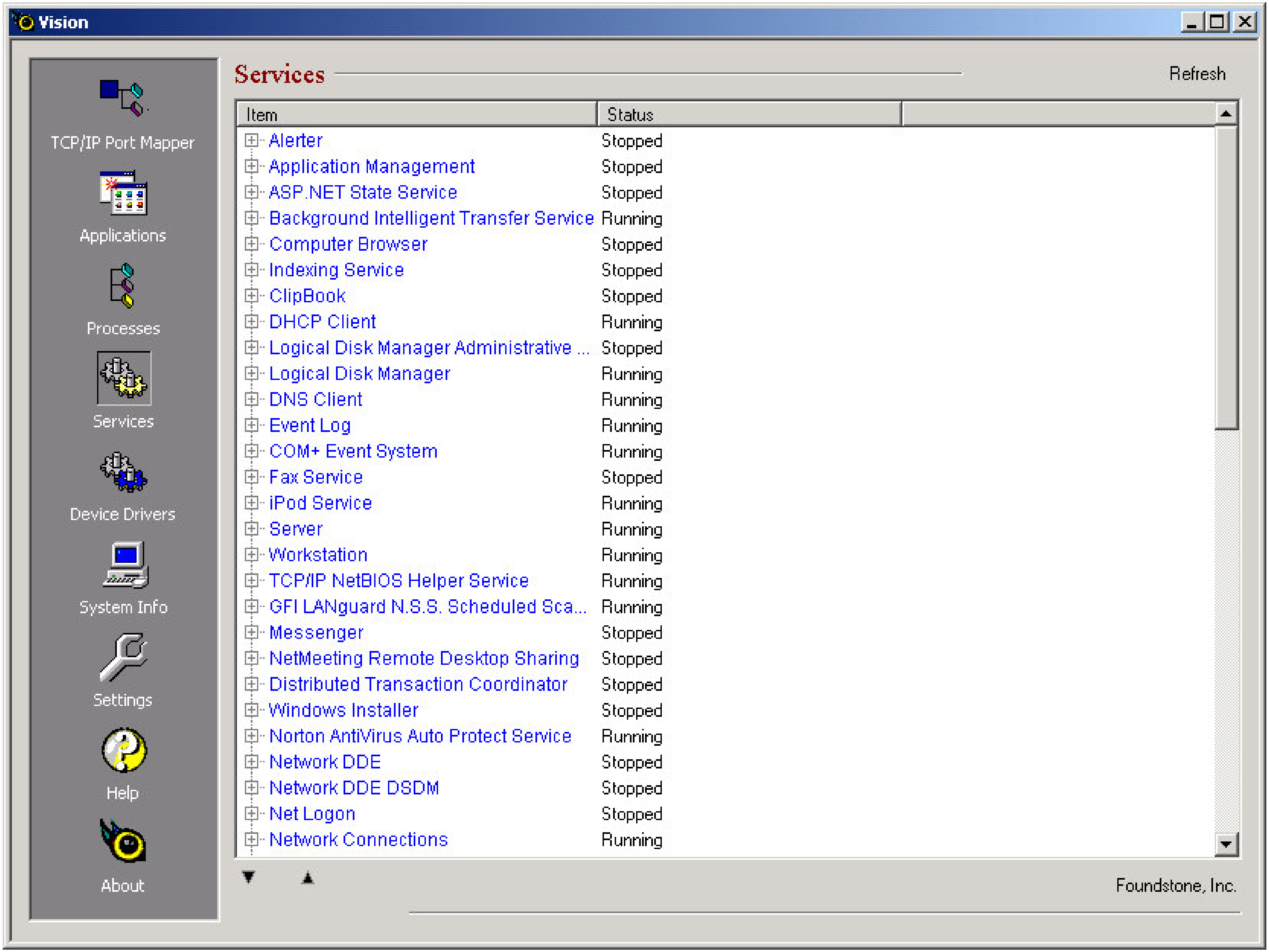
- Dedicated hardware
  - extra disk drives
  - Lots of memory
- Linux & Windows System
- Private network
- Preload tools
- Understand usage of tools

Tool Types

- Windows / Linux
- Case Management
- Network Forensics
- Auditing
- Dedicated bootable linux systems
- Attack tools

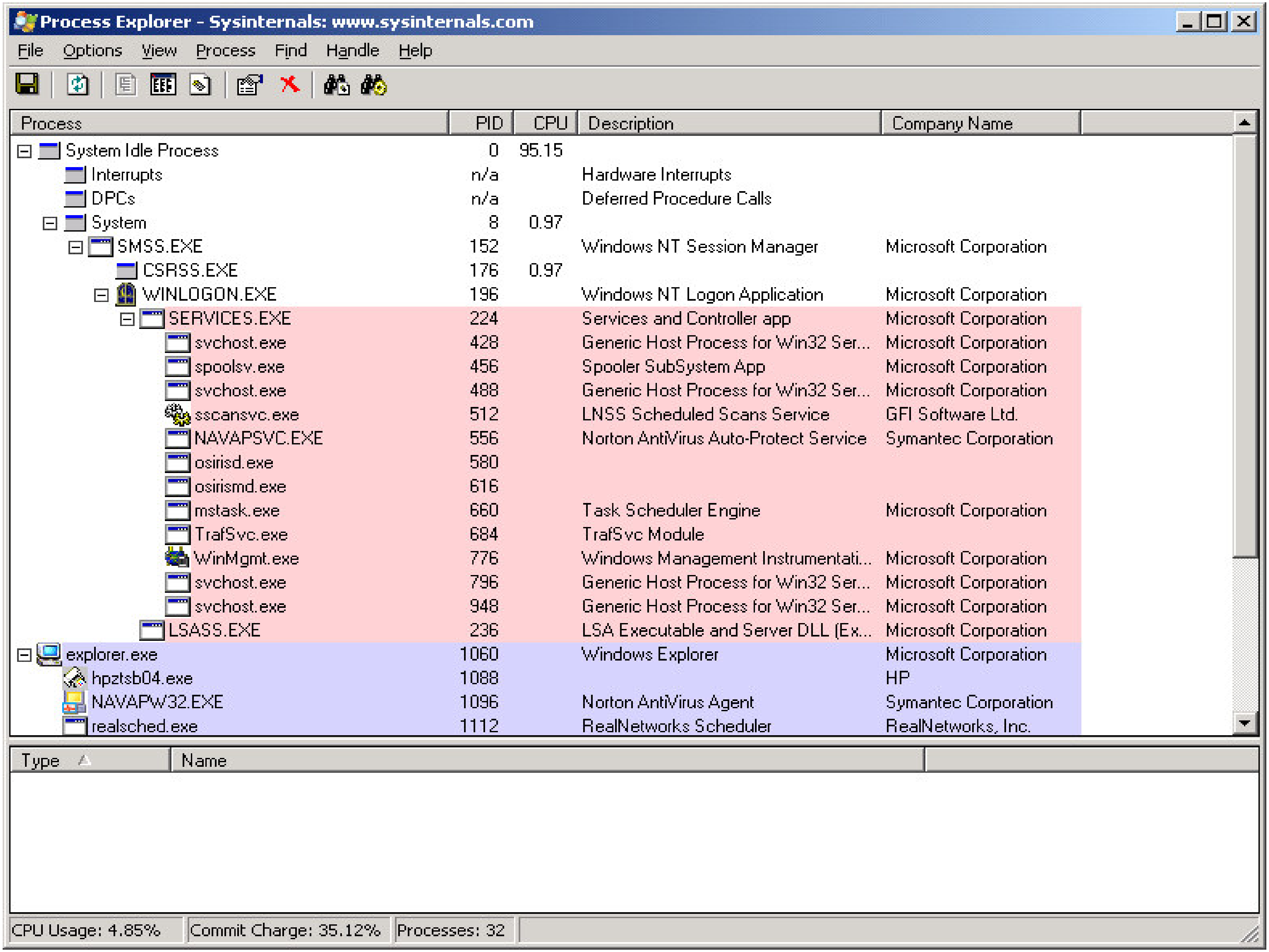
Windows Tools

- www.foundstone.com
  - Ngrep
  - Agrep
  - Fgrep
  - Grep
  - Ntlast
  - Samdump
  - vision
  - Sfind
  - Hfind
  - Filestat
  - Hashtext
  - Hunt
  - Netscan
  - Fport
- www.sysinternals.com
  - Pstools Collection
  - Filemon
  - Regmon
  - Strings
  - Tcpview
  - Process explorer
  - Diskmon
- Other – netcat, tcpdump



Services

Item	Status
Alerter	Stopped
Application Management	Stopped
ASP.NET State Service	Stopped
Background Intelligent Transfer Service	Running
Computer Browser	Stopped
Indexing Service	Stopped
ClipBook	Stopped
DHCP Client	Running
Logical Disk Manager Administrative ...	Stopped
Logical Disk Manager	Running
DNS Client	Running
Event Log	Running
COM+ Event System	Running
Fax Service	Stopped
iPod Service	Running
Server	Running
Workstation	Running
TCP/IP NetBIOS Helper Service	Running
GFI LANguard N.S.S. Scheduled Sca...	Running
Messenger	Stopped
NetMeeting Remote Desktop Sharing	Stopped
Distributed Transaction Coordinator	Stopped
Windows Installer	Stopped
Norton AntiVirus Auto Protect Service	Running
Network DDE	Stopped
Network DDE DSDM	Stopped
Net Logon	Stopped
Network Connections	Running



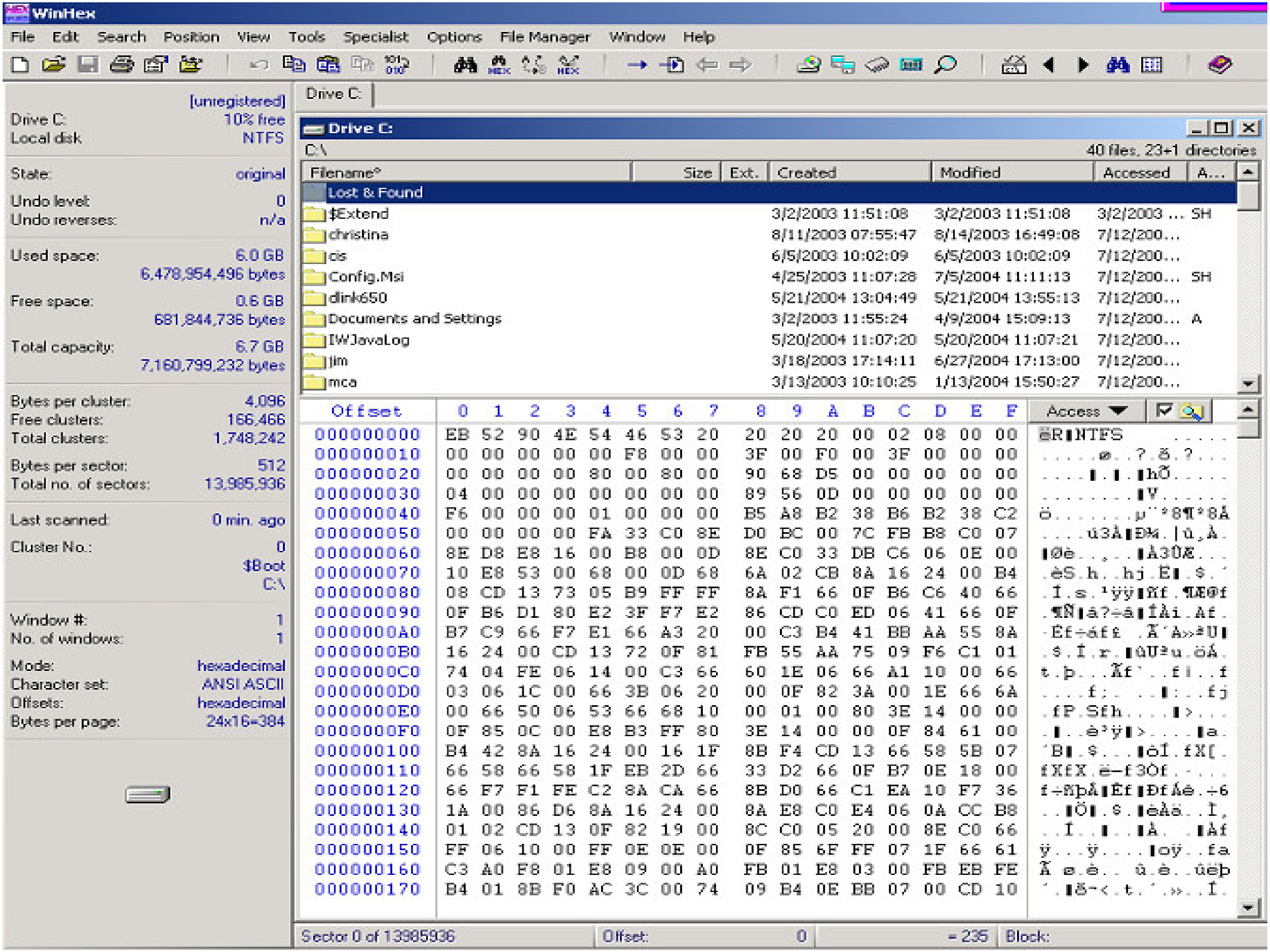
Process	PID	CPU	Description	Company Name
System Idle Process	0	95.15		
Interrupts	n/a		Hardware Interrupts	
DPCs	n/a		Deferred Procedure Calls	
System	8	0.97		
SMSS.EXE	152		Windows NT Session Manager	Microsoft Corporation
CSRSS.EXE	176	0.97		
WINLOGON.EXE	196		Windows NT Logon Application	Microsoft Corporation
SERVICES.EXE	224		Services and Controller app	Microsoft Corporation
svchost.exe	428		Generic Host Process for Win32 Ser...	Microsoft Corporation
spoolsv.exe	456		Spooler SubSystem App	Microsoft Corporation
svchost.exe	488		Generic Host Process for Win32 Ser...	Microsoft Corporation
sscansvc.exe	512		LNSS Scheduled Scans Service	GFI Software Ltd.
NAVAPSVC.EXE	556		Norton AntiVirus Auto-Protect Service	Symantec Corporation
osirisd.exe	580			
osirismd.exe	616			
mstask.exe	660		Task Scheduler Engine	Microsoft Corporation
TrafSvc.exe	684		TrafSvc Module	
WinMgmt.exe	776		Windows Management Instrumentati...	Microsoft Corporation
svchost.exe	796		Generic Host Process for Win32 Ser...	Microsoft Corporation
svchost.exe	948		Generic Host Process for Win32 Ser...	Microsoft Corporation
LSASS.EXE	236		LSA Executable and Server DLL (Ex...	Microsoft Corporation
explorer.exe	1060		Windows Explorer	Microsoft Corporation
hpztsb04.exe	1088			HP
NAVAPW32.EXE	1096		Norton AntiVirus Agent	Symantec Corporation
realsched.exe	1112		RealNetworks Scheduler	RealNetworks, Inc.

Type	Name

CPU Usage: 4.85% | Commit Charge: 35.12% | Processes: 32

Windows Tools

- www.x-ways.net/
  - winhex
- winmerge.sourceforge.net/
  - winmerge
- www.ultraedit.com
  - ultraedit


WinHex
File Edit Search Position View Tools Specialist Options File Manager Window Help
Drive C:
Access

[unregistered]

Drive C:	10% free
Local disk	NTFS
State:	original
Undo level:	0
Undo reverses:	n/a
Used space:	6.0 GB 6,478,954,496 bytes
Free space:	0.6 GB 681,844,736 bytes
Total capacity:	6.7 GB 7,160,799,232 bytes
Bytes per cluster:	4,096
Free clusters:	166,466
Total clusters:	1,748,242
Bytes per sector:	512
Total no. of sectors:	13,985,936
Last scanned:	0 min. ago
Cluster No.:	0 $Boot C:\
Window #:	1
No. of windows:	1
Mode:	hexadecimal
Character set:	ANSI ASCII
Offsets:	hexadecimal
Bytes per page:	24x16=384

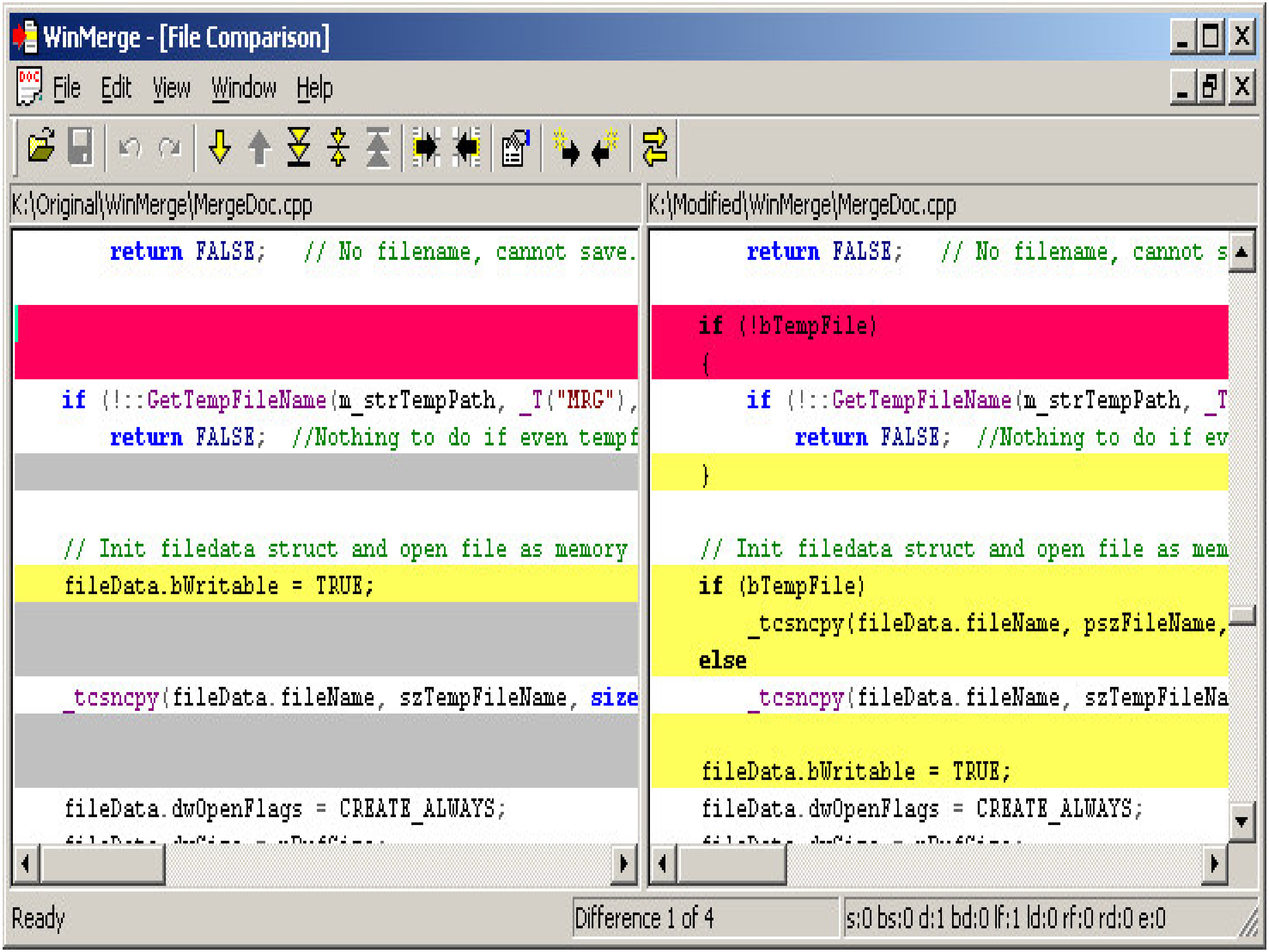
Drive C:

C:\ 40 files, 23+1 directories

Filename*	Size	Ext.	Created	Modified	Accessed	A...
Lost & Found						
$Extend			3/2/2003 11:51:08	3/2/2003 11:51:08	3/2/2003 ...	SH
christina			8/11/2003 07:55:47	8/14/2003 16:49:08	7/12/200...	
cis			6/5/2003 10:02:09	6/5/2003 10:02:09	7/12/200...	
Config.Msi			4/25/2003 11:07:28	7/5/2004 11:11:13	7/12/200...	SH
dlink650			5/21/2004 13:04:49	5/21/2004 13:55:13	7/12/200...	
Documents and Settings			3/2/2003 11:55:24	4/9/2004 15:09:13	7/12/200...	A
IWJavaLog			5/20/2004 11:07:20	5/20/2004 11:07:21	7/12/200...	
jim			3/18/2003 17:14:11	6/27/2004 17:13:00	7/12/200...	
mca			3/13/2003 10:10:25	1/13/2004 15:50:27	7/12/200...	

```
  Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
000000000   EB 52 90 4E 54 46 53 20  20 20 20 00 02 08 00 00   ëR▮NTFS    .....
000000010   00 00 00 00 00 F8 00 00  3F 00 F0 00 3F 00 00 00   .....ø..?.ð.?...
000000020   00 00 00 00 80 00 80 00  90 68 D5 00 00 00 00 00   ....▮.▮.▮hÕ.....
000000030   04 00 00 00 00 00 00 00  89 56 0D 00 00 00 00 00   ........▮V......
000000040   F6 00 00 00 01 00 00 00  B5 A8 B2 38 B6 B2 38 C2   ö.......µ¨²8¶²8Â
000000050   00 00 00 00 FA 33 C0 8E  D0 BC 00 7C FB B8 C0 07   ....ú3À▮Ð¼.|û¸À.
000000060   8E D8 E8 16 00 B8 00 0D  8E C0 33 DB C6 06 0E 00   ▮Øè..¸..▮À3ÛÆ...
000000070   10 E8 53 00 68 00 0D 68  6A 02 CB 8A 16 24 00 B4   .èS.h..hj.Ë▮.$.´
000000080   08 CD 13 73 05 B9 FF FF  8A F1 66 0F B6 C6 40 66   .Í.s.¹ÿÿ▮ñf.¶Æ@f
000000090   0F B6 D1 80 E2 3F F7 E2  86 CD C0 ED 06 41 66 0F   .¶Ñ▮â?÷â▮ÍÀí.Af.
0000000A0   B7 C9 66 F7 E1 66 A3 20  00 C3 B4 41 BB AA 55 8A   ·Éf÷áf£ .Ã´A»ªU▮
0000000B0   16 24 00 CD 13 72 0F 81  FB 55 AA 75 09 F6 C1 01   .$.Í.r.▮ûUªu.öÁ.
0000000C0   74 04 FE 06 14 00 C3 66  60 1E 06 66 A1 10 00 66   t.þ...Ãf`..f¡..f
0000000D0   03 06 1C 00 66 3B 06 20  00 0F 82 3A 00 1E 66 6A   ....f;. ..▮:..fj
0000000E0   00 66 50 06 53 66 68 10  00 01 00 80 3E 14 00 00   .fP.Sfh....▮>...
0000000F0   0F 85 0C 00 E8 B3 FF 80  3E 14 00 00 0F 84 61 00   .▮..è³ÿ▮>....▮a.
000000100   B4 42 8A 16 24 00 16 1F  8B F4 CD 13 66 58 5B 07   ´B▮.$...▮ôÍ.fX[.
000000110   66 58 66 58 1F EB 2D 66  33 D2 66 0F B7 0E 18 00   fXfX.ë-f3Òf.·...
000000120   66 F7 F1 FE C2 8A CA 66  8B D0 66 C1 EA 10 F7 36   f÷ñþÂ▮Êf▮ÐfÁê.÷6
000000130   1A 00 86 D6 8A 16 24 00  8A E8 C0 E4 06 0A CC B8   ..▮Ö▮.$.▮èÀä..Ì¸
000000140   01 02 CD 13 0F 82 19 00  8C C0 05 20 00 8E C0 66   ..Í..▮..▮À. .▮Àf
000000150   FF 06 10 00 FF 0E 0E 00  0F 85 6F FF 07 1F 66 61   ÿ...ÿ....▮oÿ..fa
000000160   C3 A0 F8 01 E8 09 00 A0  FB 01 E8 03 00 FB EB FE   Ã ø.è.. û.è..ûëþ
000000170   B4 01 8B F0 AC 3C 00 74  09 B4 0E BB 07 00 CD 10   ´.▮ð¬<.t.´.».Í.
```

Sector 0 of 13985936 Offset: 0 = 235 Block:



K:\Original\WinMerge\MergeDoc.cpp

```
        return FALSE;   // No filename, cannot save.


    if (!::GetTempFileName(m_strTempPath, _T("MRG"),
        return FALSE;  //Nothing to do if even tempf


    // Init filedata struct and open file as memory
    fileData.bWritable = TRUE;


    _tcsncpy(fileData.fileName, szTempFileName, size


    fileData.dwOpenFlags = CREATE_ALWAYS;
```

K:\Modified\WinMerge\MergeDoc.cpp

```
        return FALSE;   // No filename, cannot s

    if (!bTempFile)
    {
        if (!::GetTempFileName(m_strTempPath, _T
            return FALSE;  //Nothing to do if ev
    }

    // Init filedata struct and open file as mem
    if (bTempFile)
        _tcsncpy(fileData.fileName, pszFileName,
    else
        _tcsncpy(fileData.fileName, szTempFileNa

    fileData.bWritable = TRUE;
    fileData.dwOpenFlags = CREATE_ALWAYS;
```

Ready

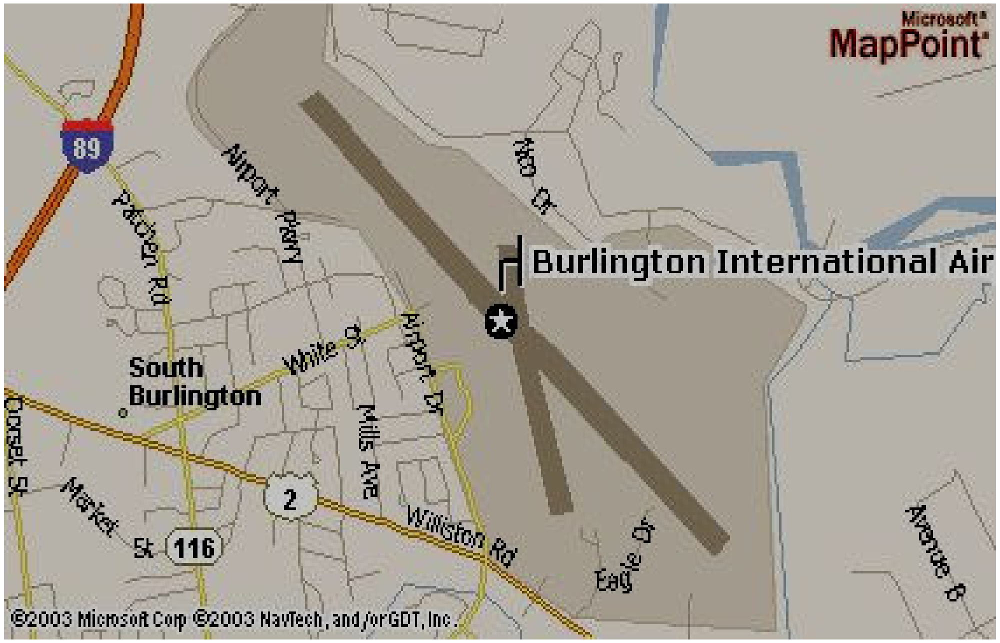
Difference 1 of 4

s:0 bs:0 d:1 bd:0 lf:1 ld:0 rf:0 rd:0 e:0

Stegonography – “Hiding in Plain Site”

- File formats used to hide files
  - jpeg
  - bmp
  - wav
  - mp3
  - exe
  - excel
  - ra/ram
  - gif
  - png
- Tools
  - stools
  - Stego
  - hideseek
  - mp3stego
  - gargoyle
  - stegowatch

Map

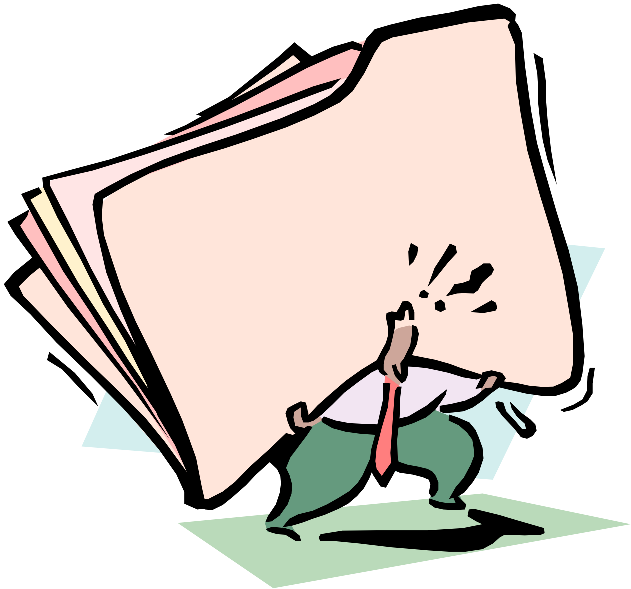


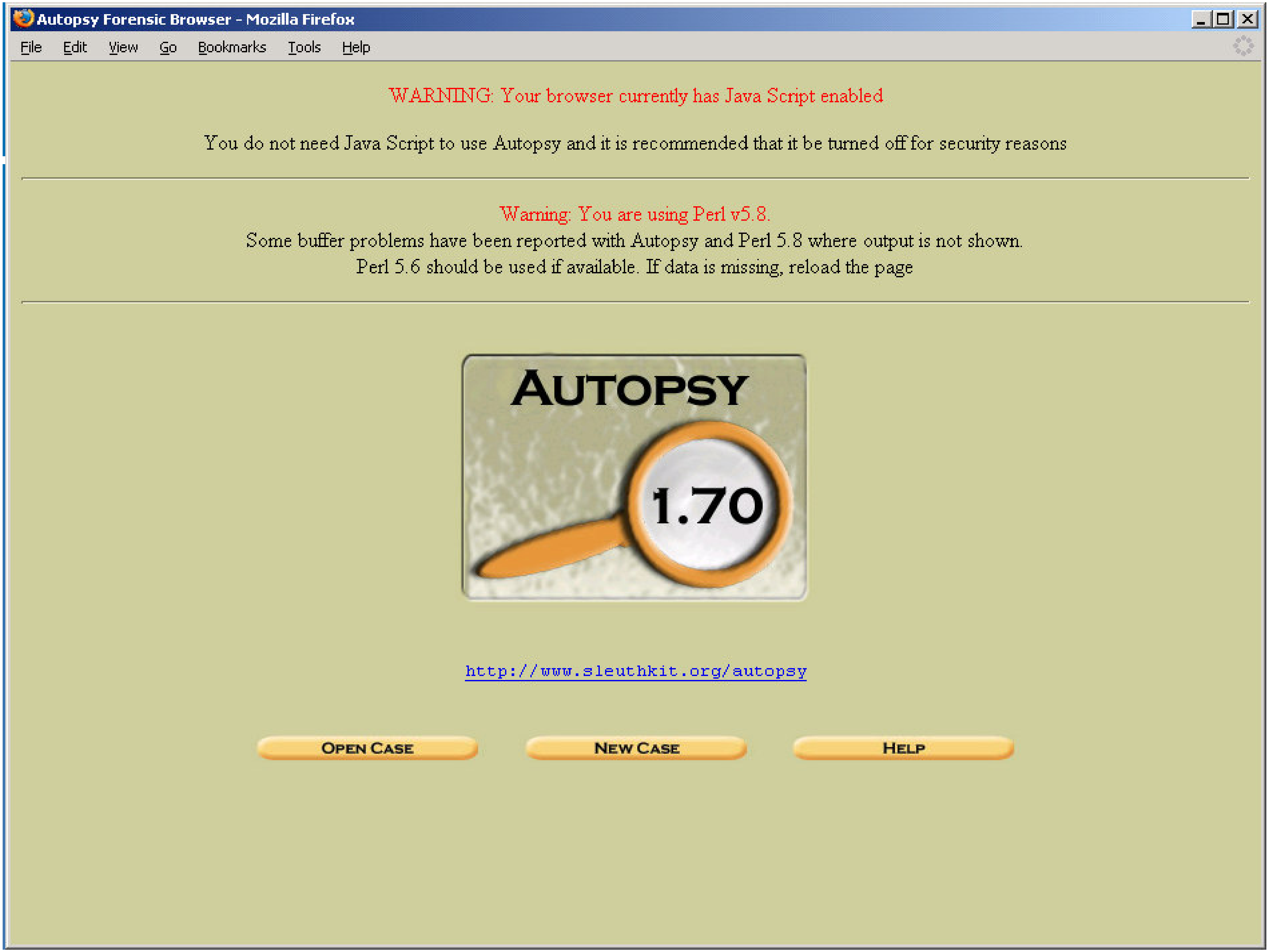
GIF Carrier File

GIF Carrier File & Map

Tool Types

- Windows / Linux
- Case Management
- Network Forensics
- Auditing
- Dedicated bootable linux systems
- Attack tools





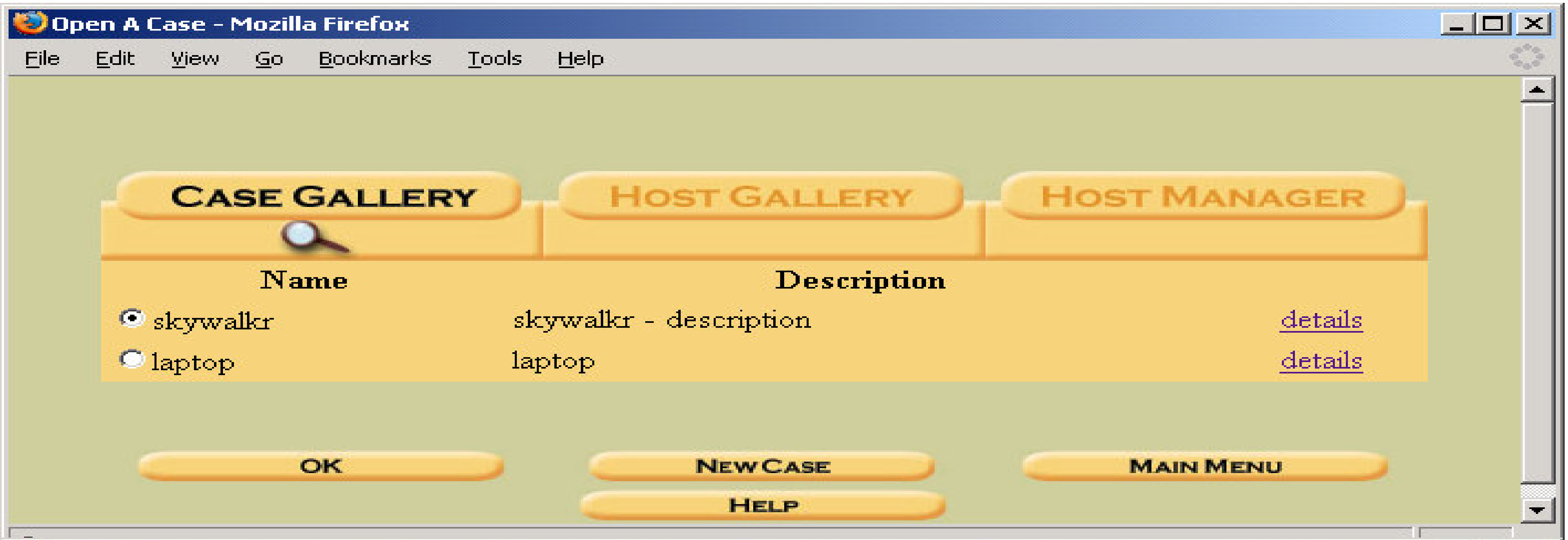
Autopsy Forensic Browser - Mozilla Firefox
File Edit View Go Bookmarks Tools Help

WARNING: Your browser currently has Java Script enabled

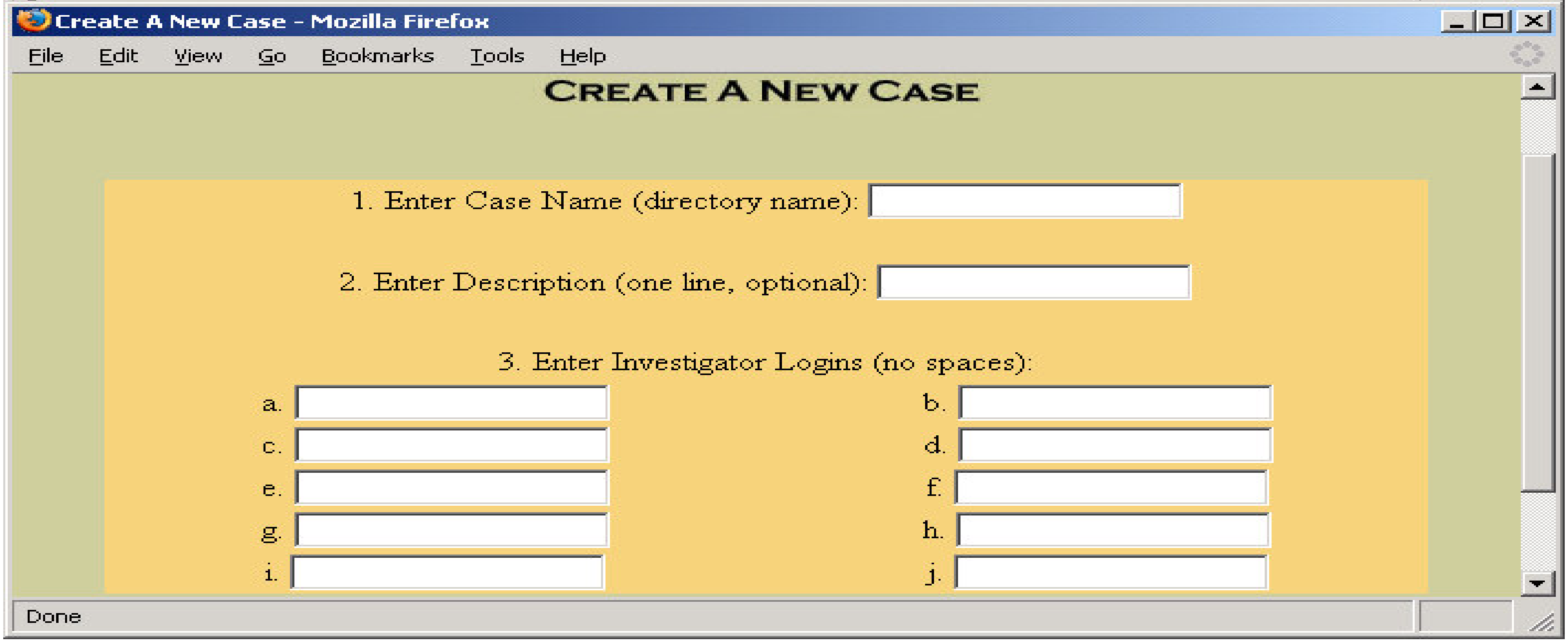
You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons

Warning: You are using Perl v5.8.
Some buffer problems have been reported with Autopsy and Perl 5.8 where output is not shown.
Perl 5.6 should be used if available. If data is missing, reload the page

http://www.sleuthkit.org/autopsy



	Name	Description	
●	skywalkr	skywalkr - description	details
○	laptop	laptop	details



CREATE A NEW CASE

1. Enter Case Name (directory name):

2. Enter Description (one line, optional):

3. Enter Investigator Logins (no spaces):

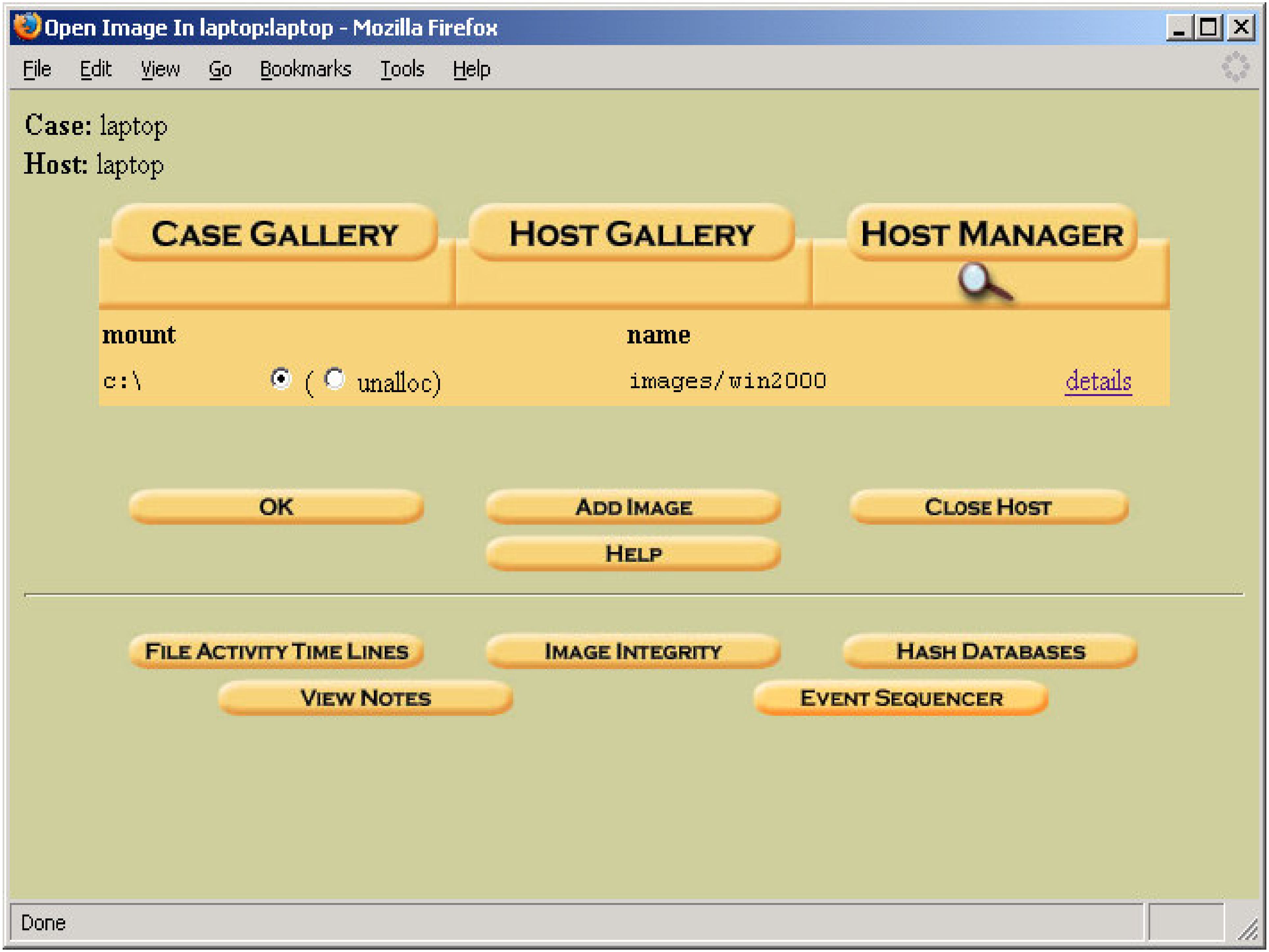
a. b.

c. d.

e. f.

g. h.

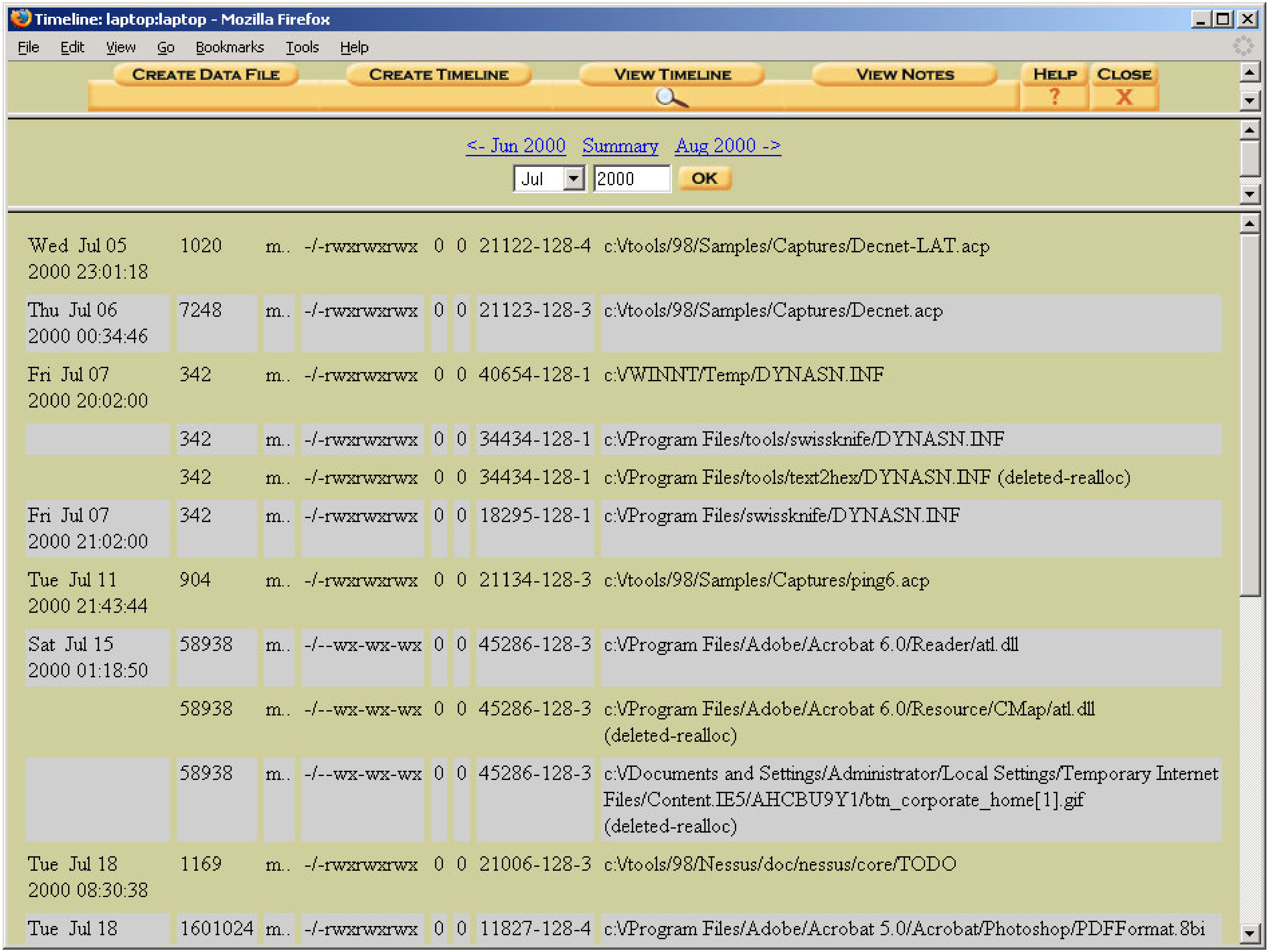
i. j.



Case: laptop

Host: laptop

mount		name	
c:\	● (○ unalloc)	images/win2000	details



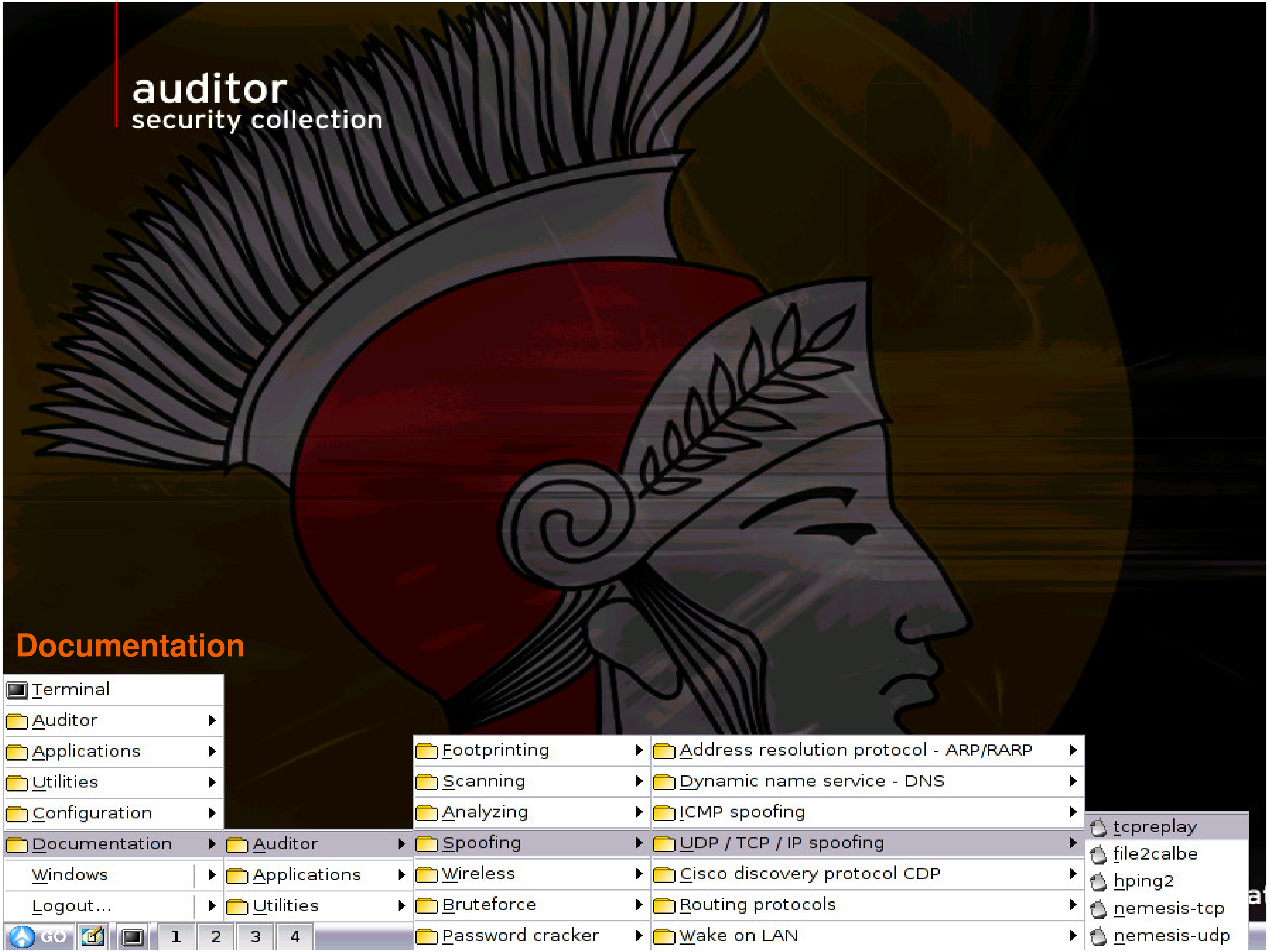
Jul 2000

```
Wed Jul 05      1020     m..  -/-rwxrwxrwx  0  0  21122-128-4  c:Vtools/98/Samples/Captures/Decnet-LAT.acp
2000 23:01:18
Thu Jul 06      7248     m..  -/-rwxrwxrwx  0  0  21123-128-3  c:Vtools/98/Samples/Captures/Decnet.acp
2000 00:34:46
Fri Jul 07      342      m..  -/-rwxrwxrwx  0  0  40654-128-1  c:VWINNT/Temp/DYNASN.INF
2000 20:02:00
                342      m..  -/-rwxrwxrwx  0  0  34434-128-1  c:VProgram Files/tools/swissknife/DYNASN.INF
                342      m..  -/-rwxrwxrwx  0  0  34434-128-1  c:VProgram Files/tools/text2hex/DYNASN.INF (deleted-realloc)
Fri Jul 07      342      m..  -/-rwxrwxrwx  0  0  18295-128-1  c:VProgram Files/swissknife/DYNASN.INF
2000 21:02:00
Tue Jul 11      904      m..  -/-rwxrwxrwx  0  0  21134-128-3  c:Vtools/98/Samples/Captures/ping6.acp
2000 21:43:44
Sat Jul 15      58938    m..  -/--wx-wx-wx  0  0  45286-128-3  c:VProgram Files/Adobe/Acrobat 6.0/Reader/atl.dll
2000 01:18:50
                58938    m..  -/--wx-wx-wx  0  0  45286-128-3  c:VProgram Files/Adobe/Acrobat 6.0/Resource/CMap/atl.dll
                                                               (deleted-realloc)
                58938    m..  -/--wx-wx-wx  0  0  45286-128-3  c:VDocuments and Settings/Administrator/Local Settings/Temporary Internet
                                                               Files/Content.IE5/AHCBU9Y1/btn_corporate_home[1].gif
                                                               (deleted-realloc)
Tue Jul 18      1169     m..  -/-rwxrwxrwx  0  0  21006-128-3  c:Vtools/98/Nessus/doc/nessus/core/TODO
2000 08:30:38
Tue Jul 18      1601024  m..  -/-rwxrwxrwx  0  0  11827-128-4  c:VProgram Files/Adobe/Acrobat 5.0/Acrobat/Photoshop/PDFFormat.8bi
```

Tool Types

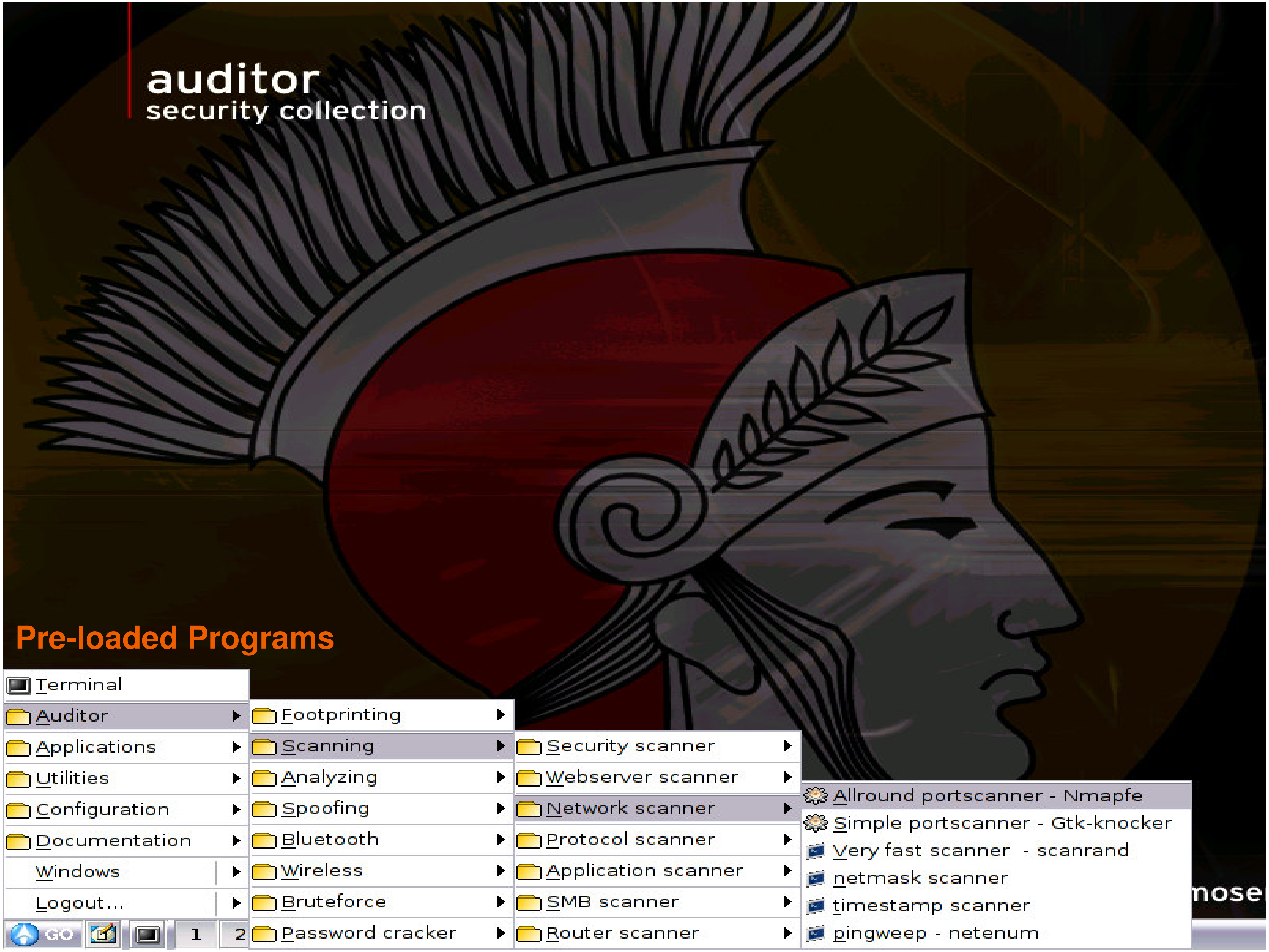
- Windows / Linux
- Case Management
- Network Forensics
- Auditing
- Dedicated bootable linux systems
- Attack tools

HP WORLD 2004
Solutions and Technology Conference & Expo



Documentation

Pre-loaded Programs



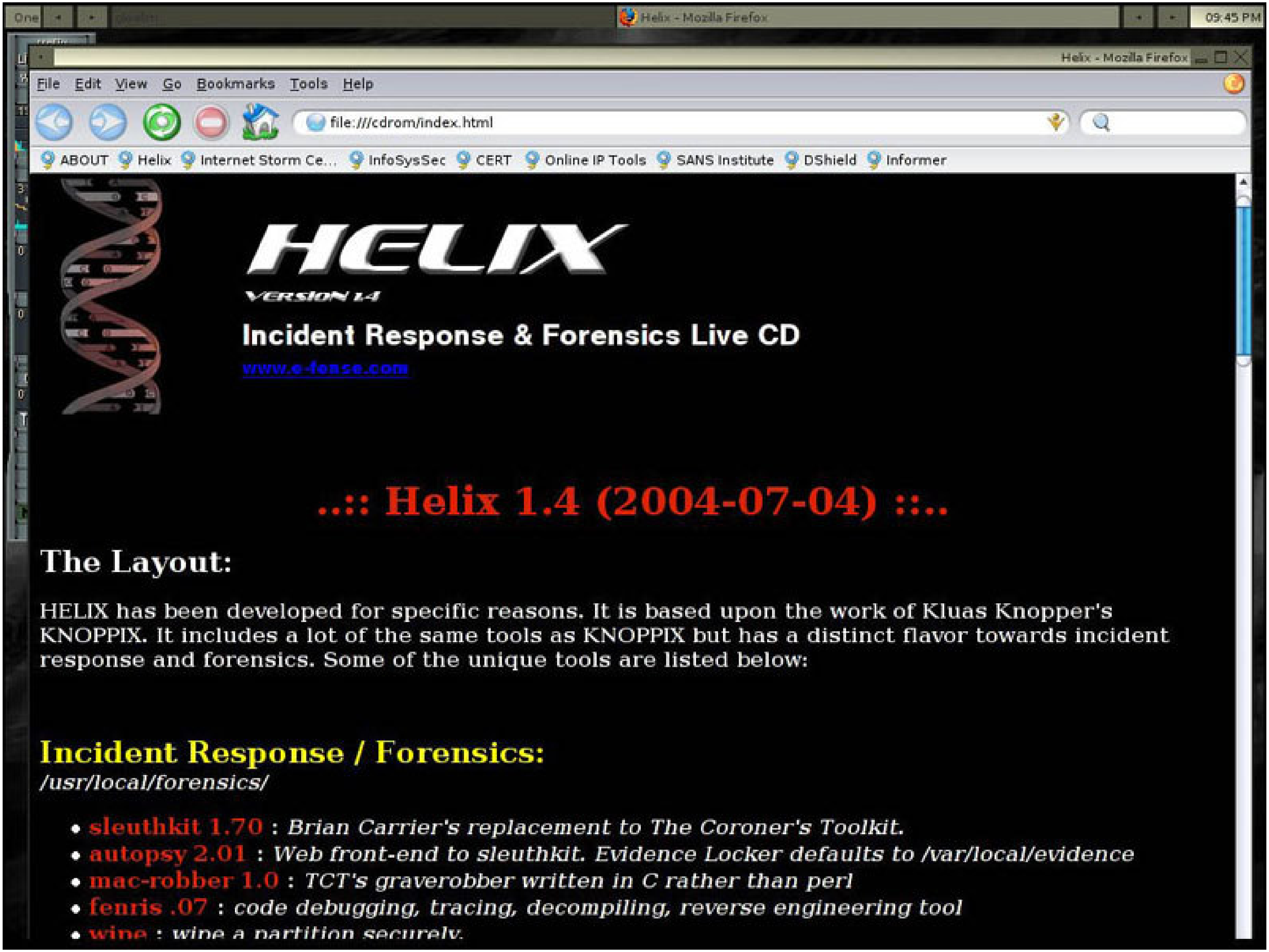
Auditor Security Tool List

Here you can find a list of tools included in the Auditor security collection CD-ROM.

Footprinting, Scanner, Network Analyzers, Spoofing, Wireless, Bluetooth, Forensics, Applications, Tools, Daemons

Category	Name	Version	X11	License	In Menu	Description
footprinting	greenwich	0.5.2	1	GPL	1	Whois client
footprinting	gnetutil	1.0-Auditor	1	GPL	1	Networking toolset
footprinting	host	991529	0	GPL	0	Nameresolution
footprinting	dig	9.2.3	0	GPL	0	Nameresolution
footprinting	traceroute	1.4a12	0	GPL	1	Packet traceing
footprinting	itrace	Unknown	0	Phenoelit	1	Packet traceing
footprinting	tctrace	Unknown	0	Phenoelit	1	Packet traceing
footprinting	tkmib	Unknown	1	GPL	1	SNMP tool
footprinting	snmpwalk	5.1	0	GPL	1	SNMP tool

HP WORLD 2004 Solutions and Technology Conference & Expo



Incident Response & Forensics Live CD

www.e-fense.com

..:: Helix 1.4 (2004-07-04) ::..

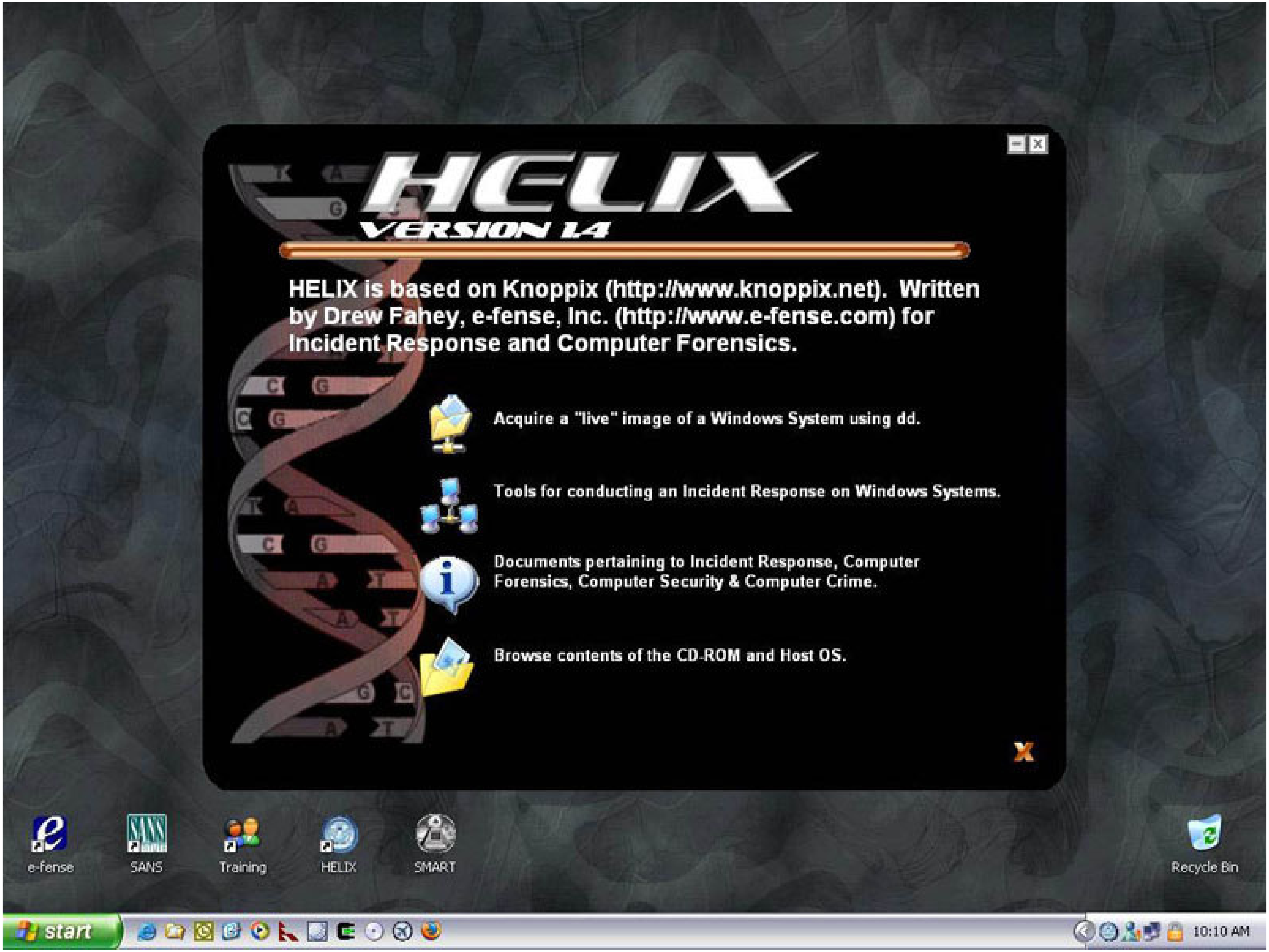
The Layout:

HELIX has been developed for specific reasons. It is based upon the work of Kluas Knopper's KNOPPIX. It includes a lot of the same tools as KNOPPIX but has a distinct flavor towards incident response and forensics. Some of the unique tools are listed below:

Incident Response / Forensics:

/usr/local/forensics/

- sleuthkit 1.70 : *Brian Carrier's replacement to The Coroner's Toolkit.*
- autopsy 2.01 : *Web front-end to sleuthkit. Evidence Locker defaults to /var/local/evidence*
- mac-robber 1.0 : *TCT's graverobber written in C rather than perl*
- fenris .07 : *code debugging, tracing, decompiling, reverse engineering tool*
- wipe : *wipe a partition securely.*



HELIX is based on Knoppix (http://www.knoppix.net). Written by Drew Fahey, e-fense, Inc. (http://www.e-fense.com) for Incident Response and Computer Forensics.

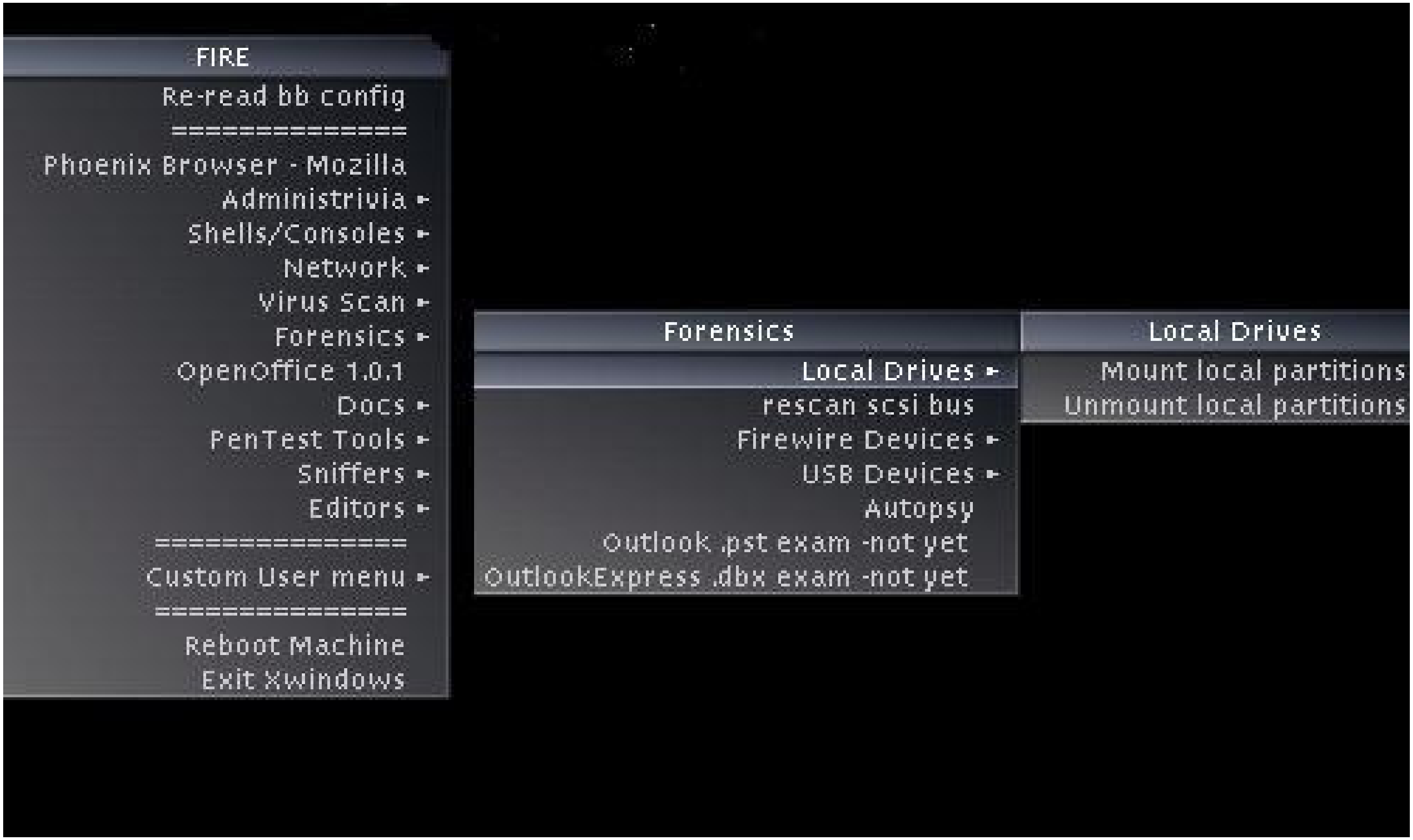
Acquire a "live" image of a Windows System using dd.

Tools for conducting an Incident Response on Windows Systems.

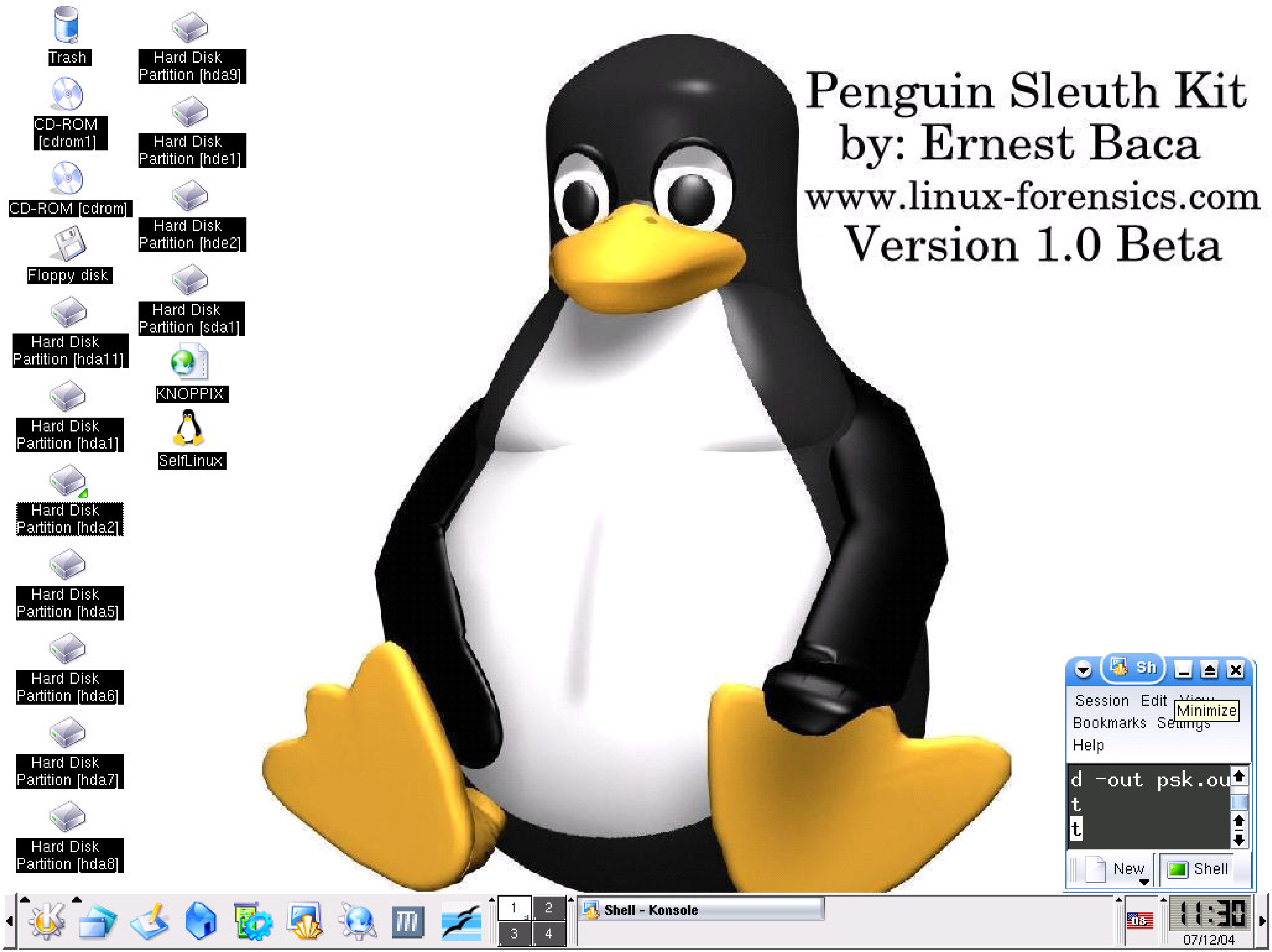
Documents pertaining to Incident Response, Computer Forensics, Computer Security & Computer Crime.

Browse contents of the CD-ROM and Host OS.

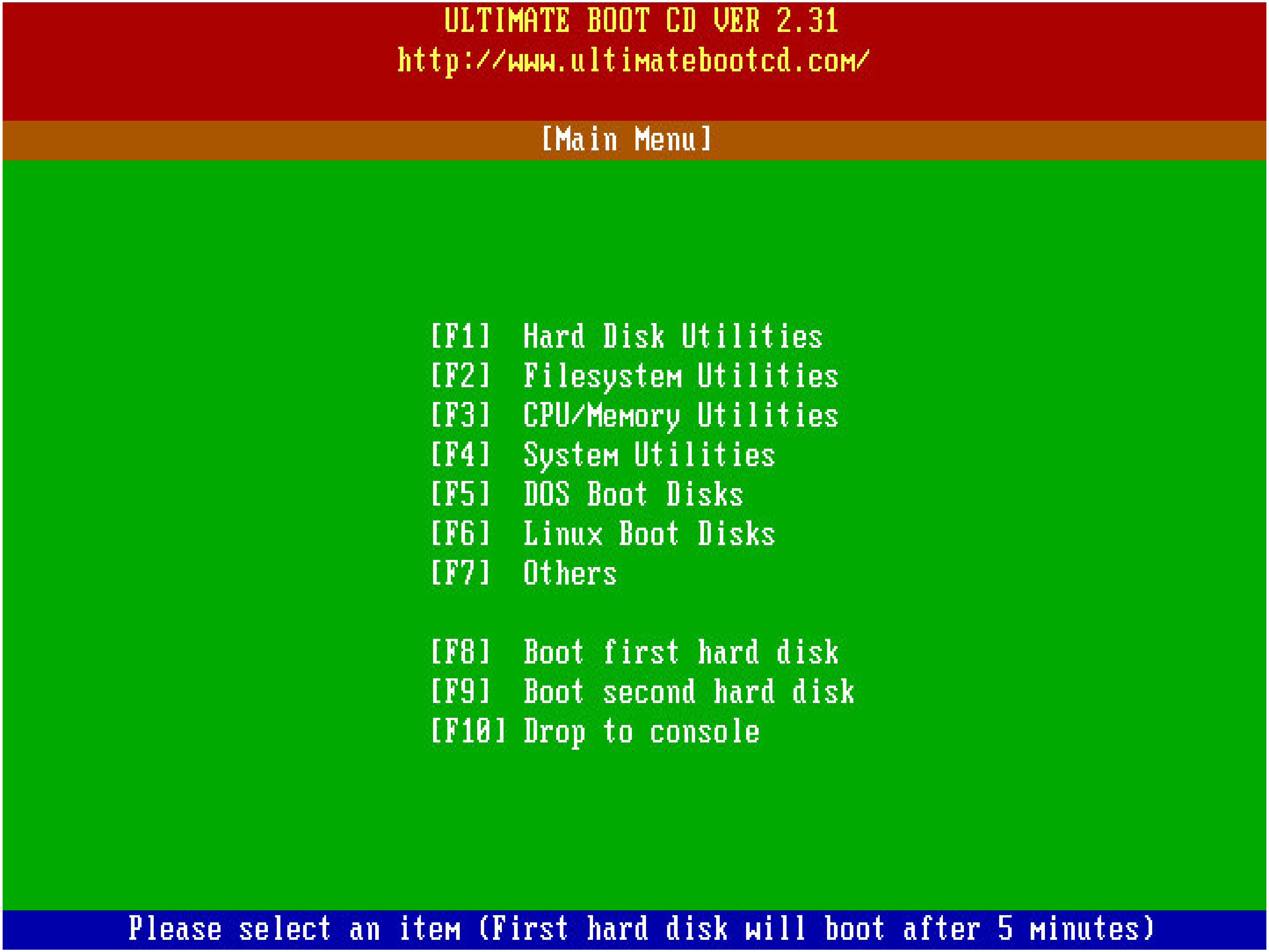
F.I.R.E - Bootable Linux System



http://fire.dmzs.com/


Penguin Sleuth Kit
by: Ernest Baca
www.linux-forensics.com
Version 1.0 Beta
Trash
CD-ROM [cdrom1]
CD-ROM [cdrom]
Floppy disk
Hard Disk Partition [hda11]
Hard Disk Partition [hda1]
Hard Disk Partition [hda2]
Hard Disk Partition [hda5]
Hard Disk Partition [hda6]
Hard Disk Partition [hda7]
Hard Disk Partition [hda8]
Hard Disk Partition [hda9]
Hard Disk Partition [hde1]
Hard Disk Partition [hde2]
Hard Disk Partition [sda1]
KNOPPIX
SelfLinux
Sh
Session Edit View
Bookmarks Settings
Help
Minimize
New
Shell
1 2 3 4
Shell - Konsole
US
11:30
07/12/04

```
d -out psk.ou
t
t
```



```
                      ULTIMATE BOOT CD VER 2.31
                   http://www.ultimatebootcd.com/

                             [Main Menu]




                    [F1]  Hard Disk Utilities
                    [F2]  Filesystem Utilities
                    [F3]  CPU/Memory Utilities
                    [F4]  System Utilities
                    [F5]  DOS Boot Disks
                    [F6]  Linux Boot Disks
                    [F7]  Others

                    [F8]  Boot first hard disk
                    [F9]  Boot second hard disk
                    [F10] Drop to console




     Please select an item (First hard disk will boot after 5 minutes)
```

Cain & Abel

- Protected Storage Password Manager
- LSA Secrets Dumper
- Users, Groups, Shares and Services Enumeration
- SID Scanner
- Local/Remote Service Manager
- APR (ARP Poison Routing) ENABLES SNIFFING on switched networks. (more info in the topics area)
- Sniffer filters for HTTP-BASIC, HTTP-FORM, HTTP-COOKIE, HTTP-NTLMv1, HTTP-NTLMv2, HTTP-NTLMSSP, POP3, IMAP, FTP, VNC, HSRP, SMTP, NNTP, TDS (Sybase and MS-SQL), MS-Kerberos5 Pre-Auth, VRRP, RIPv2, OSPF, SMB (ClearText, NTLMv1, NTLMv2), NTLMSSP (NTLMv1, NTLMv2, NTLM Session Security), RADIUS, IKE Aggressive Mode Pre-Shared Keys, ICQ and MySQL authentications
- HSRP, VRRP, RIPv1, RIPv2, EIGRP, OSPF Monitors
- Full Telnet sessions sniffer
- Full SSH-1 sessions sniffer for APR (FULL-DUPLEX, stealth, supports DES, 3DES, Blowfish symmetric ncryption algorithms, auto-downgrade to SSH-1 if server version is v1.99)

Cain & Abel

- Full HTTPS sessions sniffer for APR
- Automatic HTTPS Certificates Collector
- Auto IP-MAC Discovery
- MAC Address Scanner with OUI fingerprint
- Promiscuous-mode Scanner based on ARP packets
- Wireless Scanner

- Access (9x/2000/XP) Database Passwords Decoder
- Base64, Cisco type-7 and VNC Password Decoders
- Enterprise Manager Password Decoder (SQL Server 7.0 and SQL Server 2000 supported)
- Remote Desktop Password Decoder (decode passwords in .RPD files)
- Dialup Password Decoder
- Password Crackers for common Hashes (MD2, MD4, MD5, SHA-1 and RIPEMD-160).

Why use Computer/Digital Forensics ?

- ➢ Methodology/Framework developed and continuing to improve
- ➢ Tools
- ➢ Great Time Saver
- ➢ Limited experience, great way to learn

- ➢ ***The End***

“Windows Tool References”

- www.foundstone.com
- ubcd.sourceforge.net/
  - ubcd boot cd
- www.sysinternals.com
- www.wetstonetech.com
  - Gargoyle
  - Stego suite
- Nelson Soft, Inc.
  - Gif-it-Up

If I have forgotten to reference some one’s name or company my apologies.

“Unix Tool References”

- www.foundstone.com
- www.ntcn.org
- www.forensics-intl.com
- biatchux.dmzs.com
- www.linux-forensics.com/links.html
- www.atstake.com
- www.sluethkit.org -
  - The Sleuth Kit, Autopsy

Forensics References

- www.computerforensics.net
- www.sans.org
- Sans Article – Computer Forensics an Overview, Dorothy Lunn
- New Technologies Inc.
- Jonathan Isner – Computer Forensics: An emerging Practice in the Battle Against Cyber Crime
- @Stake, Inc.
- Gary Kessler – An Overview of Steganography

Forensics Tools

- Eric Cole – “Hiding in Plain Site”

- Cain & Abel – www.oxid.it

HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:

interex

shared knowledge • shared power

encompass

AN HP USER GROUP