

# Forensics Tools and Processes for Windows XP

Larry Leibrock - Ph.D.

Black Hat  
Windows - Security  
February 26, 2003

Forensics Tools &  
Processes for XP - Larry  
Leibrock

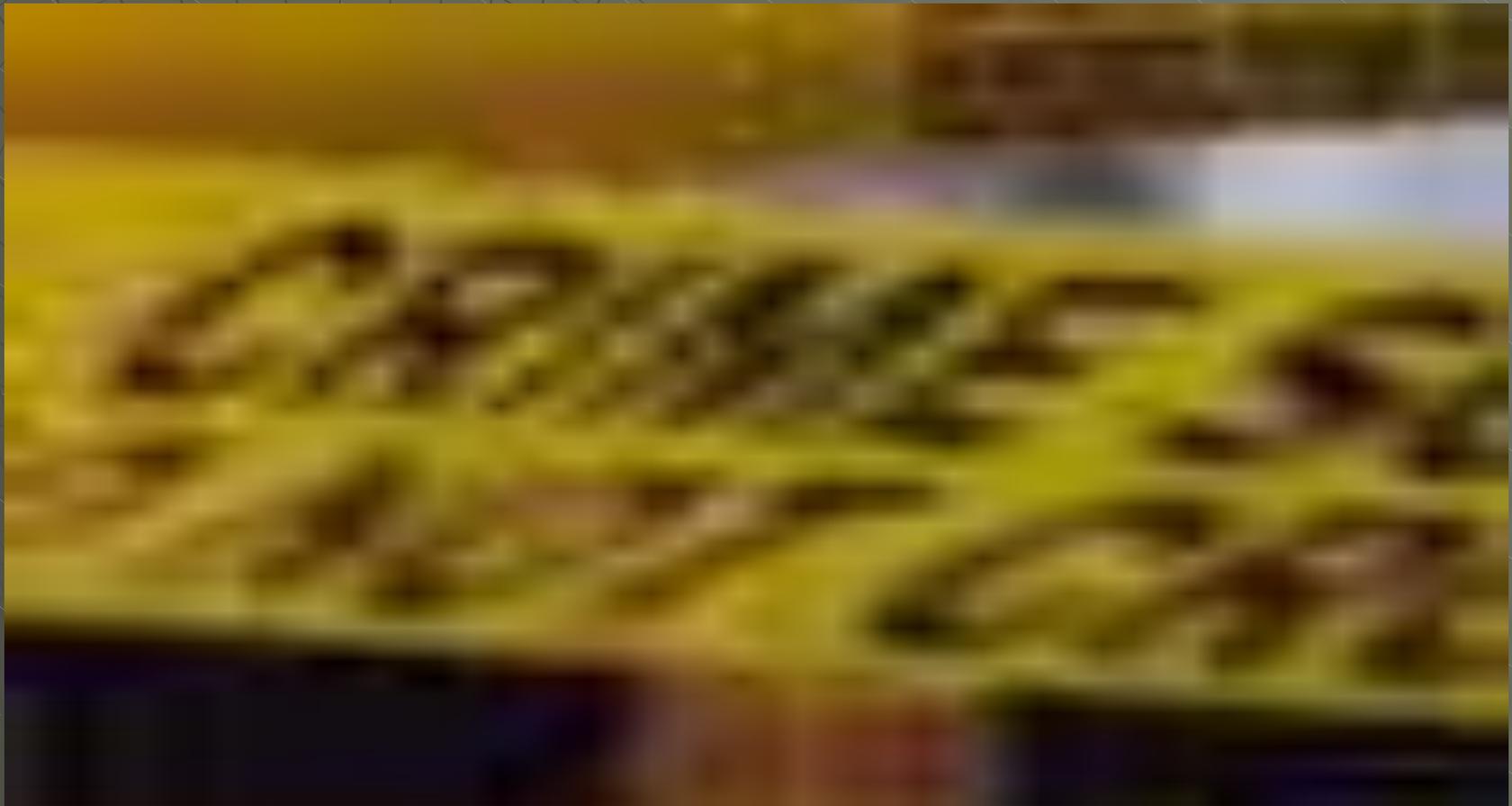
# Introduction

- ◆ Intent of this talk:
  - Very fast paced – a lot of material – The Slides
  - Introduction to digital forensics – exposure to practices – techniques – some tools
  - Not any hands-on training class
  - Provide conceptual frame and pointers about some tools, forensics techniques to engage your professional interest
  - Specifically geared for the needs of the IT technical professional community.

# My goals for today's discussion

-  **Conceptualize** content clearly,
-  **Speak** plainly,
-  **Frame** a range of forensics concepts,
-  **Describe** some competency models, tools and instruments
-  **Establish** some present & future digital forensic challenges

# Welcome and Disclaimers



Forensics Tools &  
Processes for XP - Larry  
Leibrock

# A Protocol

Γ Please Ask Questions –  
whenever you need to. Let's  
collectively feed our brains.

- Your Slides WE WILL NOT USE EVERY SLIDE -
- Very focused on clinical practice - no real attention to theory
- Me and what I do.

I am not a Practicing Attorney – however, I am on the teaching faculty of a University of Texas Law School



# Larry Leibrock, - Notices.

- ◆ I am **not** an attorney. I have a range of forensic investigative experience and in court, at trial, expert testimony. In the past, I have served as:
  - A prosecution (consulting) expert,
  - Both consulting and testifying defense expert and
  - Court appointed special master in these judicial matters.
- ◆ I have received formal training in 5 digital forensics tools. I have conducted the forensics analysis in these domains
  - Client platforms
  - Servers
  - PDA's
  - Software Code - Intellectual property

# Risks of Use Notice

- ◆ *The entire risk of the use or the results of the use of this document remains solely with the user.*
- ◆ *The names of companies, products, people, characters, and/or data mentioned in cases herein are deemed fictitious.*
- ◆ *These names are in no way intended to accurately represent any real individual, company, product, or investigative event, unless otherwise noted.*

# Caveats

- ◆ No discussion about the efficacy of search warrants, wiretap procedures, trapping mechanisms (i.e. honey pots - sand boxes) or creation of forensics investigation policies for the organization is contained in this material.
- ◆ Reiterate Slides - We will not use every slide in today's work - we will adjust order.

# Definitions & Forensics Practice and a little Theory

## Objectives

-  **Some Terms and Context for Digital Forensics**
-  **Describe Challenges to Digital Forensics**
-  **Provide Some Terms and Context**
-  **Features of Information Integrity**
-  **Digital Forensics as a Relevant Business Issue**
-  **Systems- security-forensics must have interaction among these domains**

# Terms, Context and Content

- Document – the data in context –
- Record – the document preserved
- Archive – the document preserved for enduring value
- Digital Information – binary representation 1 and 0's
- Human Interactions with these digital devices create information changes, leaves "artifacts" and "remnants"

# The Challenges

- ◆ The Medium Investigation
  - The investigation of the physical media on which the information resides
- ◆ The Technology Preservation
  - The investigation and “refreshment” of the information technology from legacy to current.
- ◆ The Evidential Investigation
  - Addressing the integrity & authentication of the information (protection to changes)

# Features of Information Integrity



## **Content**

The substance on the digital object



## **Fixity**

The time or changes to the digital object over time



## **Reference**

- The identification of the object



## **Provenance**

Origin and chain of custody of the digital object



## **Context**

The way this digital object occurs and the dependencies of the linkage

**Reference** Task Force on Archiving Digital Information, 1996 (web location  
Forensics Tools &  
Processes for XP - Larry  
Leibrock

# The Problem of Defining Forensics

- ◆ Science versus Technical Debate
- ◆ “Standard” of Science
  - 📁 Body of Knowledge - Experimentation based on theory
  - 📁 Acceptable procedures and Practices
- Henry Lee’s Scientific Considerations
  - Recognition
  - Identification
  - Comparison
  - Individualization
  - Reconstruction

# Computer Forensics Definition - Kruse & Heiser

- ◆ Computer forensics involves the preservation, identification, extraction, documentation and interpretation of computer media for evidentiary and/or root cause analysis.

**Reference** Computer Forensics – Incident Response

Essentials, 2002

Processes for XP - Larry

Leibrock

# FBI Agent - Mark Pollitt

- ◆ Computer forensics is the application of science and engineering to the legal problem of digital evidence. It is the synthesis of science and law.

*Forensic Computing, ISBN 1-85233-299-9*

# Forensics – Clinical Definition

- ◆ As related to computer systems – forensics is the *tradecraft* of conducting a proper and documented investigation of the alleged misuse of a system, its users, its artifacts and services. The forensics investigation is based on the proper management of evidentiary materials, use of proper techniques and methods necessary to present a set of defensible expert observations for use in administrative, civil or criminal review.

(Larry Leibrock, 1995).

# Some Definitional Constructs

- ◆ Forensics phases (3 Primary Phases):
  1. **Investigation (including acquisition and verification).**
  2. **Analysis and Preparation** of a report of an incident which involve an allegation(s) of a believed misuse of a system.
    - ◆ System = platform, network device, application, users are part of the notional system,
    - ◆ Platforms = desktop, workgroup, line-of business, enterprise.
  3. **Defense of expert report.**
    - ◆ Review of observations.
    - ◆ Conclusions derived by appropriate managerial, law enforcement or judicial authorities.

# Overarching Forensic Themes

- ◆ Forensics is a business and risk/management function to help an organization defend attacks against:
  - Systems,
  - Platforms.
  - Use of systems - systems services.
  - Applications,
  - Data and reputation.

# Overarching Forensic Themes

- ◆ Forensics is one example of management's fiduciary responsibility to preserve and protect the ongoing business operations of the firm.
- ◆ Forensics are key to the use of sanctions:
  - Administrative.
  - Civil.
  - Criminal.

# Overarching Course Themes (Continued)

Forensics are inherently both multi-disciplinary and collaborative in both scope and process.

Restated Forensics has three phases:

-  Acquisition & Investigation.
-  Preparation of findings and observations.
-  Defense of expert report.

Forensics require a implicit framework of:

1. People.
2. Processes. (these are in each phase).
3. Tools.
4. Measures.

# Data on XP Platforms/Devices



**Hard Disks**



**Floppy Disks**



**Printers**



**Support Chip Complement**



**Input/Output Devices**



**Recovery Media**



**Legacy Files – Pack-ups and Back-ups**



**Processors (Processor ID)**



**Running Memory – Solid Memory**



**Networking (Logs and MAC Addresses)**



**Network and Server Logs**



**ISP and Phone Records**

# Data Stores

- ◆ Binary ( on – off) 1 or zero
- ◆ Typically in groupings of 7 or 8 bits per character/number – termed byte
- ◆ Hexadecimal Representation
- ◆ International representation
  - ASCII – American Standard Code for Information Exchange (256 Characters)
    - ◆ Character A = 1100001
  - EBCDIC – Extended Binary Coded Decimal Interchange Code – (IBM Mainframes)
- ◆ Both Text, Sound and Graphics are stored in binary formats
- ◆ File conventions determine actual formats

# Physical Media

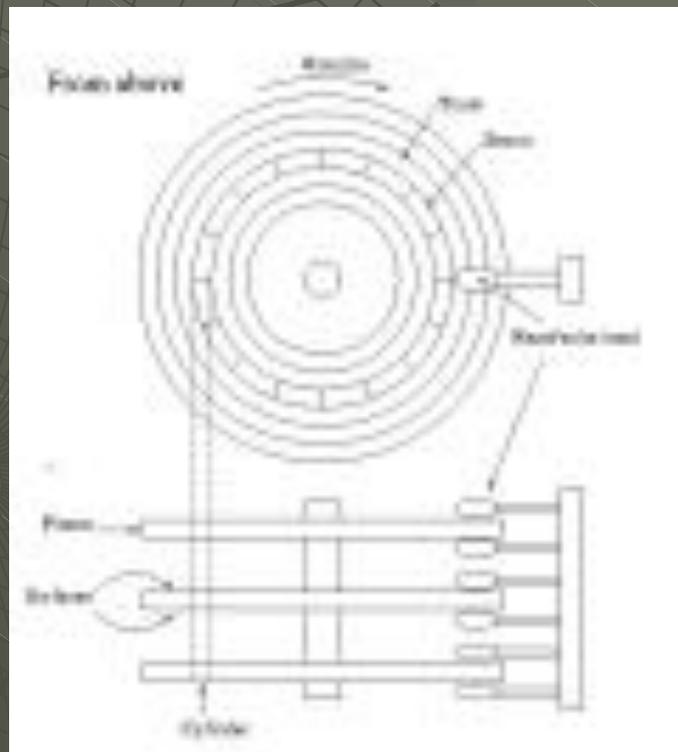
- ◆ Magnetic media use principles of electromagnetism to record and change data
- ◆ Optical media used light in the form of lased to alter reflectance on the surface of the media
- ◆ Printing uses either laser, dye or physical devices to provide the image on paper or film.

# Some Terms

- ◆ Physical Device
  - ◆  Single Disk (SLED)
  - ◆  Redundant Disks )RAID
  - ◆  Platter and Cylinder
- ◆ Logical Device
- ◆ Partition
- ◆ Tracks
- ◆ Sectors

# Hard Drives

- ◆ Illustrative Schematic





# Forensics Data

## ◆ Hardware Identifiers

- Systems Serial
- Some Controllers have unique numbers
- Processor ID – Intel Pentium 3
- National Semiconductor do not have a PSN but have other security tokens
- Disk Serial Number
- EPROM – BIOS Processor
- MAC Address on Network Card - IEEE Organizationally Unique Identifier (OUI)
- Cell Phones - Universal Identifiers (UIDs)
- PDA's have Universal Identifiers (UIDs)

# Forensics Data

- ◆ Software Identifiers

- Operating Version and Systems Build
- Registry

**Hive: HKEY\_CURRENT\_USER**

**Key: Control Panel\Desktop\**

**Name: PaintDesktopVersion**

**Type: REG\_DWORD**

**Value: 0**

- User Accounts
- File and Volume Information
- Application Install Dates

# Folders and Files

- ◆ Recycle Bin
- ◆ Hidden Folders
- ◆ Users – Systems Folder
- ◆ Word/Excel Files
  - MS Office Encryption
- ◆ Graphics Folder
- ◆ Browser Folder
- ◆ Emergency Recovery Disks
- ◆ Registry
- ◆ Paging or Swap Files
- ◆ Print Files
- ◆ Backup Files – Applications
- ◆ Special Tokens

# Microsoft Security ID

- ◆ The SID
- ◆ Open Registry Editor and navigate to:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion  
\ProfileList

- ◆ Under the ProfileList key, you will see the SIDs. By selecting each one individually, you can look at the value entry and see what user name is associated with that particular SID

# Microsoft Special ID's

- ◆ **Encrypted File System Information**  
Displays information about encrypted files on NTFS partitions
- ◆ **Event Logging Utility**  
Logs events to a local or remote computer
- ◆ **Get MAC Address**  
Gets a computer's MAC (Ethernet) layer address and binding order
- ◆ **Get Security ID**  
Compares the security ID's of two user accounts
- ◆ **GUID to Object**  
Maps a GUID to a distinguished name
- ◆ **Processor.vbs**  
Gets the CPU information for a machine
- ◆ **Registry Dump**  
Dumps all of or part of the registry to standard output.

# Microsoft Special ID's

- ◆ **Registry Find**  
Searches and optionally replaces registry data.
- ◆ **Registry Reference**  
Detailed description of Windows 2000 registry content
- ◆ **Registry Restoration**  
Restores all or part of the registry
- ◆ **Registry Scan**  
Searches for a string in registry keynames, valuenames and value data
- ◆ **SystemAccount.vbs**  
Displays system account information

# Microsoft Special ID's

- ◆ **Up Time**  
Displays system uptime
- ◆ **Virtual Address Dump**  
Shows the state and size of each segment of virtual address space
- ◆ **Where**  
Locates files on a hard disk or network
- ◆ **Visual File Information**  
Retrieves and generates detailed information on files, such as attributes, versions and flags
- ◆ **XacIs**  
Displays and modifies security options for system folders

# DOS/Windows Files Attributes

File attributes can be used to write-protect, hide, and unhide files. The attributes are called Read Only, Hidden, Archive, and System, and are described below:

- ◆ **Read Only:** A file that is marked Read Only cannot be altered. It can be read, but it cannot be changed or deleted.
- ◆ **Hidden:** By default, hidden files do not appear in a directory listing.
- ◆ **Archive:** The Archive attribute can be used to selectively back up or copy files.
- ◆ **System:** System files are files flagged for use by the operating system and are not usually displayed in a directory listing.

# File Properties

You can also see the attributes by examining the file's properties (right-click the file and select Properties). You will notice that in **Windows Explorer's** details view that attributes are shown as a single letter. Here are the definitions of those letters:

**R** - Read-only

**A** - Archive

**S** - System

**H** - Hidden

- ◆ Some programs may display them in a different order - such as the order they appear on disk, which is **ASHR**.
- ◆ Example - Encase reports CAWS - Create Access Written and System

# File Attributes

- ◆ **Read-only** - This is normally set for files which we do not wish to alter in any way. Some programs can over-ride the read-only attribute but you are warned before being allowed to do so.
- ◆ **Archive** this attribute gets set every time you create a new file or edit an existing one. It denotes that the file has changed since it was last backed up using a backup program
- ◆ **System** - Files marked with the System attribute are generally used by the OS.
- ◆ **Hidden** - Files marked with the Hidden attribute are files which can be hidden from Windows and DOS. Although it is possible to show hidden files (their icons appear "dimmed")
- ◆ **Folders** are just like any other file - they just don't (and can't) contain any data. They can contain files, but the data in a file belongs to the file, not the folder. On disk, a folder has no size. However, the amount of data in a file is considered part of the folder's size. Folders can also have **Read-Only**, **System** and **Hidden** attributes,

# File Attributes

- ◆ Clear

```
attrib -s -h -r filename.ext
```

- ◆ Add

```
attrib +h filename.ext
```

- ◆ Alter Date, Time, & Attributes  
without leaving Windows or going  
into DOS

# Attribute Bit Flags

<b>Attribute</b>	<b>Bit Code</b>
<b>Read-Only</b>	00000001
<b>Hidden</b>	00000010
<b>System</b>	00000100
<b>Volume Label</b>	00001000
<b>Directory</b>	00010000
<b>Archive</b>	00100000

# *File Extensions*

- ◆ A file in DOS does not need to have an extension. You can test this quite easily by creating a file called **FOO** and saving it in your DOS test directory. Do a directory listing using the DIR command, and you will see it listed. But the file extension does have its uses in DOS. Certain file extensions have built-in meanings in DOS, such as:
  - EXE = An executable file
  - COM = A command file
  - SYS = A system file
  - BAT = A batch file
- ◆ Other extensions are created by a particular software program, or by you when you create a file. One thing that is very different in DOS, when compared to Windows, is that DOS does not have the "associations" that Windows has.

# Problems with XP File Forensics

- ◆ File Names
- ◆ Duplicate files
- ◆ Name and Contents
- ◆ DOS vs. Windows Naming Conventions
- ◆ Folder – Application – File Interactions – MS Office/Exchange
- ◆ Non-English Syntax
- ◆ Unicode - is the universal character encoding scheme for written characters and text. It defines a consistent way of encoding multilingual text.
- ◆ Special File Conventions
  - Microsoft Data Streams

# File Types

- ◆ <http://www.filespecs.com>, to help categorize and collect the vast number of file formats available on the net. Please take a look and remember that comments and feedback are always encouraged.
- ◆ <http://www.wotsit.org>, can help id files

# Microsoft Data Streams

- ◆ Each file typically contains attributes such as name, timestamp, size and location.
- ◆ In NTFS, this information is stored in the Master File Table (MFT). All file attributes are part of this MFT. However, some files of less than 1500 bytes can be stored entirely inside the MFT. In addition, the MFT can hold file attribute information that is *resident* (stored inside the MFT) or *nonresident* (stored somewhere else on the disk).
- ◆ This is where the data streams are utilized. As with the attribute information, data can also be stored outside the conventional boundaries of the file using pointers to locate different portions of the file that can physically be located throughout the storage device

# Anti-Forensics Tools

- ◆ Backdoor “Santas”
- ◆ Cleaning the Registry – Regedit32
- ◆ Disk Scrubbers – Secure Delete
- ◆ Encryption – typically PGP
- ◆ Evidence Eliminator Application
- ◆ Hidden or Encrypted Partitions
- ◆ Special RAM based Personal Computers(2600 18:4)
- ◆ Special Steganography tools
- ◆ Windows Washer Application

# Forensics Tool Kits



# The Encase Forensics Model

- ◆ Data Acquisition
- ◆ Verification
- ◆ Analysis
- ◆ Reporting

# Forensics Imaging Tools (Bit Copy)

- ◆ Hardware

***Intelligent Computer Solutions***

<http://www.ics-iq.com>

***Logiccube*** <http://www.logiccube.com>

- ◆ Software

SnapBack DatArrest

[http://www.cdp.com/CDP\\_dot\\_com/index.htm](http://www.cdp.com/CDP_dot_com/index.htm)

**Safeback** <http://www.forensics-intl.com>

Forensics Tools &  
Processes for XP - Larry  
Leibrod

**Nero5 CD** <http://www.nero.com>

# Investigation Tools

- ◆ **Access Data – Forensics Tool Kit**  
<http://www.accessdata.com>
- ◆ **Encase -**  
<http://www.guidancesoftware.com/html/index.html>
- ◆ **Hex Workshop – and Vidor**  
<http://www.bpsoft.com>
- ◆ **ILook (Law Enforcement Only)**  
<http://www.ilook-forensics.org>

# Investigation Tools

- ◆ **Maresware**

<http://www.dmares.com>

- ◆ **Norton**

<http://www.symantec.com/nu>

- ◆ **Paraben**

<http://www.paraben.com/html/index.html>

# Some Professional Tradecraft

-  Create authentic replicant(s)
-  Perform a summary enumeration
-  Perform an detailed investigation and catalog observations
-  **Revalidate** your observations
-  Prepare your forensics report
-  Defend your findings

# Some Professional Tradecraft

-  Commit to learn your profession and forensics science
-  Start with a “close to the metal” tools – then graphics-based forensics environments
-  Attend forensics and systems training
-  Cross validate tools
-  Practice
-  Use a crawl – walk – run leaning model

# Tools - Forensic Copying of Digital Evidence (Forensic Replicant)

Prepare authoritative evidentiary copy of evidence.

- Make an evidentiary “replicant” - I personally use case number conventions R1 - R2 - R3.
- Insure replica is identical - Instruments: checksum or MD5 hash. X509r3 key signing, PGP.
- “Never” conduct any “intrusive” investigation of any non-replica evidence - without special court order. (Avoid allegation of any destruction of evidence - “**spoliation**”).
- Be prepared for making distinctions between intrusive and non-intrusive investigation.
- Know - test - validate your replicant instrument.

# Tools - Summary Enumeration of Evidence (Replicant)

- 📁 Data contained on subject device (watch for hidden artifacts)
- 📄 Applications - versions
- 📄 User tokens
- 📄 Devices (disks - CD, platforms, printed media)
- 📄 Operating systems - versions - build number (watch for hidden artifacts) (OS startup directives -services/processes)
  - ◆ GUID
  - ◆ SUID
  - ◆ Application tokens

# Tools - Summary Enumeration of Evidence (Replicant)

-  Network artifacts - IDS and firewall logs
-  File systems, file system, metadata - steganographic methods
-  Disk geometry - disk ids (caution about non-authoritative instrumentation report)
-  BIOS - disk drive BIOS (term of practice - data stuffing)
-  Manufacturers serial numbers, product number, country of origin markings

# Tools - Prepare a Catalog of All of the Attributes

Carefully characterize the Attributes of the Evidence contained on the Evidentiary Replicant

- Date/Time tokens
- Character of Data - ASCII, Text - Unicode
- Metadata
- Any Cryptographic Token observed?
- Images - graphics - “Steganography” Materials
- Software Applications
- BIOS - Physical media ID’s

# Tools - Prepare a Catalog of All of the Attributes.

- ◆ Insure that the catalog is correct, complete, dated and signed.
- ◆ This catalog absolutely must be exhaustive - omit nothing.
- ◆ Insure that the date of the catalog is authoritative.
  - The Atomic Clock anecdote.
  - NNTP and Win Time.
- ◆ Recommend both paper and digital media for storage of catalog.
- ◆ Consider versioning of catalog iterations.

# Tools - Conduct the Forensic Investigation (Instruments)

-  Have either formal training or experience in the specific instruments that you intend to use in this investigation.
-  Rationalize your use of the specific instruments.
-  Obtain and document the versions of all instruments, make sure your licenses are in order.
-  Understand the strengths and weaknesses of all instruments.
-  Be able to explain and demonstrate the operation and “reporting” of the particular instruments.

# Tools - Conduct the Forensic Investigation

-  Make a set of Observations - Recommend you consider having a working limits of 5 +/- 2 observations.
-  Retest - Revalidate your observations.
-  Cross-validate observations and re-verify the instrument reporting data.
-  Record instrument outputs - screen shots and documentation references.
-  Contact "trusted parties" to test any anomalies or untrusted observations derived from instruments.

# Tools - Prepare the Forensic Report

-  Document your observations in a set of working papers by chronological notes contained in the particular work record.
-  Report in your work record, your assessment of instruments, data reports, facts, observations and judgments.
-  List of references you used or consulted.
-  Recommend major observations be limited to about 5 +/- 2 - avoid unnecessary complexity.

# The Generalized Framework

1. Protect seized evidence
  2. Recover deleted files
  3. Discover (enumerate) files contained in seized materials (notable text, binary, hidden & encrypted)
  4. Discover swap, temp/tmp, file slack meta-data and artifacts
  5. Explore all unallocated space
  6. Conduct searches for key terms, special data – imagery
  7. Note any observed versus expected files, folders binaries, www data, emails and file conditions
  8. Prepare a written report – archive data, findings
- Provide expert consultation and testimony, as necessary

# Problems with this Forensics Model

- ◆ User versus person (suspect)
- ◆ Ignores meta-data and registry “richness”
- ◆ Alphabetical character representation
- ◆ Ignores malicious code and the mobility of malicious code
- ◆ Ignores anti-forensics tools
- ◆ Probative links are not apparent – meaning lack of clear key linkages –

# Anti-Forensics Tools

- ◆ Backdoor “Santas”
- ◆ Cleaning the Registry – Regedit32
- ◆ Disk Scrubbers – Secure Delete
- ◆ Encryption – typically PGP
- ◆ Evidence Eliminator Application
- ◆ Hidden or Encrypted Partitions
- ◆ Special RAM based Personal Computers
- ◆ Special Steganography tools
- ◆ Windows Washer Application

# A Forensics Model

- ◆ A more flexible method that centers on people – processes – tools – measures
- ◆ Explore and better describe the linkages among
  1. User to a Platform (device – operating environment – connectivity)
  2. Platform to Applications
  3. Applications to Notable Data
  4. Note special data and device artifacts beyond our typical notions of disk media
  5. Characterize time and timing meta-data

# Human Judgment Factors (measures) for the Forensics Practitioner

1. Are all procedures, processes, and instruments (tools) involved in the forensics examination – understandable, sound, subject to public demonstration & auditable?
2. Can the prosecutor – (law enforcement) prove the subject (person) was the sole user on the subject platform?
3. Could the evidentiary data have been altered or in any way modified for seizure to deposition?

# Human Judgment Factors (measures) for the Forensics Practitioner

4. Is any evidentiary data been compromised under attorney/client privilege?
5. Is there a possibility that another user, network access or malicious code placed or altered any data on the subject platform?
6. Was the search – lawful, given the nature of the allegation or offense?

# Evidence

- ◆ Notable items versus evidence
- ◆ Broad tests for all forensics notable items and evidence
  1. Authenticity
  2. Reliability
  3. Completeness
  4. Free from interference and contamination

# Some prevailing frameworks for forensics investigations

- ◆ US Laws
- ◆ Federal Guidelines
  - DOJ – FBI
  - DOD
  - NIST
- ◆ IOCE Guidelines
- ◆ Some national and EU Privacy Issues
- ◆ The prevailing model
  - Seizure, forensics (bit copy), examination, report, deposition, testimony, archiving
  - Data extracted from both logical and physical media (active and recovered) files, data artifacts, swap space and file – device slack
  - Focus is on finding data contained in files

# The Generalized Framework

1. Protect seized evidence
  2. Recover deleted files
  3. Discover (enumerate) files contained in seized materials (notable text, binary, hidden & encrypted)
  4. Discover swap, temp/tmp, file slack meta-data and artifacts
  5. Explore all unallocated space
  6. Conduct searches for key terms, special data – imagery
  7. Note any observed versus expected files, folders binaries, www data, emails and file conditions
  8. Prepare a written report – archive data, findings
- Provide expert consultation and testimony, as necessary

# A Forensics Model

- ◆ A more flexible method that centers on people – processes – tools – measures
- ◆ Explore and better describe the linkages among
  1. User to a Platform (device – operating environment – connectivity)
  2. Platform to Applications
  3. Applications to Notable Data
  4. Note special data and device artifacts beyond our typical notions of disk media
  5. Characterize time and timing meta-data

# Recommended Computer Forensics Professional Development

- ◆ Initially focus on a single client platform (
- ◆ Start using “close to the metal” tools – consider shareware first
- ◆ Learn by practice and from peers
- ◆ Experiment – Test you findings and new ideas
- ◆ Read and study your craft
- ◆ As your skills build – invest in more advanced tool courses - conferences

# A Great Set of Forensics Tools

## Thanks to 2002 George M. Garner Jr

### [Forensic Acquisition Utilities-1.0.0.1029\(beta1\) Release Notes](#)

Included in this release are the following modules: Copyright ©

- ◆ [dd.exe](#): A modified version of the popular GNU dd utility program
- ◆ [md5lib.dll](#): A modified version of Ulrich Drepper's MD5 checksum implementation in Windows DLL format.
- ◆ [md5sum.exe](#): A modified version of Ulrich Drepper's MD5sum utility.
- ◆ [Volume\\_dump.exe](#): An original utility to dump volume information
- ◆ [wipe.exe](#): An original utility to sterilize media prior to forensic duplication.
- ◆ [zlibU.dll](#): A modified version of Jean-loup Gailly and Mark Adler's zlib library based on zlib-1.1.4.
- ◆ [nc.exe](#): A modified version of the netcat utility by Hobbit.
- ◆ [getopt.dll](#): An implementation of the Posix getopt function in a Windows DLL format.
- ◆ Thanks to 2002 George M. Garner Jr
- ◆ This is on your CD File Name is forensic acquisition utilities-1.0.0.1029(beta1)
- ◆ The Hash is D8D0C7E13DD646582C1B2470D6244A4C

# Specialist Forensics Tools

- ◆ Forensics Computers [www.ics-iq.com](http://www.ics-iq.com)



- ◆ Firewire 1394 Drive Blockers <http://www.scsipro.com>



Forensics Tools &  
Processes for XP - Larry  
Leibrock

# My Appreciation

- ◆ Thank you for your time and interest
- ◆ Thank you for your support of the forensics community of practice
- ◆ I request your written evaluation
- ◆ My Coordinates
  - [Larry.Leibrock@eforensics.com](mailto:Larry.Leibrock@eforensics.com)
  - <http://www.eforensics.com>
  - Austin, Texas (512) 471-1650
  - GMT Time -5

# Useful References



# General Forensic Investigations

- ◆ ***Beyond the Crime Lab*** ISBN 0-471-25466-5
- ◆ ***Criminalistics-The Profession of Forensics Sciences***  
ISBN 0-13-592940-7
- ◆ ***Cybercrime*** ISBN 0-415-21326-6
- ◆ ***Dark Ages II- When the Digital Data Die*** ISBN 0-13-066107-4
- ◆ ***Henry Lee's Crime Scene Handbook*** ISBN 0-12-440830-3
- ◆ ***High-Technology Crime*** ISBN 0-9648171-0-1
- ◆ ***High-Technology Investigators Handbook-Working in the Global Information Environment*** – ISBN 0-7506-7029-0

# Computer Forensic Investigations

- ◆ **Computer Forensics** ISBN 0-201-70719-5
- ◆ **Computer Forensics & Privacy** ISBN 1-58053-283-7
- ◆ **Digital Evidence and Computer Crime** ISBN 0-12-162885-X
- ◆ **Disk Detective** ISBN 0-87364-992-3
- ◆ Farmer & Venema's Forensic Computing Workshop  
<http://www.porcupine.org> Papers also in Dr. Dobbs Journal
- ◆ **Forensics Computing-A Practitioners Guide** ISBN 1-85233-299-9
- ◆ **Investigating Computer-Related Crime** ISBN 0-8493-2218-9
- ◆ **Investigating Computer Crime** Franklin ISBN 0-8493-8158-4
- ◆ **Information Hiding Techniques for Steganography and Digital Watermarking** ISBN 1-58053-4

Forensic Computing  
Processes for XP - Larry  
Leibrock