



Forensics Tools and Processes for Windows XP Clients

Larry Leibrock, Ph.D.

Singapore
October 3, 2002

I am *not* a Practicing Attorney - however, I am on the teaching faculty of a University of Texas - Law School and Business School



Caveats and Rights of Use

- My skills, background - forensics profession and at trial experience
- This tutorial is *not - legal advice or legal opinion*
- Who do I speak for? - *me* - no university or governmental affiliations -
- No warranty for fitness - express or implied

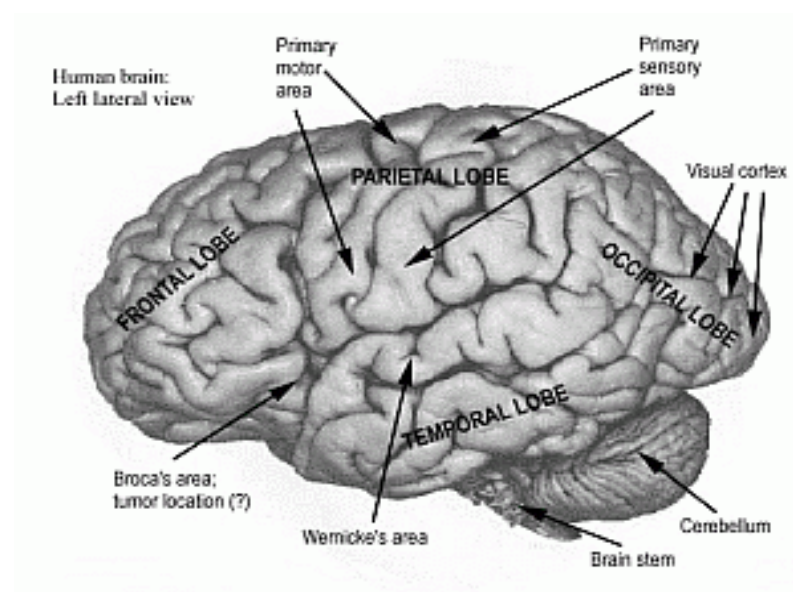
Caveats and Rights of Use

- No grant of license for software or technology that may be developed that supports this material
- Risk of use - are expressly yours - *not mine*
- Your attendance in this talk, from here on, marks your agreement to these aforementioned caveats, conditions and limitations

Your Questions A Protocol

Γ Please Ask Questions - whenever you need to.

- I reserve the obligation to ask you questions
- Let's collectively feed our brains.



Introduction

- What you should learn in this tutorial
 - Focus - Forensics Tradecraft - little attention to forensics “science-theory” or computing theory
 - Overview of Windows XP in context of Forensics Investigation - in both
 - non-liturgical and
 - liturgical settings
- The intended level of knowledge for this material
 - Not deep expert level skills for - experienced practitioners - there are more day and week long expert-level courses
 - This is intended to be an in-depth overview for both managerial and technical IT leaders

Work Plan and Agenda

Time available ~ 11:30 until 13:00 1.5 hours

The primary topics

1. Define Forensics
2. Discuss some Human Factors related to Forensics
3. The Windows XP - Intel Platform
4. The Applications - The Data
5. A selected tool set and forensics instruments
6. Special Items of Forensics Interest

Forensics Defined

- Two primary classes of computer forensics Investigations

Φ Liturgical

Φ Non-Liturgical

- Question - Why should one consider or perform a non-liturgical forensics examination in your business settings ?

Forensics Defined

- Forensics Defined - collection of people - processes - tools - measures to gather ??????? which support or refute certain allegations of misuse involving computer system(s).
- Let's Discuss - The notions of evidence versus items of note, artifacts, findings, materials and data

Forensics Defined

- **People**

- Demonstrated Expertise in using, explaining the forensics procedures and findings
- Dis-Interested Relationship - both Firm/Investigator and Subject/Investigator
- Examiner Qualifications - knowledge - training - skills - experience

- **Processes**

- Accepted
- Auditable
- Chain of Custody
- Peer-review
- Repeatability
- (understandable and can be explained to non-technical people)

Forensics Defined

- **Tools (Instruments)**

- Avoid Data contamination (non-intrusion)
- Findings of facts - Cross-validation
- Prior Use
- Validity

- **Measures**

- Fact-based - testable (True or False Assertion)
- The inter-dependending tests for integrity, validity and reliability
- In a final sense - **Truthful** - from which a court can render judgments



Forensics Operationalized

- Forensics, the computer, the device, the data (electrons)
- Some Definitions
 1. Investigating what has happened
 2. Audit relative to use - event - policy
 3. Sanctions: - Criminal - civil - administrative

Forensics Defined: collection of people - processes - tools - measures that support or refute certain allegations or suspicions of misuse which involve a computer system

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 and 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?

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
9. 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 - “Nexus Problem”

An exemplar - Windows XP as a forensics platform

- Some details
 - Organization
 - Present Variant & Builds
 - Installations
 - Supported Computers
 - Physical Media
 - Partitions
 - File Types
 - File Hashing of known good and known suspect



XP Organization

- Better Device Support -ACPI and APM for mobile platforms
- File systems - some cryptographic mechanisms
- New User Interface
- Off-line resources
- Primarily- 32 bit Intel - “little endian”
- Replaces Windows 2000 and seeks to support both Home and Corporate Environments.
- The XP Platform “Hash”
- Unicode Compliant
- XP Product is largely based on Windows 2000 code base

Present XP Variants



- XP Home
- XP Professional
- XP .Net Standard Server
- XP .Net Standard Enterprise
- XP .Net Standard Datacenter
- XP 64-bit
- XP SP 1
- How to determine - cmd - ver or System Info Applet



Differences between XP Professional and XP Home

	XP Home	XP Professional
User Accounts	All users are Administrators	Different Accounts & Levels of Rights
Multiple Processors	One	Two
Networking	Peer to Peer	Peer to Peer and Domain
Backup Utility	No	Yes
Dynamic Disks	No <small>Copyright 2002</small>	Yes

XP Professional - Tools and Accessories

- Administrative Tools
- Boot Configuration Manager
- Driver Query
- Multi-Lingual Interface
- NTFS Encryption
- Offline Files and Folders
- Open Files
- Performance and Security Logs
- Remote Desktop
- Scheduled Tasks Console
- Security Template
- Task kill
- Task list
- Telnet Administrator
- Logs are very rarely operative in most installation

Different Installations

- Microsoft recommends clean Installation
- Upgrades leave a lot of residue est. 200 - 500 files
- NT 3.51 & Win 95 and Below - requires clean install
- Win 98, ME, W2K Upgrade
- Microsoft Hardware Compatibility List
- Resources
 - <http://www.microsoft.com/hcl>

Here's What You Need to Use Windows XP Professional

- PC with 300 megahertz or higher processor clock speed recommended; 233 MHz minimum required (single or dual processor system);* Intel Pentium/Celeron family, or AMD K6/Athlon/Duron family, or compatible processor recommended
- 128 megabytes (MB) of RAM or higher recommended (64 MB minimum supported; may limit performance and some features)
- 1.5 gigabytes (GB) of available hard disk space*
- Super VGA (800 _ 600) or higher-resolution video adapter and monitor
- CD-ROM or DVD drive (Not really true)
- Keyboard and Microsoft Mouse or compatible pointing device
- **Related Links**
<http://www.microsoft.com/windowsxp/pro/evaluation/sysreqs.asp>

Physical Media

- Name some Physical Media
 1. Internal Hard Drives
 2. External Hard Drives
 3. Floppies
 4. Zips
 5. Tapes
 6. Smart Media
 7. Keyboards - Mice
 8. Cameras
 9. Printers -
 10. RAM drives

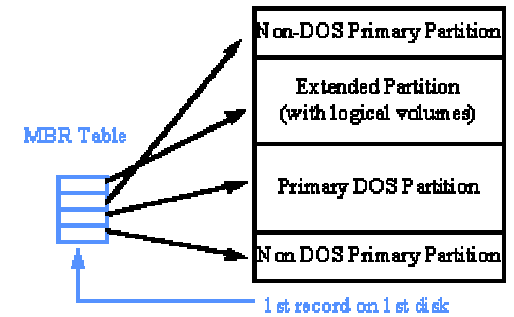


Partitions

- Question - What is the purpose?
- How many partitions?
- Name the types?

1. Active
2. Extended
3. Hidden
4. None
5. Special types

- Resources <http://www.sysinternals.com/insidew2k.shtml>



Do not do	
FAT32 Windows 95	NTFS Windows NT
Can be done, both OS on one volume	
FAT16 NT and Windows 95	
Win95 and NT - Dual boot	
FAT16 Windows 95 and Boot Partition	Windows NT - Extended Partition
Windows NT	
NTFS All NT, no 95	

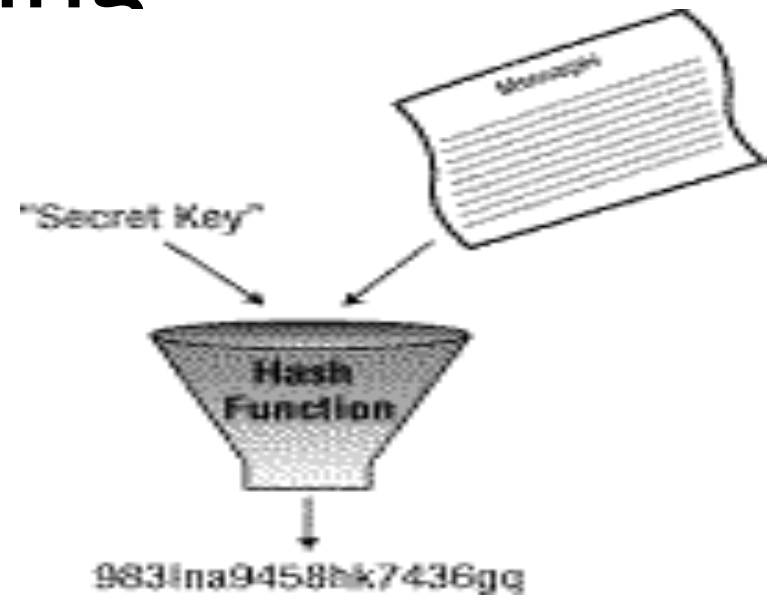
Prevailing XP File Types

- Extended - exceeds arbitrary 4 partition limit - must create logical within this partition
- FAT 12 - uses a FAT - 512 kb cluster scheme
- FAT 16 - for partitions beyond ~ 8GB
- FAT 32 - 256 MB to 2 TB
- NTFS Journal (bit-map) FS - > 400MB - 10 TB
 - EFS
- CDFS
- Question - What is the relevance of FAT?

File Types

- Windows XP does not fully correlate file signatures (metadata) to file extension
- Prevailing extensions
 - DLL
 - EXE
 - XLS
 - TXT
 - HTM or HTML
 - JPG
 - DOC
- Resources
 - <http://www.computeruser.com/resources/dictionary/filetypes.html>
 - <http://filext.com/>

File Hashing

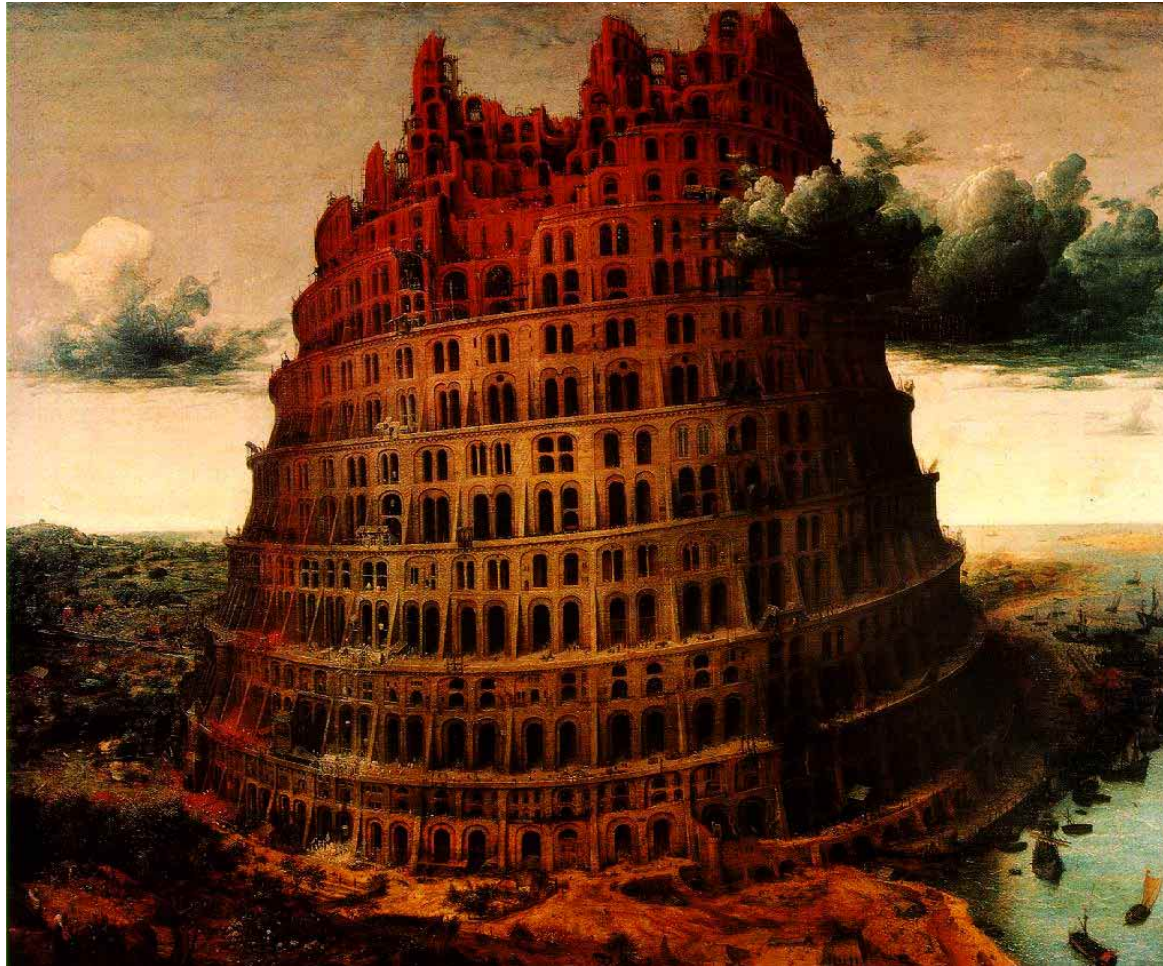


- Window XP Hash Sets?
- What do we need these?
- Where are these located?
- Working to host these items?

Hashing - Explained

- A so-called digest is, similar to a checksum, a characteristic number used for verification of data authenticity. But digests are more than that - digests are strong one-way hash codes.
- It is computationally feasible to manipulate any data in such a way that its checksum remains unaffected. Verifying the checksum in such a case would lead to the assumption that the data has not been changed, although it has.
- Therefore, digests are used instead of checksums if malicious (i.e. not mere random) modifications to the original data are to be detected. It is computationally infeasible to find any data that corresponds to a given digest. It is even computationally infeasible to find two pieces of data that correspond to the same digest.

Some Special Points relative to XP



Copyright 2002

The XP Registry

- Hierarchical data based that defines the configuration of the platform (folders and sub-folders).
- Legacy
 - Win.ini
 - System.ini
- W2k Size is Restricted to 150 MB
- XP Unrestricted except object entry is limited to 1MB

The XP Registry

- Located in %SystemRoot%\system32\
 - Organized in 5 sections - termed hives
 - Each hive has keys and subkeys which contain a value entry
 - Each value entry has a name, data-type and value
- The XP Registry
 1. HKEY_CLASSES_ROOT (file name - OLE - streams)
 2. HKEY_CURRENT_USER (SID - user - desktop)
 3. HKEY_LOCAL_MACHINE (Configuration, memory last boot)
 4. HKEY_USERS (all user account profiles)
 5. HKEY_CURRENT_CONFIG (running image)
- Note about .SAV files

Typical Window XP Files - Hiding Places

- Browser - history and favorites
- Cluster slack
- Compressed or encrypted folders
- Disconnected Hard-Drive in Chassis
- Email residue
- ERD and Backups
- Files marked for deletion
- Hidden files

Typical Window XP Files - Hiding Places

- Online messenger services
- Normally named files
- Other OS Partition or Virtual Machine
- Print Spool (online and offline)
- RAM Resident Files
- Renamed and Mismatched files
- Sleep or Hibernate Mode Files
- Swap or page files
- Temp and tmp (Word and Excel)
- Zip Drives, CD Devices, Floppies and portable drives

Person or suspect information

Windows XP

- Application logs
- Email accounts
- FTP and Telnet
- IRC - clients
- Paper and key logging
- Special devices (Smartcard and PDA's)
- System Logs
- The XP Registry

The Registry

- Browser settings are stored
- Most de-installations leave forensics “residue”
- Most Recently used
- My Documents
- Recycle or Trash Bin
- Some Application passwords are stored
- Some Applications register name, company, license and sometimes address and install time/date
- Usenet Messages for newsgroups

The Windows XP Intel Platform

- The Disk Drive(s) and engineer-service-order (ESO) sectors or tracks
- The MAC address
- The Platform Hash
- The Processor ID
- The Registry and its form in XP

The Windows XP - The Applications Interface

- Focus
- Folders
- My Computer
- Network Neighborhood
- Quick Launch
- Recycle Bin
- Short cut - (links)
- Start Button
- Task Bar

Windows XP - The Files, Folders and Disks

- Disks A-Z - default consecutively
- Pathnames C:\windows\system\color
- UNC \box21\C\games\warez.txt
- DOS 8.3 and LFN
- LFN up to 260 characters
- Case preserving
- Maximum Path is 80 characters
- File and folder attributes - read - system, hidden, compressed and encrypted

The Windows XP - Special Items of Forensics Interest

- Anti-Forensics Tools
- Applications Meta-data
- Concealed media (logical or physical)
- Data Encryption applications or data
- Digital Cameras
- Global Positioning Devices - maps
- Offline media
- Printers
- Scanners
- Steganography applications
- Windows XP Hardware Hash

Windows XP and Times

- Boot Sequence
- The BIOS
- Windows XP Time Services
- Time and File metadata
- Temporal Challenges among platforms, applications, files and logs
- Time servers
- NTP and clocks
- Investigation times
- Time zone conventions

The Forensics Processes and Working tools

1. Seizure Process
2. bit copy Process (Use special tool - Preliminary Data set)
3. Examination Process
4. Reporting Process
5. Archiving Process
6. Deposition & testimony Process

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

Non-Liturgical Examination

1. Isolate (quarantine) equipment protect from tampering and secure the scene
2. Copy suspect media - rebuild system on new platform
3. Disable user account - create new admin account
4. Track internet use
 - Mail
 - Web
 - Cookies
 - Bookmark
 - History Buffer
 - Cache
 - Temp Internet Files
 - Bookmarks

Non-Liturgical Examination (continued)

5. Internet log times - Contact network administration
6. Recent Documents
7. Enumerate *.exe files
8. Microsoft System Information
9. Walk Registry
10. Enumerate Hidden and archive file
11. Correlate use patterns
12. Document notes

Anti-Forensics Tools

- Backdoor “Santas” - Remote Desktop access
- 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

Forensics Windows XP

A Review for this Tutorial

- Defined and Operationalized Forensics
- Differentiated liturgical and non-liturgical forensics examinations
- The Windows XP - Intel Platform
- The OS Applications - The Data
- Discussed a selected tool set and forensics instruments
- Special Items of Forensics Interest

Parting Points

- Learn the forensics key processes
- Spend time in high-quality forensics tool training after learning shareware tools
- Never “hang on a single nail” when you are doing computer forensics
- Invest in a range of tools, cross-validate your observations
- Build on Dan Farmers idea - do forensics on your on your own system

Recommended Computer Forensics Professional Development

- Initially focus on a single client platform (Windows XX, LINUX, SOLARIS, MAC OS.
- 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

Parting Points

- Know what you know - avoid doing what you do not know - example BEOS assignment
- Practice the Forensics Tradecraft - consider using this learning model:



Crawl



Walk



Run

Windows XP - Notable Resources & Instruments

 (CRAWL) Learning About Forensics Tools

1. Forensic Acquisition Utilities

<http://users.erols.com/gmgarner/forensics>

2. WinGrep and Hurricane Editor

<http://www.hurricanesoft.com>

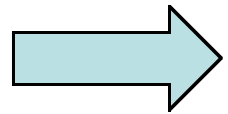
3. WinHex 10.47 <http://www.sf-soft.de/winhex/index-m.html>

4. Evidor <http://www.sf-soft.de/evidor/>

5. Snagit <http://www.techsmith.com/>

6. Various Tools <http://www.tucofs.com/tucofs/tucofs.asp?mode=mainmenu>

Windows XP - Notable Resources & Instruments



(Walk) Learning About Forensics Tools
Registry

1. DumpSec, DumpReg & DumpEvt

<http://www.systemtools.com>

2. Registry Crawler 4.0

<http://www.4dev.com>

3. ECSF

<http://www.winternals.com>

Windows XP - Notable Resources & Instruments

 (RUN) Expert Tools and Instruments

1. FTK <http://www.accessdata.com>
2. Encase - <http://www.encase.com>
3. Solo www.ics-iq.com
4. Paraben - www.paraben-forensics.com
5. ProDiscover DFT - <http://www.techpathways.com>

Specialist Forensics Tools

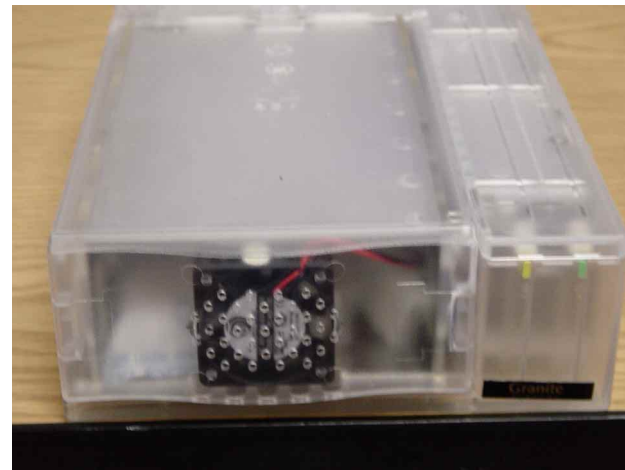
- Forensics Computers

www.ics-iq.com



- Firewire 1394 Drive Blockers

<http://www.scsipro.com>



Special Note and Terms

- Tools are useful - never authoritative
- The tool - instrument reports that_____.
- The following are resources, tools & instruments that I have personal experience -
- I do not sell or derive any compensation from any selling any “product”?

Useful tools

- PC Support Viewer -
<http://www.support-works.com/products/pcaud.htm>
- PC Inspector
<http://www.pcinspector.de/>
- Pest Patrol <http://www.saferite.com/>
- WinHex 10.47 - Professional Version
<http://www.sf-soft.de/winhex/upgrade.html>

Useful - Resources

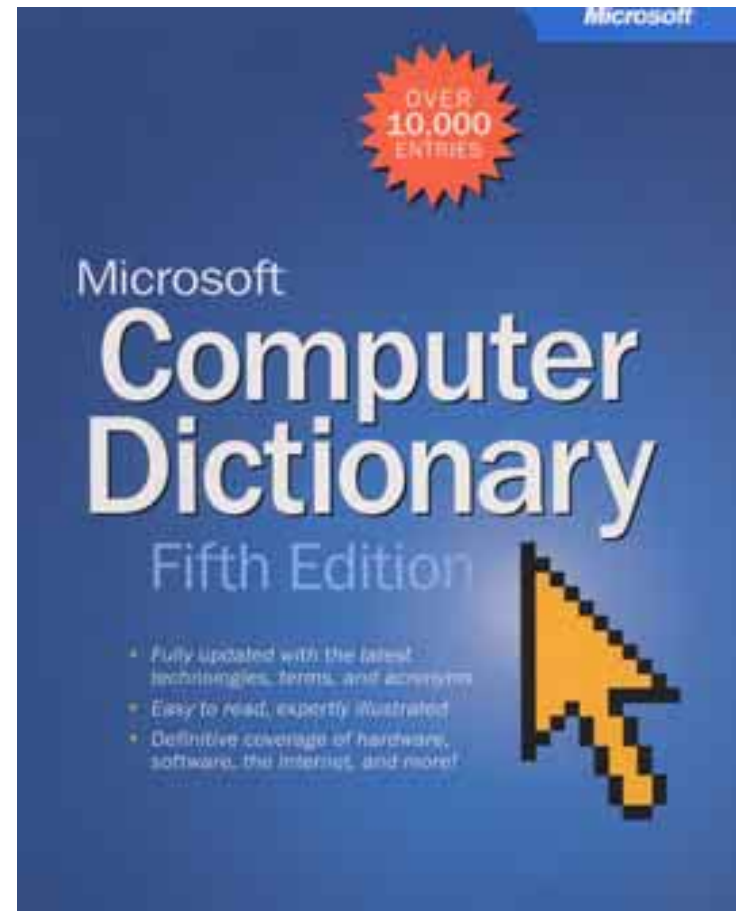
Explaining IT and Physical Logical Concepts

- ***Microsoft Computer Dictionary 5th Edition*** - ISBN 0-7356-149504
- ***How Computers Work 6th Edition*** - ISBN 0-7897-2682-3
- ***New York Time Circuits - How Electronic Things Work*** - ISBN 0-312-28439-X

Notable Resources & Instruments

Explaining Concepts & Terms

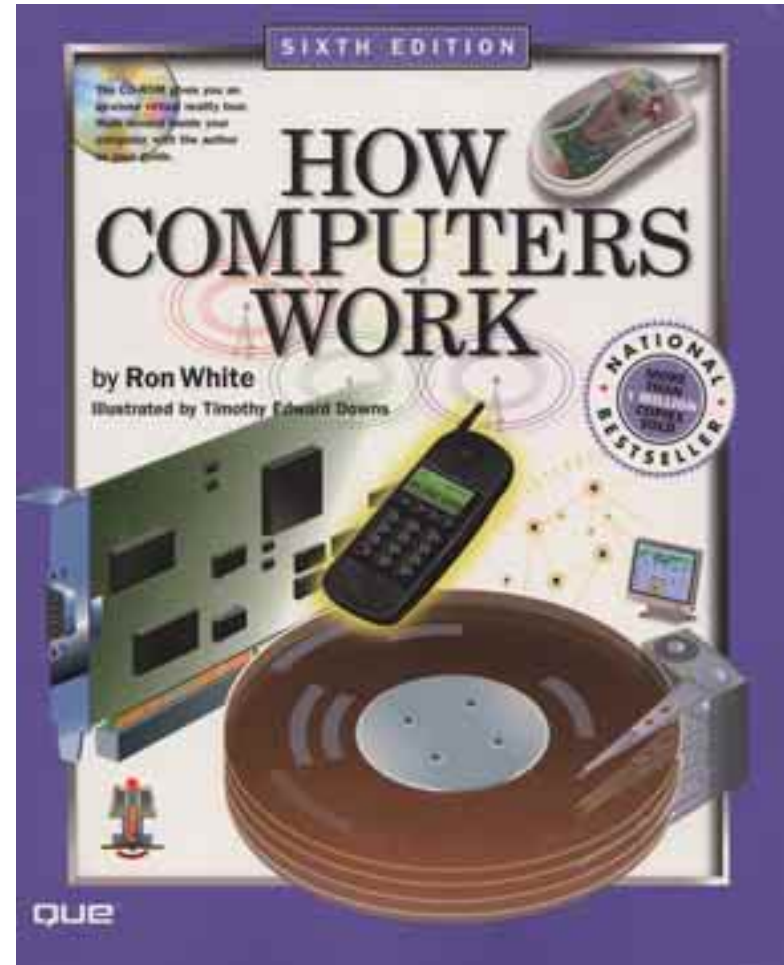
- ***Microsoft Computer Dictionary 5th Edition*** - ISBN 0-7356-149504



Notable Resources & Instruments

Explaining Concepts & Terms

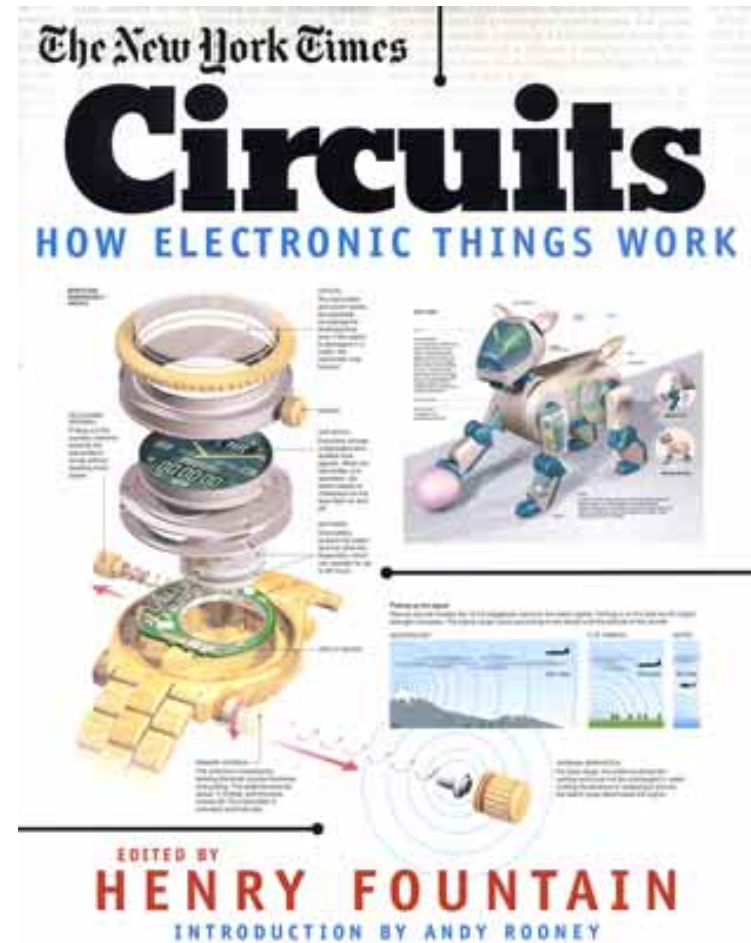
- ***How Computers Work 6th Edition*** - ISBN 0-7897-2682-3



Notable Resources & Instruments

Explaining Concepts & Terms

- ***New York Time Circuits - How Electronic Things Work*** - ISBN 0-312-28439-X



Useful - Resources

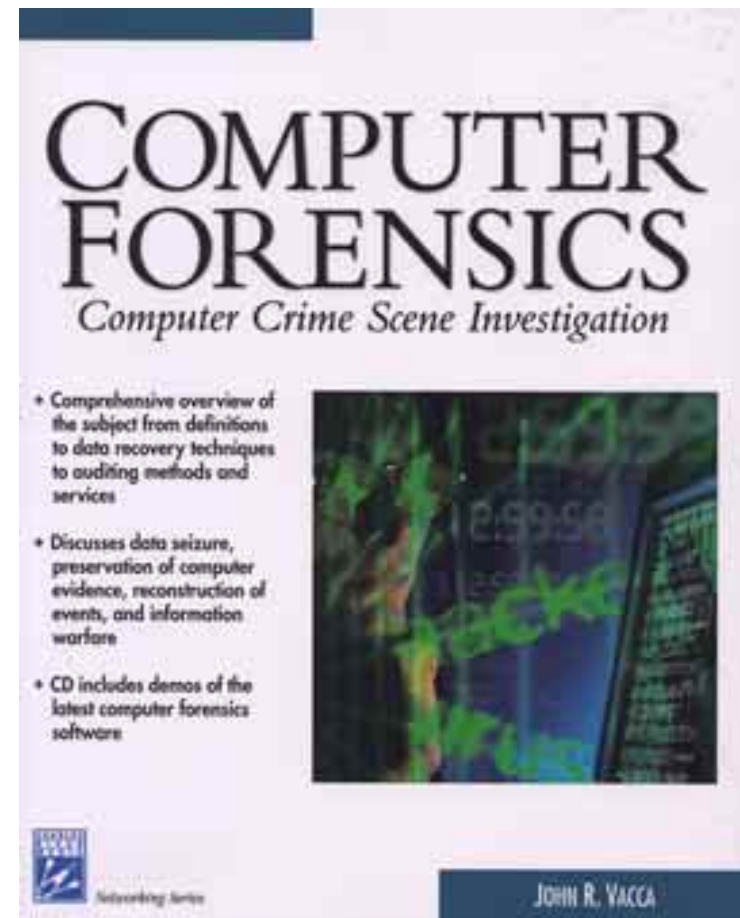
Explaining Forensics

- ***Computer Forensics - Computer Crime Scene Investigation*** - ISBN 1-58450-018-2
- ***Computer Forensics Incident Response*** - ISBN 0-201-70719-5
- ***Cyber Crime Investigators Field Guide*** - ISBN 0-8493 - 1192-6
- ***Cyber Forensics: A Field Manual for Collecting, Examination and Preserving Evidence for Computer Crimes*** - ISBN 0-8493-0955-7
- ***Forensics Computing*** - ISBN 1-89233-299-9
- ***Handbook of Computer Crime Investigation*** - ISBN 0-12-163103-6

Notable Resources & Instruments

Explaining Forensics

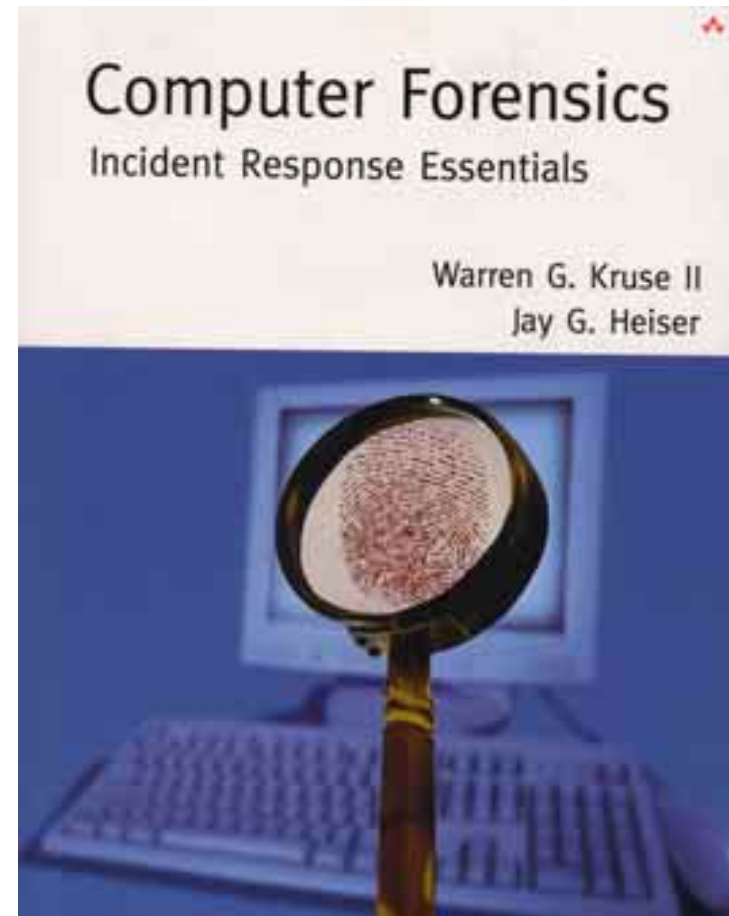
- ***Computer Forensics - Computer Crime Scene Investigation - Investigation -***
ISBN 1-58450-018-2



Notable Resources & Instruments

Explaining Forensics

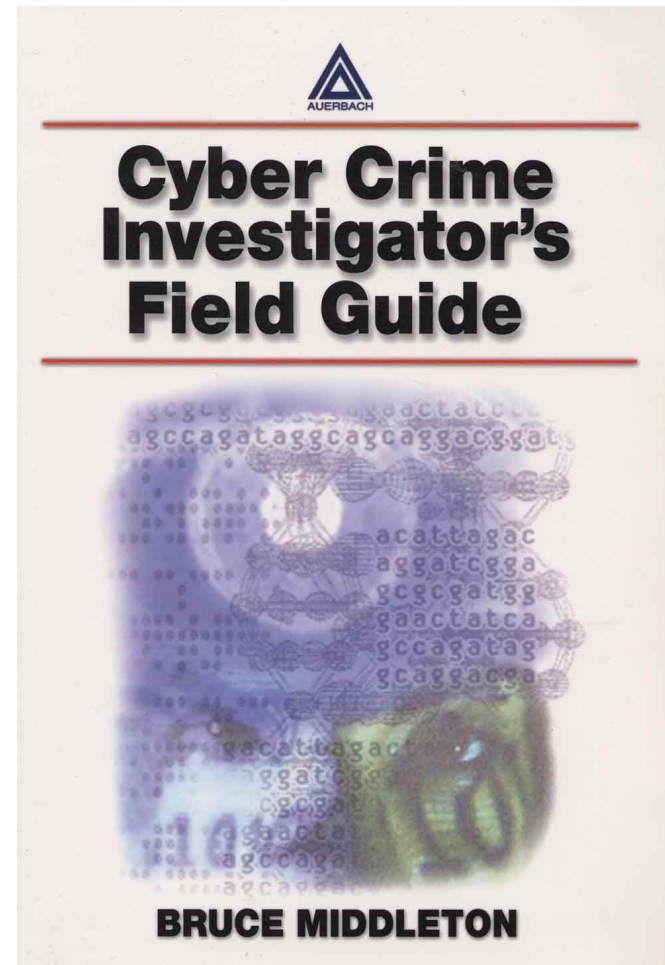
- ***Computer Forensics Incident Response*** - ISBN 0-201-70719-5



Notable Resources & Instruments

Explaining Forensics

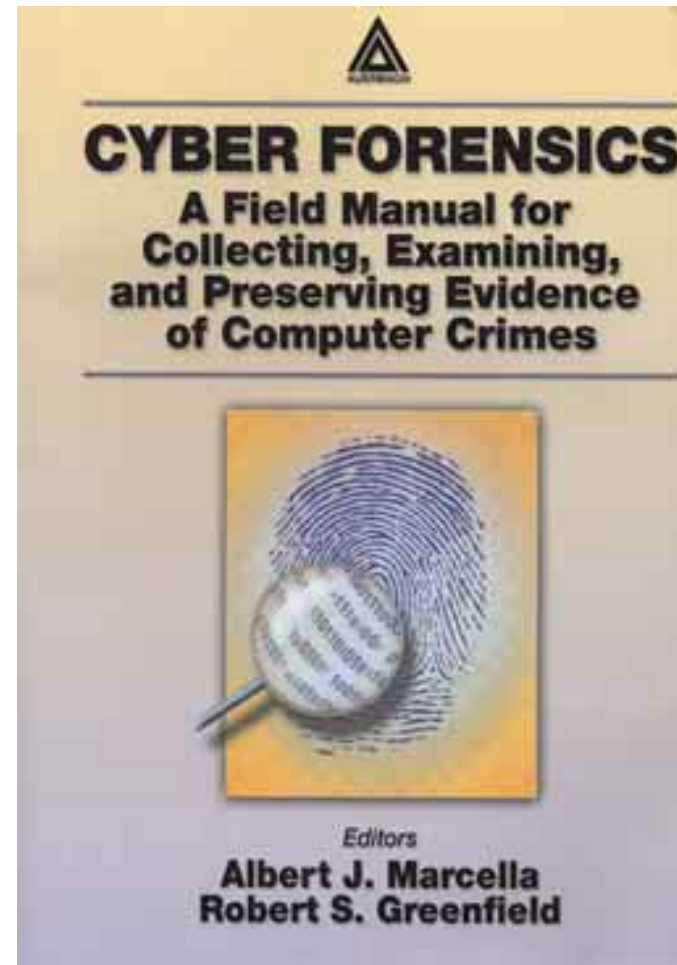
- ***Cyber Crime Investigators Field Guide*** - ISBN 0-8493 - 1192-6



Notable Resources & Instruments

Explaining Forensics

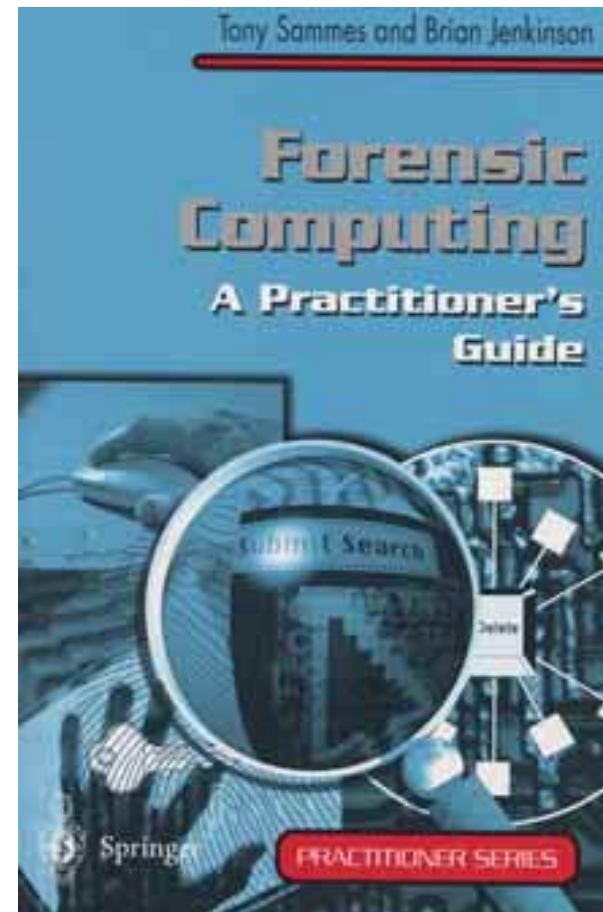
- *Cyber Forensics: A Field Manual for Collecting, Examination and Preserving Evidence for Computer Crimes*
- ISBN 0-8493-0955-7



Notable Resources & Instruments

Explaining Forensics

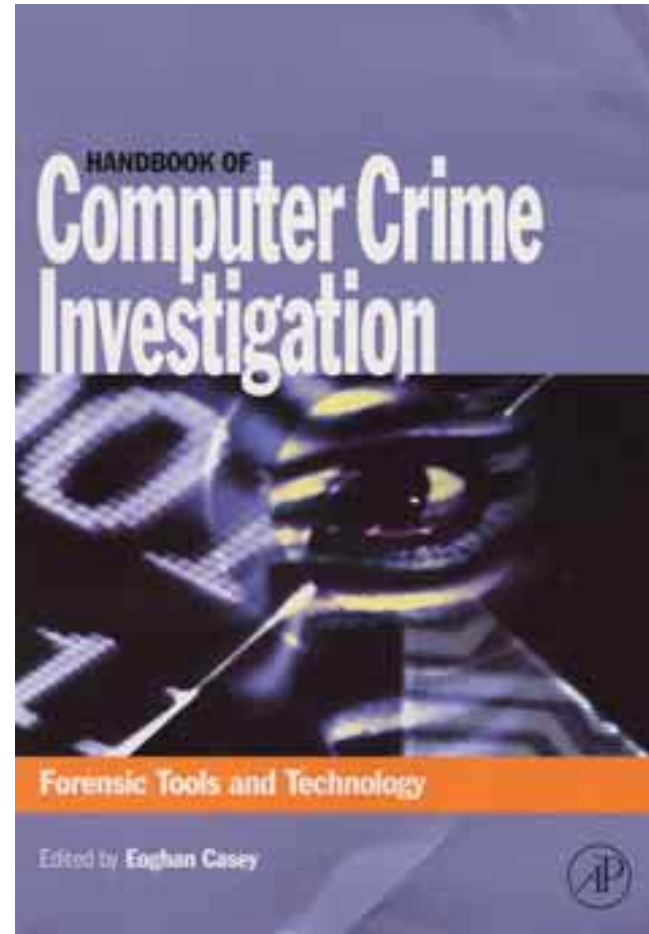
- ***Forensics Computing -***
ISBN 1-89233-299-9



Notable Resources & Instruments

Explaining Forensics

- ***Handbook of Computer Crime Investigation*** - ISBN 0-12-163103-6



Useful - Resources

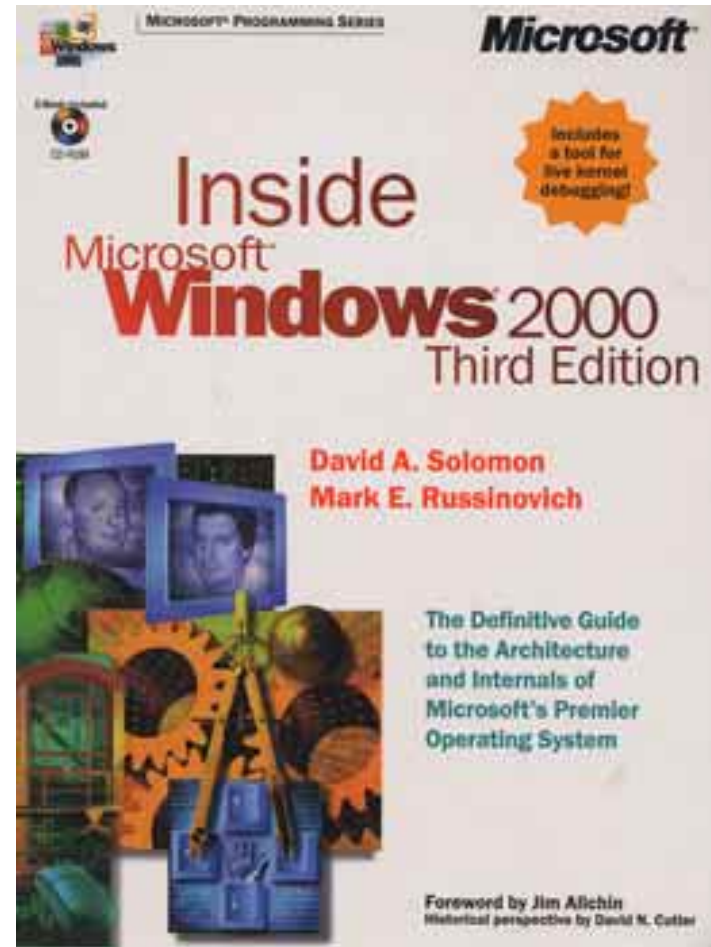
Explaining Windows XP

- ***Inside Windows 2000***- ISBN 0-7356-1021-5
- ***Microsoft Windows XP*** - ISBN 0-7356-1485-7
- ***Windows 2000 Registry*** - ISBN 1-56592-943
- ***The Windows 2000 Registry***- ISBN 01-57610-348-x
- ***Windows XP in A Nutshell***- ISBN 0-596-00249-1
- ***Windows XP Registry*** - ISBN 0-7821-2987-0
- ***Windows XP Tips & Techniques*** - ISBN 0-07-222334-0

Notable Resources & Instruments

Explaining Forensics

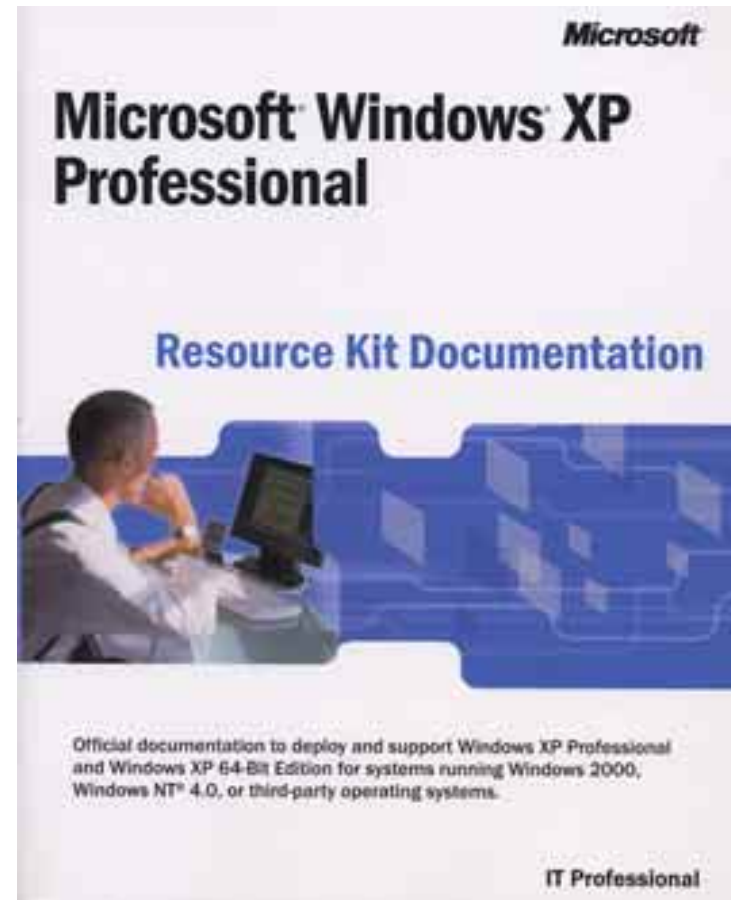
- ***Inside Windows 2000***- ISBN 0-7356-1021-5



Notable Resources & Instruments

Explaining Forensics

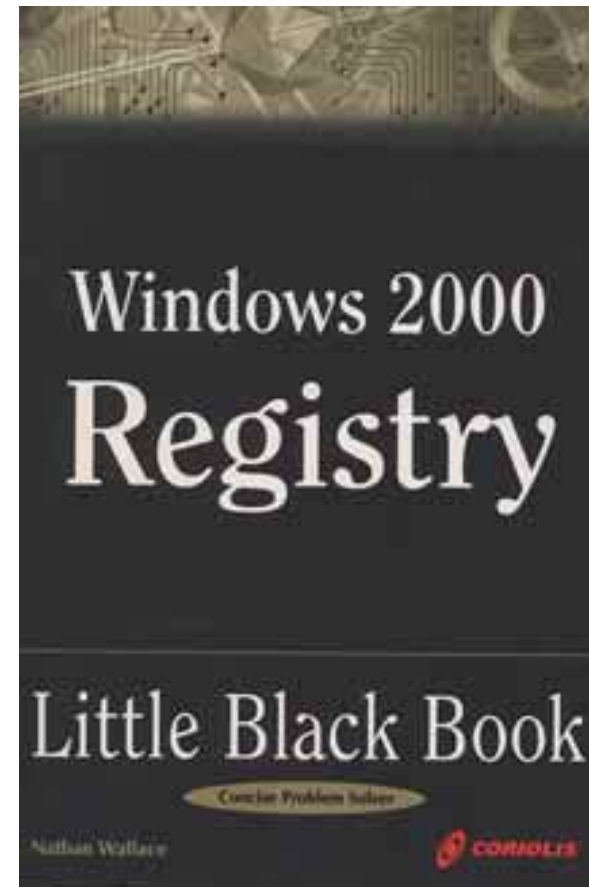
- ***Microsoft Windows XP -***
ISBN 0-7356-1485-7



Notable Resources & Instruments

Explaining Forensics

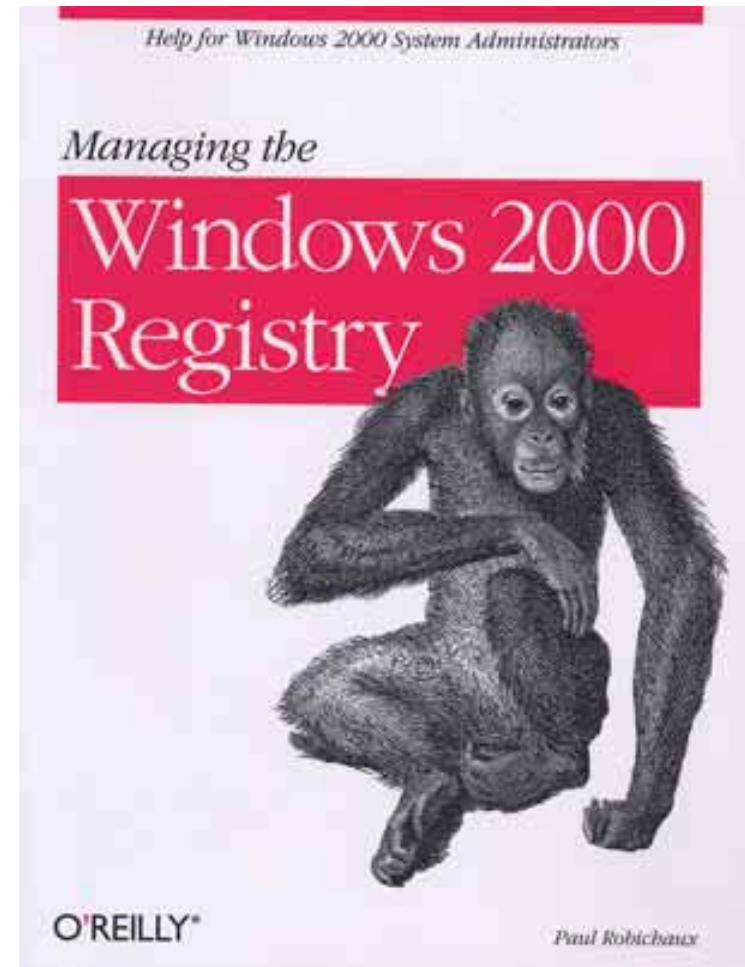
- ***Windows 2000 Registry*** - ISBN 1-56592-943



Notable Resources & Instruments

Explaining Forensics

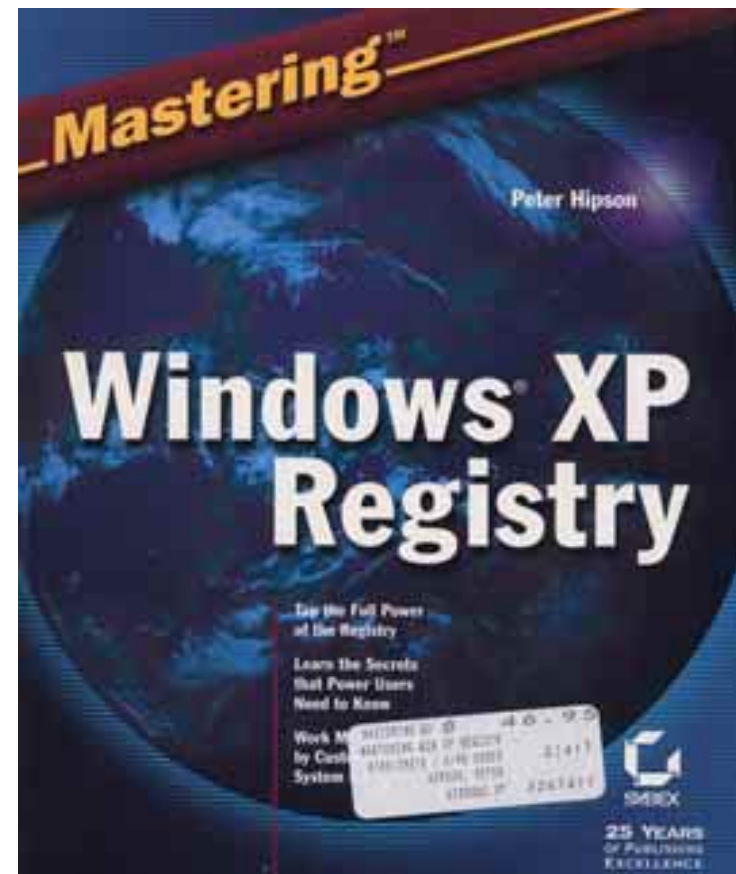
- ***The Windows 2000 Registry-***
ISBN 01-57610-348-
X



Notable Resources & Instruments

Explaining Forensics

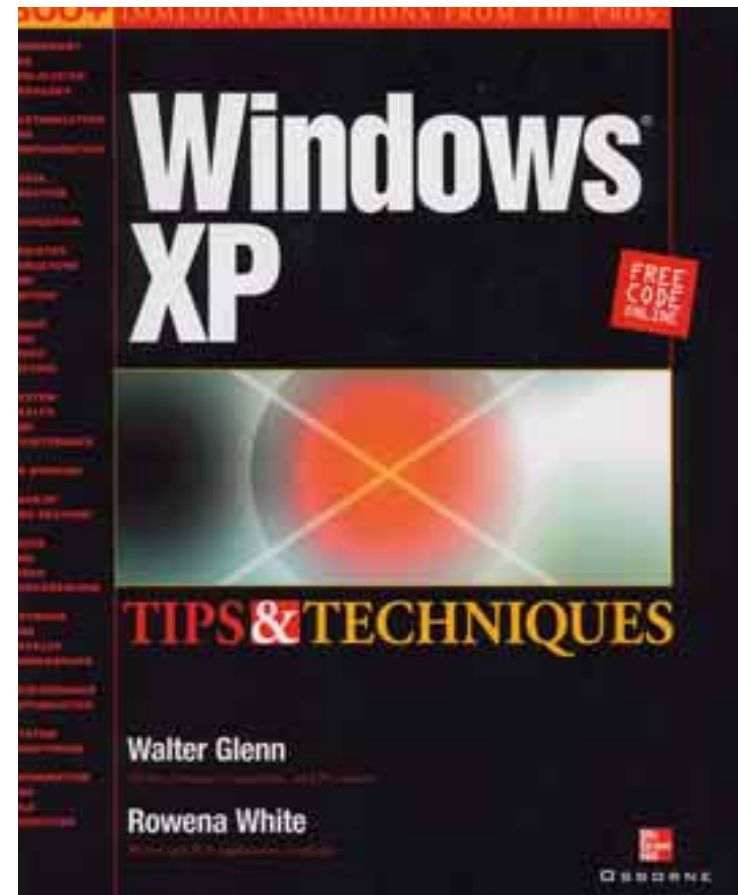
***Windows XP
Registry -
ISBN 0-7821-
2987-0***



Notable Resources & Instruments

Explaining Forensics

- ***Windows XP
Tips &
Techniques*** -
ISBN 0-07-
222334-0



Your Questions

My Appreciation

- Thank you for your time and interest
- I request your written evaluation
- My Coordinates
 - Larry.Leibrock@eforensics.com
 - <http://www.eforensics.com>
 - Austin, Texas (512) 471-1650
 - GMT Time -5