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.

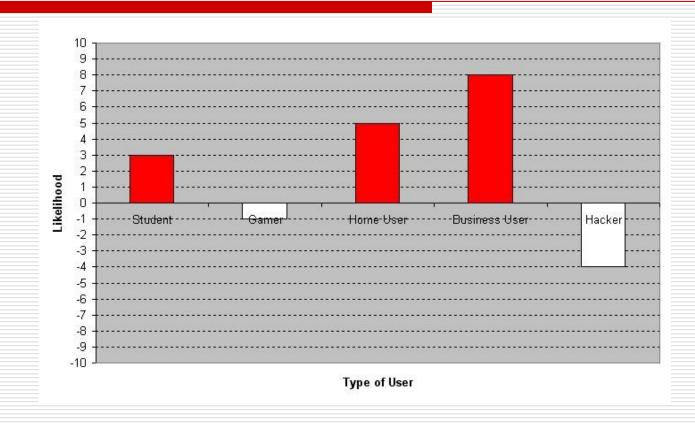
It is!

- "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

🖄 My Yahoo! - Microsoft Internet Explorer provided by Comcast	
File Edit View Favorites Tools Help	C
🔇 Back 🔻 🕤 🕐 🖹 😰 🏠 🔑 Search 👷 Favorites 🤗 🖉 + 😓 🦉 🧔 🦉 🦉 🦉 🦓 🖓	
Address 🕘 http://my.yahoo.com/	Go Links
Google - 💽 Search - 🖉 🐼 PageRank 🕥 - 🕸 1362 blocked 👫 Check - 🌾 Look for Map - 😨 AutoFill 😱 - 🛃 Options 🖉	nagIt 🛃
🝸 🔹 🆉 🗸 🔽 🗸 Search Web 🔹 🖉 🔂 😓 🖓 🌚 🎂 🖉 🦓 Web 🕫 🖓 Yahoo! 🔹 🖂 HotMail 🔹 💱 Binary Revolution 🔹 🎯 Messenger 🍘 Briefcase 🖓 GeoCities 🔹 🌺 Groups 🔹 🕅 Bookmarks 👻 🐺 Fantasy Si	ports • X

- 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!

🕲 My Yahoo! - Mozilla Firefox	
<u>File Edit Vi</u> ew <u>G</u> o <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp	
	C,
🖅 My Yahoo! 🍀 StankDawg's Dawg H 🔢 Binary Revolution - T 🗋 Digital DawgPound 🕼 Google 🐭 Yahoo! Search 📢 MSN Search 😻 IMDB 🕼 Google Local 🗋 Make TinyURL! 🗋 Post to Memestream 🗋 Wayback 🗋 Strip Dir! 🗋 Press It - Digital Daw	
외 Stumble! All= 🔌 I like it! 🖗 💭 🔤 🗹 🍯 🖓 🖆 🕒 = 🚨 Menu=	
Google - 🔽 🔶 G Search - 💼 🕫 🖄 M 💖 PageBank 🗊 - 🎸 Check - 🔧 AutoLink 🚾 Options 🖉	

- Links?
- Plug-ins?
- Other?

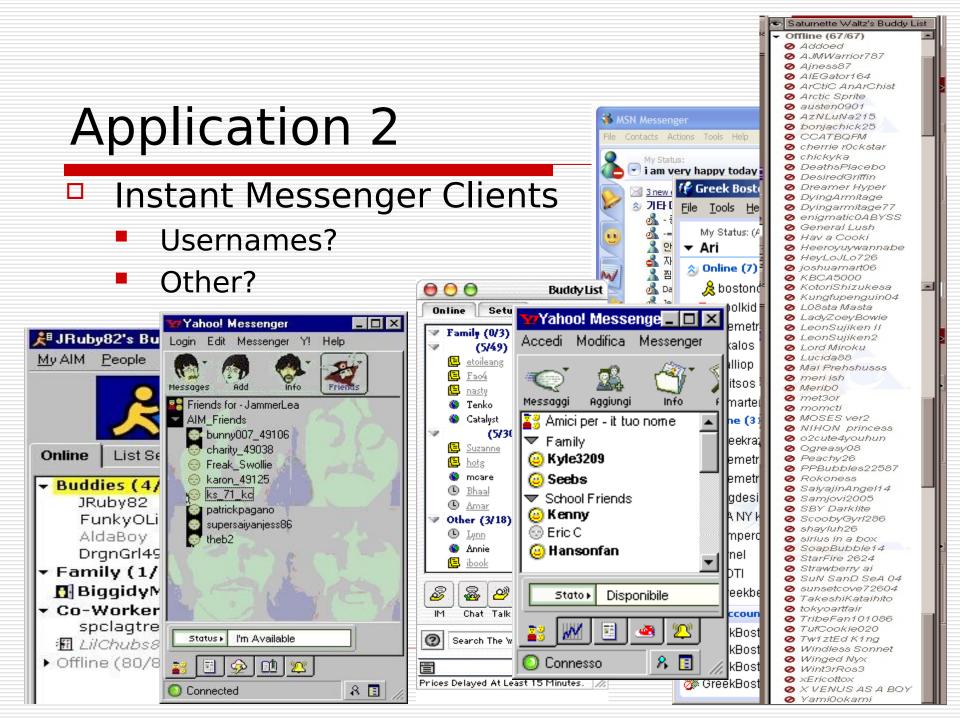
Application 1

mIRC

RC
view Favorites Tools Commands Window Help
ALnet jumper 🗐 #binrev 🔄 🕅 Dr´ZigMan{D 📰 BlackRatchet{
tatus: jumper1337 [+i] on DALnet (rumble.fl.us.dal.net:6668)
For Help with services: http://www.dal.net
Server's Official channel: /join #rumble.dal.net
ii ++ ii
IMPORTANT:
#/binrev [56] [+cnt]: Official Channel of Binary Revolution www.binrev.com "The Revolution Will Be Digitized!" Binrev Radio 134 this Tuesday 9:30 PM EST with guest Mark Spencer.
* Set by Strom_C on Sun Feb 05 17:02:22

Server?

- 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 <span style='font-size:
- 1691 8.0pt;mso-bidi-font-size:10.0pt'> <![if !supportAnnotations]><a
- 1692 href="#_msoanchor_1" class=msocomoff>[ms1]<![endif]>This
- 1693 section gets us nowhere. We are airing
- 1694 our dirty laundry and this supports the notion that we pickec on 2 kids. We claim a bunch of things and they deny
- 1696 them?!

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 kundry and this supports the notion that we pickee 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></xml>
		14	<o:documentproperties></o:documentproperties>
		15	<o:author>gsmith</o:author>
		16	<o:lastauthor>StankDawg</o:lastauthor>
		17	<pre><c:revision>2</c:revision></pre>
sttlment agree.doc Properties	? 🗙	10	<o:totaltime>9</o:totaltime> <o:lastprinted>2003-07-16T03:49:00Z</o:lastprinted>
stument agree. doc Properties		20	<pre><0:Created>2005-02-05703:41:002</pre>
		21	<pre></pre>
General Custom Summary		22	<pre><c:pages>l</c:pages></pre>
		23	<o:words>532</o:words>
		24	<o:characters>2968</o:characters>
Property Value	~	25	<o:company>Sutherland Asbill & Brennan LLP</o:company>
		26	<o:lines>49</o:lines>
Pages 1		27	<0:Paragraphs>9 0:Paragraphs
🗋 Word Count 506		28	<pre><c:characterswithspaces>3491</c:characterswithspaces></pre>
Character Count 2886		29	<o:version>10.6735</o:version>
		30	
Line Count 24		31	<o:customdocumentproperties></o:customdocumentproperties>
Paragraph Count 5		32	<pre><o:docnumber dt:dt="string">W0 201910.1</o:docnumber></pre>
		34	 [endif] [if gte mso 9] <xml></xml>
🗋 Scale No		35	<pre></pre>
Links Dirty? 101		36	<pre><w:trackrevisions></w:trackrevisions></pre>
Comments		37	<pre><w:displayhorizontaldrawinggridevery>0</w:displayhorizontaldrawinggridevery></pre>
Commences		38	<w:displayverticaldrawinggridevery>0</w:displayverticaldrawinggridevery>
		39	<w:usemarginsfordrawinggridorigin></w:usemarginsfordrawinggridorigin>
Origin		40	<w:documentvariables></w:documentvariables>
		41	<w:idinfo>Y</w:idinfo>
Author gsmith		42	
		43	<w:browserlevel>MicrosoftInternetExplorer4</w:browserlevel>
🗋 Last Saved By 🛛 default		44	
Revision Number 2			[endif] [if !supportAnnotations]
Application Name Microsoft Wor	0.0 0	46	<style id="dynCom" type="text/css"><!></style>
			+1+2+3+4+5+
Company Sutherland As	ibill & Brennan LLP	1577	<pre>SETTLEMENT</pre>
Date Created 7/15/2003 9:5	56 PM	1578	ANOUNCEMENT
Date Last Saved 7/15/2003 9:5		= 1579	
		1580	<0:p>
Last Printed 7/15/2003 9:4	19 PM 🔤 🗌	1581	
🗋 Edit time 12:00 AM	100	1582	<pre><span< pre=""></span<></pre>
	× .	1583	<pre>style='font-size:8.0pt;mso-bidi-font-size:10.0pt'><a style="mso-comment-reference:</pre></th></tr><tr><th></th><th></th><th>1584</th><th><pre>ms_l"><!--[if !supportAnnotations]--><a <="" class="msocomanchor" id="_anchor_l" onmouseover="msoCommentShow('_anchor_l','_com_l')" pre=""></pre>
	<< Simple	1586	onmouseout="msoCommentHide(' com 1')" href="# msocom 1" language=JavaScript ==
			name=" msoanchor 1">[ms1] [endif] <span< th=""></span<>
		1588	style='mso-special-character:comment'>
ОК	Cancel Apply		style='font-size:11.0pt;mso-bidi-font-size:10.0pt'>Blackboard Inc. and
		= 1590	
		1591	the lawsuit filed by Blackboard against for Defendants Hoffman and Griffith on
		1592	the following terms: <o:p></o:p>
		1593	
		1594	<span< th=""></span<>
		1595	<pre>style='mso-spacerun:yes'> <0:p></pre>
		1504	

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?

Property	Value
Image	
🗅 width	2304 pixels
🗋 Height	1728 pixels
Horizontal Resolution	230 dpi
🗋 Vertical Resolution	230 dpi
Bit Depth	24
🗋 Frame Count	1
🗋 Equipment Make	EASTMAN KODAK COMPANY
Camera Model	KODAK CX7430 ZOOM DIGITAL
Color Representation	sRGB
Shutter Speed	1/128 sec.
Lens Aperture	F/5.7
🗋 Flash Mode	
ieneral Security Summa	ry I
Property	Value
	Value
Focal Length	6 mm
 Focal Length F-Number 	
	6 mm
F-Number Exposure Time Metering Mode	6 mm F/5.6 1/125 sec. Pattern
F-Number Exposure Time Metering Mode Light Source	6 mm F/5.6 1/125 sec. Pattern Unknown
 F-Number Exposure Time Metering Mode Light Source Exposure Program 	6 mm F/5.6 1/125 sec. Pattern Unknown Normal
 F-Number Exposure Time Metering Mode Light Source Exposure Program Exposure Compensati 	6 mm F/5.6 1/125 sec. Pattern Unknown Normal ion 0 step
 F-Number Exposure Time Metering Mode Light Source Exposure Program 	6 mm F/5.6 1/125 sec. Pattern Unknown Normal
 F-Number Exposure Time Metering Mode Light Source Exposure Program Exposure Compensati 	6 mm F/5.6 1/125 sec. Pattern Unknown Normal ion 0 step
 F-Number Exposure Time Metering Mode Light Source Exposure Program Exposure Compensati Date Picture Taken 	6 mm F/5.6 1/125 sec. Pattern Unknown Normal ion 0 step
 F-Number Exposure Time Metering Mode Light Source Exposure Program Exposure Compensati Date Picture Taken 	6 mm F/5.6 1/125 sec. Pattern Unknown Normal ion 0 step
 F-Number Exposure Time Metering Mode Light Source Exposure Program Exposure Compensati Date Picture Taken Description Title	6 mm F/5.6 1/125 sec. Pattern Unknown Normal ion 0 step
 F-Number Exposure Time Metering Mode Light Source Exposure Program Exposure Compensati Date Picture Taken Description Title Subject	6 mm F/5.6 1/125 sec. Pattern Unknown Normal ion 0 step
 F-Number Exposure Time Metering Mode Light Source Exposure Program Exposure Compensati Date Picture Taken Description Title Subject Keywords Comments	6 mm F/5.6 1/125 sec. Pattern Unknown Normal ion 0 step
 F-Number Exposure Time Metering Mode Light Source Exposure Program Exposure Compensati Date Picture Taken Description Title Subject Keywords Comments	6 mm F/5.6 1/125 sec. Pattern Unknown Normal ion 0 step
 F-Number Exposure Time Metering Mode Light Source Exposure Program Exposure Compensati Date Picture Taken Description Title Subject Keywords Comments Origin Author	6 mm F/5.6 1/125 sec. Pattern Unknown Normal ion 0 step 11/17/2005 1:26 PM
 F-Number Exposure Time Metering Mode Light Source Exposure Program Exposure Compensati Date Picture Taken Description Title Subject Keywords Comments Origin Author	6 mm F/5.6 1/125 sec. Pattern Unknown Normal ion 0 step

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 p	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 D)eduction\
Read-only: No	
Title:	
Description:	
Keywords:	
Horizontal Resolution: 72 d	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...

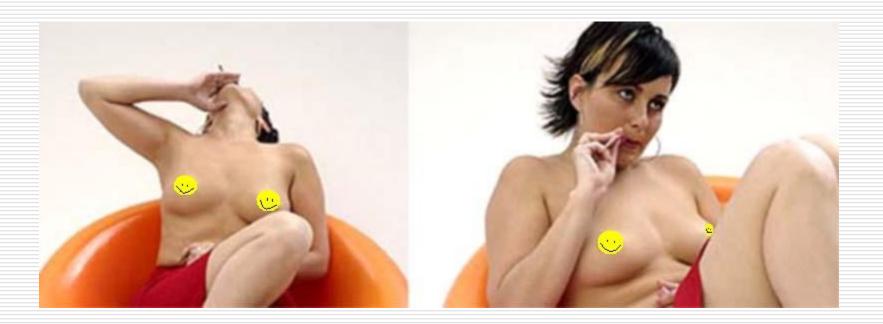
How do I find MetaData?

		Q	1	2	3	4	Ş	6	7	ş	9	ą	þ	ç	þ	ę	f		
· · · ·	00000000h:	FF	D8	FF	E1	17	C7	45	78	69	66	00	00	4D	4D	00	24	2	ÿØÿá.ÇExifMM.*
Hex editing	00000010h:	00	00	00	08	00	08	01	OF	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	2.0	. ^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	1	‡i
	00000070h:	00	01	00	00	01	FA	00	00	OA	B2	00	00	00	00	00	00	;	ú²
	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	;	
	10.0.0.0.00.00.0000																		
	10.0.0.0.0.0000000	10.54	10.54	10.54	10.54	10.54	10.54	10.54	10.53	20.53	20.53	10.54	10.54	10.54	10.54	10.54	10.5%		
	00000110h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	1	
	10.0.0.0.0.00000000																		
	00000130h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
	00000140h:	10.54	10.54	10.54	10.54	10.54	10.54	10.54	10.53	20.53	20.53	10.54	10.54	10.54	10.54	10.54	10.5%		
	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:																		
	00000180h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
	00000190h:																		
	000001a0h:																		
	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
	10.0.0.0.0.000 States																		ANY.KODAK CX7430
	000001e0h:																		ZOOM DIGITAL CA
	10.0.0.0.0.0.00000000000000000000000000																		MERAæ
	10.00.00.00.000000000000000000000000000																		.æ\$,š
	1993 (1993) (1993) (1993) (1993) (1993)																		à,0è
	100000000000000000000000000000000000000																		* "
	00000230h:	00	00	00	04	30	32	32	31	90	03	00	02	00	00	00	14	;	02210

Should I be worried?

I don't know should you be?

Embarrassment factor (private pictures)



Should I be worried?

Piracy

Micro\$oft == Pirates?

 00015030h:
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00

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.



More Info:

Dimensions: 228 × 153 Device make: Canon Device model: Canon EOS 20D Color space: RGB Profile name: sRGB IEC61966-2.1 Focal length: 200

Exposure time: 0.10000007

City: Roland State or Province: OK Country: USA

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

- stankdawg.com

 my personal site.
- Binary Revolution
 - <u>binrev.com</u> ← the addiction.
- BR407 & BR561 (<u>binrevmeetings.com</u>)
- Rockit & everyone at Interzone!

Questions?

