The Art of Electronic Deduction

By: StankDawg
Introduction

- What is “electronic deduction”?
  - A form of footprinting
  - Finding patterns
    - Discovering software
    - Web sites
This sounds pretty simple.

- It is!
  - “Common sense hacking” – Fubster
  - Anyone can do it.
    - Level of depth varies
      - Experience
      - Time available
      - Physical access
What is the goal?

- Build a case, detective style
- Define: “Preponderance of evidence”
  - Coincidental evidence is useless by itself
  - A collection of coincidental evidence can build a case.
Analyzing Results

- This will be interactive!
TaskBar 1

- OS (Windows XP)
- Hardware (Laptop, speakers muted, AC Power)
- Software (MS outlook, Trillian)
- Other (Networking icon showing, Timestamp)
TaskBar 2

- Audience Participation!

- OS?
- Hardware?
- Software?
- Other?
- Conclusion?
Start Menu

- OS (Windows XP, obviously)
- What programs do you see?
- What about desktop files?
- Anything else?
Browser 1

- Browser/OS (WinXP, IE from Comcast)
- Links (hotmail, Binary Revolution)
- Plug-ins (Google/Yahoo, others?)
- Other (obscure icons?)
Browser 2

- Lots of information here for follow-up!

- Links?
- Plug-ins?
- Other?
Application 1

- mIRC

- Server?
- Usernames?
- Other?
Application 2

- Instant Messenger Clients
  - Usernames?
  - Other?
We get it, move on!

- Not limited to screenshots/shoulder surfing.
- What if you can actually get physical access to some of the files? Even temporarily.
- One word: Metadata!
What is MetaData?

- Wikipedia: “data about data”
- What kind of files use metadata?
  - Images
  - Documents
  - Music
  - Could be anything!
- What kind of data do they attach?
- Example: ID3 Tag in MP3 files.
  - Author
  - Title
  - Genre
  - Etc...
- MetaData can be GREAT! (XML = teh r0x0r!)
META DATA in MS Office

Interz0ne 2 – The Blackboard case

SETTLEMENT ANNOUNCEMENT

Blackboard Inc. and Defendants Billy Hoffman and Virgil Griffith have agreed to settle and resolve the lawsuit filed by Blackboard against Defendants Hoffman and Griffith on the following terms:

A. Defendants Hoffman and Griffith each agree that it would be wrong to use any instrument to open a closed circuit box attached to the System without Blackboard's permission, to tap

Comment: This section gets us nowhere. We are airing our dirty laundry and this supports the notion that we picked on 2 kids. We claim a bunch of things and they deny them!
MetaData in MS Office
MetaData in photos

- EXIF Properties in WinXP
  - Equipment
    - Brand (Kodak)
    - Model (CX7430)
  - Date/Time
    - Pinpoint where/when
  - General settings
    - Circumstantial evidence
  - Description/Origin
    - Did you enter these and forget to remove them?
MetaData in photos

- Thumbnails

**CIMG0102_001.jpg**

- **Type:** JPEG Image
- **Dimensions:** 1600 x 1200 pixels
- **Size:** 847 KB
- **Modified:** 2/2/2006 11:23:22 PM
- **Created:** 2/2/2006 11:27:29 PM
- **Location:** E:\misc\Art of Deduction\Read-only: No
- **Title:**
- **Description:**
- **Keywords:**
- **Horizontal Resolution:** 72 dpi
- **Vertical Resolution:** 72 dpi
- **Bit Depth:** 24
- **Frame Count:** 1
MetaData in photos

- Thumbnails

We <3 Elonka!
How do I find MetaData?

- Application support
  - Native in OS
  - Application specific (ID3 tag support)

- Tools:
  - JHead ([http://www.sentex.net/~mwandel/jhead/](http://www.sentex.net/~mwandel/jhead/))
  - metadata-extractor-2.3.1.jar libraries
  - NLNZ Metadata extractor
  - MetaReaper (coming soon from the DDP!)
  - Many more...
How do I find MetaData?

- Hex editing
Should I be worried?

- I don’t know should you be?
  - Embarrassment factor (private pictures)
Should I be worried?

- Piracy
  - Micro$oft == Pirates?

- Look on your system right now!
  - C:\WINDOWS\Help\Tours\WindowsMediaPlayer\Audio\Wav
Should I be worried?

- Legalities (keep in mind defense!)
  - 0x80 interview in the Washington Post (2/19/2006) had IPTC information. (A form of metadata)

- From the article:
  - Age: 21
  - Hair: Blonde, covering his eyebrows
  - Skinny (“wiry frame”+“tall and lanky”)
  - Smokes (prefers Marlboro)
  - Lives with parents in a “brick rambler”
  - Mother is “Really Christian”
  - Has a Dog (“small with matted fur”)
  - Heavy Southern accent
  - High School dropout
  - Was an AOL Customer 7 years ago.
  - Lives near: a used-car lot, a gas station/convenience store and a strip club.

- Keep going, using that profile:
  - FACT: Roland, OK = population ~3000.
  - Probably went to Roland or Muldrow HS.
  - City-data.com reports ~40 people in town that were his age in the year 2000.
  - Google Maps finds the nearby businesses and we can guess his house to be at 35.507985 * -94.527268 lat/long.
Before we wrap it up...

- What kind of profile did you make about me during this presentation?
  - What brand laptop did I use?
  - What software was clearly used in the presentation or did I admit that I used?
  - What references did I make about who I know or are friends with?
  - What web sites did I admit to using where follow-up research could be done?

- Do you have a good profile about me?
Shoutz!

- The Digital DawgPound
  - digitaldawgpound.org ➔ the blawg.
  - stankdawg.com ➔ my personal site.
- Binary Revolution
  - binrev.com ➔ the addiction.
- BR407 & BR561 (binrevmeetings.com)
- Rockit & everyone at Interzone!
Questions?