The Art of Electronic Deduction

By: StankDawg

Introduction

- What is “electronic deduction”?
  - A form of footprinting
  - Finding patterns
    - Discovering software
    - Web sites

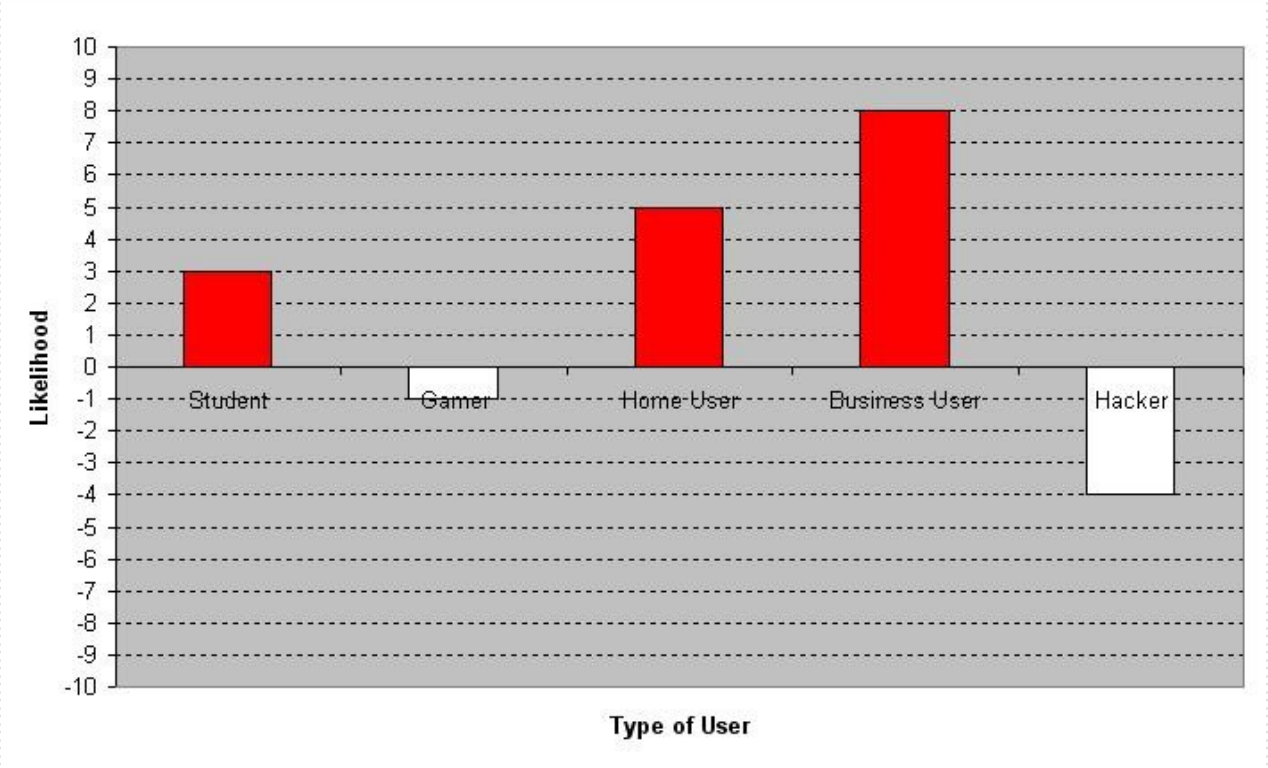
This sounds pretty simple.

- 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

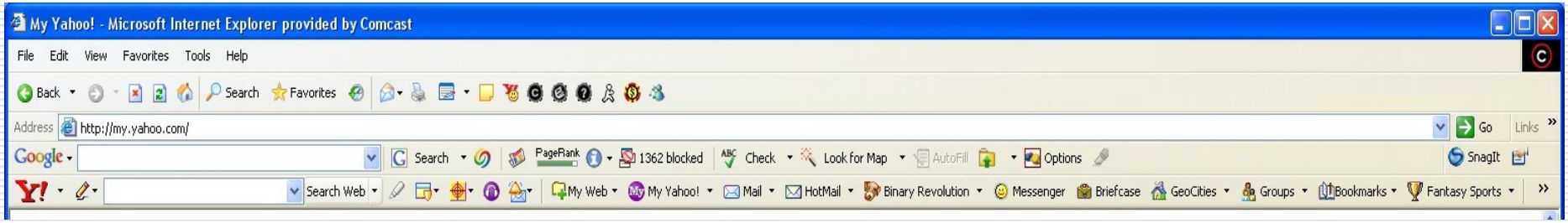
- Audience Participation!

- OS?
- Hardware?
- Software?
- Other?
- Conclusion?

Start Menu

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

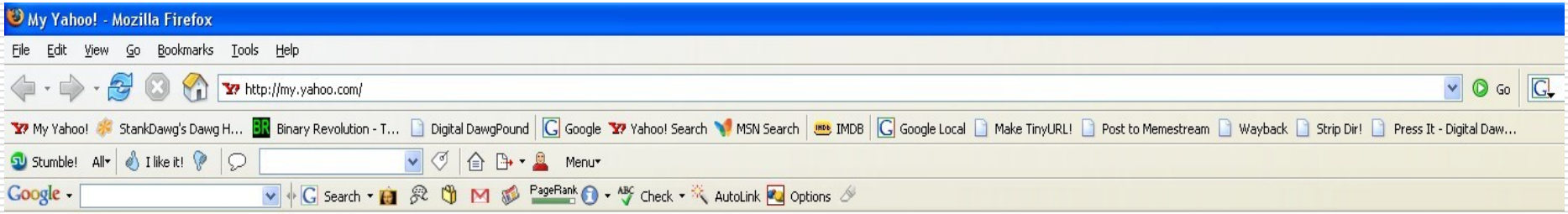
Browser 1



- 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?

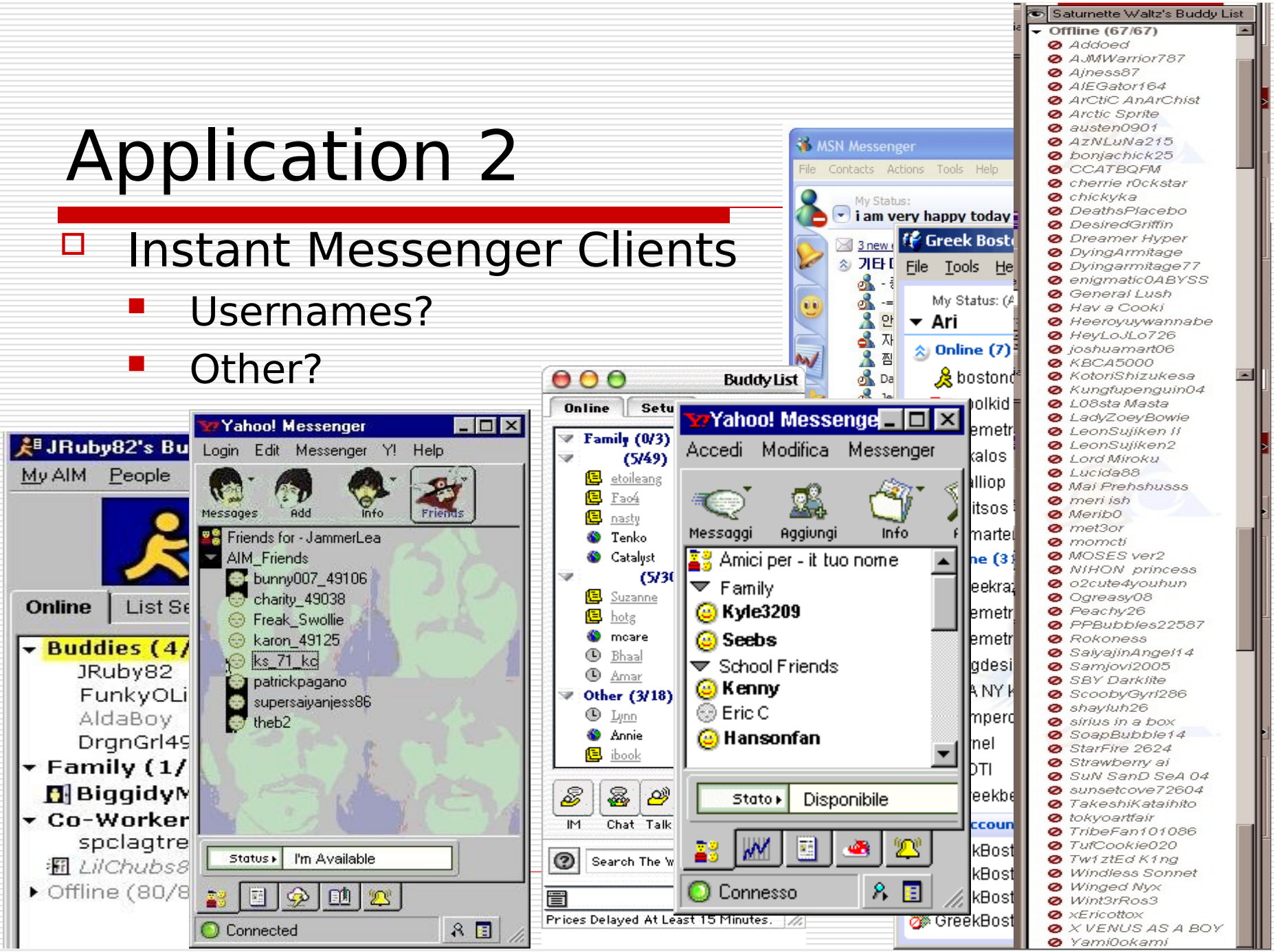
Application 1

- 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!

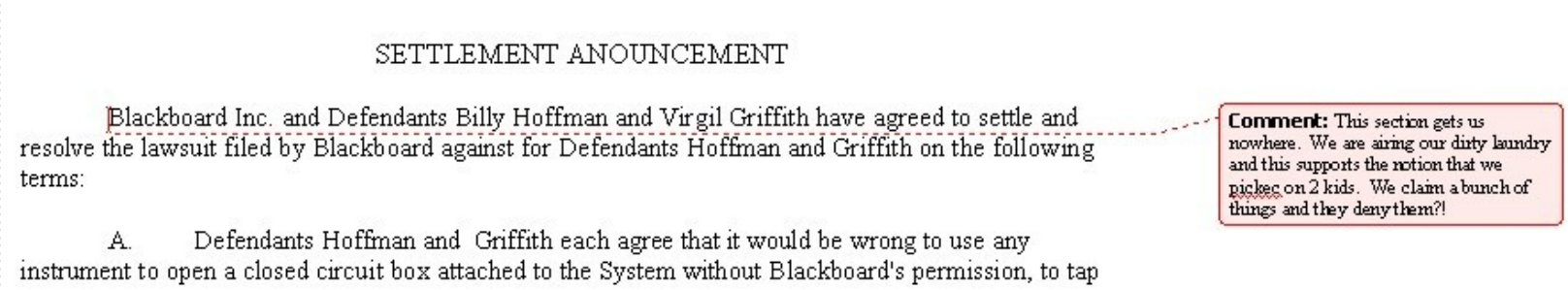
What is MetaData?

- 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!)

MetaData in MS Office

- Interz0ne 2 – The Blackboard case

```
1689
1690 <p class=MsoCommentText><span class=MsoCommentReference><span style='font-size:
1691 8.0pt;mso-bidi-font-size:10.0pt'><span style='mso-special-character:comment'> <![if !supportAnnotations]><a
1692 href="#_msoanchor_1" class=msocomoff>[msl]</a><![endif]></span></span></span>This
1693 section gets us nowhere. <span style='mso-spacerun:yes'> </span>We are airing
1694 our dirty laundry and this supports the notion that we pickec on 2 kids.<span
1695 style='mso-spacerun:yes'>  </span>We claim a bunch of things and they deny
1696 them?!</p>
```



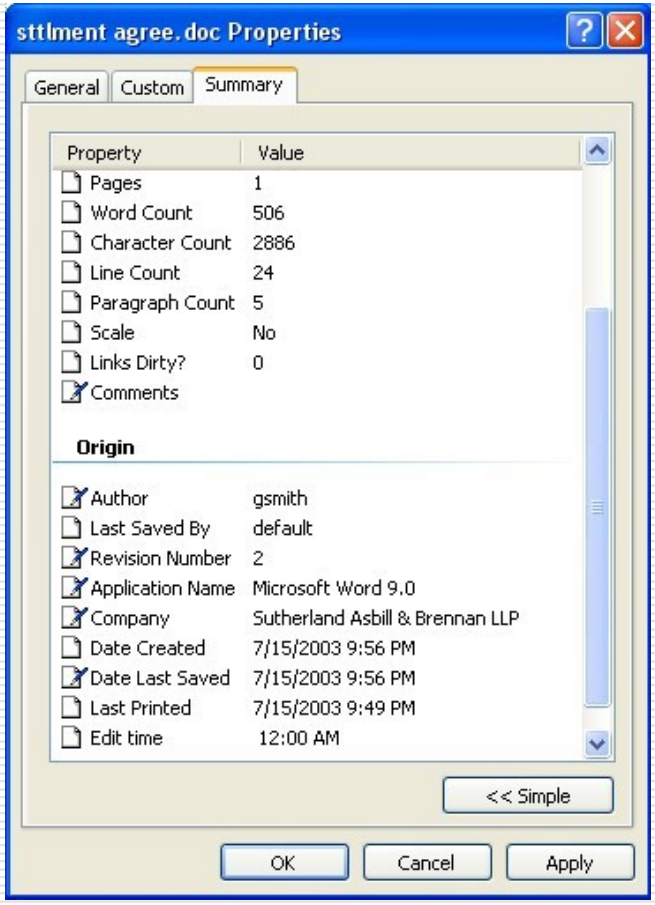
SETTLEMENT ANOUNCEMENT

Blackboard Inc. and Defendants Billy Hoffman and Virgil Griffith have agreed to settle and resolve the lawsuit filed by Blackboard against for 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 pickec on 2 kids. We claim a bunch of things and they deny them?!

MetaData in MS Office

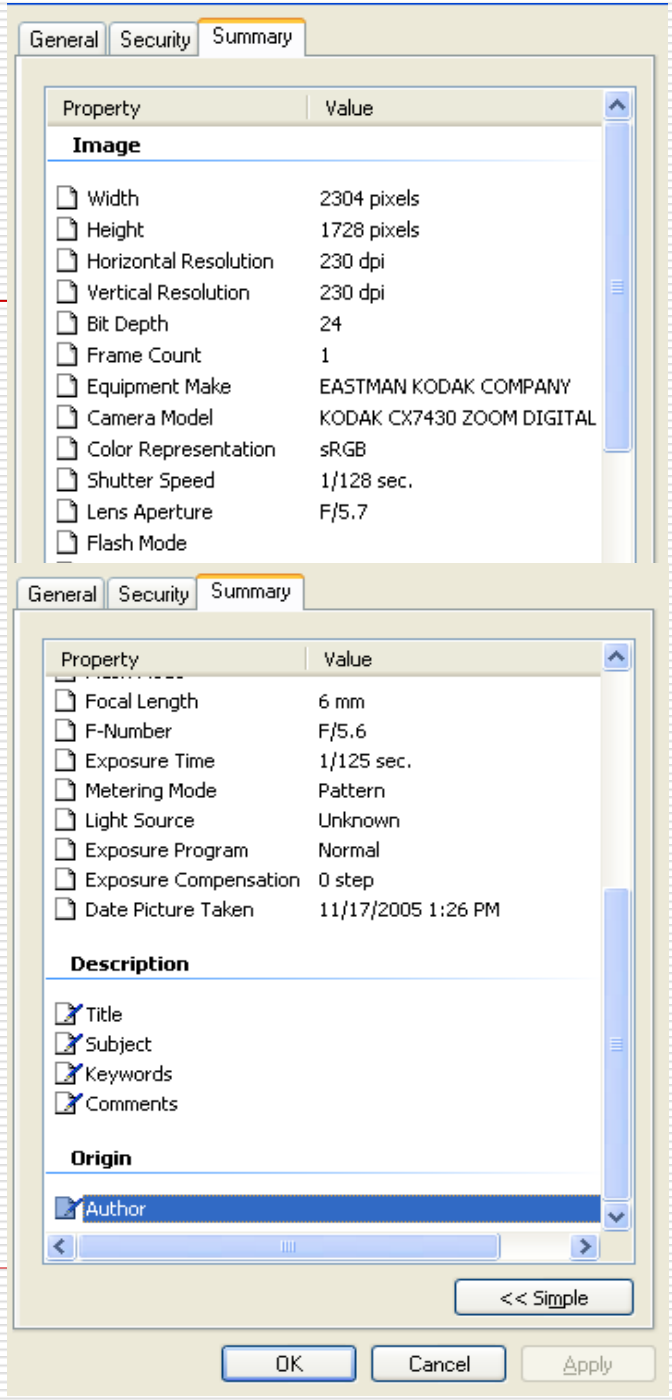



```
12 <title>EXHIBIT D</title>
13 <!--[if gte mso 9]><xml>
14  <o:DocumentProperties>
15   <o:Author>gsmith</o:Author>
16   <o:LastAuthor>StankDawg</o:LastAuthor>
17   <o:Revision>2</o:Revision>
18   <o:TotalTime>9</o:TotalTime>
19   <o:LastPrinted>2003-07-16T03:49:00Z</o:LastPrinted>
20   <o:Created>2006-02-06T03:41:00Z</o:Created>
21   <o:LastSaved>2006-02-06T03:41:00Z</o:LastSaved>
22   <o:Pages>1</o:Pages>
23   <o:Words>532</o:Words>
24   <o:Characters>2968</o:Characters>
25   <o:Company>Sutherland Asbill &amp; Brennan LLP</o:Company>
26   <o:Lines>49</o:Lines>
27   <o:Paragraphs>9</o:Paragraphs>
28   <o:CharactersWithSpaces>3491</o:CharactersWithSpaces>
29   <o:Version>10.6735</o:Version>
30  </o:DocumentProperties>
31  <o:CustomDocumentProperties>
32   <o:DocNumber dt:dt="string">WO 201910.1</o:DocNumber>
33  </o:CustomDocumentProperties>
34 </xml><![endif]--><!--[if gte mso 9]><xml>
35  <w:WordDocument>
36   <w:TrackRevisions/>
37   <w:DisplayHorizontalDrawingGridEvery>0</w:DisplayHorizontalDrawingGridEvery>
38   <w:DisplayVerticalDrawingGridEvery>0</w:DisplayVerticalDrawingGridEvery>
39   <w:UseMarginsForDrawingGridOrigin/>
40   <w:DocumentVariables>
41    <w:IDInfo>Y</w:IDInfo>
42   </w:DocumentVariables>
43   <w:BrowserLevel>MicrosoftInternetExplorer4</w:BrowserLevel>
44  </w:WordDocument>
45 </xml><![endif]--><![if !supportAnnotations]>
46 <style id="dynCom" type="text/css"><!-- --></style>
```

```
1577 <p class=MsoNormal align=center style='text-align:center'>SETTLEMENT
1578 ANOUNCEMENT</p>
1579
1580 <p class=MsoNormal><o:p> </o:p></p>
1581
1582 <p class=MsoNormal style='text-indent:.5in'><span class=MsoCommentReference><span
1583 style='font-size:8.0pt;mso-bidi-font-size:10.0pt'><a style='mso-comment-reference:
1584 ms_1'></a><![if !supportAnnotations]><a class=msocomanchor id="_anchor_1"
1585 onmouseover="msoCommentShow('_anchor_1','_com_1')"
1586 onmouseout="msoCommentHide('_com_1')" href="#_msocom_1" language=JavaScript
1587 name="_msoanchor_1">[ms1]</a><![endif]><span style='display:none;mso-hide:all'><span
1588 style='mso-special-character:comment'> </span></span></span></span><span
1589 style='font-size:11.0pt;mso-bidi-font-size:10.0pt'>Blackboard Inc. and
1590 Defendants Billy Hoffman and Virgil Griffith have agreed to settle and resolve
1591 the lawsuit filed by Blackboard against for Defendants Hoffman and Griffith on
1592 the following terms:<o:p></o:p></span></p>
1593
1594 <p class=MsoNormal><span style='font-size:11.0pt;mso-bidi-font-size:10.0pt'><span
1595 style='mso-spacerun:yes'>  </span><o:p></o:p></span></p>
```

MetaData in photos

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



MetaData in photos

- Thumbnails

CIMG0102_001.jpg

Picture properties Less

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

Copy of CIMG0102_001.jpg

Picture properties Less

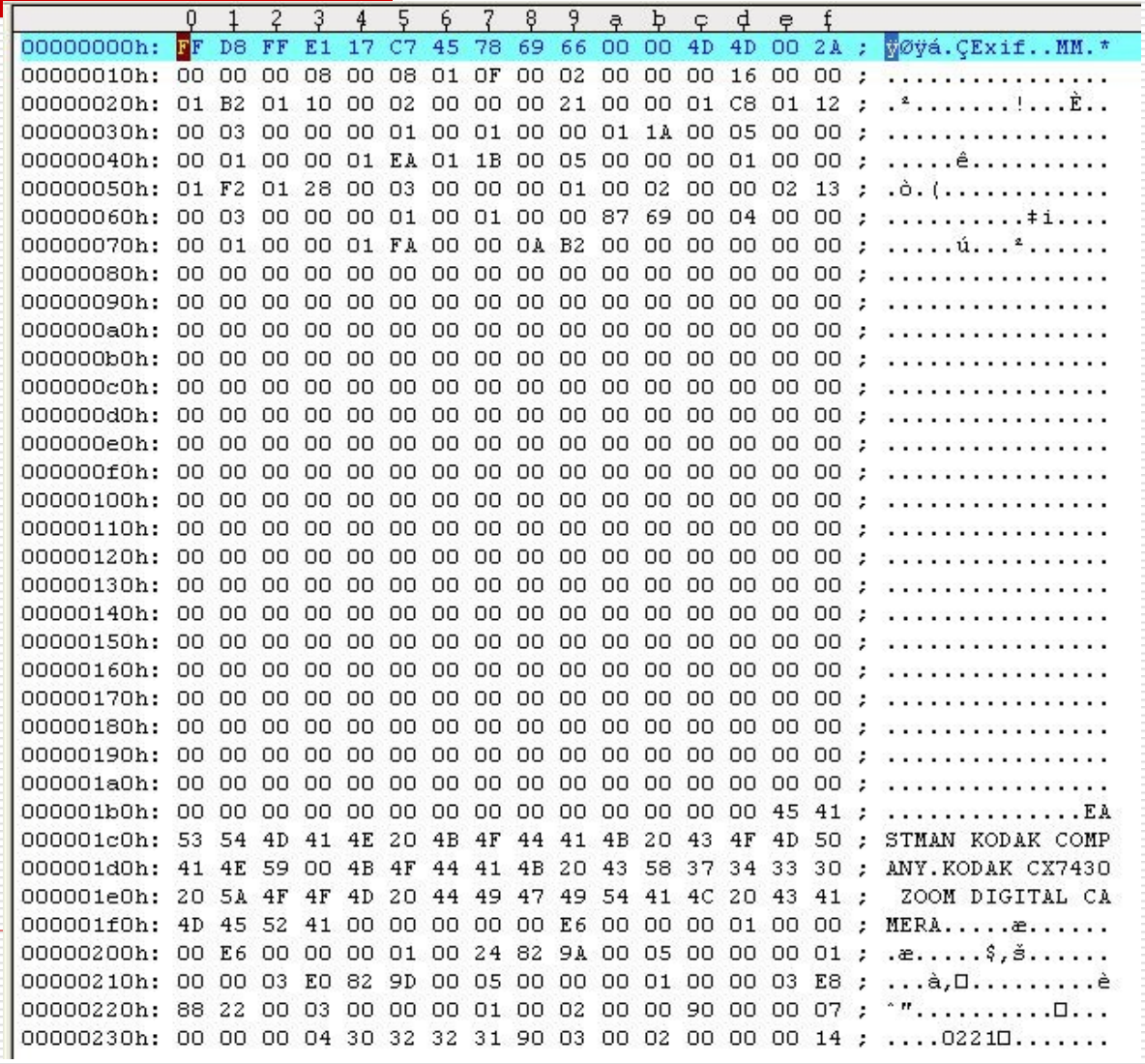
Type: JPEG Image
Dimensions: 1600 x 1200 pixels
Size: 163 KB
Modified: 2/2/2006 11:25:14 PM
Created: 2/2/2006 11:27:31 PM
Location: E:\misc\Art of Deduction\
Read-only: No
Title:
Description:
Keywords:
Horizontal Resolution: 72 dpi
Vertical Resolution: 72 dpi
Bit Depth: 24
Frame Count: 1

How do I find MetaData?

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



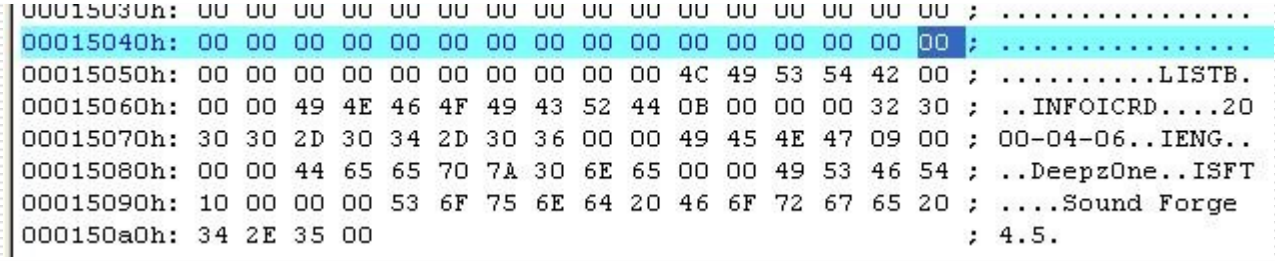
```
          0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00000000h: FF D8 FF E1 17 C7 45 78 69 66 00 00 4D 4D 00 2A ; ÿØÿá.ÇExif..MM.*
00000010h: 00 00 00 08 00 08 01 0F 00 02 00 00 00 16 00 00 ; ................
00000020h: 01 B2 01 10 00 02 00 00 00 21 00 00 01 C8 01 12 ; .².......!...È..
00000030h: 00 03 00 00 00 01 00 01 00 00 01 1A 00 05 00 00 ; ................
00000040h: 00 01 00 00 01 EA 01 1B 00 05 00 00 00 01 00 00 ; .....ê.........
00000050h: 01 F2 01 28 00 03 00 00 00 01 00 02 00 00 02 13 ; .ò.(...........
00000060h: 00 03 00 00 00 01 00 01 00 00 87 69 00 04 00 00 ; ..........‡i....
00000070h: 00 01 00 00 01 FA 00 00 0A B2 00 00 00 00 00 00 ; .....ú...².....
00000080h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000090h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000a0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000b0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000c0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000d0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000e0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000f0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000100h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000110h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000120h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000130h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000140h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000150h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000160h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000170h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000180h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000190h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000001a0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000001b0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 45 41 ; ..............EA
000001c0h: 53 54 4D 41 4E 20 4B 4F 44 41 4B 20 43 4F 4D 50 ; STMAN KODAK COMP
000001d0h: 41 4E 59 00 4B 4F 44 41 4B 20 43 58 37 34 33 30 ; ANY.KODAK CX7430
000001e0h: 20 5A 4F 4F 4D 20 44 49 47 49 54 41 4C 20 43 41 ;  ZOOM DIGITAL CA
000001f0h: 4D 45 52 41 00 00 00 00 00 E6 00 00 00 01 00 00 ; MERA.....æ......
00000200h: 00 E6 00 00 00 01 00 24 82 9A 00 05 00 00 00 01 ; .æ.....$‚š......
00000210h: 00 00 03 E0 82 9D 00 05 00 00 00 01 00 00 03 E8 ; ...à‚□.........è
00000220h: 88 22 00 03 00 00 00 01 00 02 00 00 90 00 00 07 ; ˆ"..........□...
00000230h: 00 00 00 04 30 32 32 31 90 03 00 02 00 00 00 14 ; ....0221□.......
```

Should I be worried?

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

Should I be worried?

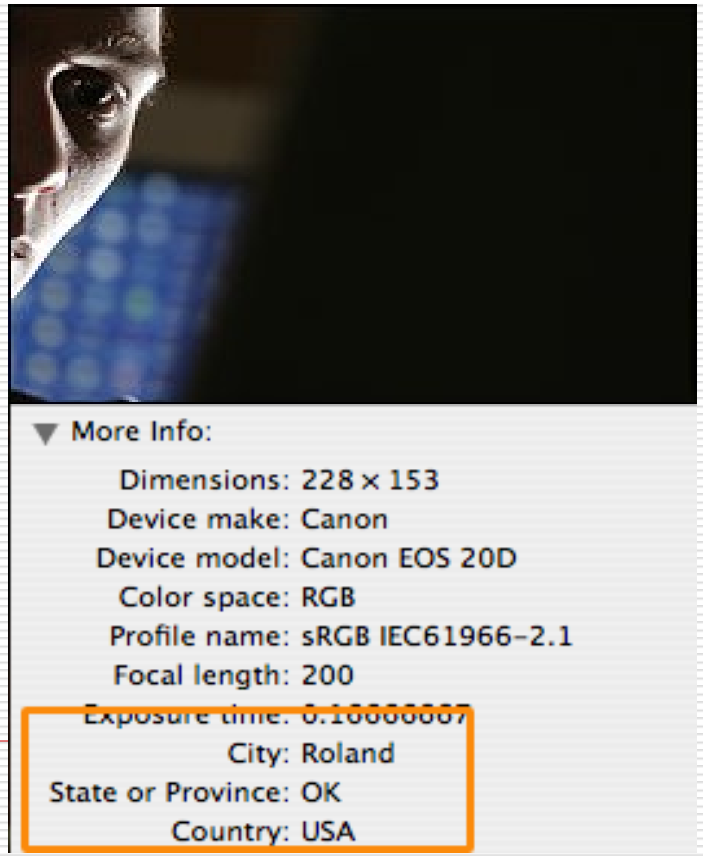
- Piracy
  - Micro$oft == Pirates?



- 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?