

BlackHat 2003 Case Tutorial

Digital Information, User Tokens, Privacy and Forensics Investigations: Windows XP Platform

*Larry Leibrock, Ph.D.
eForensics LLC*





***MY SLIDES & YOUR SLIDES ARE
DIFFERENT***



I am an Information Technologist focusing on Digital Evidence.

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





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 – in the context of this tutorial
- 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 tutorial, from here on, marks your agreement to these aforementioned caveats, conditions and limitations



Notes for Materials

- All materials – slides and case materials and discussion sets are at <http://www.eforensics.com>
- I will ***not*** use/discuss each slide in this set. There are numerous slides in this set.
- The slides support a notional case – We will use the case as a discussion-leadership vehicle to explore the intersection of

Digital Information, User Tokens, Privacy and International Forensics

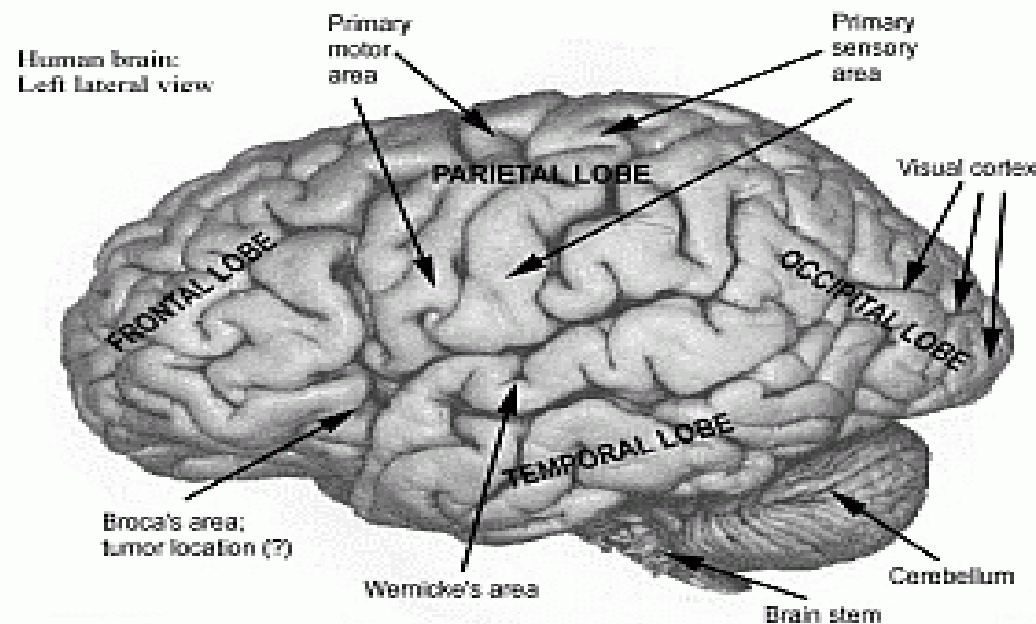
Investigations

Black Hat Briefings

A Protocol – for this Tutorial

Please Ask Questions – whenever you need to.

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





My Bias

- Digital Forensics is an emerging profession.
- The notion of a profession
 - Body of Knowledge - Competency
 - Tests
- Science, Theory and Peer Review are necessary but not sufficient to supporting the digital forensics profession – we need a community of practice among forensics professionals that is also tested with questions of human rights, privacy and ethics.



Forensics

- What does this term imply?



Ubiquity of Digital Devices in everyday life

- **Characteristics**
 - IT technology everywhere and embedded in everything
 - Global connectivity and always on
 - Physical world joining virtual
 - cyberspace acts can affect real-world processes and vice versa
 - Web pages and portals for everything
 - documents, people, things, places, events, processes
 - pages give access to files, sensors, actuators, controls
- **Enablers**
 - Business performance: more bang for buck in less space
 - Mobility – Knowledge work
 - Criminal
 - Non-Criminal
 - Proscribed Activity



Questions

- Review certain tokens (taggants) inherent in digital forensics
- What is a token?
- What is a taggant?
- Can we derive some terms?



Digital

- Data
- Fragment
- Token
- Information
- Findings
- Evidence
- Knowledge
- Judgment



Some Forensics Theory

- Science and Law Intersection?



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



The Windows Client

- Its' Role
- The Platform
- The Build
- File System
- Registry
- The Forensics Corpus



Forensics Instruments



Privacy and Our Government



Responses

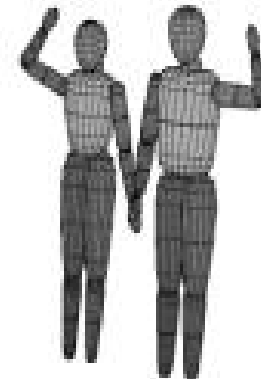
- Privacy Needs
- Shredders
- Anti-Forensics
- Encryption
- Special Methods



The Emerging Tensions







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



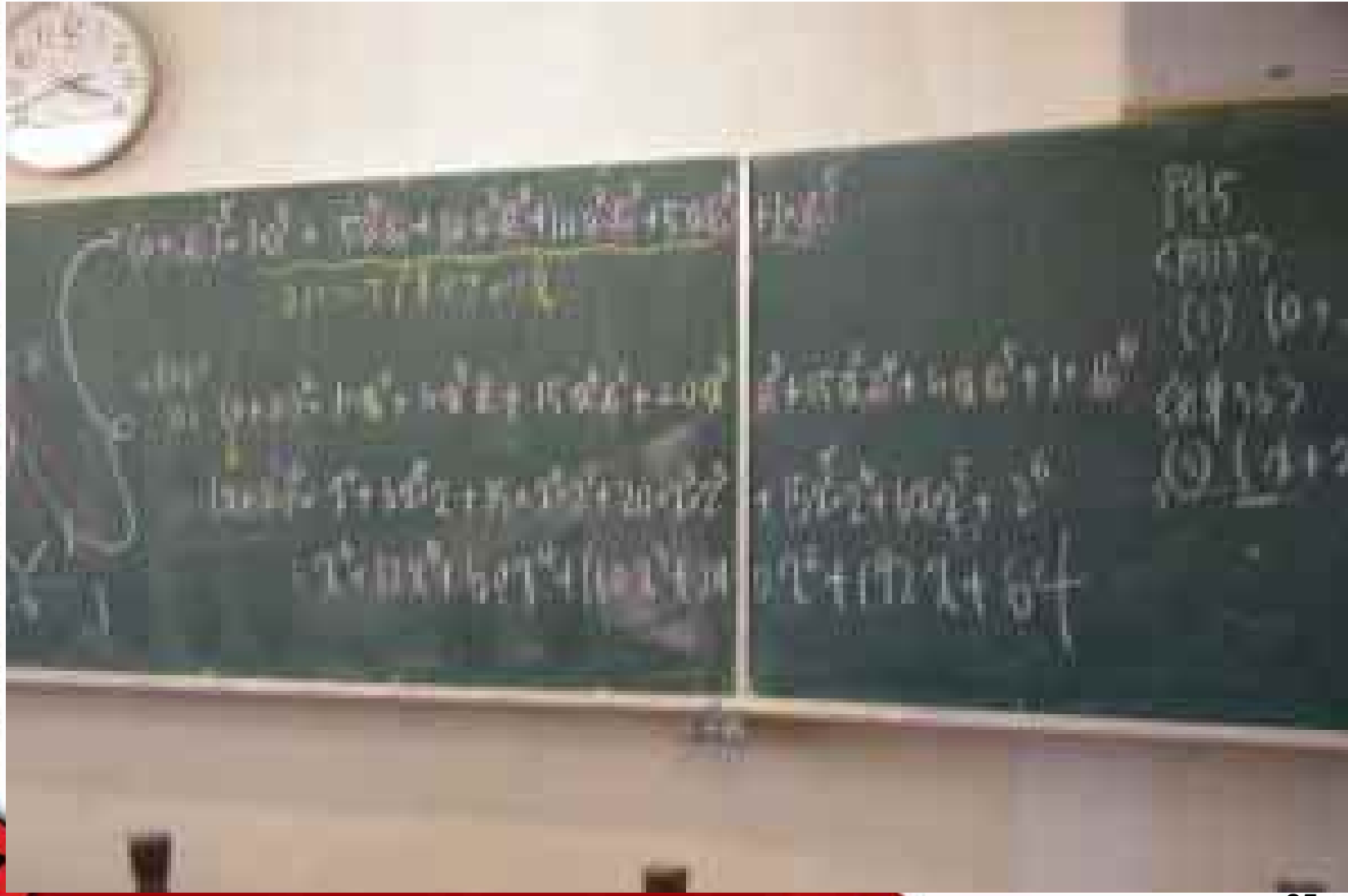
Some prevailing frameworks for forensics investigations



- US Laws
- Federal Guidelines
 - DOJ – FBI
 - DOD
 - NIST
- International Organization on Computer Evidence IOCE Guidelines
<http://www.ioce.org>
- Some national and EU Privacy Issues – European Commission on Human Rights – UK RIPA
- Patriot Act October 26,2001
- Data Retention Policies in the Enron Context
- US Sorbane-Oxley – US Corrupt Activities and RICO Statutes
- 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



Your Questions



My Appreciation

- Thank you for your time and interest
- My Coordinates
 - Larry.Leibrock@eforensics.com
 - <http://www.eforensics.com>
 - Austin, Texas (512) 656-7161
 - GMT Time (-5)

