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
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!
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
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
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
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

- www.sysinternals.com
  - Ptools Collection
  - Filemon
  - Regmon
  - Strings

- Other – netcat, tcpdump
## Services

<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alerter</td>
<td>Stopped</td>
</tr>
<tr>
<td>Application Management</td>
<td>Stopped</td>
</tr>
<tr>
<td>ASP.NET State Service</td>
<td>Stopped</td>
</tr>
<tr>
<td>Background Intelligent Transfer Service</td>
<td>Running</td>
</tr>
<tr>
<td>Computer Browser</td>
<td>Stopped</td>
</tr>
<tr>
<td>Indexing Service</td>
<td>Stopped</td>
</tr>
<tr>
<td>ClipBook</td>
<td>Stopped</td>
</tr>
<tr>
<td>DHCP Client</td>
<td>Running</td>
</tr>
<tr>
<td>Logical Disk Manager Administrative Volume Control Service</td>
<td>Stopped</td>
</tr>
<tr>
<td>Logical Disk Manager</td>
<td>Running</td>
</tr>
<tr>
<td>DNS Client</td>
<td>Running</td>
</tr>
<tr>
<td>Event Log</td>
<td>Running</td>
</tr>
<tr>
<td>COM+ Event System</td>
<td>Running</td>
</tr>
<tr>
<td>Fax Service</td>
<td>Stopped</td>
</tr>
<tr>
<td>iPod Service</td>
<td>Running</td>
</tr>
<tr>
<td>Server</td>
<td>Running</td>
</tr>
<tr>
<td>Workstation</td>
<td>Running</td>
</tr>
<tr>
<td>TCP/IP NetBIOS Helper Service</td>
<td>Running</td>
</tr>
<tr>
<td>GFI LANguard N.S.S. Scheduled Scanner</td>
<td>Running</td>
</tr>
<tr>
<td>Messenger</td>
<td>Stopped</td>
</tr>
<tr>
<td>NetMeeting Remote Desktop Sharing</td>
<td>Stopped</td>
</tr>
<tr>
<td>Distributed Transaction Coordinator</td>
<td>Stopped</td>
</tr>
<tr>
<td>Windows Installer</td>
<td>Stopped</td>
</tr>
<tr>
<td>Norton AntiVirus Auto Protect Service</td>
<td>Running</td>
</tr>
<tr>
<td>Network DDE</td>
<td>Stopped</td>
</tr>
<tr>
<td>Network DDE DSDM</td>
<td>Stopped</td>
</tr>
<tr>
<td>Net Logon</td>
<td>Stopped</td>
</tr>
<tr>
<td>Network Connections</td>
<td>Running</td>
</tr>
<tr>
<td>Process</td>
<td>PID</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>System Idle Process</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td>Interrupts</td>
<td>n/a</td>
</tr>
<tr>
<td>DPCs</td>
<td>8</td>
</tr>
<tr>
<td>SMSS.EXE</td>
<td>152</td>
</tr>
<tr>
<td>CSRSS.EXE</td>
<td>176</td>
</tr>
<tr>
<td>WINLOGON.EXE</td>
<td>196</td>
</tr>
<tr>
<td>SERVICES.EXE</td>
<td>224</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>428</td>
</tr>
<tr>
<td>spoolsv.exe</td>
<td>456</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>488</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>512</td>
</tr>
<tr>
<td>NAVAPSVC.EXE</td>
<td>556</td>
</tr>
<tr>
<td>osiris.exe</td>
<td>580</td>
</tr>
<tr>
<td>osirismd.exe</td>
<td>616</td>
</tr>
<tr>
<td>mstask.exe</td>
<td>660</td>
</tr>
<tr>
<td>TrafSvc.exe</td>
<td>684</td>
</tr>
<tr>
<td>WinMgmt.exe</td>
<td>776</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>796</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>948</td>
</tr>
<tr>
<td>LSASS.EXE</td>
<td>236</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>1060</td>
</tr>
<tr>
<td>hpztst04.exe</td>
<td>1088</td>
</tr>
<tr>
<td>NAVAPW32.EXE</td>
<td>1096</td>
</tr>
<tr>
<td>realsched.exe</td>
<td>1112</td>
</tr>
</tbody>
</table>

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
return FALSE;  // No filename, cannot save.

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

// Init filedata struct and open file as memory
fileData.bWritable = TRUE;
_tcsncpy(fileData.fileName, szTempFileName, size

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

fileData.dwOpenFlags = CREATE_ALWAYS;
fileData.dwSize = _DwSize:
Steganography – “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
  - gargoyles
  - stegowatch
An Overview of Steganography – Gary Kessler
GIF Carrier File & Map
Tool Types

- Windows / Linux
- **Case Management**
- Network Forensics
- Auditing
- Dedicated bootable linux systems
- Attack tools
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
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. 
   d. 
   e. 
   f. 
   g. 
   h. 
   i. 
   j.
Case: laptop
Host: laptop

- **Mount:**
  - C:\ (unalloc)

- **Name:** images/win2000

Buttons:
- OK
- Add Image
- Close Host
- Help
- File Activity Time Lines
- Image Integrity
- Hash Databases
- Event Sequencer

Links:
- View Notes
- Details
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Type</th>
<th>Size</th>
<th>Time</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wed Jul 05 2000 23:01:18</td>
<td>1020 m. -rw-rw-rx 0 0 21122-128-4</td>
<td>c:\tools\98\Samples\Captures\Decnet-LAT.acp</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thu Jul 06 2000 00:34:46</td>
<td>7248 m. -rw-rw-rx 0 0 21123-128-3</td>
<td>c:\tools\98\Samples\Captures\Decnet.acp</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri Jul 07 2000 20:02:00</td>
<td>342 m. -rw-rw-rx 0 0 40654-128-1</td>
<td>c:\WINNT\Temp\DYNASN.INF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>c:\Program Files\tools\swissknife\DYNASN.INF (deleted-realloc)</td>
</tr>
<tr>
<td>Fri Jul 07 2000 21:02:00</td>
<td>342 m. -rw-rw-rx 0 0 18295-128-1</td>
<td>c:\Program Files\swissknife\DYNASN.INF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tue Jul 11 2000 21:43:44</td>
<td>904 m. -rw-rw-rx 0 0 21134-128-3</td>
<td>c:\tools\98\Samples\Captures\ping6.acp</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sat Jul 15 2000 01:18:50</td>
<td>58938 m. -rw-rw-wx 0 0 45286-128-3</td>
<td>c:\Program Files\Adobe\Acrobat 6.0\Reader\atl.dll</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>c:\Program Files\Adobe\Acrobat 6.0\Resource\CMap\atl.dll (deleted-realloc)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>c:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AHCBU9Y1\btn_corporate_home[1].gif (deleted-realloc)</td>
</tr>
<tr>
<td>Tue Jul 18 2000 08:30:38</td>
<td>1169 m. -rw-rw-rx 0 0 21006-128-3</td>
<td>c:\tools\98\Nessus\doc\nessus\core\TODO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tue Jul 18 2000 1601024 m. -rw-rw-rx 0 0 11827-128-4</td>
<td>c:\Program Files\Adobe\Acrobat 5.0\Acrobat\Photoshop\PDFFormat.8bi</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Tool Types

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

<table>
<thead>
<tr>
<th>Category</th>
<th>Name</th>
<th>Version</th>
<th>X11</th>
<th>License</th>
<th>In Menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>footprinting</td>
<td>footprinting</td>
<td>greenwich</td>
<td>0.5.2</td>
<td>1</td>
<td>GPL</td>
<td>1</td>
</tr>
<tr>
<td>footprinting</td>
<td>footprinting</td>
<td>gnetutil</td>
<td>1.0-Auditor</td>
<td>1</td>
<td>GPL</td>
<td>1</td>
</tr>
<tr>
<td>footprinting</td>
<td>footprinting</td>
<td>host</td>
<td>991529</td>
<td>0</td>
<td>GPL</td>
<td>0</td>
</tr>
<tr>
<td>footprinting</td>
<td>footprinting</td>
<td>dig</td>
<td>9.2.3</td>
<td>0</td>
<td>GPL</td>
<td>0</td>
</tr>
<tr>
<td>footprinting</td>
<td>footprinting</td>
<td>traceroute</td>
<td>1.4a12</td>
<td>0</td>
<td>GPL</td>
<td>1</td>
</tr>
<tr>
<td>footprinting</td>
<td>footprinting</td>
<td>itrace</td>
<td>Unknown</td>
<td>0</td>
<td>Phenoelit</td>
<td>1</td>
</tr>
<tr>
<td>footprinting</td>
<td>footprinting</td>
<td>tctrace</td>
<td>Unknown</td>
<td>0</td>
<td>Phenoelit</td>
<td>1</td>
</tr>
<tr>
<td>footprinting</td>
<td>footprinting</td>
<td>tkmib</td>
<td>Unknown</td>
<td>1</td>
<td>GPL</td>
<td>1</td>
</tr>
<tr>
<td>footprinting</td>
<td>footprinting</td>
<td>snmpwalk</td>
<td>5.1</td>
<td>0</td>
<td>GPL</td>
<td>1</td>
</tr>
</tbody>
</table>
HELIX
VERSION 1.4
Incident Response & Forensics Live CD
www.e-forens.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
- wine: wine a partition securely.

- Acquire a "live" image of a Windows System using dd.
- Tools for conducting an Incident Response on Windows Systems.
- 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
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 encryption 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