

Every Contact Leaves a Trace.

BSides Dublin 2023

Ken Westin

`kwestin@gmail.com`

`/in/kwestin`

`infosec.exchange/@kwestin`

`cybersecurity.io`

Target: Ken Westin

Home Location: Newport, Oregon, USA

Hobbies: Guitar, Records, BJJ, Shitposting

Employer: Panther, San Francisco

Cybereason, Elastic, Splunk, Tripwire, GadgetTrak

Career: 15 Years Cybersecurity

Current Location: BSides Dublin

Contact Info

kwestin@gmail.com

infosec.exchange/@kwestin

Cybersecurity.io

linkedin.com/in/kwestin



CASE CLOSED



April 2012
Virginia



March 2012
Virginia



February 2012
Miami, FL



February 2012
Gump's Papa, OR



January 2012
New York, NY



January 2012
Cocoa Bay, FL



November 2009
Missouri
Tracked stolen laptop



September 2009
Oakland, California
Stolen laptops



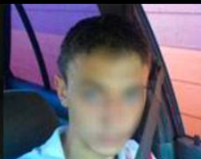
November 2011
Boulder, CO



October 2011
Olympia, WA



August 2011
Los Angeles, CA



August 2011
Portland, OR



July 2011
Cantile, Brazil



June 2011
Portland, Oregon



August 2009
Schenectady, New York



June 2009
Edmond, Oklahoma



May 2011
Richmond, California
Banned Michael



February 2011
Portland, Oregon
Stolen MacBook Pro



January 2011
Napa, California



February 2010
Portland, Oregon



January 2010
Springfield, Oregon



November 2009
Portland, Oregon



February 2009
Dallas, Texas



November 2008
Buckeye, Arizona

BBC

NEWS

'I'm a professional cyberstalker'

© 10 August 2015 • Comments



KEN WESTIN

Ken Westin uses advanced techniques to track down suspected thieves

By Dave Lee >

North America technology reporter

"Stupidity is the best vulnerability. That and greed."

Ken Westin openly, and enthusiastically, calls himself a professional cyberstalker. And foolish people are his target.

He uses some of the tools that are popular with the web's creepiest patrons, hacks used to spy on webcams.

But if you're wondering why he's so proud of it, it's because he believes that



MOTHERBOARD
TECH BY VICE

Meet the Real-Life Mr. Robot

Confessions of a professional cyber stalker.



By J.M. Porup

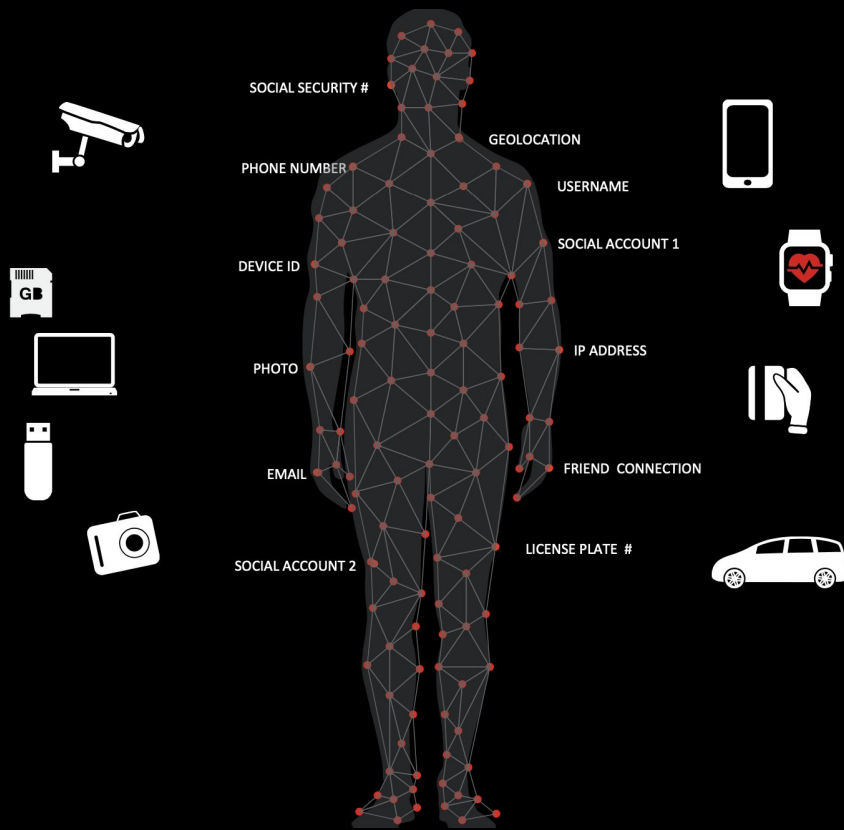
October 20, 2015, 7:04am [Share](#) [Tweet](#) [Snap](#)





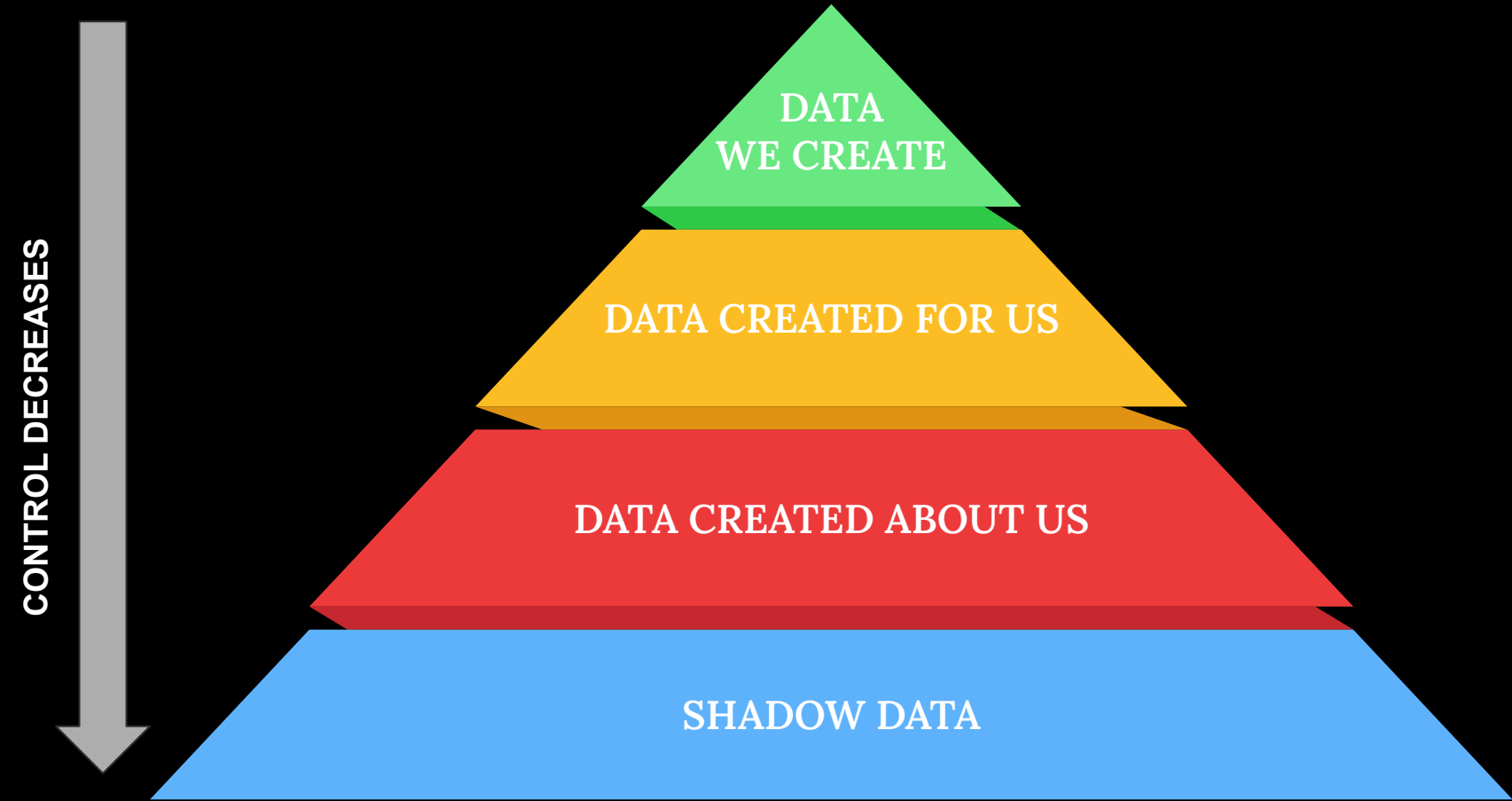
EVERY CONTACT LEAVES A TRACE.

The Quantified Self-Pwn





Hierarchy of Data Bleed



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

Happy Little Spyware

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](#)

MP3 Players

Apple

Archos

Cowon



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

Zumo 550, Street pilot C550, c580

Go 910, one, Go 510 iWay 500C

Cell Phones

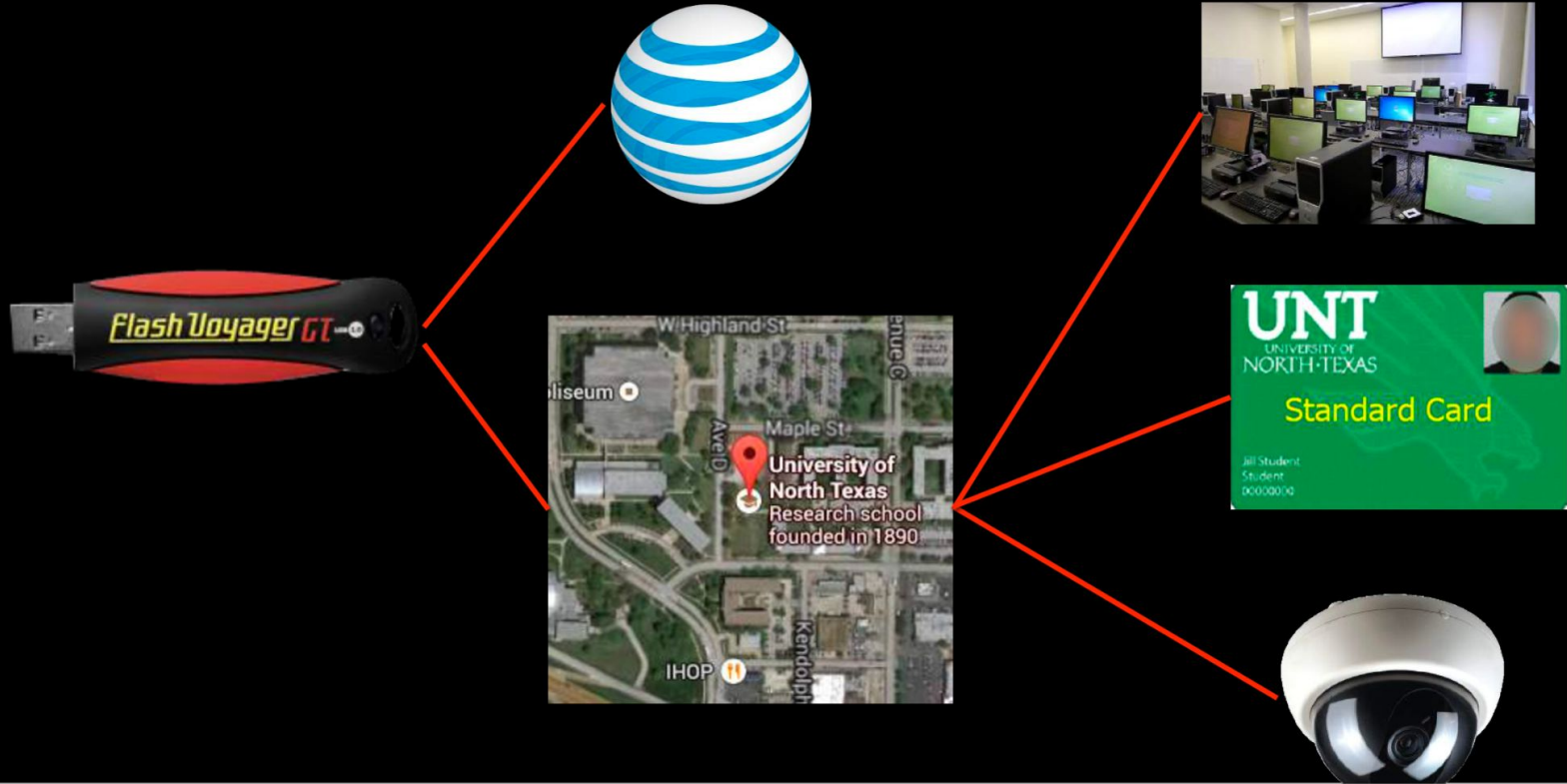
Sony Ericsson	Nokia	Helio
K 550, K750i, K800i, W200a, W600i, W810, W880, W950, M600, P990	5300, 6070, 7610, N73, N7-, N80	Ocean, Fin, Drift

Other Devices

Sony Playstation Portable (PSP)
PalmOne Lifestrive
LaCie External USB hard drives

Expanding Investigative Scope

2009-02-21 23:43:49



Commercial Trojan



FLIR ThermaTrak™

If your IR camera is lost or stolen, ThermaTrak™ can track where it is and who has it.



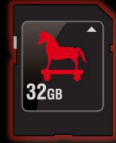
- Custom tracking system for lost, stolen or missing IR Cameras
- Notification by email when stolen IR camera "found"
- ThermaTrak™ is embedded by FLIR's Service Department in the camera's firmware
- Ideal for asset management of multiple IR cameras
- Proven software solution for mobile equipment
- Aid to law enforcement in finding camera and prosecuting theft
- Available as an annual subscription or **Included FREE with an Extended Warranty**
- Exclusive, patented technology from FLIR and powered by GadgetTrak

The First Theft Tracking System for IR Cameras!

Remote activation triggers theft detection — Owners who fall victim to

ThermaTrak in action — The software must be installed on your camera and

One-time activation required at Service Center — In order to activate



Further Down the Rabbit Hole: Tracking Laptops



Building a Better Laptop Trap



flickr®
Home You Organize Contacts Groups Explore

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)

The screenshot shows a Flickr page with a navigation bar at the top. Below the navigation bar is a search bar. The main content area features a photograph of a blue Muppet character wearing a yellow and red hat and a colorful scarf. Below the photo is a security alert message in a white box with a grey border. The message states that an unauthorized access attempt was detected and lists various system details collected from the 'missing Mac', including IP addresses, username, Ethernet ID, hostname, WiFi networks, and location data.

First Laptop Recovery Using Wi-Fi Positioning+ Camera



External IP address: [REDACTED] (More Information: [ip.gadgettrak.com/?ip=\[REDACTED\]](http://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]

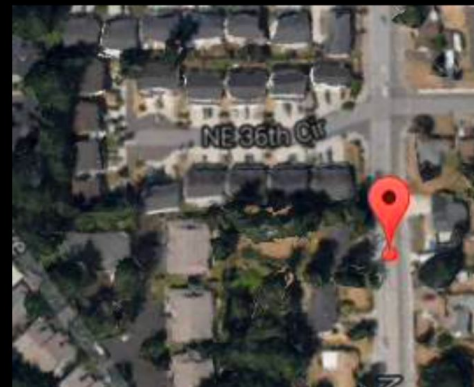
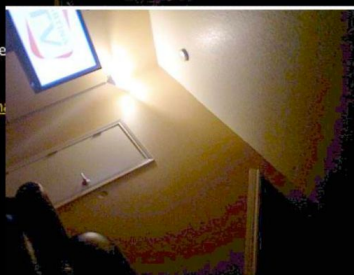
WiFi based latitude: [REDACTED]

WiFi based longitude: [REDACTED] (More Information: [maps.google.com/maps?&q=\[REDACTED\]](http://maps.google.com/maps?&q=[REDACTED]))

Thieves Targeting Portland Schools Unveil Organized Crime Group



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>)



<https://www.youtube.com/watch?v=Fyej2D1ofNI>

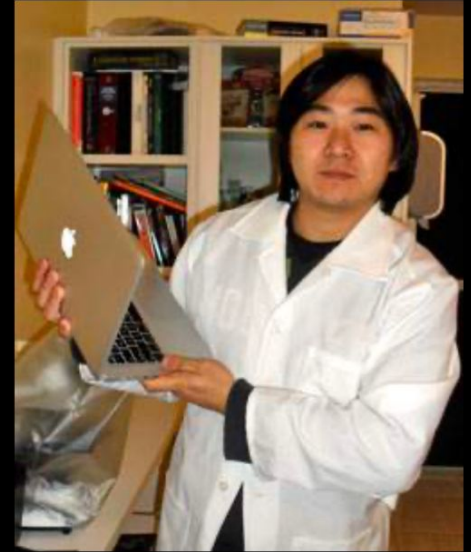
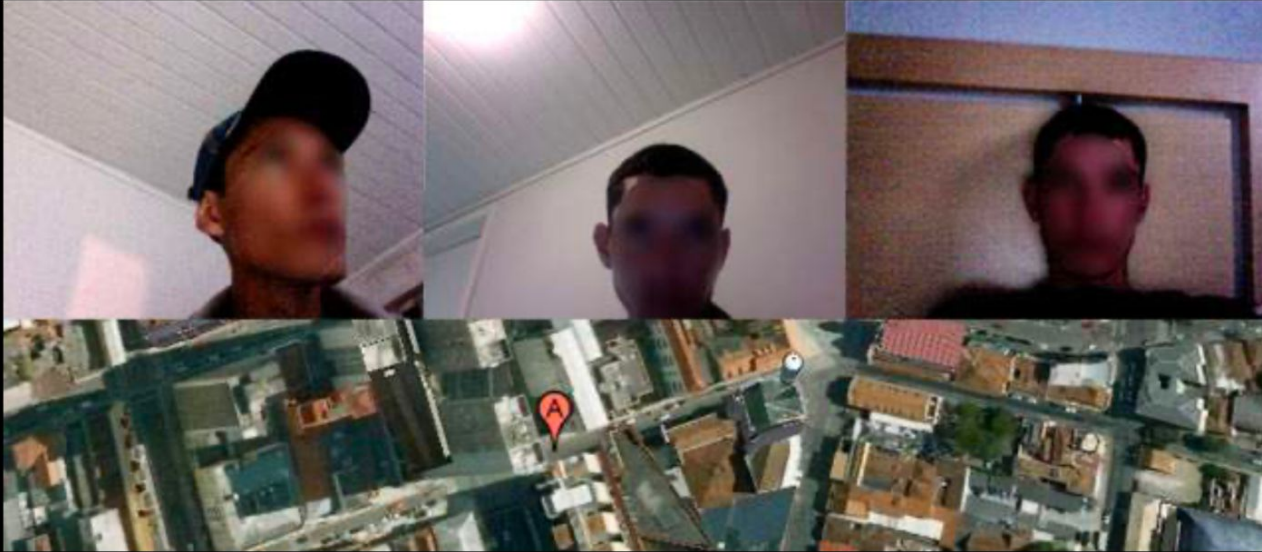
More Organized Crime & Expanding to OSINT



External IP address: 209.142. (More Information: <http://ip>)
Internal host IP: 192.168.5.156
Username: Viktor
Ethernet ID: 00:25:4b
Hostname: Macintosh.local
WiFi networks in the area: attwifi, qualityfloors, Regency2, Wayp
WiFi based latitude: 0.000000
WiFi based longitude: 0.000000 (More Information: <http://maps.google.com/maps?&q=0.000000,0.000000>)



International Tracking: Brazil Carjacking & Assault



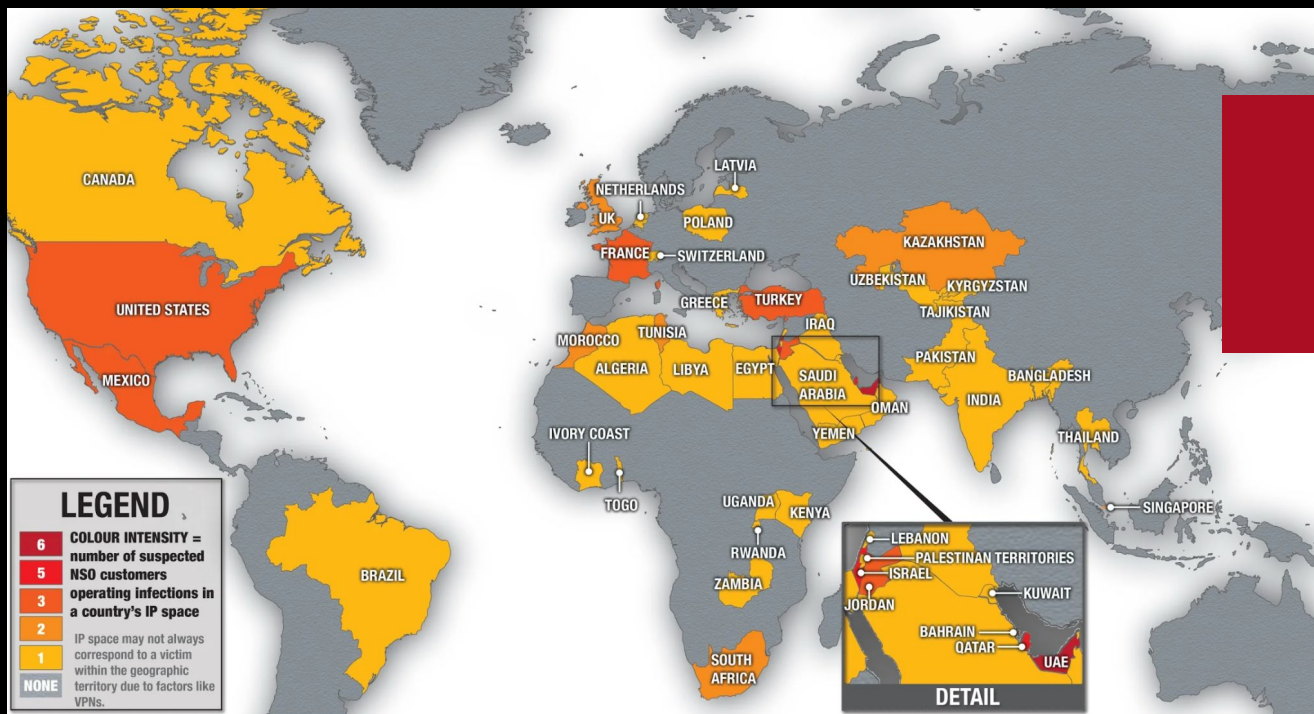
Smartphone Tracking



Fun with Smartphone Thieves



Commercial Mobile Spyware



Further Down the Rabbit Hole: EXIF Data

EXIF Data Results

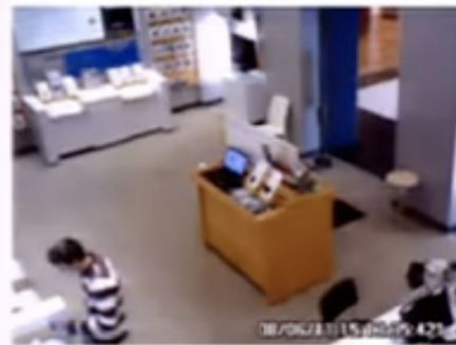
Serial Number: Not found
Photo Date: 2011:08:07 15:19:49
Make: SAMSUNG
Model:

SourceFile	upload/_4b9c5417c5fe9.38421395.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

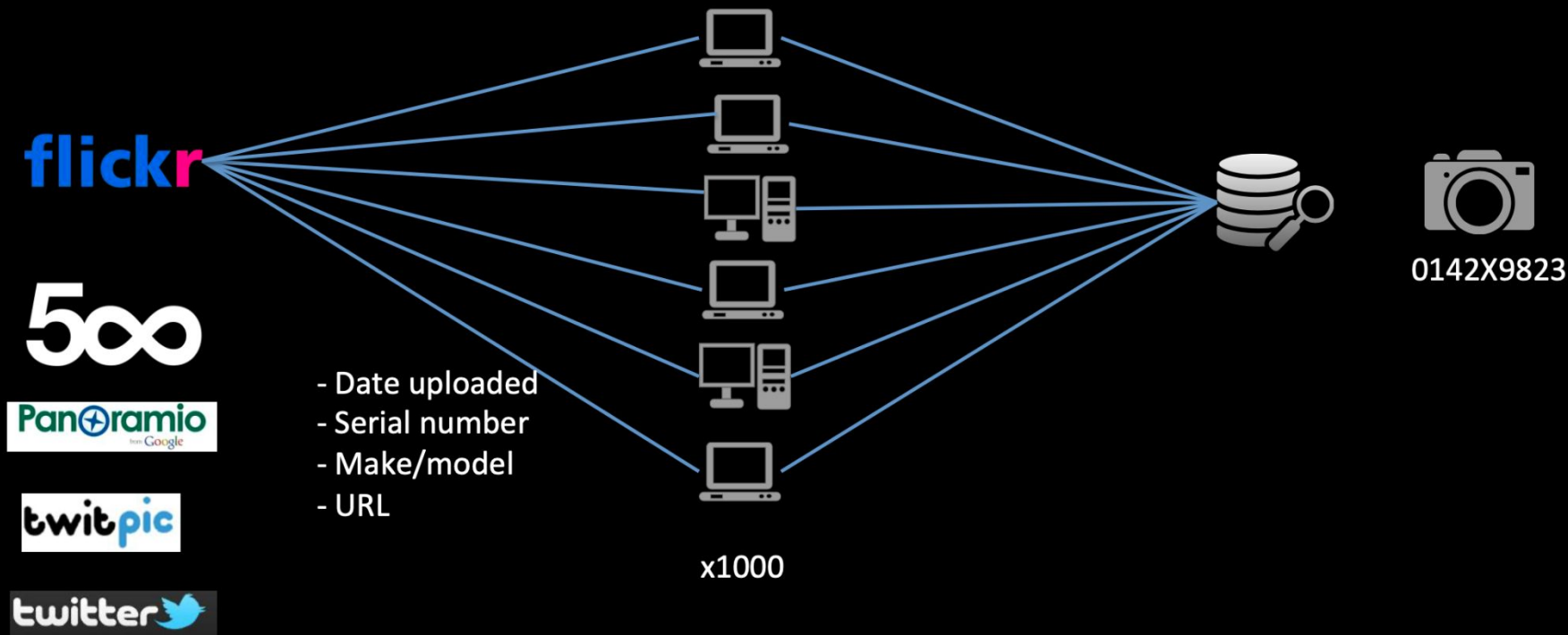


Photo Location

45.671666666667, -122.50916666667



EXIF Mining with a Legal Botnet



Holy Sh*t It Worked!

\$9K Camera Gear Recovered 1 Year After Being Stolen



Camera Model	Serial	ImgTrak Label Code
Canon EOS 350D	1130656725	GT205861

450 Photos Found

1. Camera: Canon EOS 350D Digital, Serial #1130656725
Image Taken: May 16, 2011 at 8:05pm BST
Link: <http://www.flickr.com/photos/6215885648N00/5732886655>
2. Camera: Canon EOS 350D Digital, Serial #1130656725
Image Taken: May 16, 2011 at 8:04pm BST
Link: <http://www.flickr.com/photos/6215885648N00/5732837772>
3. Camera: Canon EOS 350D Digital, Serial #1130656725
Image Taken: June 23, 2010 at 13:39am BST

flickr

facebook



craigslist

ebay

Form: RECEIPT FOR PROPERTY TAKEN INTO CUSTODY
"SAVE THIS RECEIPT"

PROPERTY TAKEN: CAMERA, SERIAL: 1130656725, MAKE: CANON, MODEL: EOS 350D, TYPE: DIGITAL

Signature: [Handwritten Signature]

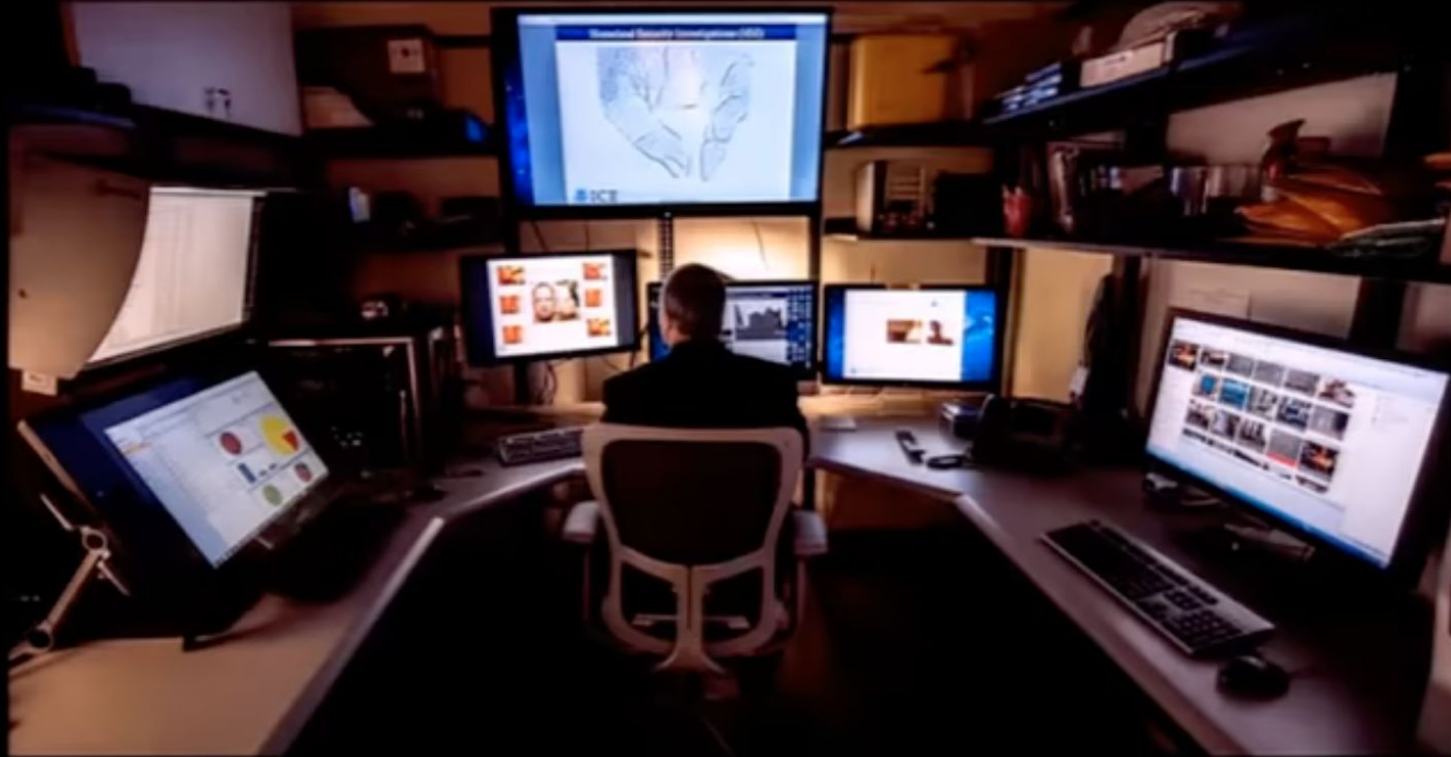
PROPERTY RELEASE COMPLETE NEXT PAGE

EXIF + OSINT

craigslist



ICE HSI Cyber Crimes Center (C3) Child Exploitation Investigations Unit



IoT Provides New Telemetry — and Targets



ISP Emails Indexed by Google

El **Economista** solicitó a **Ken Westin**, experto en seguridad cibernética. Westin, tras realizar su propia pesquiza, llegó a las siguientes conclusiones:

El hueco en la seguridad involucraba un error en una aplicación y una desconfiguración del servidor.



De acuerdo con Westin, no hay manera de saber cuánto tiempo se tardó en descubrir el hueco.

← → ↻ 📄 webmail2.prodigy.net.mx/cgi-bin/wapmail?ID=IMC4L0SxN&msgt

Prodigy mail

Buzón

Eliminar

Más

[Más Mis archivos Ignacio, confirma tu cuenta de Facebook Más...](#)

[webmail2.prodigy.net.mx/cgi-bin/wapmail?ID=IMC4L0SxN&msgt](#)

Feb 17, 2013 - Hola, [redacted] Te uniste a Facebook el 19 de octubre de 2012, pero aún no has confirmado la dirección de correo electrónico asociada a tu ...

[Tu recibo n.º 213049284337 - Prodigy](#)

[webmail2.prodigy.net.mx/cgi-bin/wapmail?ID=IMC4L0SxN&msgt](#)

Mar 25, 2013 - Facturado a: [redacted]@prodigy.net.mx. Ignacio Sánchez-Navarro García Lascurain Fuente de Leones 35. Int. 5. Edo. de México, MEX ...

[Más Mis archivos Your IBC Bank eStatement is Available Más...](#)

[webmail2.prodigy.net.mx/cgi-bin/wapmail?ID=IMC4L0SxN&msgt](#)

Mar 31, 2013 - Dear Customer: Your IBC Bank statement for the account(s) listed below is now available [redacted]2467. To view your statement online please ...

[Más Mis archivos RE: Que el agua corra.... Más Responder Mover...](#)

[webmail2.prodigy.net.mx/cgi-bin/wapmail?ID=IMC4L0SxN&msgt](#)

May 20, 2013 - Sandy Que gusto que todavía se acuerde de mí, le mando un beso y un fuerte abrazo. Siguiente >. Más, Responder, Mover, Responder a ...

[Más Mis archivos Daily Email Prize - Claim Your Mystery Box! Más...](#)

[webmail2.prodigy.net.mx/cgi-bin/wapmail?ID=IMC4L0SxN&msgt](#)

May 20, 2013 - "Great to see you again, tamer! We set aside a special gift for you. Open it up and see what's inside!" - The Sky Shop Cats ...

[Siguiente - Prodigy](#)

[webmail2.prodigy.net.mx/cgi-bin/wapmail?ID=IMC4L0SxN&msgt](#)

10+ items - Correo | Contactos | Calendario | Más. Mis archivos.

Acapulco en familia: ¡2 noches para 4 en hotel 3 Estrellas ¡No te pierdas la ... ¡Siempre seguro! Kit de alarma c/control remoto. ¡Seguridad ...

[Más Mis archivos Señorita! Más Responder Mover Responder a...](#)

[webmail2.prodigy.net.mx/cgi-bin/wapmail?ID=IMC4L0SxN&msgt](#)

De: essy saberi. A: 25/03/13. something different. SEÑORITA. Más, Responder, Mover, Responder a todos, Responder. Configuración | Cerrar sesión. TELMEX ...

[Siguiente - Prodigy](#)

[webmail2.prodigy.net.mx/cgi-bin/wapmail?ID=IMC4L0SxN&msgt](#)

5+ items - Correo | Contactos | Calendario | Más. Mis archivos.

[redacted] 20/04/13 00H20. La apuesta turística [redacted] 20/04/13 00H06. Afinación Diaria de la Concienci

[Siguiente - Prodigy](#)

[webmail2.prodigy.net.mx/cgi-bin/wapmail?ID=IMC4L0SxN&msgt](#)

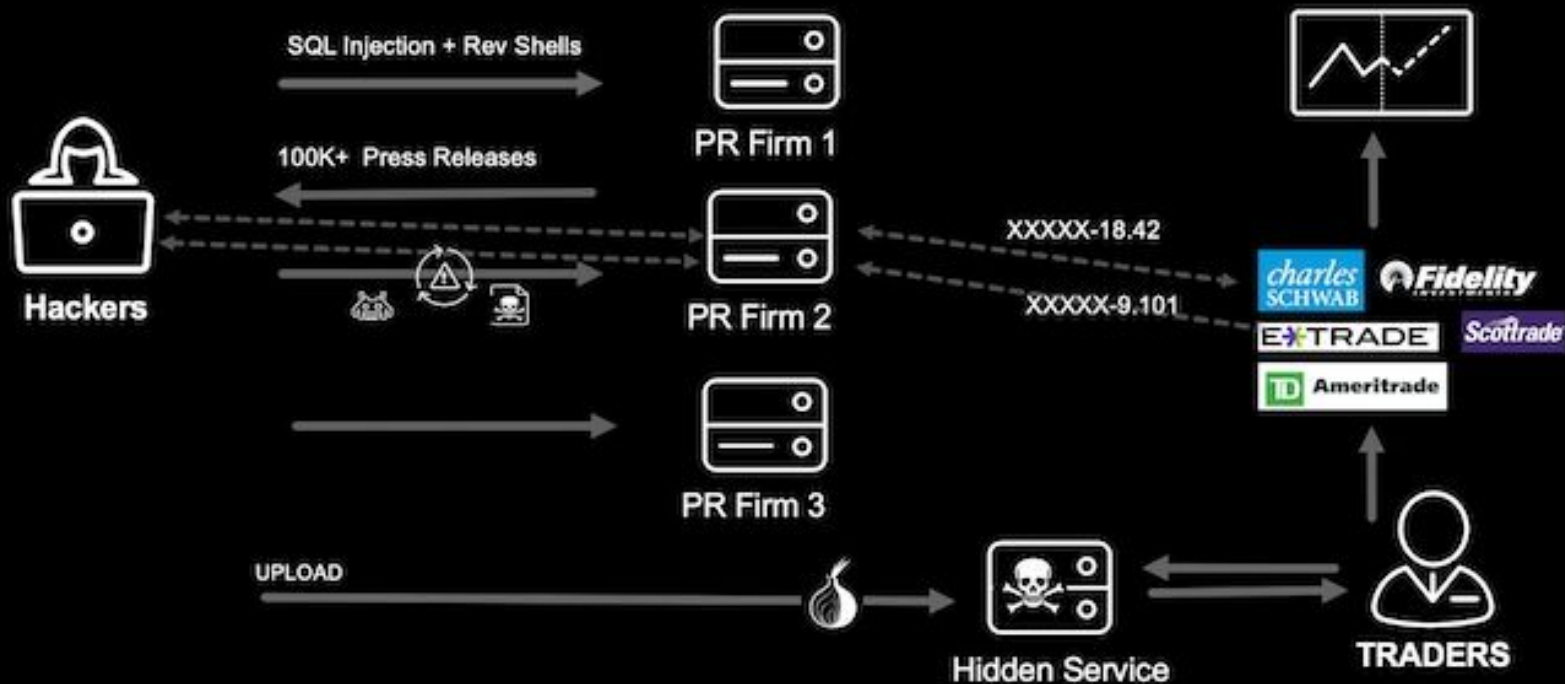
Jun 7, 2013 - tuimagenpersonal.com. Santo Domingo 22. Madrid, Madrid 28013. ES If you no longer wish to receive communication from us: Cancel

[Belleza y realidad...-rsf.pps - Prodigy](#)

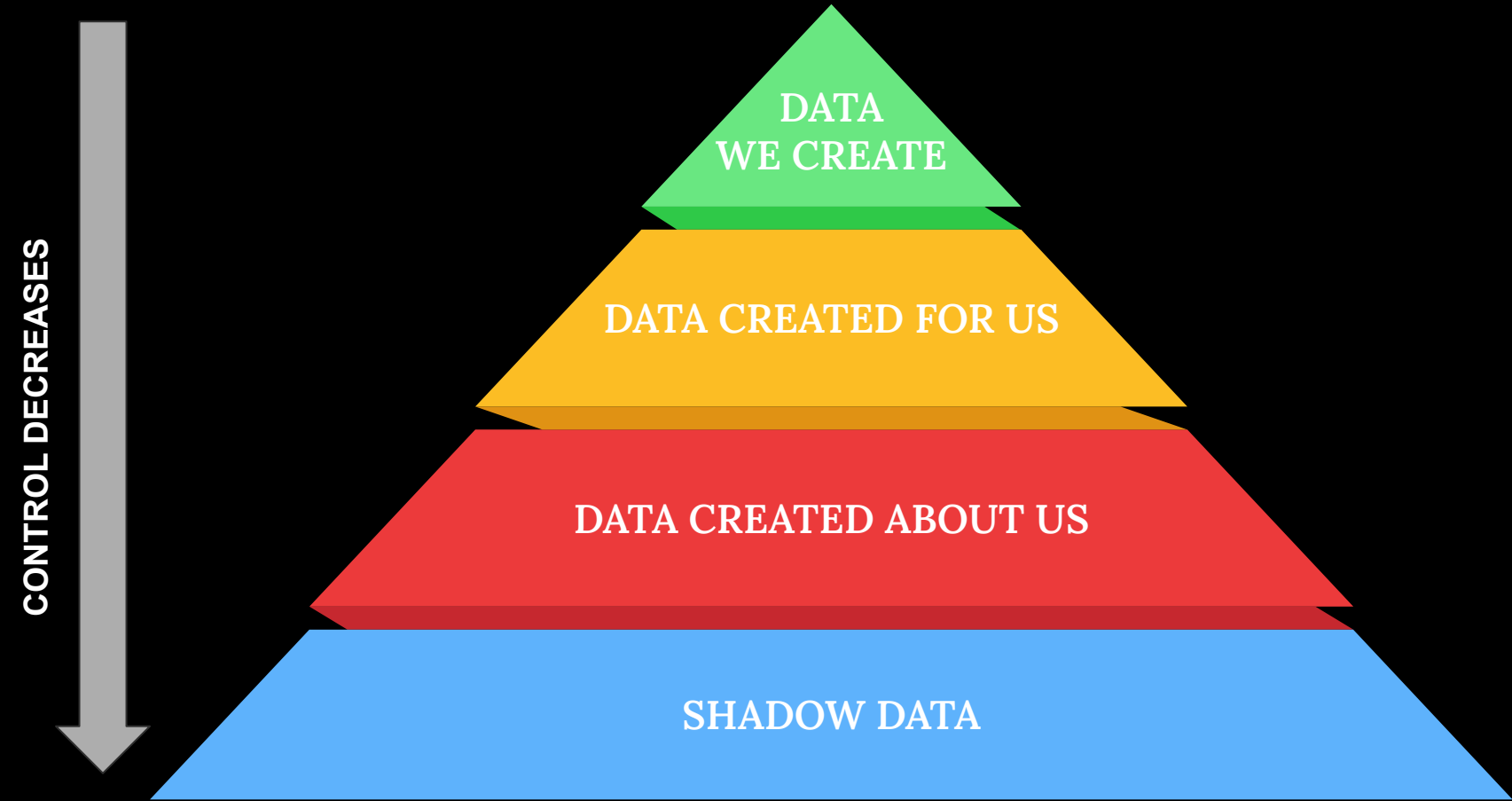
[webmail2.prodigy.net.mx/cgi-bin/wapmail?ID=IMC4L0SxN&msgt](#)

El tiempo de descarga del archivo puede ser largo. Clic en la liga para descargar el archivo. Descargar a PC - Configuración | Cerrar sesión. TELMEX - Nuevas ...

Black Hats & White Collars



Hierarchy of Data Bleed



Thank You!



`kwestin@gmail.com`
`linkedin.com/in/kwestin`
`infosec.exchange/@kwestin`
`cybersecurity.io`