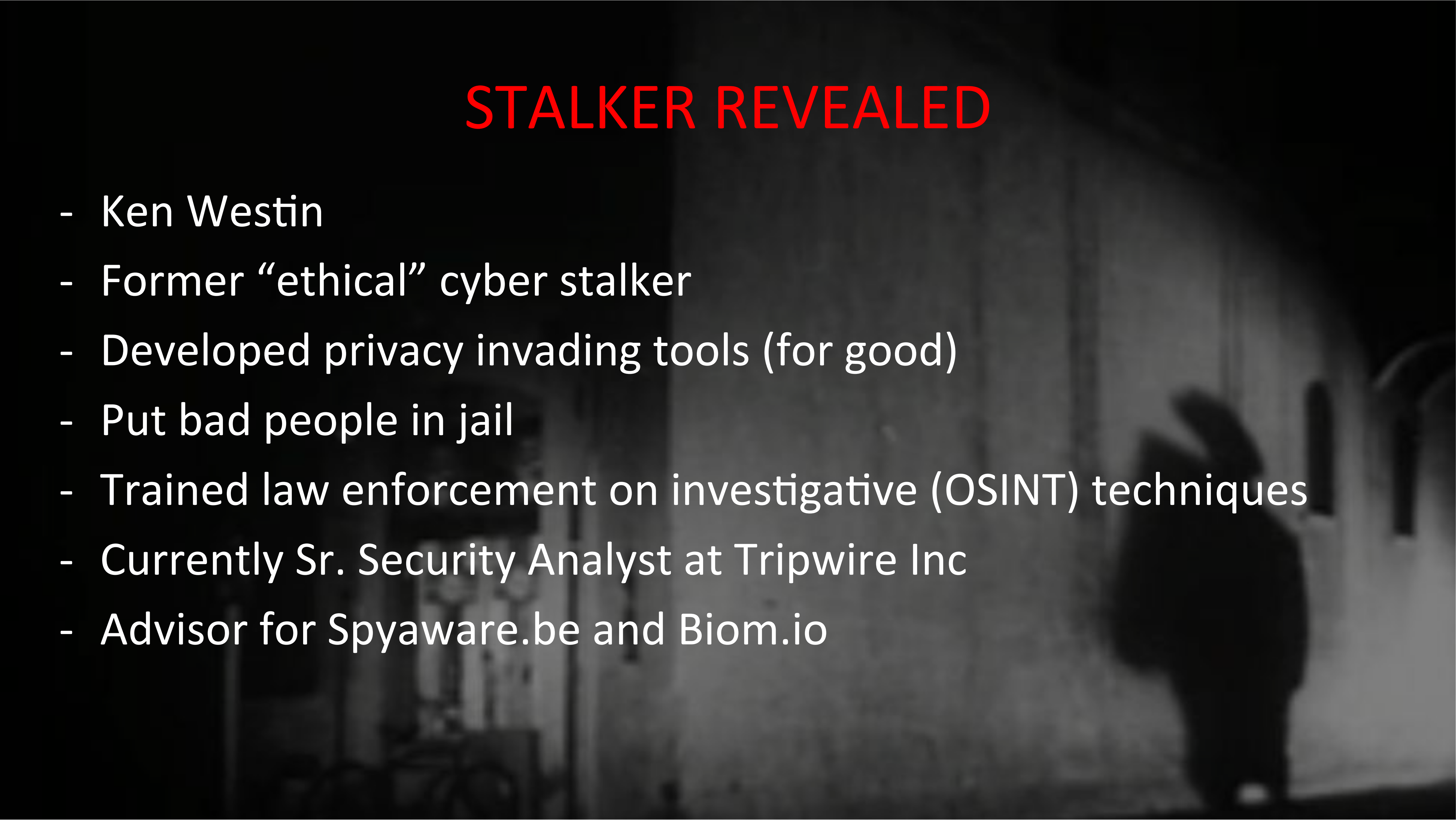
Confessions of a Professional Cyber Stalker

DEF CON 23 LAS VEGAS

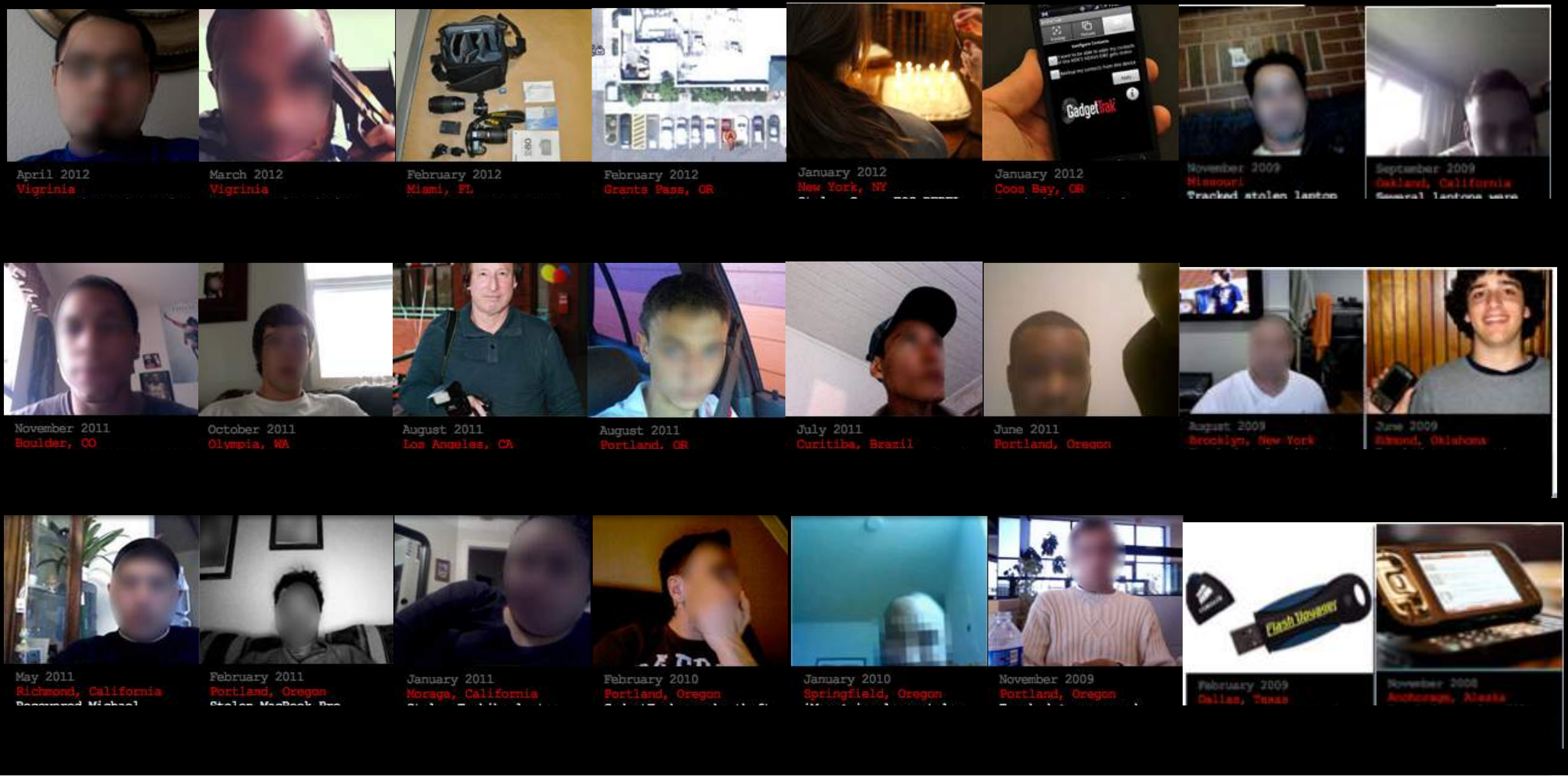
KEN WESTIN
SR SECURITY ANALYST
KWESTIN@GMAIL.COM
@KWESTIN



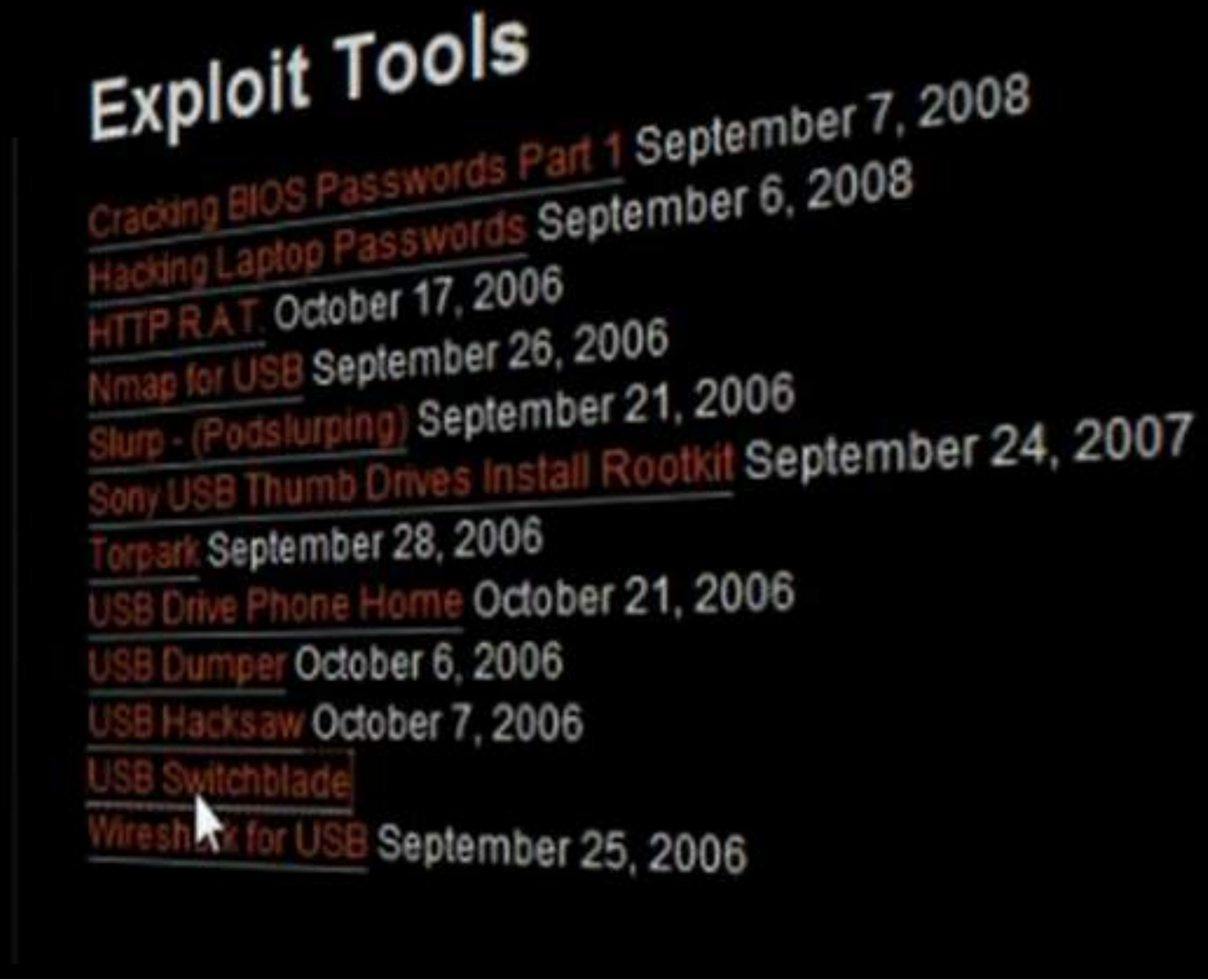
STALKER REVEALED

- Ken Westin
- Former “ethical” cyber stalker
- Developed privacy invading tools (for good)
- Put bad people in jail
- Trained law enforcement on investigative (OSINT) techniques
- Currently Sr. Security Analyst at Tripwire Inc
- Advisor for Spyaware.be and Biom.io

CASE CLOSED


April 2012
Vigrinia
March 2012
Vigrinia
February 2012
Miami, FL
February 2012
Grants Pass, OR
January 2012
New York, NY
GadgetTrak
January 2012
Coos Bay, OR
November 2009
Missouri
Tracked stolen laptop
September 2009
Oakland, California
Several laptops were
November 2011
Boulder, CO
October 2011
Olympia, WA
August 2011
Los Angeles, CA
August 2011
Portland, OR
July 2011
Curitiba, Brazil
June 2011
Portland, Oregon
August 2009
Brooklyn, New York
June 2009
Edmond, Oklahoma
May 2011
Richmond, California
Recovered Michael
February 2011
Portland, Oregon
Stolen MacBook Pro
January 2011
Moraga, California
February 2010
Portland, Oregon
January 2010
Springfield, Oregon
November 2009
Portland, Oregon
Flash Voyager
February 2009
Dallas, Texas
November 2008
Anchorage, Alaska

USB Hacks



Exploit Tools

Cracking BIOS Passwords Part 1 September 7, 2008

Hacking Laptop Passwords September 6, 2008

HTTP R.A.T. October 17, 2006

Nmap for USB September 26, 2006

Slurp - (Podslurping) September 21, 2006

Sony USB Thumb Drives Install Rootkit September 24, 2007

Torpark September 28, 2006

USB Drive Phone Home October 21, 2006

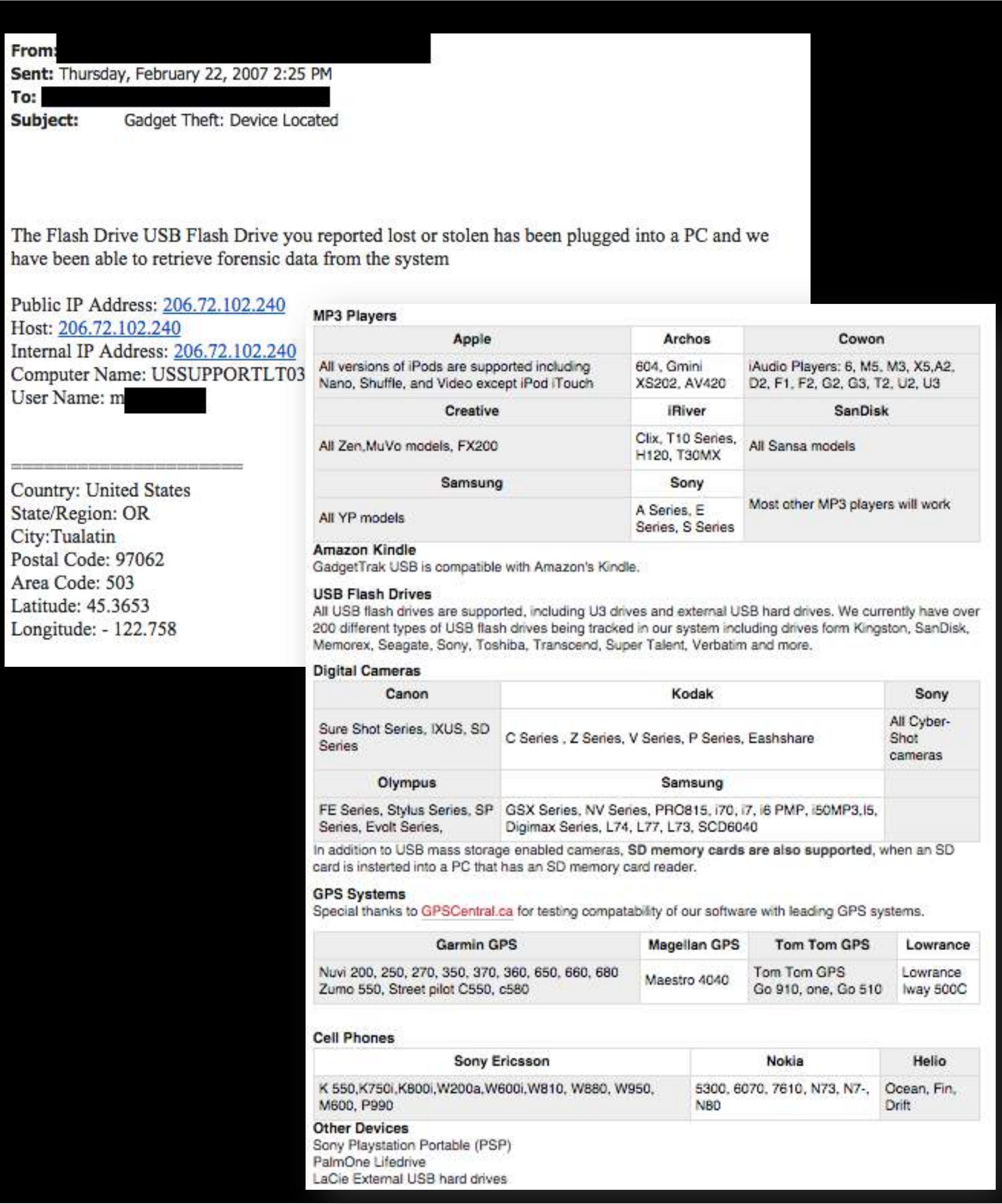
USB Dumper October 6, 2006

USB Hacksaw October 7, 2006

USB Switchblade

Wireshark for USB September 25, 2006

"THE DETECTIVES"



From: [redacted]
Sent: Thursday, February 22, 2007 2:25 PM
To: [redacted]
Subject: Gadget Theft: Device Located

The Flash Drive USB Flash Drive you reported lost or stolen has been plugged into a PC and we have been able to retrieve forensic data from the system

Public IP Address: 206.72.102.240
Host: 206.72.102.240
Internal IP Address: 206.72.102.240
Computer Name: USSUPPORTLT03
User Name: m[redacted]

=======================

Country: United States
State/Region: OR
City:Tualatin
Postal Code: 97062
Area Code: 503
Latitude: 45.3653
Longitude: - 122.758

MP3 Players

Apple	Archos	Cowon
All versions of iPods are supported including Nano, Shuffle, and Video except iPod iTouch	604, Gmini XS202, AV420	iAudio Players: 6, M5, M3, X5,A2, D2, F1, F2, G2, G3, T2, U2, U3
Creative	**iRiver**	**SanDisk**
All Zen,MuVo models, FX200	Clix, T10 Series, H120, T30MX	All Sansa models
Samsung	**Sony**	Most other MP3 players will work
All YP models	A Series, E Series, S Series	

Amazon Kindle
GadgetTrak USB is compatible with Amazon's Kindle.

USB Flash Drives
All USB flash drives are supported, including U3 drives and external USB hard drives. We currently have over 200 different types of USB flash drives being tracked in our system including drives form Kingston, SanDisk, Memorex, Seagate, Sony, Toshiba, Transcend, Super Talent, Verbatim and more.

Digital Cameras

Canon	Kodak	Sony
Sure Shot Series, IXUS, SD Series	C Series , Z Series, V Series, P Series, Eashshare	All Cyber-Shot cameras
Olympus	**Samsung**	
FE Series, Stylus Series, SP Series, Evolt Series,	GSX Series, NV Series, PRO815, i70, i7, i6 PMP, i50MP3,i5, Digimax Series, L74, L77, L73, SCD6040	

In addition to USB mass storage enabled cameras, **SD memory cards are also supported**, when an SD card is insterted into a PC that has an SD memory card reader.

GPS Systems
Special thanks to GPSCentral.ca for testing compatability of our software with leading GPS systems.

Garmin GPS	Magellan GPS	Tom Tom GPS	Lowrance
Nuvi 200, 250, 270, 350, 370, 360, 650, 660, 680 Zumo 550, Street pilot C550, c580	Maestro 4040	Tom Tom GPS Go 910, one, Go 510	Lowrance Iway 500C

Cell Phones

Sony Ericsson	Nokia	Helio
K 550,K750i,K800i,W200a,W600i,W810, W880, W950, M600, P990	5300, 6070, 7610, N73, N7-, N80	Ocean, Fin, Drift

Other Devices
Sony Playstation Portable (PSP)
PalmOne Lifedrive
LaCie External USB hard drives

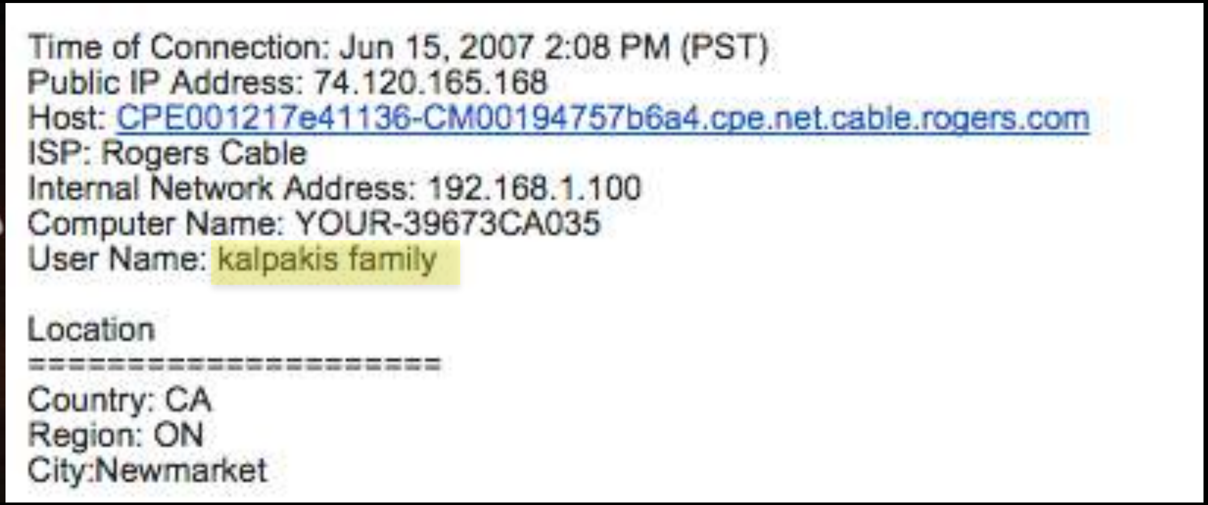
Windows USB Trojans

```
[autorun]
icon=icon.ico
open=passwords.exe
action=Install USB driver
label=My Crap
shell\open\command=passwords.exe
shell\open=Install USB driver
```

Windows Agent

- URL provided during presentation

First iPod Recovery



```
Time of Connection: Jun 15, 2007 2:08 PM (PST)
Public IP Address: 74.120.165.168
Host: CPE001217e41136-CM00194757b6a4.cpe.net.cable.rogers.com
ISP: Rogers Cable
Internal Network Address: 192.168.1.100
Computer Name: YOUR-39673CA035
User Name: kalpakis family

Location
====================
Country: CA
Region: ON
City:Newmarket
```

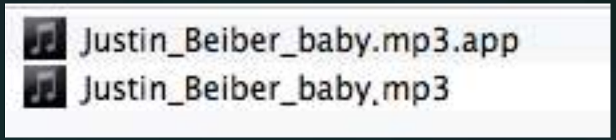
Esc
OK
32GB

BAGH-E-ZAHRA
Bandar Bushehr
بوشهر
55
TANGAK
RAYANI
Pahl
HELEYLAH
Bushehr Nuclear Power Plant

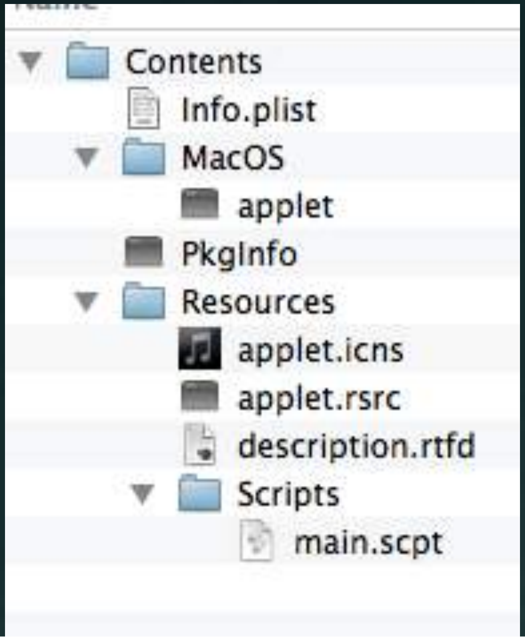
Building Apple USB Trojans

- Why AppleScript?
  - Trusted
  - Interfaces for most OS X apps

- Tricking OS X with Homoglyphs



Justin_Beiber_baby.mp3.app
Justin_Beiber_baby.mp3



```
▼ Contents
    Info.plist
  ▼ MacOS
      applet
    PkgInfo
  ▼ Resources
      applet.icns
      applet.rsrc
      description.rtfd
    ▼ Scripts
        main.scpt
```

Biting Into the AppleScript

```
set sysinfo to (system info) as record
set uname to long user name of sysinfo
set user to short user name of sysinfo
set cname to computer name of sysinfo
set sip to IPv4 address of sysinfo

-----
tell application "iTunes"
        activate
        try
          open location trackURL
        end try
end tell

do shell script “"
```

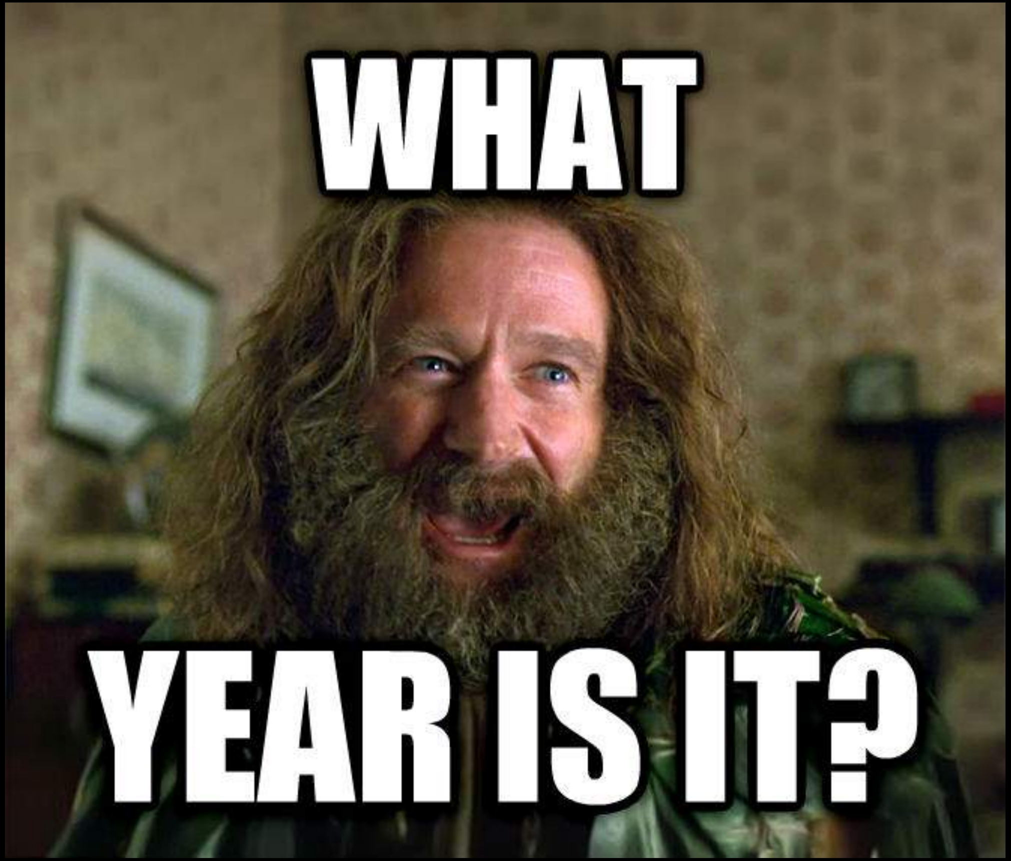
github.com/kwestin/applerazor

USB Attack Vector Still a Threat

- The Stuxnet virus was initially delivered via USB to Iranian nuclear facilities, eventually spreading to Russian facilities in the same way.

- USB Malware has even made it to the International Space Station (2008 W32.Gammima.AG worm)

- In 2012 two US power plants (ICS-CERT) were infiltrated when an employee inadvertently brought an infected USB stick onto the premises.



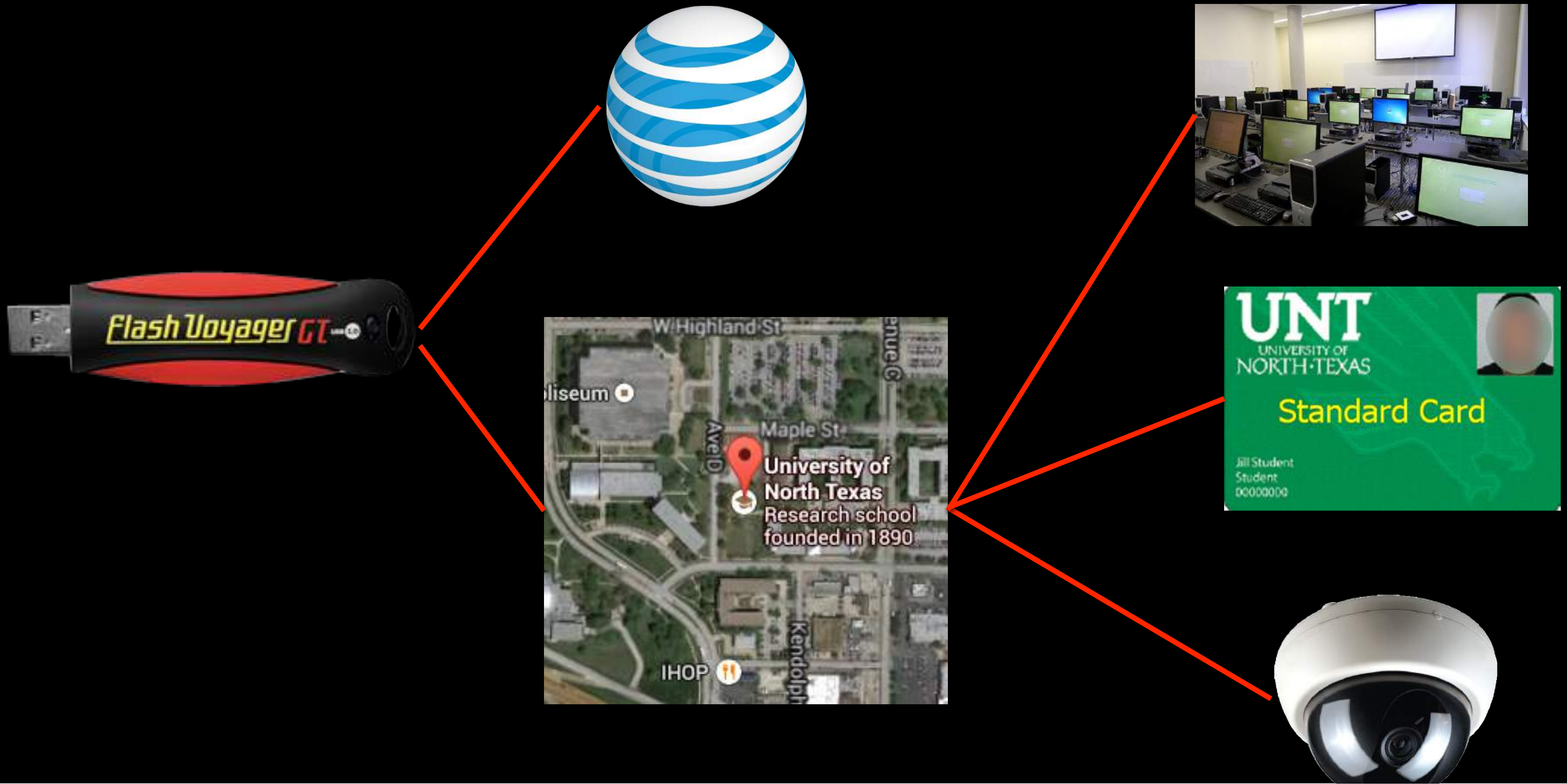
The Trouble with IP as Evidence

- Requires work by law enforcement (paperwork)
- Not identity, does not put person in front of computer
- Probable cause is a challenge
- Not always accurate (proxies etc)
- Takes a long time
- Other “theft recovery” companies use more intrusive methods

September
October
November
December
January
February
March
April
PANDA

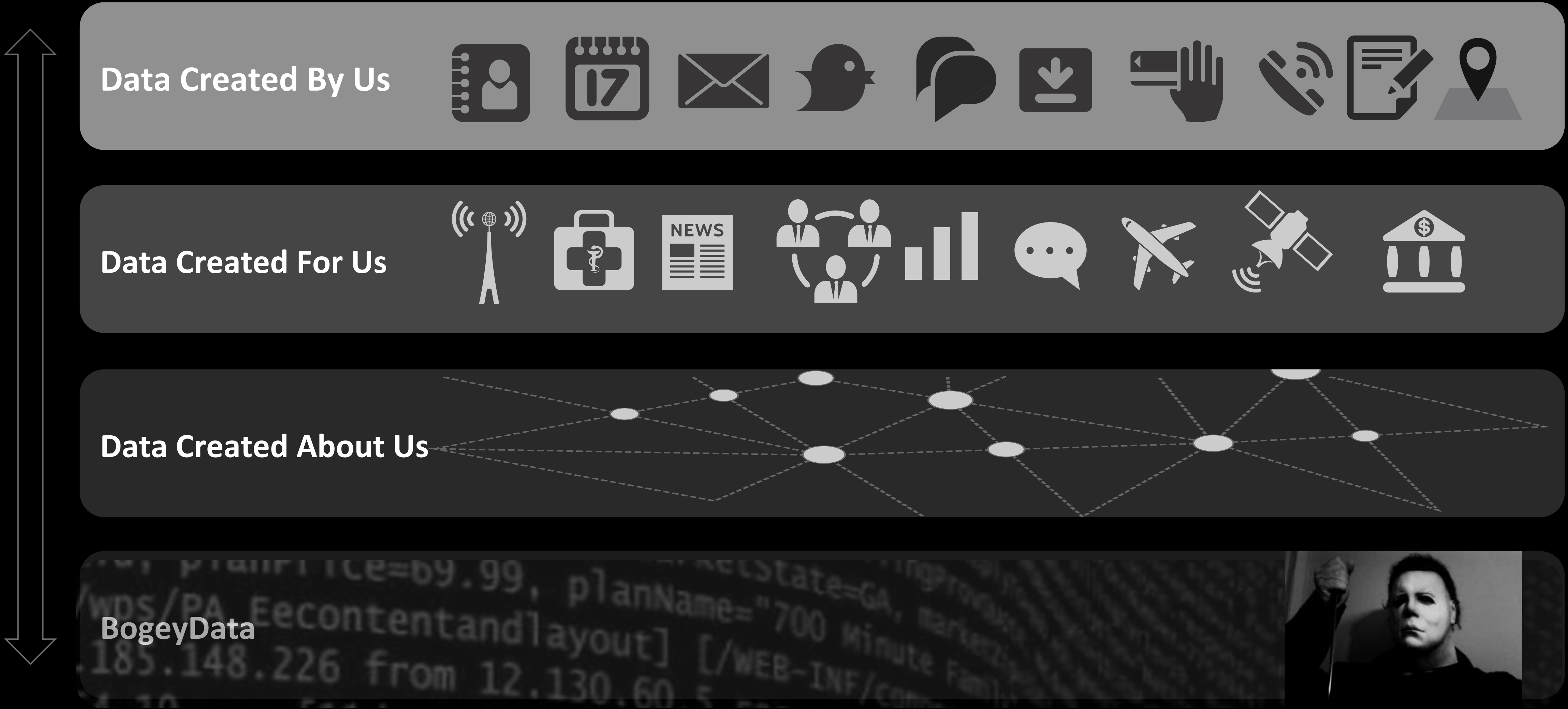
When Correlation Does Imply Causation

2009-02-21 23:43:49



EVERY CONTACT LEAVES A TRACE.

Interaction of Things



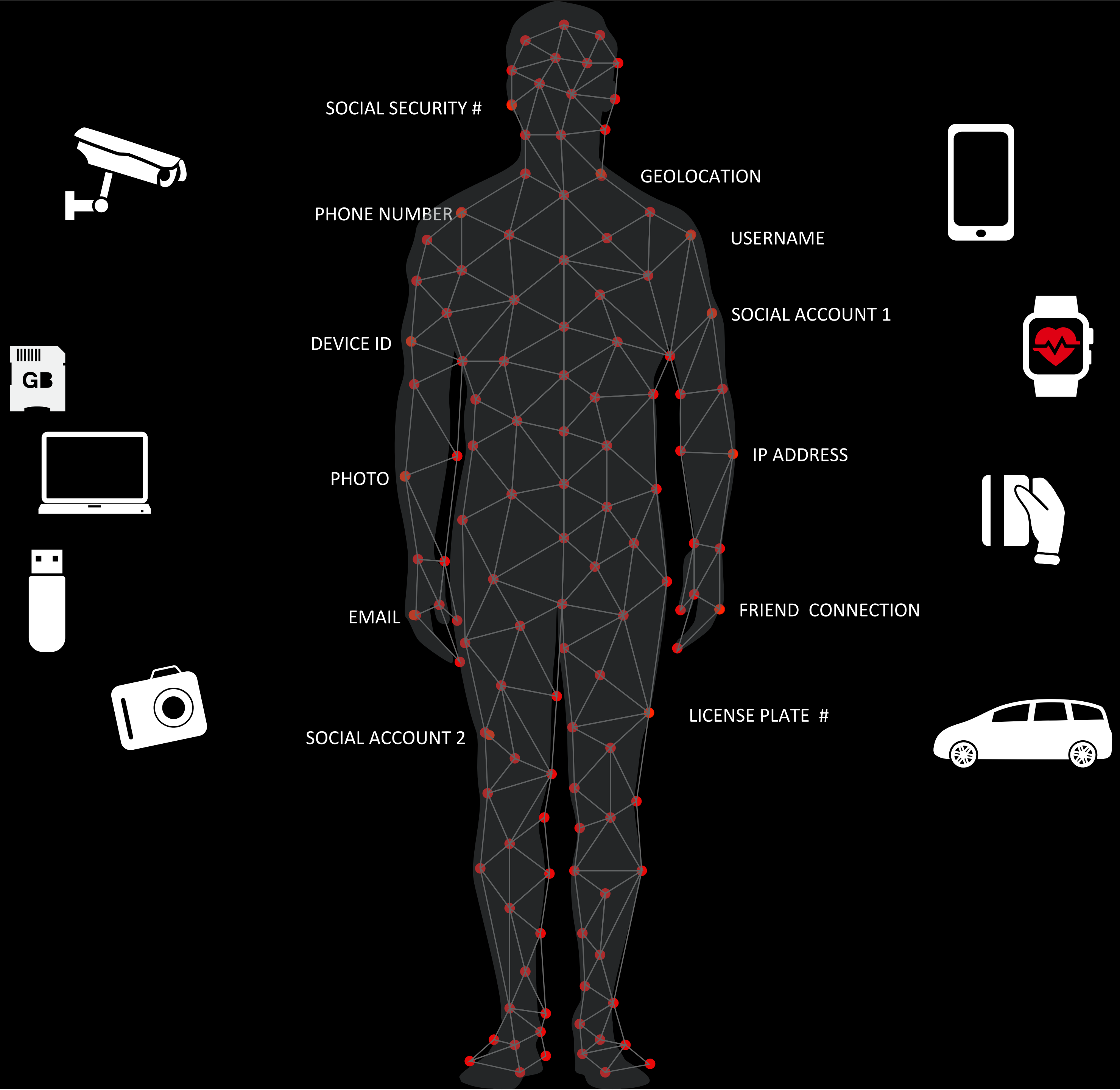
Data Created By Us

Data Created For Us

Data Created About Us

BogeyData

17
NEWS
$
planPrice=69.99, planName="700 Minute
/wps/PA_Econtentandlayout] [/WEB-INF/
185.148.226 from 12.130.60



SOCIAL SECURITY #

PHONE NUMBER

DEVICE ID

PHOTO

EMAIL

SOCIAL ACCOUNT 2

GEOLOCATION

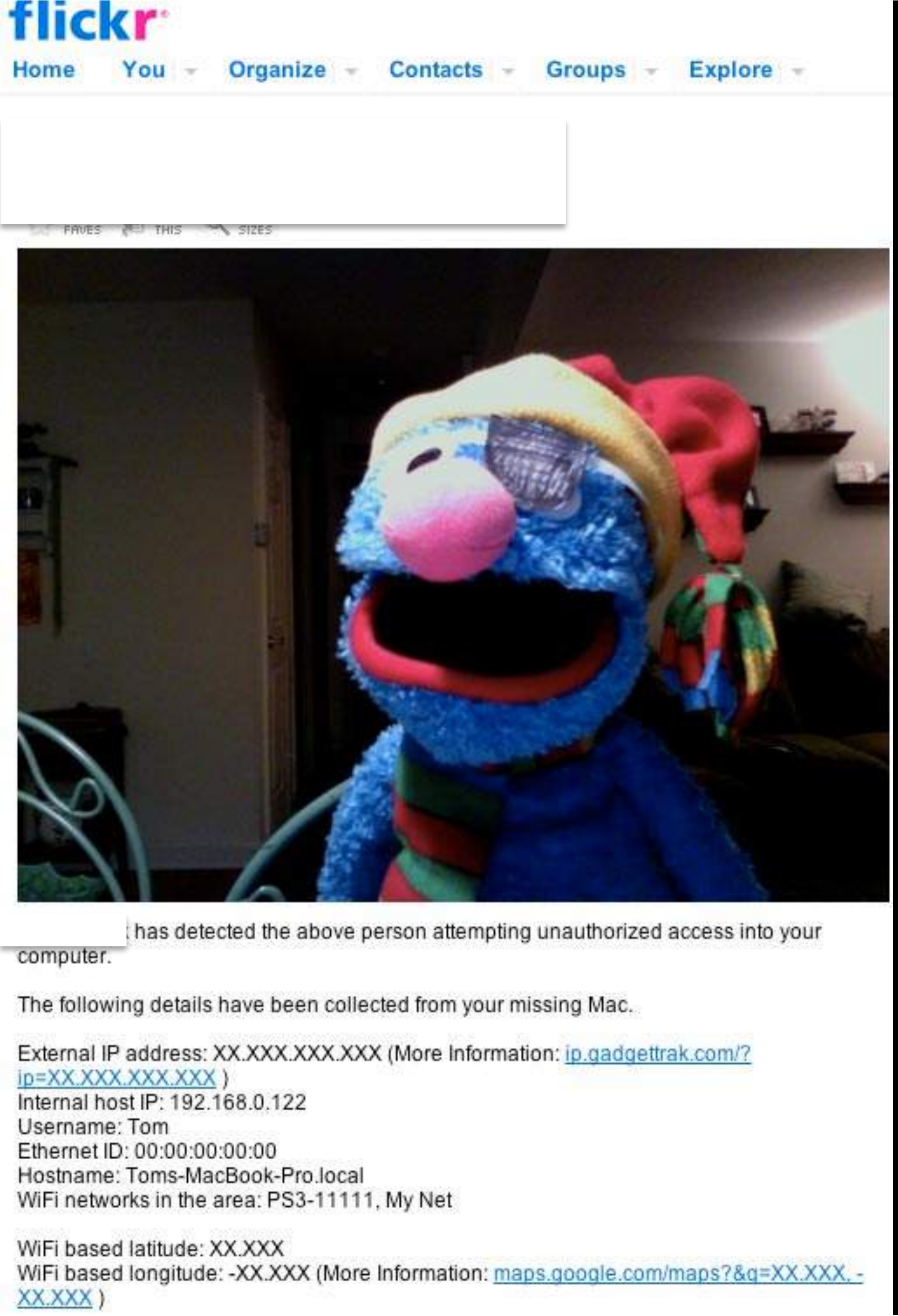
USERNAME

SOCIAL ACCOUNT 1

IP ADDRESS

FRIEND CONNECTION

LICENSE PLATE #



[redacted]

[redacted] has detected the above person attempting unauthorized access into your computer.

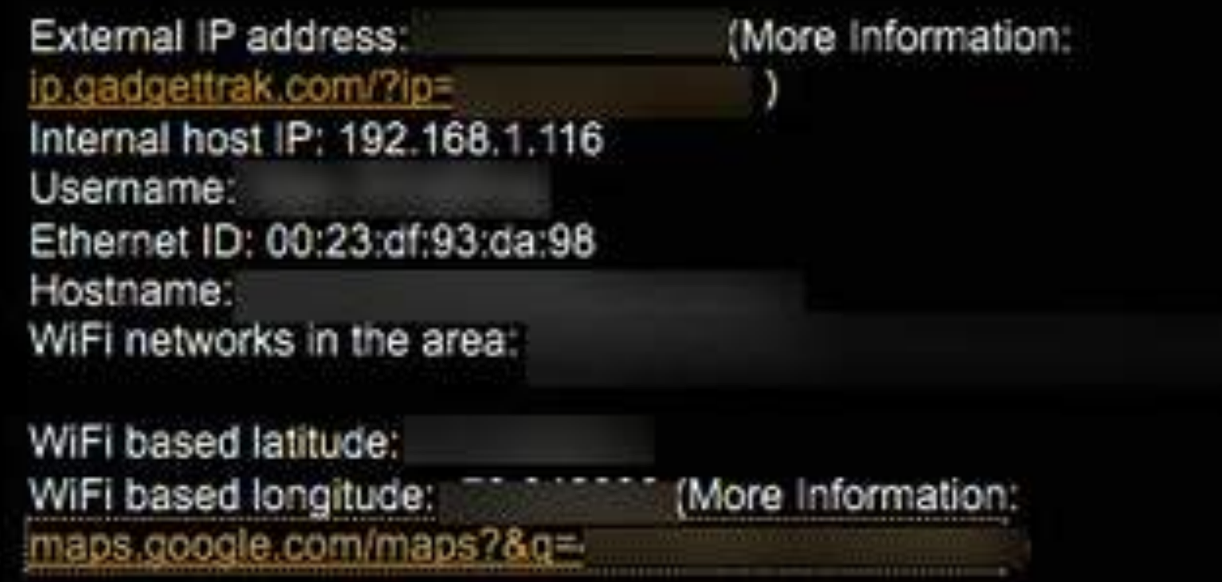
The following details have been collected from your missing Mac.

External IP address: XX.XXX.XXX.XXX (More Information: ip.gadgettrak.com/?ip=XX.XXX.XXX.XXX)
Internal host IP: 192.168.0.122
Username: Tom
Ethernet ID: 00:00:00:00:00
Hostname: Toms-MacBook-Pro.local
WiFi networks in the area: PS3-11111, My Net

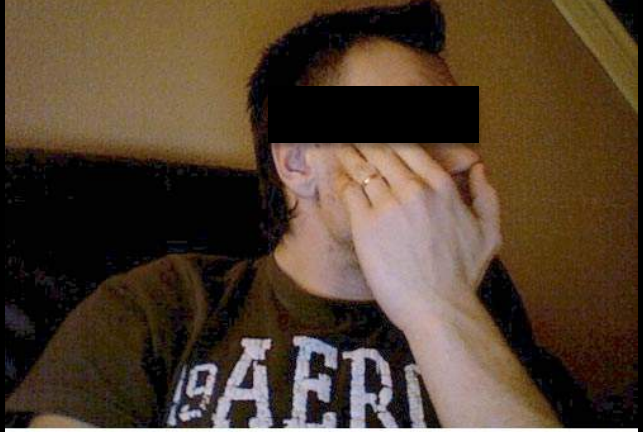
WiFi based latitude: XX.XXX
WiFi based longitude: -XX.XXX (More Information: maps.google.com/maps?&q=XX.XXX,-XX.XXX)

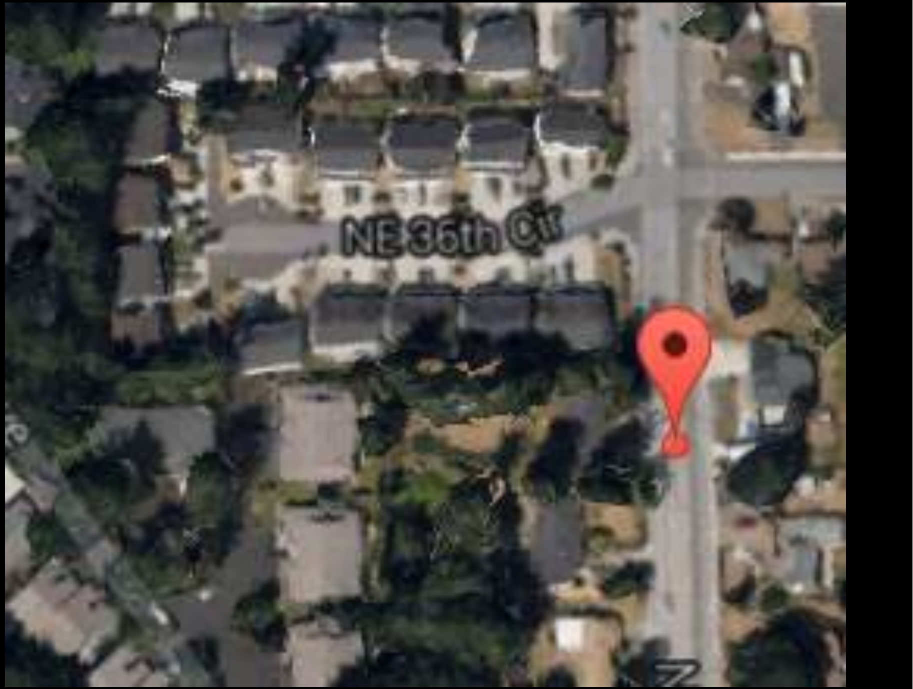
First Blood:

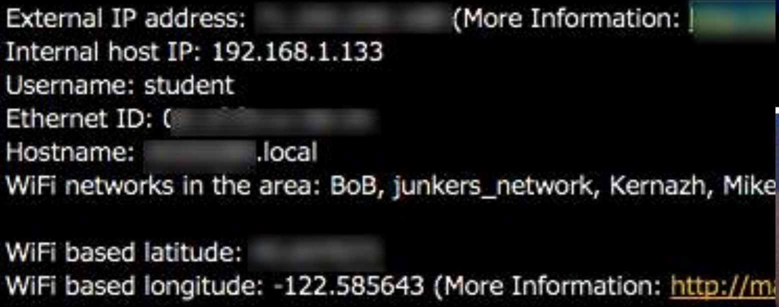
First Recovery of Laptop Using Wi-Fi Geolocation + Camera



```
External IP address: [redacted] (More Information:
ip.gadgettrak.com/?ip=[redacted] )
Internal host IP: 192.168.1.116
Username: [redacted]
Ethernet ID: 00:23:df:93:da:98
Hostname: [redacted]
WiFi networks in the area: [redacted]

WiFi based latitude: [redacted]
WiFi based longitude: [redacted] (More Information:
maps.google.com/maps?&q=[redacted]
```



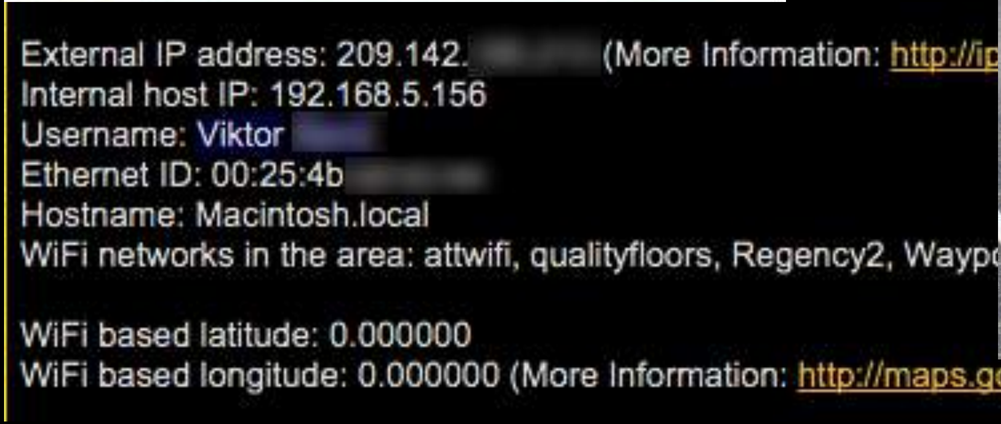




External IP address: [redacted] (More Information: [redacted]
Internal host IP: 192.168.1.133
Username: student
Ethernet ID: ([redacted]
Hostname: [redacted].local
WiFi networks in the area: BoB, junkers_network, Kernazh, Mike

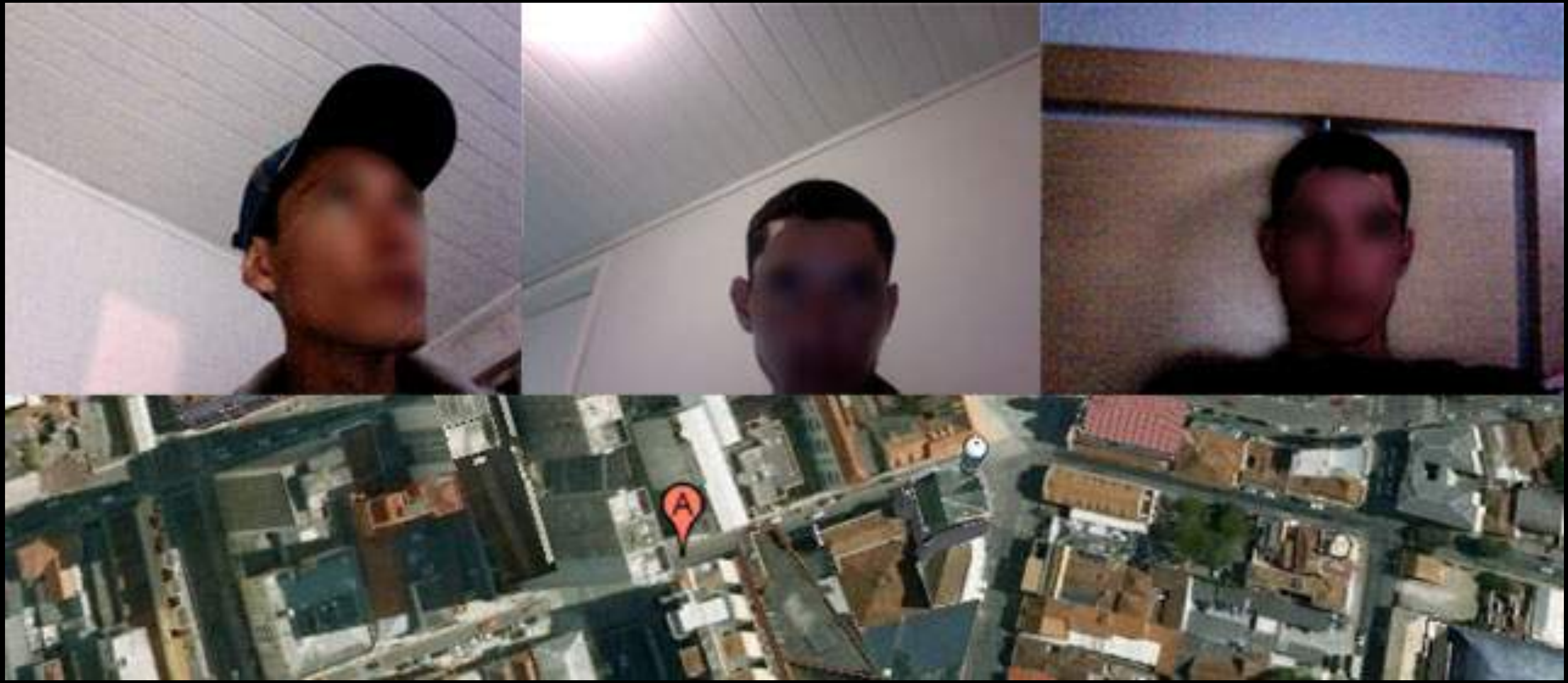
WiFi based latitude: [redacted]
WiFi based longitude: -122.585643 (More Information: http://m

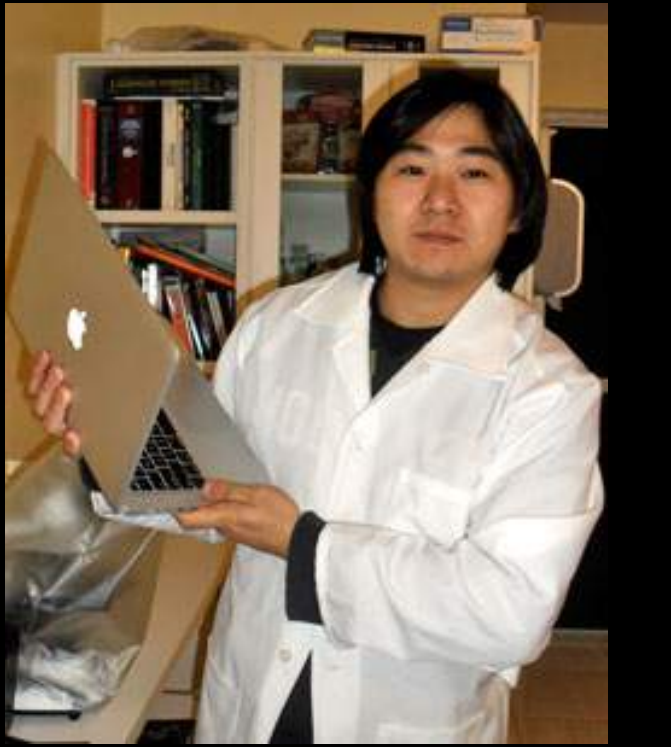
Tracking Viktor



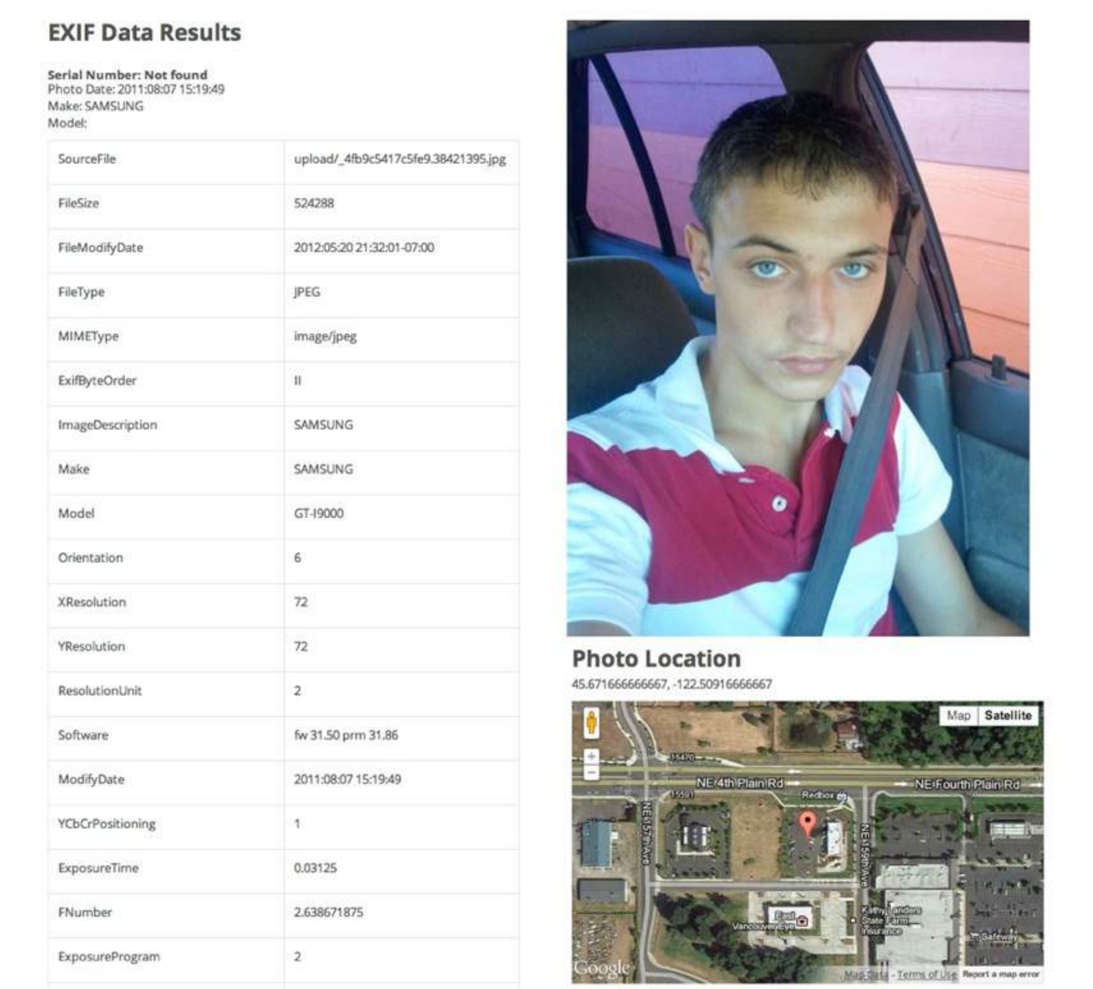
```
External IP address: 209.142.[redacted] (More Information: http://ip
Internal host IP: 192.168.5.156
Username: Viktor [redacted]
Ethernet ID: 00:25:4b[redacted]
Hostname: Macintosh.local
WiFi networks in the area: attwifi, qualityfloors, Regency2, Waypo

WiFi based latitude: 0.000000
WiFi based longitude: 0.000000 (More Information: http://maps.google.com/maps?&q=0.000000,0.000000 )
```

Carjacking In Brazil





Unit 8
Investigates
68°
6:08
8
KGW HD



EXIF Data Results

Serial Number: Not found
Photo Date: 2011:08:07 15:19:49
Make: SAMSUNG
Model:

SourceFile	upload/_4fb9c5417c5fe9.38421395.jpg
FileSize	524288
FileModifyDate	2012:05:20 21:32:01-07:00
FileType	JPEG
MIMEType	image/jpeg
ExifByteOrder	II
ImageDescription	SAMSUNG
Make	SAMSUNG
Model	GT-I9000
Orientation	6
XResolution	72
YResolution	72
ResolutionUnit	2
Software	fw 31.50 prm 31.86
ModifyDate	2011:08:07 15:19:49
YCbCrPositioning	1
ExposureTime	0.03125
FNumber	2.638671875
ExposureProgram	2

Photo Location

45.671666666667, -122.50916666667

(exifscan.com)

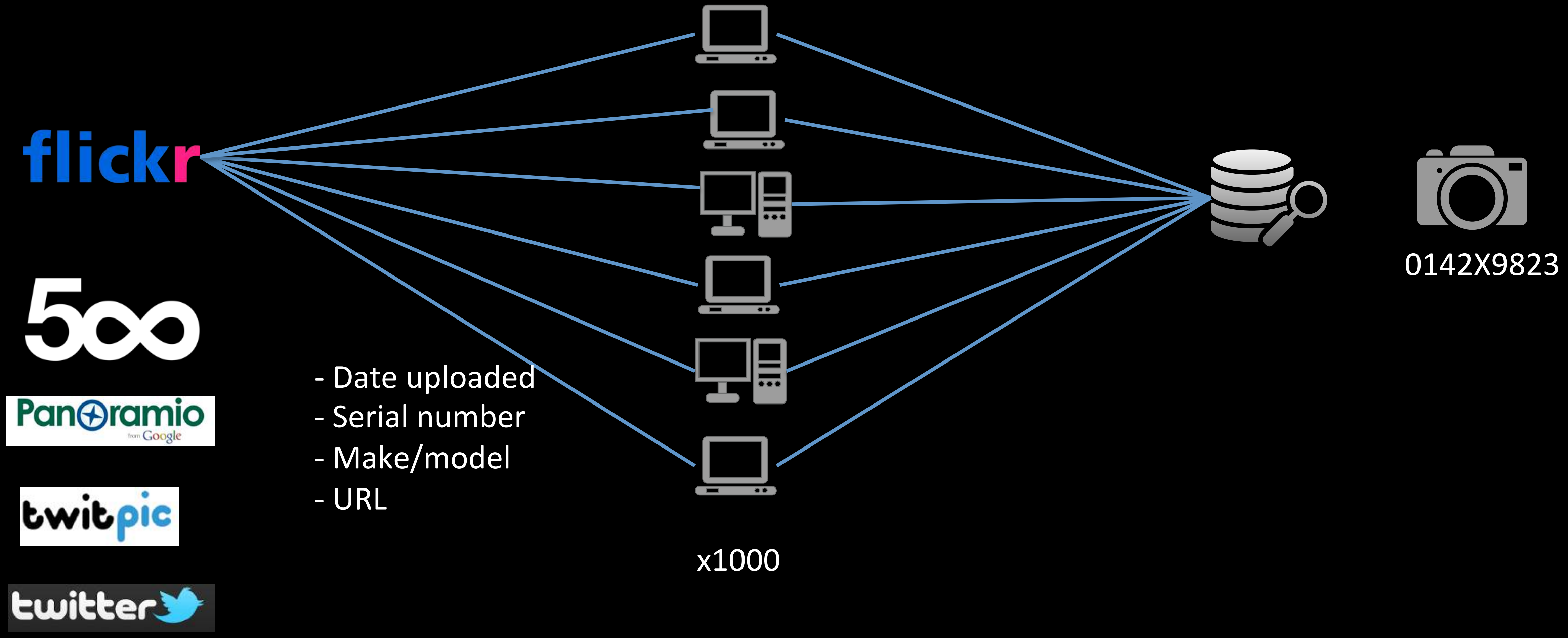
EXIF Metadata

- Meta data in images, video and audio
- Cell phone cameras embed GPS coordinates
- Timestamp
- **High end digital cameras:** make, model and serial number
- EXIF Tool http://www.sno.phy.queensu.ca/~phil/exiftool/

Nude Photos – Phone Hacked…Nope?

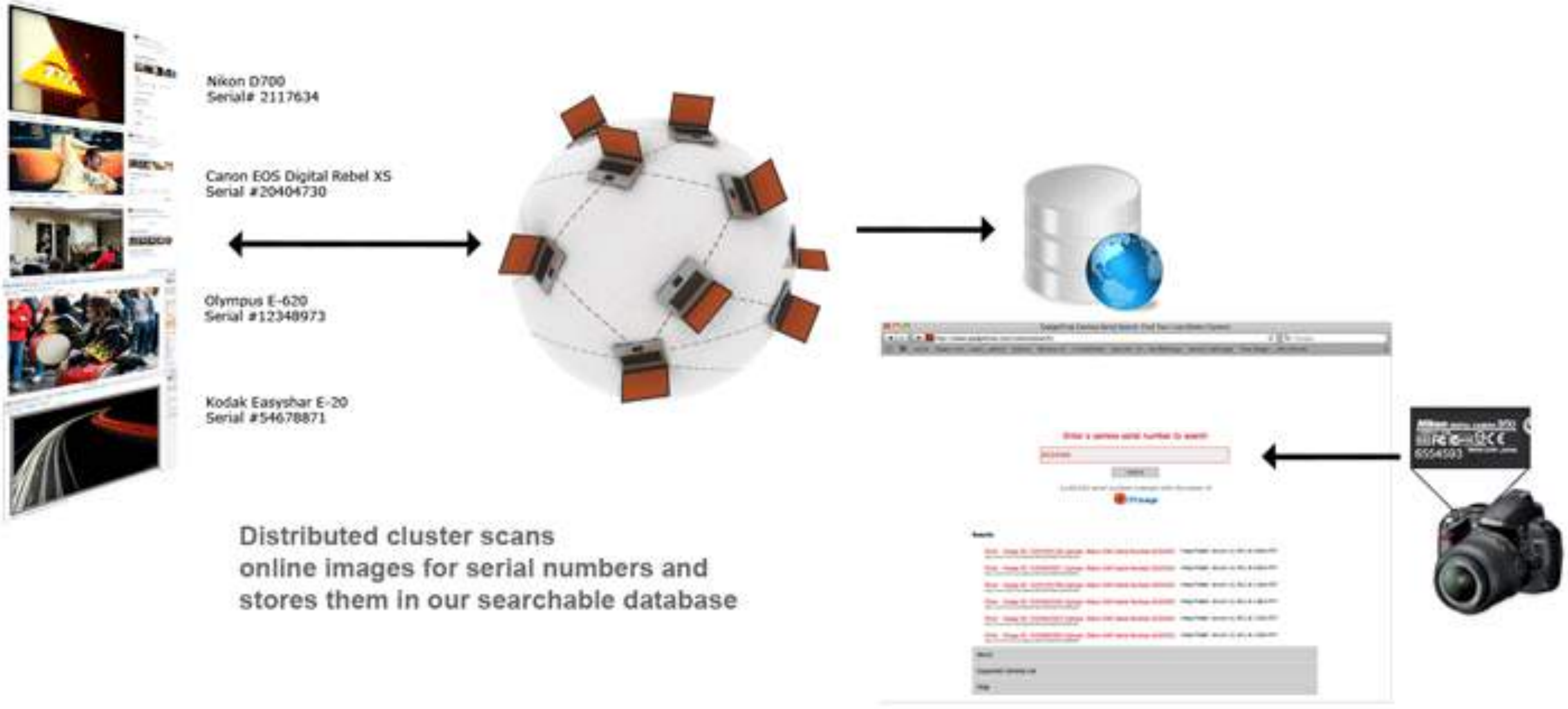
- Media claims "Phone Hacked!"
- EXIF data reveals, multiple phones, over the course of years
- Point of compromise – email
- Chris Chaney – guessed passwords now serving 10 years in jail

EXIF Data Mining



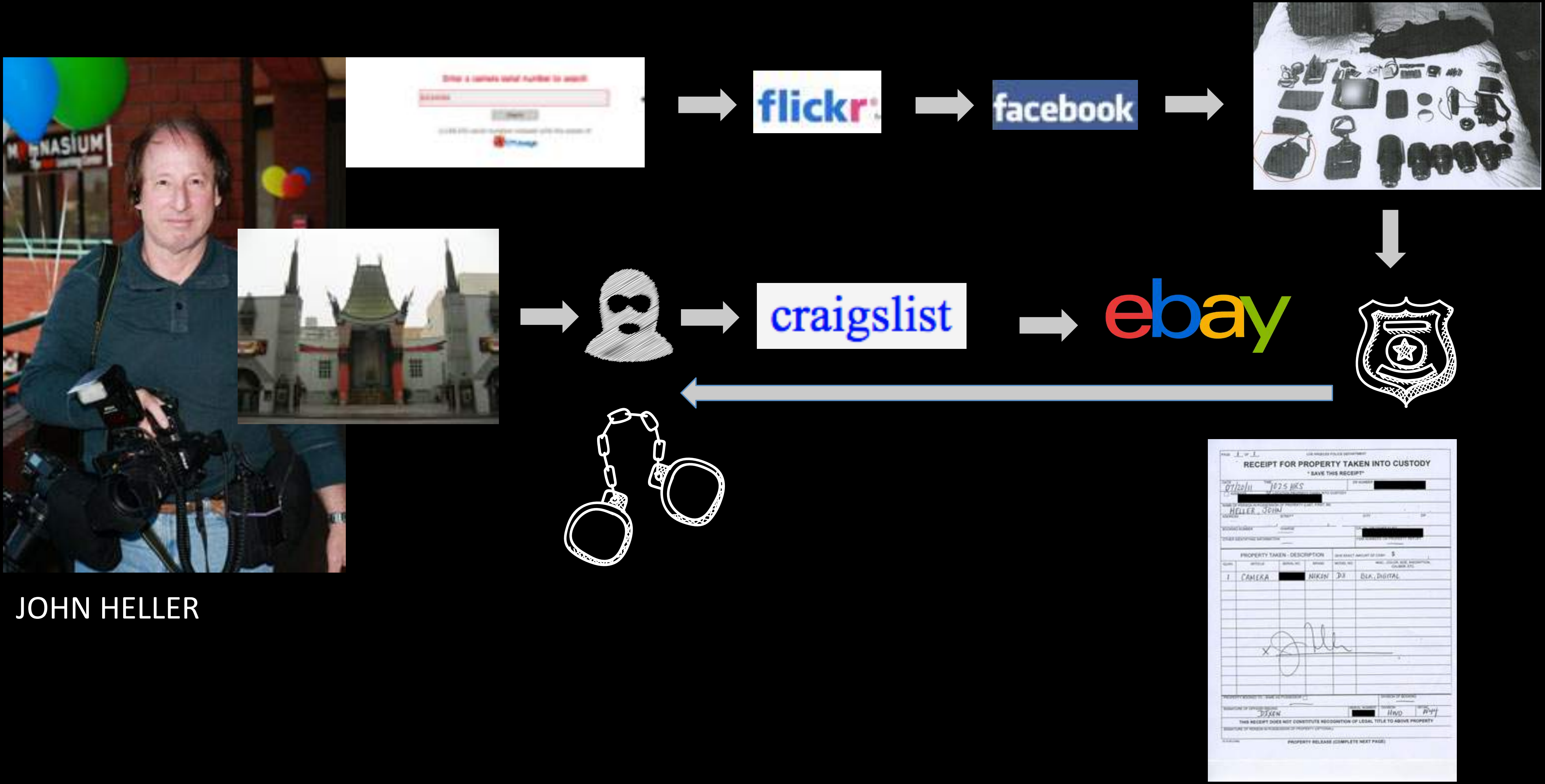
- Date uploaded
- Serial number
- Make/model
- URL

Creating an EXIF Search Engine



Distributed cluster scans
online images for serial numbers and
stores them in our searchable database

Stolen Camera Finder



JOHN HELLER

PAGE 1 OF 1

LOS ANGELES POLICE DEPARTMENT

RECEIPT FOR PROPERTY TAKEN INTO CUSTODY

* SAVE THIS RECEIPT*

07/20/11 1025 HRS [redacted]

[redacted]

HELLER, JOHN

[redacted]

PROPERTY TAKEN - DESCRIPTION $

1	CAMERA	[redacted]	NIKON	D3	BLK, DIGITAL

X

DIXEN [redacted] HWD

THIS RECEIPT DOES NOT CONSTITUTE RECOGNITION OF LEGAL TITLE TO ABOVE PROPERTY

PROPERTY RELEASE (COMPLETE NEXT PAGE)

STOLEN CAMERA HUNTING + SOCIAL STALKING

craigslist

GEOLOCATION
+
TIMESTAMP

onths)

Privacy Tips for App Developers

- Best way to secure your customer's data is not to collect or store it
- If you deal with images strip EXIF and other identifying data out
- If you store data, encrypt as much data so that not even you can access it