

**Blackhat Europe 2003 Case  
Tutorial -  
Digital Information, User  
Tokens, Privacy and  
International  
Forensics Investigations**

**Larry Leibrock, Ph.D.  
eForensics LLC**

I am an Information Technologist.  
I am on the teaching faculty of the 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.e-forensics.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*

# Introduction



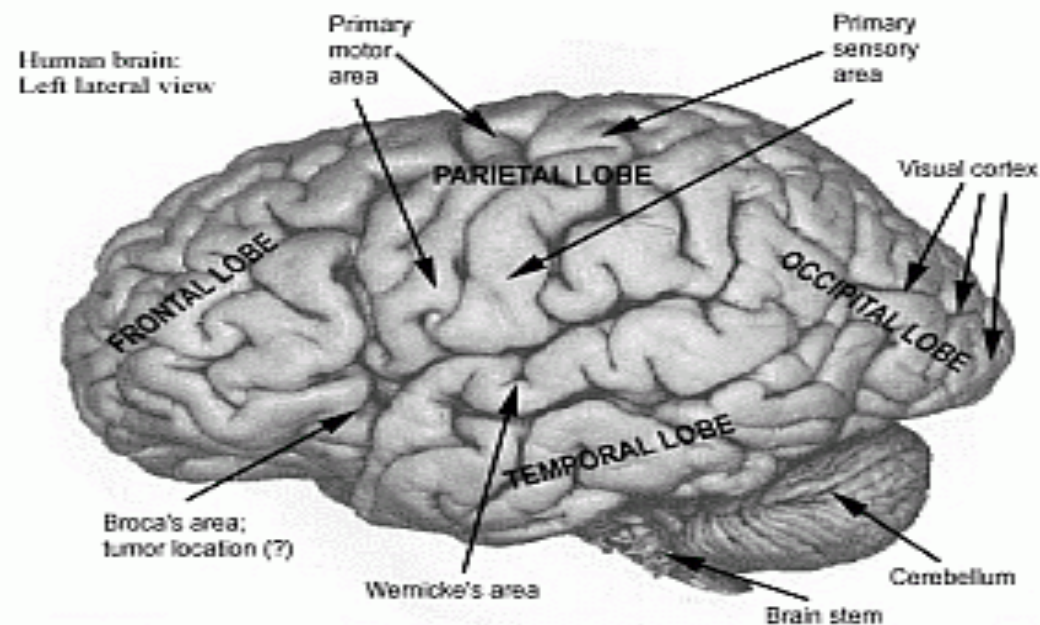
What you should learn in this case tutorial

1. **Gain** an overview of Computer Forensics focusing on the Windows XP platform
2. **Obtain** a general overview as how forensics investigation are conducted
3. **Review** certain tokens (taggants) inherent in digital forensics
4. **Assess** the tensions among privacy - right to conduct forensics in digital forensics
5. **Engage** your intellectual interests and challenge your assumptions related to the uses, investigation and user privacy in international settings.

# A Protocol - for this Tutorial

Γ 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 privacy and ethics.

# 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



# The Case: Baghdad Express



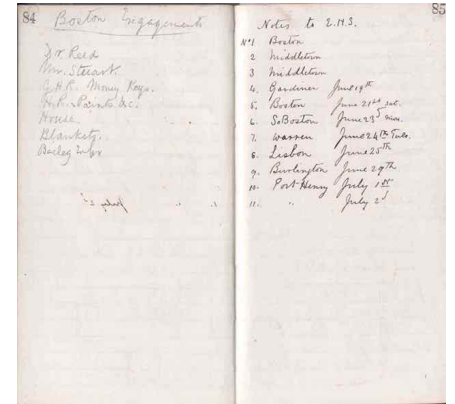
# Introduction



- The subject matter of this tutorial
  - I ask that you quickly read the brief case *Baghdad Express* - that is now being handed out
  - Prepare your responses to the 5 questions at the end of the case.
  - Prepare to present and defend your responses in a depositions setting
  - You have 5 minutes.



# Your Notes



---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---



# The Baghdad Case



- What is the case about? Your 5+/-2 Ideas?

1. \_\_\_\_\_
2. \_\_\_\_\_
3. \_\_\_\_\_
4. \_\_\_\_\_
5. \_\_\_\_\_
6. \_\_\_\_\_
7. \_\_\_\_\_

# The Baghdad Case



## My 5+/-2 Ideas

1. \_\_\_\_\_
2. \_\_\_\_\_
3. \_\_\_\_\_
4. \_\_\_\_\_
5. \_\_\_\_\_
6. \_\_\_\_\_
7. \_\_\_\_\_



# Baghdad Case

## Digital Items of Interest

1. \_\_\_\_\_

2. \_\_\_\_\_

3. \_\_\_\_\_

4. \_\_\_\_\_

5. \_\_\_\_\_

6. \_\_\_\_\_

7. \_\_\_\_\_

# 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

# What is Computer Forensics?

- Who does this?
- Why is it done?
- What can be determined?
- When is forensics done?
- Where is this done?
- How is forensics done

# Computer Forensics

## Φ Who does this?

- Why is it done?
- What can be determined?
- When is forensics done?
- Where is this done?
- How is forensics done

# Computer Forensics

- Who does this?

## **Φ Why is it done?**

- What can be determined?
- When is forensics done?
- Where is this done?
- How is forensics done

# Computer Forensics

- Who does this?
- Why is it done?

## **Φ What can be determined?**

- When is forensics done?
- Where is this done?
- How is forensics done

# Computer Forensics

- Who does this?
- Why is it done?
- What can be determined?

## **Φ** When is forensics done?

- Where is this done?
- How is forensics done

# Computer Forensics

- Who does this?
- Why is it done?
- What can be determined?
- When is forensics done?

## **Φ Where is this done?**

- How is forensics done



# Computer Forensics

- Who does this?
- Why is it done?
- What can be determined?
- When is forensics done?
- Where is this done?

## **Φ** How is forensics done

# 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



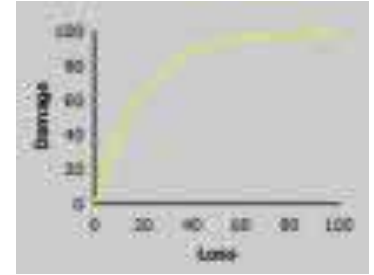
- Tools (Instruments)

- 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 Measures



## Measures (Tests)

1. Authentic
2. Accurate
3. Complete
4. In conformance with law, custom and legislative fiat in proper jurisdictions

# 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

# Forensics Defined and Forensics Operationalized

- Forensics, the computer, the device, the data (electrons)
- Some details
  - Evidence
  - Expertise
  - Procedure (science)



# 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 Problems



## Problems with Computer Forensics

- Collection or examination can alter character (state)
- Computer - Digital investigations and evidence are new to law enforcement, courts and legislative entities
- Explosive growth of digital media density and pervasive computer platforms



# ΔSome Problems



## Problems with Computer Forensics

- Indirect view of digitally represented data and meta-data
- Information technology and mission-critical nature of IT is in continual flux
- Range of skills, education and qualified forensics examiners
- Transitive character of digital 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 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?



# Questions

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

# Examples

- Tokens

- \_\_\_\_\_

- Taggants

# Examples

- Tokens
- Taggants

- \_\_\_\_\_

# 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
- 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

# Forensics

## - An Emerging Competency model



- Understanding and use of a particular approach
- Contemporized record keeping
- Understanding of evidence handling protocols
- Understanding of legal (civil-criminal) procedures
- Can examiner explain at court - the particular forensics process and particular findings



# Forensics

## - An Emerging Competency model



- Understanding of the suspect platform architecture
- Access, skill and experience in forensics tools and instruments
- Forensics examiner has maintained special knowledge - experience and training

# Practitioner

## A Set of Questions



- Chain of Custody - Data Custodial concerns?
- Forensic procedures
  - Documented and explainable
  - Can this be demonstrate to observers
  - Auditable
  - Completeness
  - Non-Intrusive Investigation
  - Media - Archiving without state-change
- Malicious software
- Sole User and Access - The Nexus Problem
- (Suspect) Can you link the particular user that had knowledge about questioned data and use of the platform

# Windows XP Tablet PC Edition

*The evolution of the notebook PC*



Tablet PC is a fully functional computer running the Windows XP Tablet PC Edition operating system. Windows XP Tablet PC Edition, which is built on top of Windows XP Professional,

## Items of Forensics Interests

1. \_\_\_\_\_

2. \_\_\_\_\_

3. \_\_\_\_\_

4. \_\_\_\_\_

5. \_\_\_\_\_

6. \_\_\_\_\_

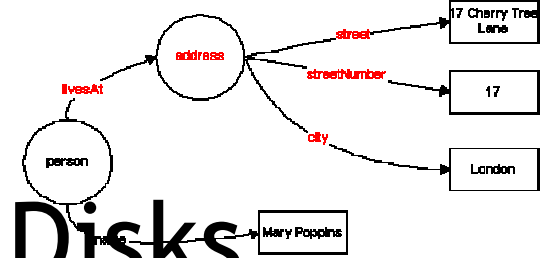
7. \_\_\_\_\_

# 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

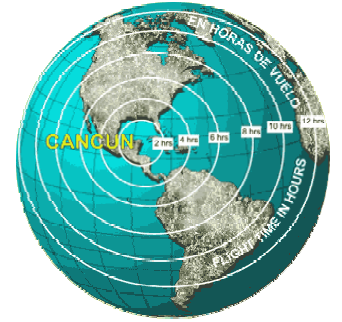


# Windows XP - The Files, Folders and Disks



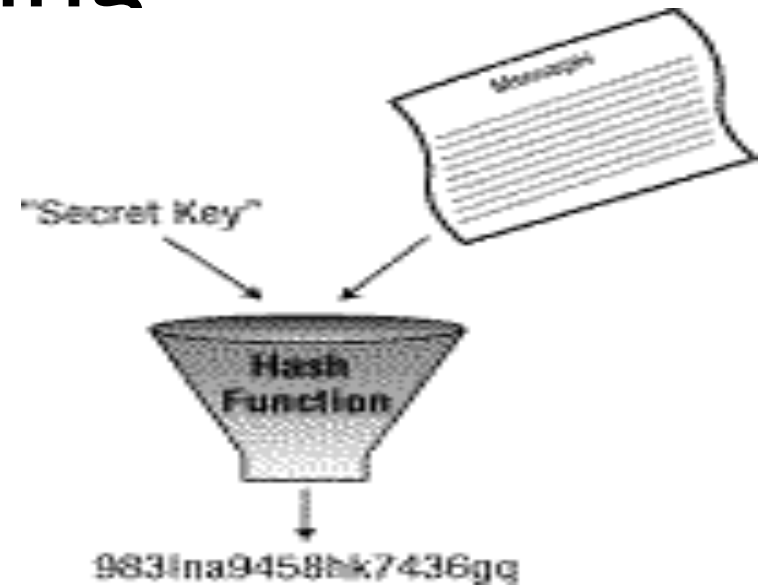
- Disks A-Z - default consecutively
- Pathnames C:\windows\system\color
- UNC \box21\C\games\warez.txt
- DOS 8.3 and LFN
- LFN up to 260 characters
- Case preserving
- Maximum Path is 80 characters
- File and folder attributes - read - system, hidden, compressed and encrypted

# 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

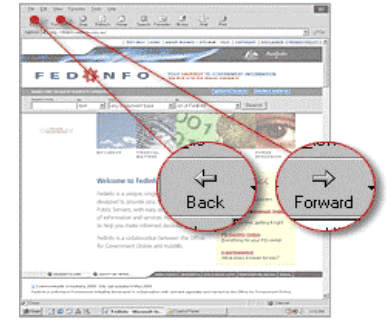
# File Hashing



- Window XP Hash Sets?
- What do we need these?
- Where are these located?



# 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

# 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





# The Registry

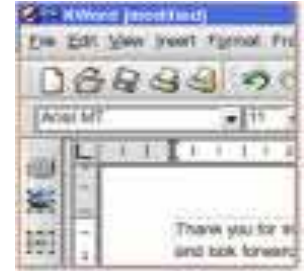
- Browser settings are stored
- Most de-installations leave forensics “residue”
- Most Recently used
- My Documents
- Recycle or Trash Bin
- Some Application passwords are stored
- Some Applications register name, company, license and sometimes address and install time/date
- Usenet Messages for newsgroups

# The Windows XP Intel Platform



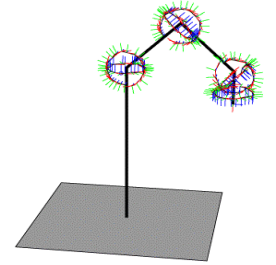
- The Disk Drive(s) and engineer-service-order (ESO) sectors or tracks
- The MAC address
- The Platform Hash
- The Processor ID
- The Registry and its form in XP

# The Windows XP - The Applications Interface



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

# A Forensics Model



Iteration: 3551 Neurons: 25 25 25 25 25 25 25

- 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

# 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



# 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

# Some Special Points relative the Bagdad Express Case



# Forensics Windows XP

## A Review for this Tutorial



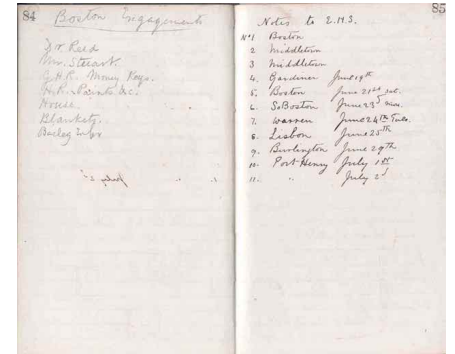
1. \_\_\_\_\_
2. \_\_\_\_\_
3. \_\_\_\_\_
4. \_\_\_\_\_
5. \_\_\_\_\_
6. \_\_\_\_\_
7. \_\_\_\_\_

# Case Summation



- Your Ideas?

# Notes



---

---

---

---

---

---

---

---

---

---

# Your Questions



# 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

# 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



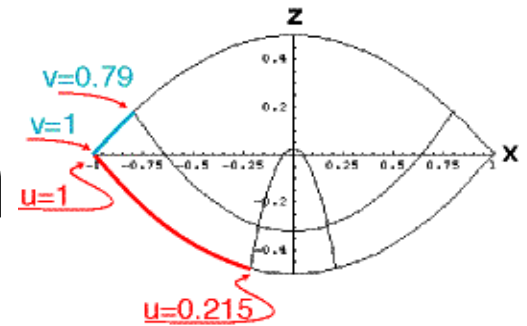
Walk



Run



# My Appreciation



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

