So You Think Your Data Is Private?

The Hackers View Of Privacy Threats

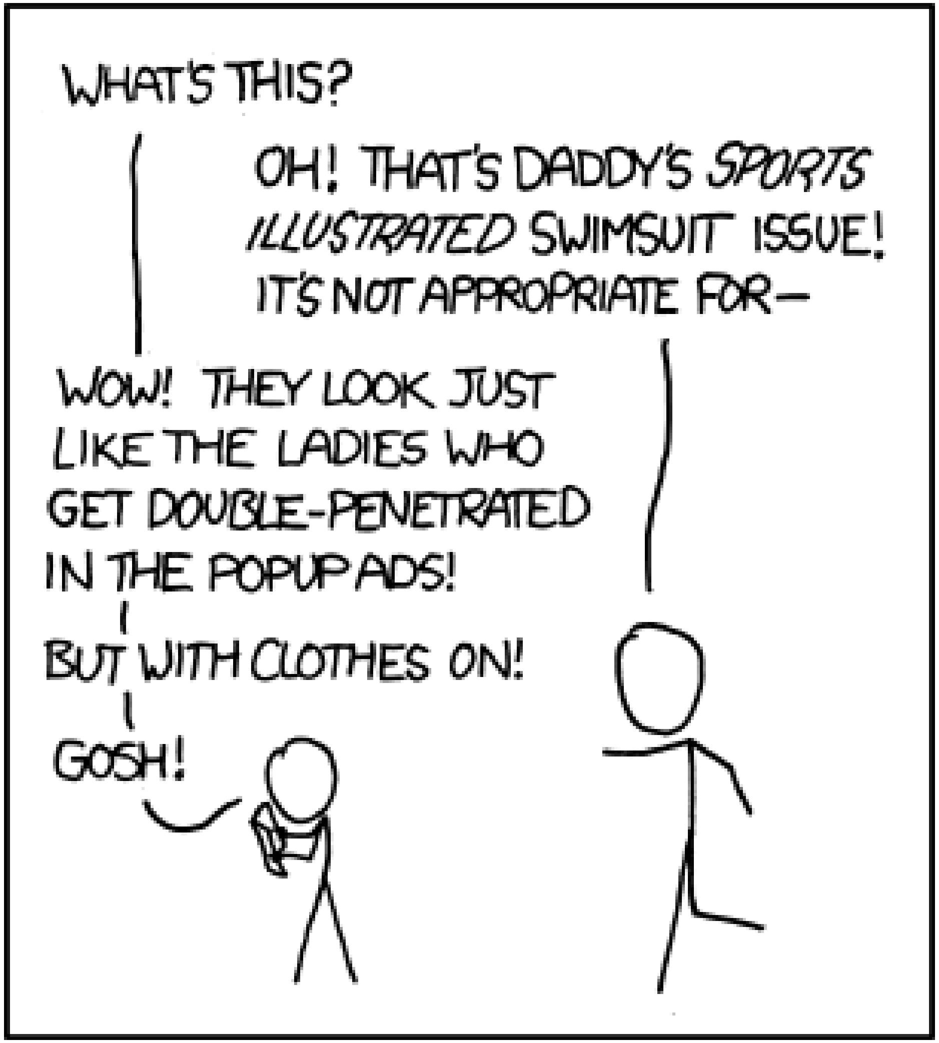
Brad “RenderMan” Haines
Hacker / Security Consultant
RenderLab.net, Churchofwifi.org, NMRC.org
render@renderlab.net

2010 Access and Privacy Conference
June 9th-11th, 2010
http://www.renderlab.net/projects/presentations

Caveats

- Some data presented here is 'Live'
- I have redacted as best I can, please respect any errors or omissions
- I have tried to contact my examples as best I can
- If it's this easy for me, imagine someone determined
- I respond to Render or Brad equally

Relevant Aside


WHAT'S THIS?
OH! THAT'S DADDY'S *SPORTS ILLUSTRATED* SWIMSUIT ISSUE! IT'S NOT APPROPRIATE FOR—
WOW! THEY LOOK JUST LIKE THE LADIES WHO GET DOUBLE-PENETRATED IN THE POPUP ADS!
BUT WITH CLOTHES ON!
GOSH!

- xkcd.com
- Relevant to growing up digital
- Childhood is never the same between generations

Who Am I?

Who Am I?

Consultant – Wireless, Physical Security

Author – 7 Deadliest Wireless Attacks, Kismet Hacking, RFID Security, etc

Trainer – Wireless and Physical security

Who Am I?

Consultant – Wireless, Physical Security

Author – 7 Deadliest Wireless Attacks, Kismet Hacking, RFID Security, etc

Trainer – Wireless and Physical security

Hacker – Renderlab.net

Security Researcher

Hacker Group Member – Church of Wifi, NMRC

Frequent Speaker – Westpoint Military Academy, Defcon, HOPE, ETC

Teach Wireless security and lockpicking

My World

- My world is unlike anything many of you have seen, It’s a frightening place
- 11 Defcons, 5 Shmoocons, 6 HOPE's, 2 SecTor's, 3 Hackcon's, 1 SecVest , 1 CONfidence, a bunch of smaller corporate and regional events and even Westpoint Academy
- Been speaking regularly for ~6 years
- Hacking is a way of life for me, met my wife at a HOPE conference (2004)

Privacy and Trust

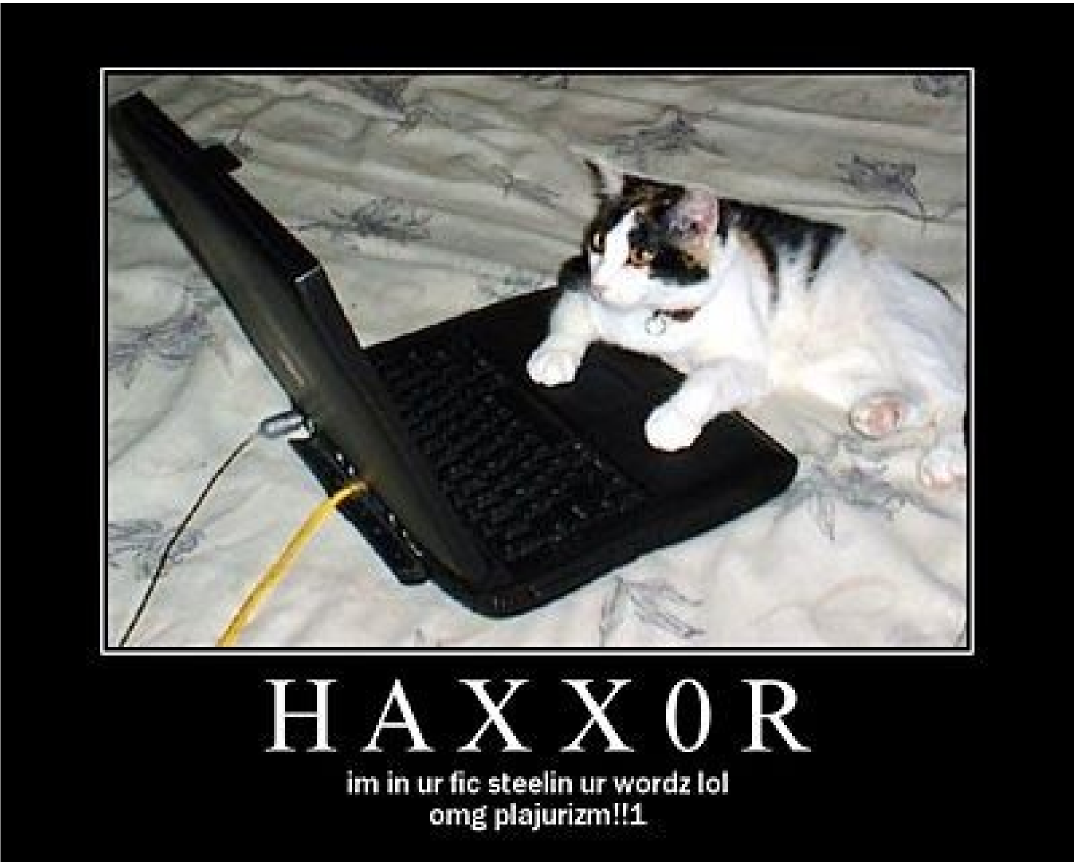
- Privacy is about trust
- People expect they can trust the caretakers of their data
- Policies expect some trust within the users
- Security trusts no one
- Trust is a currency, spend it wisely

The Problem

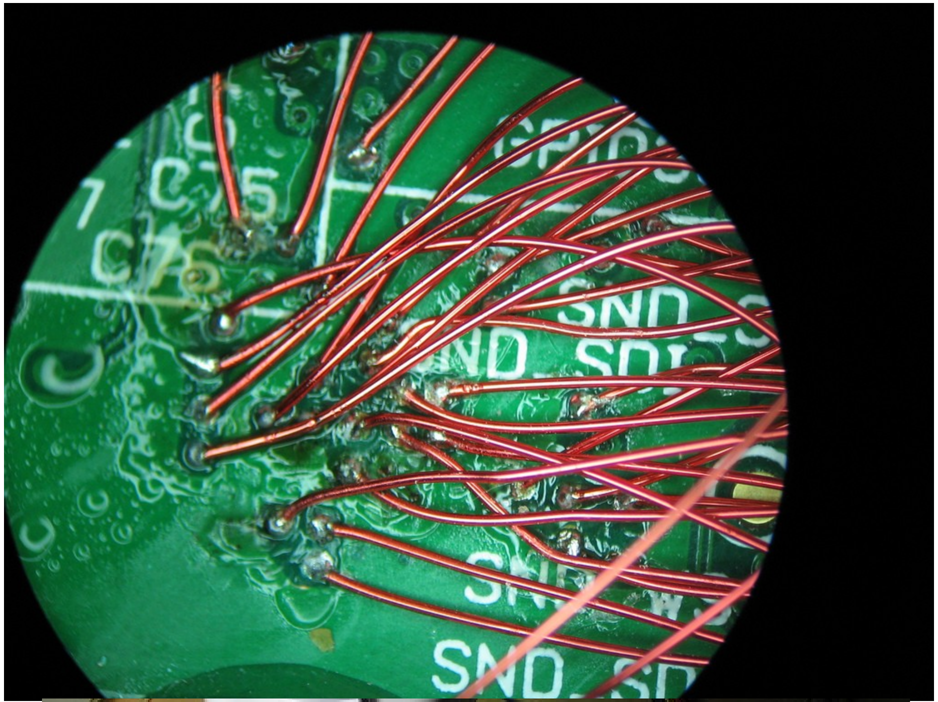
- I deal with many clients where Privacy and Security are required
- So often, the issue is one of technical knowledge
- What you don't know, *can* hurt you
- How do you solve a problem if you don't know about it?
- Policy only goes so far

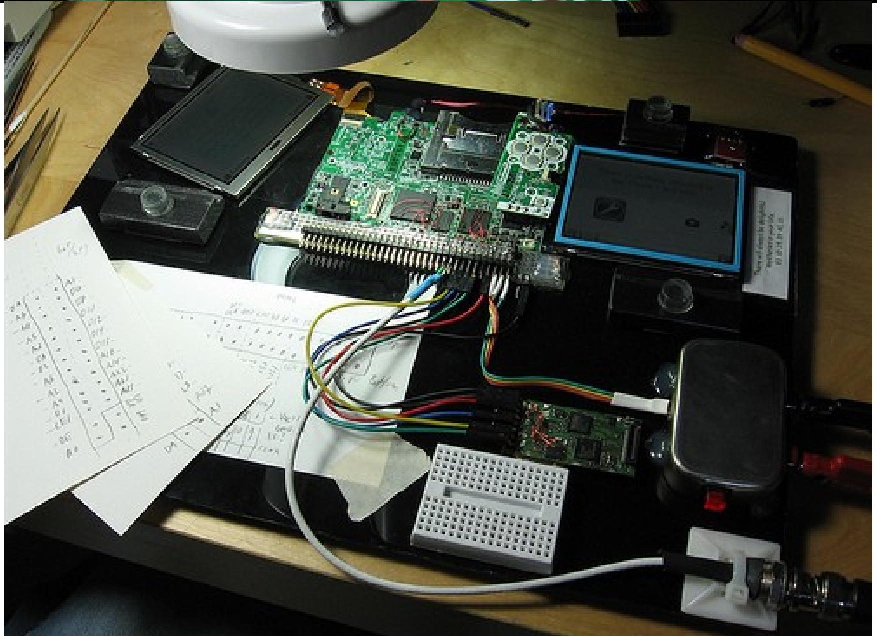
Attackers

- No longer the 'Bored Teenager'
- Major financial incentives nowadays
- Corporate interest
- TJX / Albert Gonzalez
- China/Aurora
- Infinite time, Infinite resources, Infinite patience



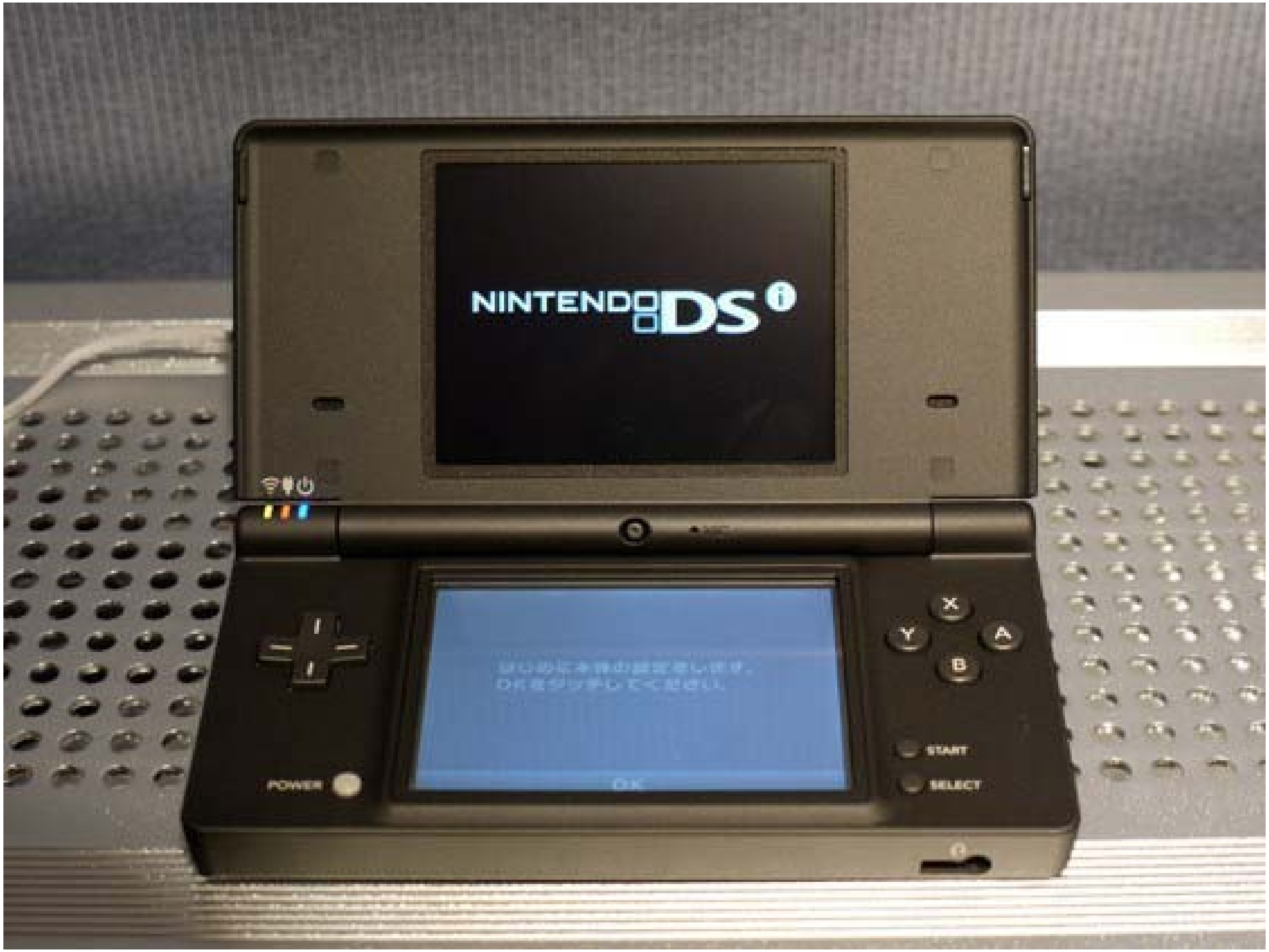
What Is This





- 0.2mm wires
- Hand soldered to read RAM contents
- FPGA's and custom clock interface
- Any guess what it is?

Nintendo DSi



Thinking Security

- Books and classes are great, but have limits
- Defending against the last attack does little to defend against the next
- Thinking like a bad guy does not make you a bad guy, just an informed defender
- Anyone says that 'your secure' is lying, they just haven't found the hole yet
- On the Internet, you are < 100ms away from every jerk in the world

Threats

- Hackers are a useful source of information on the 'up and coming' threats
- We think about this stuff differently, likely to spot non-obvious leaks and threats
- Hackers 2-5 years ahead of the threat curve
- Paying attention to hacker culture can give you a lot of insights to the future
- Hackerspaces: an untapped information resource

Threat #1: Cordless Phones

- Ubiquitous in most homes
- Headsets nearly standard issue in business
- Great fun for a bored hacker in a park downtown
- Old issue with a new twist

Threat #1: Cordless Phones

- Older units operate on common frequencies (900Mhz, 1.2Ghz)
- Common wireless scanners can easily listen in on phones, baby monitors, radios, etc
- Just because you make something illegal, doesn't mean it can't happen (Thanks China!)
- Newer phones now digital and encrypted
- All is well, right?

Threat #1: Cordless Phones

- Digital Enhanced Cordless Telecommunications (DECT)
- Digital, 1.9Ghz, Very flexible standard
- Encryption in the DECT standard
- Encryption not mandatory.....
- Many manufacturers not implementing crypto
- Marketing touts DECT's security, but they aren't using it. No external indications of this

Proof

“I Picked The Wrong Week To Stop Sniffing Glue” - Airplane

- Hackcon, Norway, February 2010
- When I get bored, bad things happen
- Fired up deDECTed and started sniffing
- Not long to find something interesting
- Not long until I got scared...

Proof

- Caught several unencrypted phone calls in progress, recorded the results
- Unfortunately encrypted to me (Norwegian)
- Had native speaker listen and select a clip without any identifying details
- Realized where I was and the potential gravity of the situation
- Got out of the country successfully!

Bluetooth

- Discoverable Bluetooth devices can give away information to an attacker
- From Wednesday morning session:
  - Removed for obvious reasons
- Turn off discoverability!

Wireless Mics

- Wireless Mics are generally unencrypted (unless you pay ALOT!)
- Anyone can listen within a fairly short range
    - 789.900 Mhz
    - 668.050 Mhz
    - 663.025 Mhz
    - 1142.975 Mhz
- Private meetings can suddenly be very public
- Would you go and give a private talk at a radio station?

Threat #1 Mitigation

- Have a complete understanding of the capabilities of your products
- Just because the standard has the capability, does not mean it is using it, how do you know?
- Keep up to date on latest research and abstracts from conferences, lets you know where to look
- Hold manufacturers to task for explicit information rather than marketing
- Trust, but verify it's doing what it is supposed to!

Threat #2: Metadata

- Metadata – Data about data, information embedded within electronic files, about the files
- Usernames, modification dates, revision history, network paths, editing markups, etc
- Can reveal more than you intend
- 2003 Downing Street Iraq War dossier
- Photo EXIF Data

Threat #2: Metadata

```
ExifTool Version Number         : 7.82
File Name                       : photo.jpg
Directory                       : .
File Size                       : 144 kB
File Modification Date/Time     : 2010:06:01
06:54:19-06:00
File Type                       : JPEG
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Exif Byte Order                 : Big-endian (Motorola,
MM)
Make                            : Apple
Camera Model Name               : iPhone 3GS
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Software                        : 3.1.3
Modify Date                     : 2010:05:04 07:57:34
Y Cb Cr Positioning             : Centered
Exposure Time                   : 1/120
F Number                        : 2.8
Exposure Program                : Program AE
ISO                             : 132
Exif Version                    : 0221
```

Threat #2: Metadata

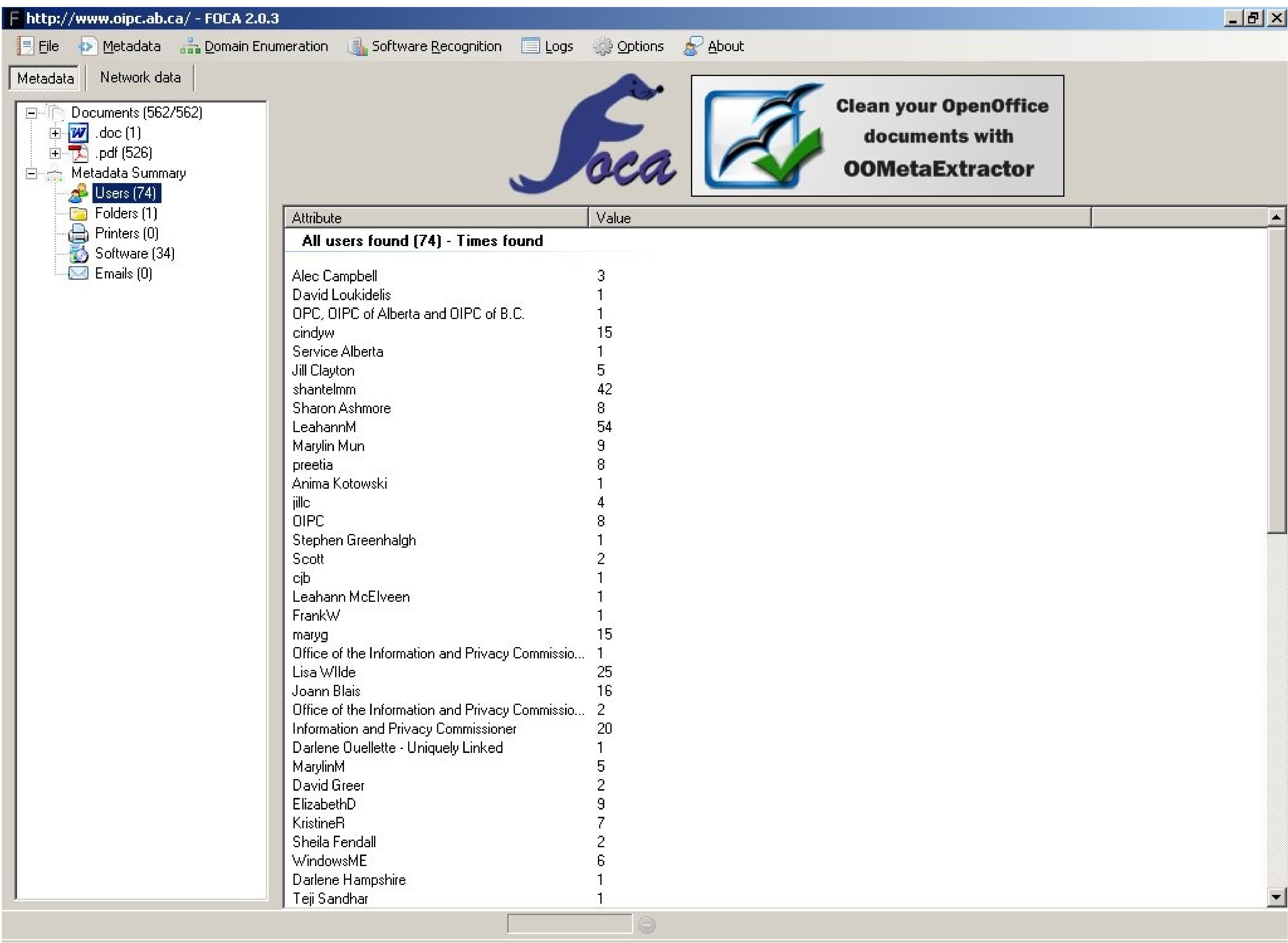
```
Date/Time Original              : 2010:05:04
07:57:34
Create Date                     : 2010:05:04 07:57:34
Shutter Speed Value             : 1/120
Aperture Value                  : 2.8
Metering Mode                   : Average
Flash                           : No flash function
Focal Length                    : 3.9 mm
Flashpix Version                : 0100
Color Space                     : sRGB
Exif Image Width                : 800
Exif Image Height               : 600
Sensing Method                  : One-chip color area
Exposure Mode                   : Auto
White Balance                   : Auto
Sharpness                       : Soft
GPS Latitude Ref                : North
GPS Longitude Ref               : West
GPS Altitude Ref                : Above Sea Level
GPS Time Stamp                  : 07:57:34.6
GPS Dilution Of Precision       : 3
GPS Img Direction Ref           : Magnetic North
GPS Img Direction               : 354
Image Width                     : 800
Image Height                    : 600
```

Threat #2: Metadata

```
Encoding Process                : Baseline DCT,
Huffman coding
Bits Per Sample               : 8
Color Components               : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Aperture                      : 2.8
GPS Altitude                   : 633 m Above Sea
Level
GPS Latitude                   : *******
GPS Longitude                   : *******
GPS Position                   : ********
Image Size                     : 800x600
Shutter Speed                   : 1/120
Focal Length                   : 3.9 mm
Light Value                    : 9.5
```

Threat #2: Metadata

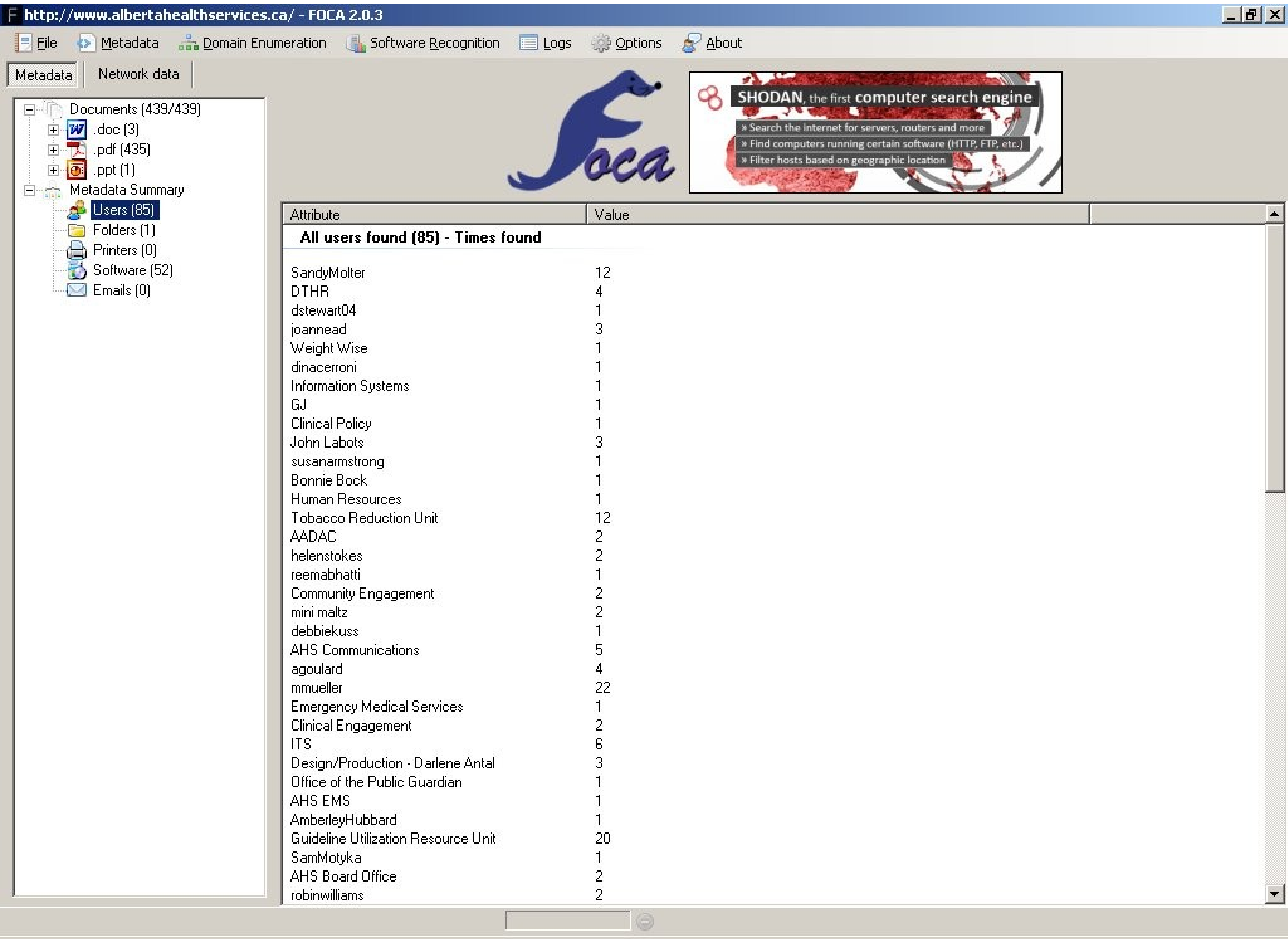
- FOCA – Fingerprinting Organizations Collected Archives - http://www.informatica64.com/foca/
- Online or download versions
- Uses search engines to locate documents
- Download, extract and organize metadata from entire sites
- What's a good site to search?


http://www.oipc.ab.ca/ - FOCA 2.0.3
File
Metadata
Domain Enumeration
Software Recognition
Logs
Options
About
Metadata
Network data
Clean your OpenOffice documents with OOMetaExtractor

Documents (562/562)
- .doc (1)
- .pdf (526)

Metadata Summary
- Users (74)
- Folders (1)
- Printers (0)
- Software (34)
- Emails (0)

Attribute	Value
All users found (74) - Times found	
Alec Campbell	3
David Loukidelis	1
OPC, OIPC of Alberta and OIPC of B.C.	1
cindyw	15
Service Alberta	1
Jill Clayton	5
shantelmm	42
Sharon Ashmore	8
LeahannM	54
Marylin Mun	9
preetia	8
Anima Kotowski	1
jillc	4
OIPC	8
Stephen Greenhalgh	1
Scott	2
cjb	1
Leahann McElveen	1
FrankW	1
maryg	15
Office of the Information and Privacy Commissio...	1
Lisa WIlde	25
Joann Blais	16
Office of the Information and Privacy Commissio...	2
Information and Privacy Commissioner	20
Darlene Ouellette - Uniquely Linked	1
MarylinM	5
David Greer	2
ElizabethD	9
KristineR	7
Sheila Fendall	2
WindowsME	6
Darlene Hampshire	1
Teji Sandhar	1


http://www.albertahealthservices.ca/ - FOCA 2.0.3
File
Metadata
Domain Enumeration
Software Recognition
Logs
Options
About
Metadata
Network data
Documents (439/439)
.doc (3)
.pdf (435)
.ppt (1)
Metadata Summary
Users (85)
Folders (1)
Printers (0)
Software (52)
Emails (0)
Foca
SHODAN, the first computer search engine
» Search the internet for servers, routers and more
» Find computers running certain software (HTTP, FTP, etc.)
» Filter hosts based on geographic location

Attribute	Value
All users found (85) - Times found	
SandyMolter	12
DTHR	4
dstewart04	1
joannead	3
Weight Wise	1
dinacerroni	1
Information Systems	1
GJ	1
Clinical Policy	1
John Labots	3
susanarmstrong	1
Bonnie Bock	1
Human Resources	1
Tobacco Reduction Unit	12
AADAC	2
helenstokes	2
reemabhatti	1
Community Engagement	2
mini maltz	2
debbiekuss	1
AHS Communications	5
agoulard	4
mmueller	22
Emergency Medical Services	1
Clinical Engagement	2
ITS	6
Design/Production - Darlene Antal	3
Office of the Public Guardian	1
AHS EMS	1
AmberleyHubbard	1
Guideline Utilization Resource Unit	20
SamMotyka	1
AHS Board Office	2
robinwilliams	2

Threat #3: Metadata Mitigation

- Documents can contain more than you think
- Learn about the tools you use, learn which end is sharp
- Many tools available to 'scrub' documents to be made public, depending on format
- Educate users that 'Track changes' can be dangerous and anything typed can be recorded
- Don't release metadata rich documents like .doc files, use .pdf or others instead

Threat #3: Wireless Networks

- Wireless networks are everywhere
- We all use them, hard to imagine life without them
- Threats that were minimal with wires are amplified with wireless
- Most people don't understand what is actually being sent over the air
- Provided hundreds of hours of entertainment at conferences, hotels, airports, etc

Passwords

```
06/01/10 20:34:56 tcp 192.168.55.133.49197 -> sv15.*****server.net.110 (pop3)
USER nishino@*******tech.co.jp
PASS tato1330

-----------------
06/01/10 20:35:01 tcp 192.168.55.133.49195 -> pop.dj9.******.ne.jp.110 (pop3)
USER nishino9@dj9.******.ne.jp
PASS tn3576

-----------------
06/01/10 20:35:06 tcp 192.168.55.133.49279 -> pop.dj9.******.ne.jp.110 (pop3)
USER nishino9@dj9.******.ne.jp
PASS tn3576
```

Web Surfing

```
192.168.55.133 - - [01/Jun/2010:19:35:39 -0600] "GET
http://www.monex.co.jp/image/top/seminar_heading_02.gif HTTP/1.1" - - "
http://www.monex.co.jp/

192.168.55.101 - - [01/Jun/2010:19:37:14 -0600] "GET
http://www.eramuslim.com/tpl/new7/img/accent-grey-dots-horizontal.gif
HTTP/1.0" - - "http://www.eramuslim.com/manhaj-dakwah/gerakan-masa-
depan/"
```

Porn Surfing

```
wsip-70-165-253-13.lv.lv.cox.net - - [02/Jun/2010:06:25:49 -0600] "GET
http://images.imagefap.com/images/mini/42/144/1441605645.jpg

wsip-70-165-253-13.lv.lv.cox.net - - [02/Jun/2010:06:25:49 -0600] "GET
http://images.imagefap.com/images/mini/42/451/451240244.jpg

wsip-70-165-253-13.lv.lv.cox.net - - [02/Jun/2010:06:25:50 -0600] "GET
http://images.imagefap.com/images/mini/42/193/1930587975.jpg
```

Threat #3: Wireless Networks

- Wireless operates on 2.4Ghz/5Ghz
- ISM band, license free
- Encryption available on all units, not necessarily used
- Many situations cant' use encryption (Coffee Shops, Hotels, Conferences)
- Protocols designed for wired not expecting wireless
- Many common protocols offer no protection (pop, smtp, http, etc)

Treat #3: Wireless Networks

- Open Network - Data is sent in the clear, anyone can 'listen' to anything sent
- WEP – Trivially broken in 60 seconds
- Websites visited, search queries, emails, instant messages, etc
- SSL offers some protection, easily neutralized in the right environment

Google Wardriving Controversy

- Classic case of over reaction due to lack of technical understanding
- Streetview cars collecting locations of wireless networks for use as alternative geolocation service

Google Wardriving Controversy

- Header information is unencrypted, sent to broadcast
- Everyone is an intended recipient (Broadcast)
- Combined with GPS coordinates, provides alternative geolocation mechanism
- Many others doing similar (Skyhook)
- Google accidentally collecting 'data' payloads, admitted error to relevant privacy authorities
- Encrypted data still encrypted, only risk comes from open networks

Google Wardriving Controversy

- Google uses Kismet, open source wireless sniffer, with some additional custom software
- One change in config file to avoid recording data packets
- If your running an open network, you are part of the problem
- Amount of data is minimal and fragmented
- Everyone freaking out at Google for doing this, larger question is, “Who has been listening long before them”?

Threat #3: Wireless Mitigation

- Force a VPN on any wireless network (encrypted or not)
- Ensure users are aware of dangers
- Prevent users from using Open Access Points
- Be aware that access points broadcast their presence 100 times/sec
- Data (even encrypted) can be captured for later analysis
- Wait till you can use a wire for sensitive stuff

Threat #4: Hidden Data Storage

- 'Secure' deletion a common policy
- Do you know where all your data is to delete it?
- Photocopiers, cameras, PDA's, etc
- CBS news made a splash recently with Photocopiers
- Most modern copiers contain a hard drive for storage, buffering or other functions

Threat #4: Hidden Data Storage

- A practical example:
- ENTS neighbor was a copier repair office
- Left after lease was up and left a large number of copiers
- ENTS was given them to strip for parts, incl. Hard drives
- Hard drives were handed to me for forensics practice
- Results were surprising and appropriate to this venue

Threat #4: Hidden Data Storage

- 8 drives, various sizes
- Using open source tools, proceeded to image and extract any information left on the drive
- None of the drives were in full working order
- All contained some small amount of data, typically web admin pages, images
- 2 contained a wealth of information
- One elementary school, one consulting outfit
- Both were contacted, no word from either

Drive #1

- Receipts

Drive #1

- Receipts
- Defamation Lawsuit

Drive #1

- Receipts
- Defamation Lawsuit
- Project proposals

Drive #1

- Receipts
- Defamation Lawsuit
- Project proposals
- Confidential faxes

Drive #1

- Receipts
- Defamation Lawsuit
- Project proposals
- Confidential faxes
- Confidential documents
- Lots of other docs I don't want to show publicly
- Nothing earth shattering, but still not happy

Drive #2

- Elementary school in Red Deer
- Classroom lessons
- Administrative notes home
- Report cards with Student info
- Lots more I can't show

Lessons

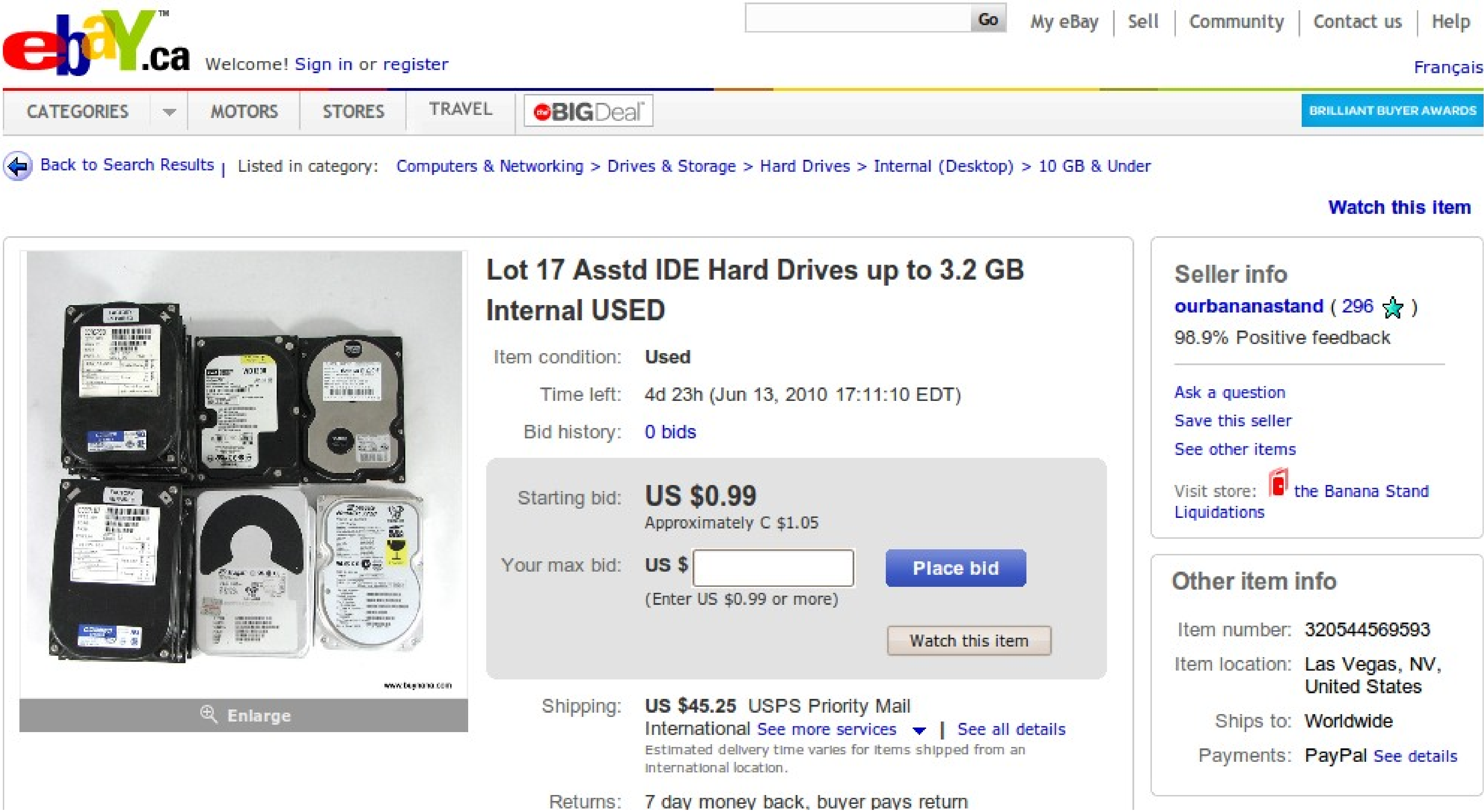
Administrative Notes

Report Cards

Threat #4: Hidden Data Mitigation

- Be aware of what devices contain, ask questions
- Need to make sure everyone knows issues
- Big sticker on copiers, devices
- Make agreements on leased devices for assuring deletion of data
- As a rule, don't throw out any storage media, ensure it's secure destruction by any means necessary

Don't Do This!



Back to Search Results | Listed in category: Computers & Networking > Drives & Storage > Hard Drives > Internal (Desktop) > 10 GB & Under

Watch this item

Lot 17 Asstd IDE Hard Drives up to 3.2 GB Internal USED

Item condition:	**Used**
Time left:	4d 23h (Jun 13, 2010 17:11:10 EDT)
Bid history:	0 bids
Starting bid:	**US $0.99** Approximately C $1.05
Your max bid:	**US $** (Enter US $0.99 or more)
Shipping:	**US $45.25** USPS Priority Mail International See more services | See all details Estimated delivery time varies for items shipped from an international location.
Returns:	7 day money back, buyer pays return

Seller info

ourbananastand (296 ☆)

98.9% Positive feedback

Ask a question

Save this seller

See other items

Visit store: the Banana Stand Liquidations

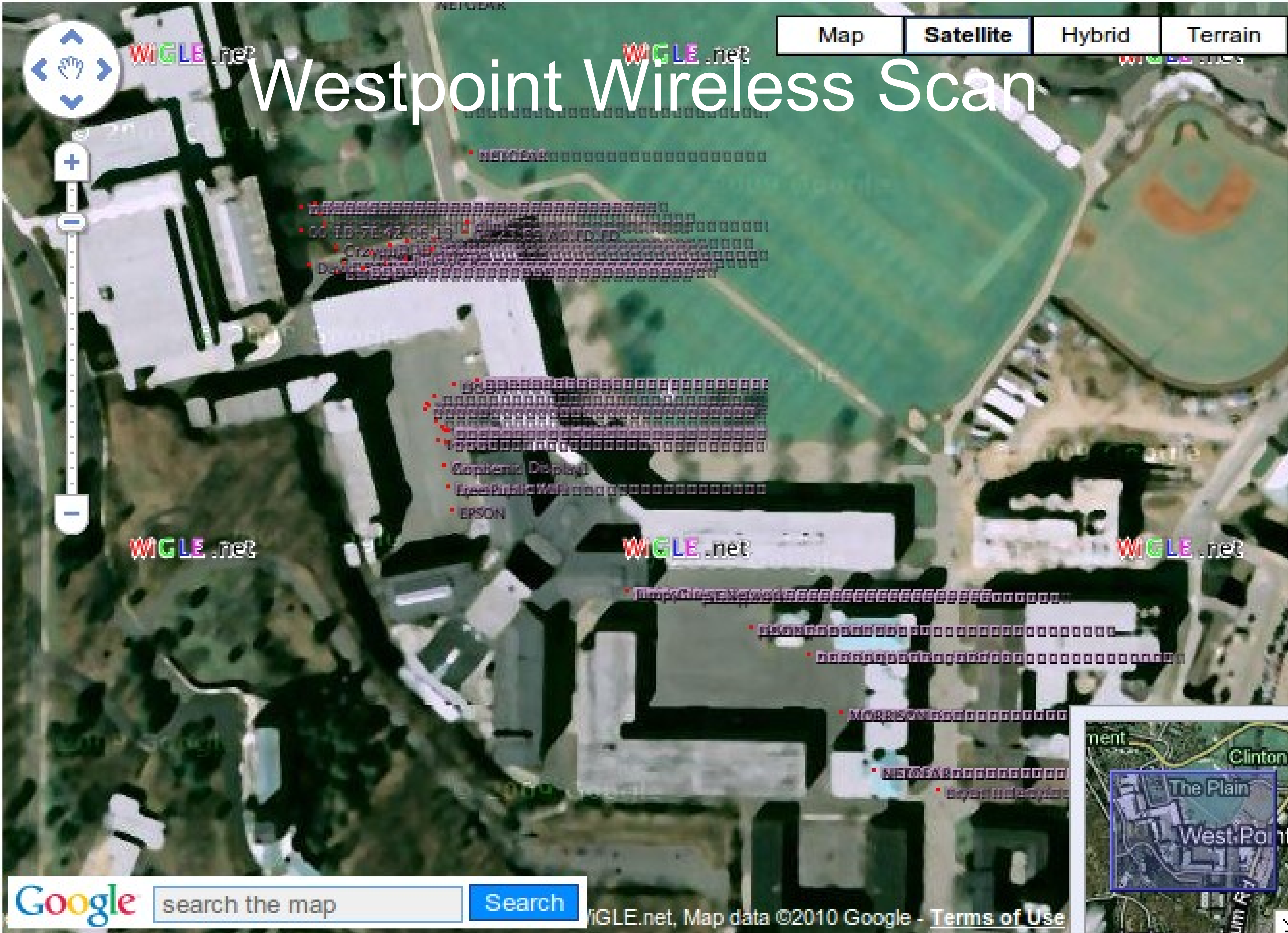
Other item info

Item number:	320544569593
Item location:	Las Vegas, NV, United States
Ships to:	Worldwide
Payments:	PayPal See details

Thoughts

- All these issues are old news in the Hacker community, we've moved on
- Some still seen as 'new' by the public, I could go on for hours
- Mistakes happen, but this is epidemic
- Educational uptake too slow
- There are people out there who can help, find them, use them!
- Never doubt that someone will try anything to get data....

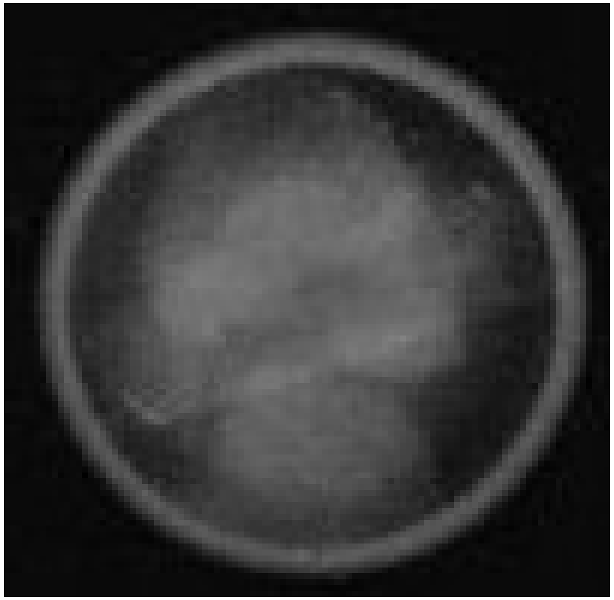
Westpoint Wireless Scan

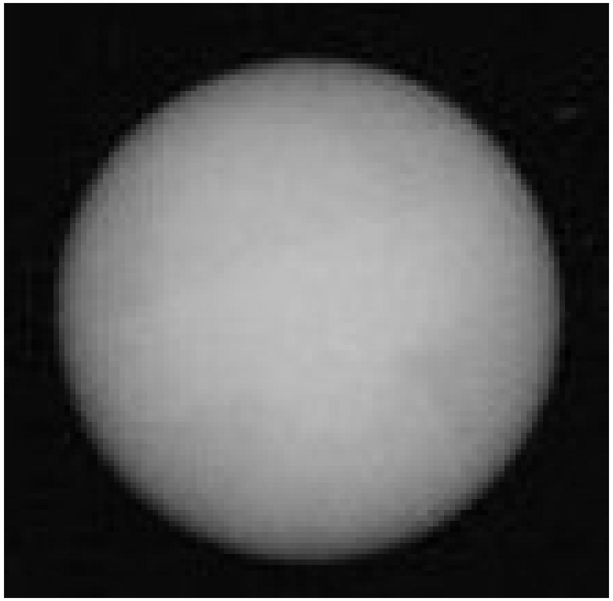


Parliament Wireless Scan

Final Thoughts

- Things are not always what they seem
- It takes a special eye to spot the non obvious threat even when it's right in front of you





Questions?

www.RenderLab.net
Render@RenderLab.net
Brad.Haines@Shaw.ca

http://www.renderlab.net/projects/presentations/