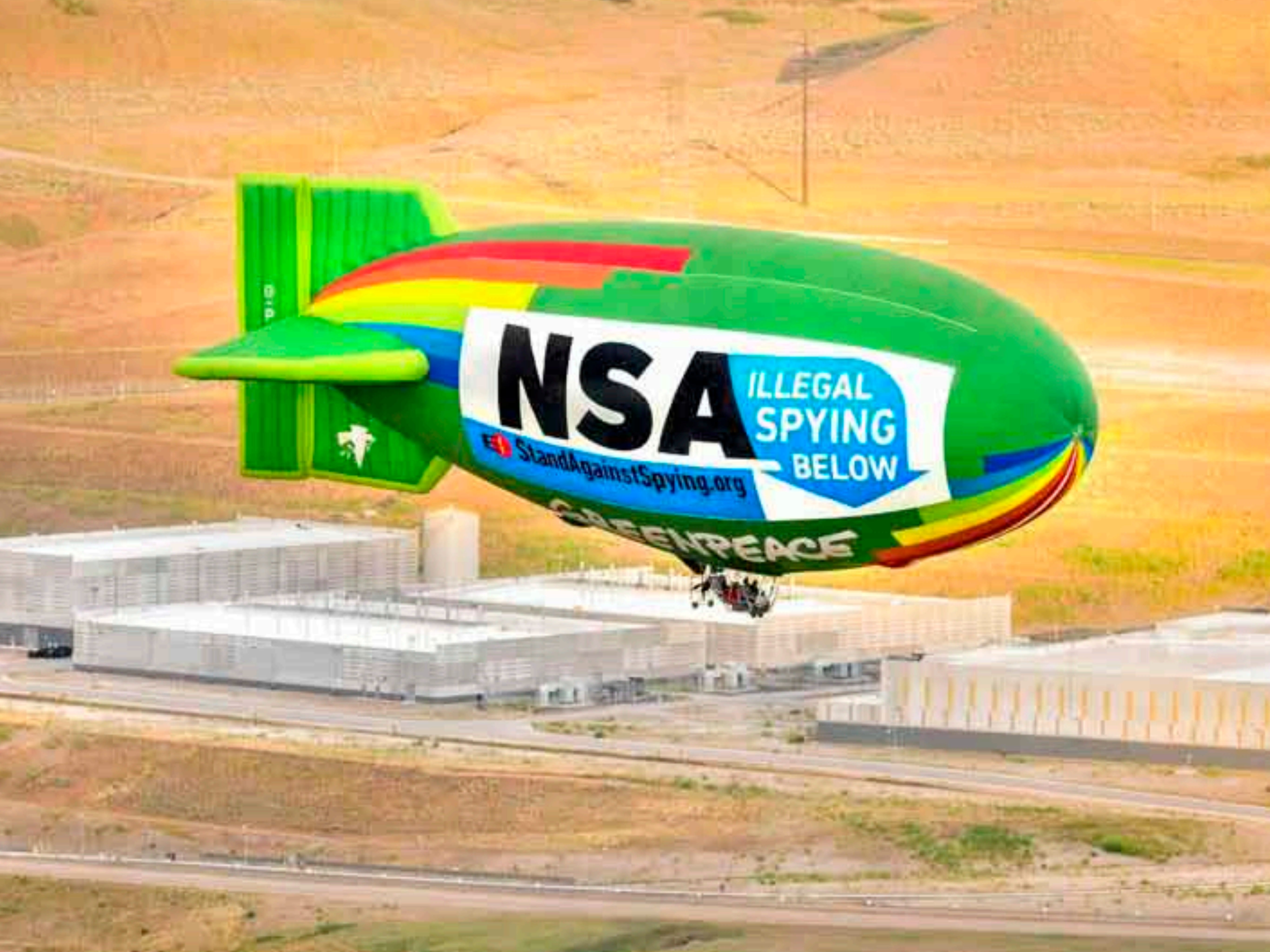
Electronic Opsec: Protect Yourself From Online Tracking And Surveillance

HackCon

The Norwegian cyber security conference

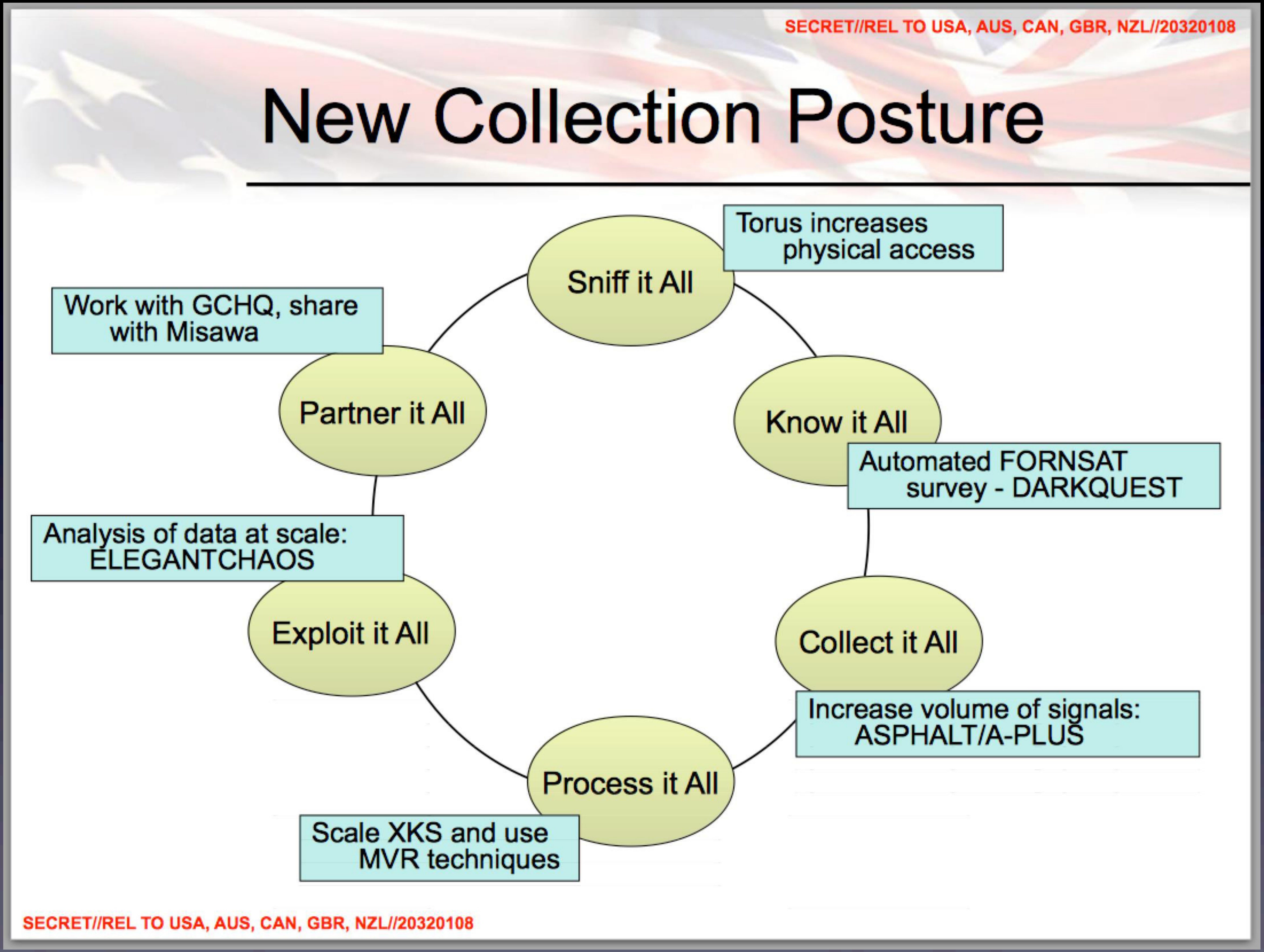
Zoz


NSA
ILLEGAL SPYING BELOW
StandAgainstSpying.org
GREENPEACE

Surveillance is the business model of the internet.
-- Bruce Schneier

When we use Google to find out things on the Web, Google uses our Web searches to find out things about us.
-- Siva Vaidhyanathan

New Collection Posture



Sniff it All

Torus increases physical access

Know it All

Automated FORNSAT survey - DARKQUEST

Collect it All

Increase volume of signals: ASPHALT/A-PLUS

Process it All

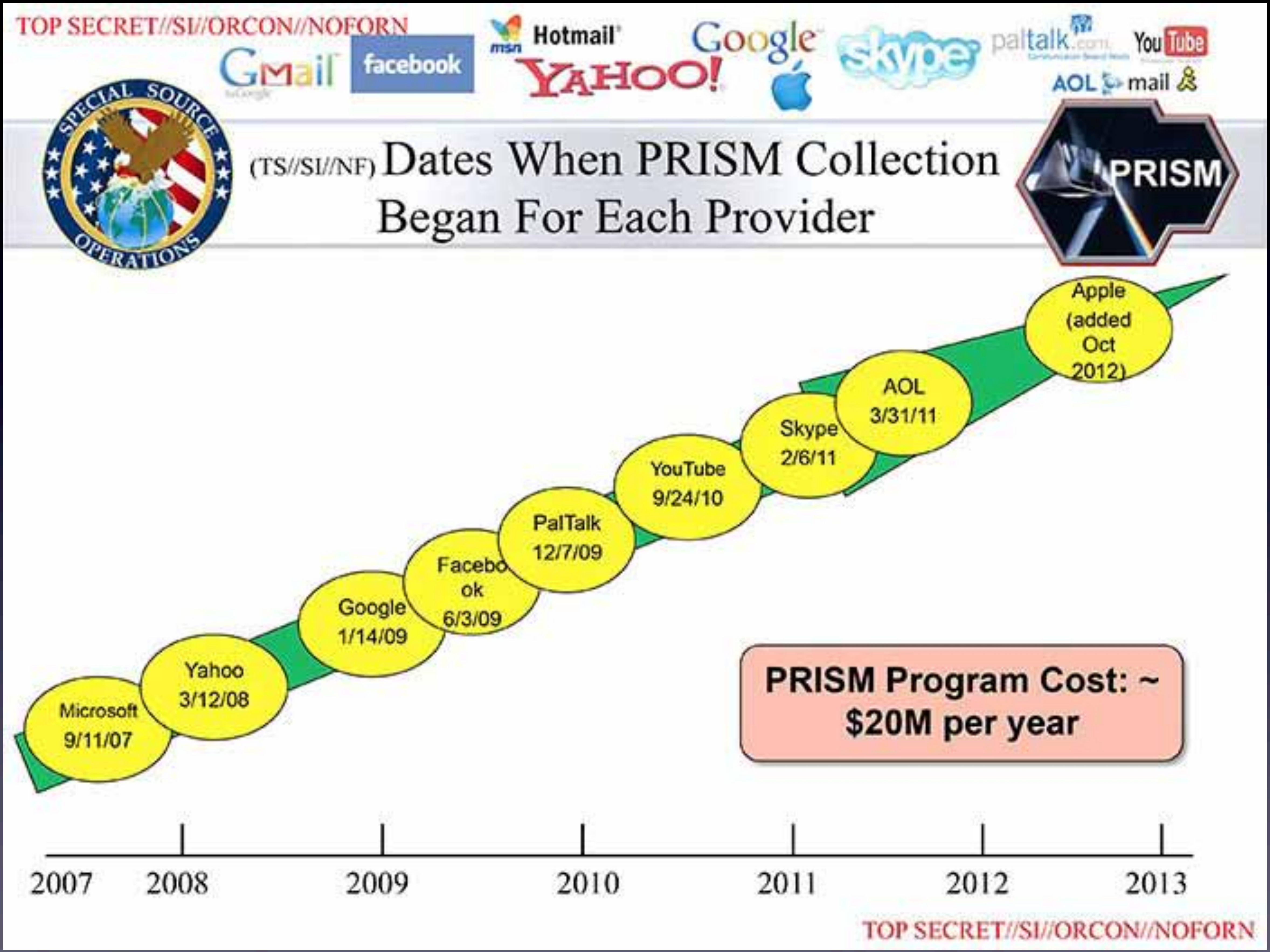
Scale XKS and use MVR techniques

Exploit it All

Analysis of data at scale: ELEGANTCHAOS

Partner it All

Work with GCHQ, share with Misawa


Gmail
facebook
msn
Hotmail
YAHOO!
Google
skype
paltalk.com
YouTube
AOL mail
SPECIAL SOURCE OPERATIONS
PRISM

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider

Microsoft 9/11/07

Yahoo 3/12/08

Google 1/14/09

Facebo ok 6/3/09

PalTalk 12/7/09

YouTube 9/24/10

Skype 2/6/11

AOL 3/31/11

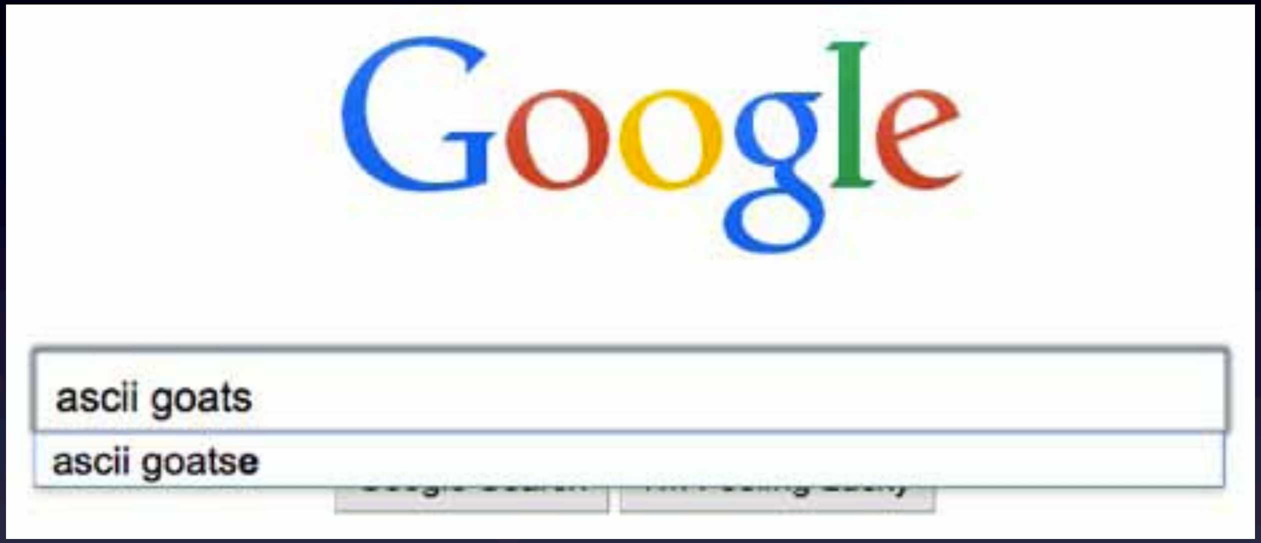
Apple (added Oct 2012)

PRISM Program Cost: ~ $20M per year

2007 2008 2009 2010 2011 2012 2013

TOP SECRET//SI//ORCON//NOFORN

"On the Internet, nobody knows you're a dog."



ascii goats

ascii goatse

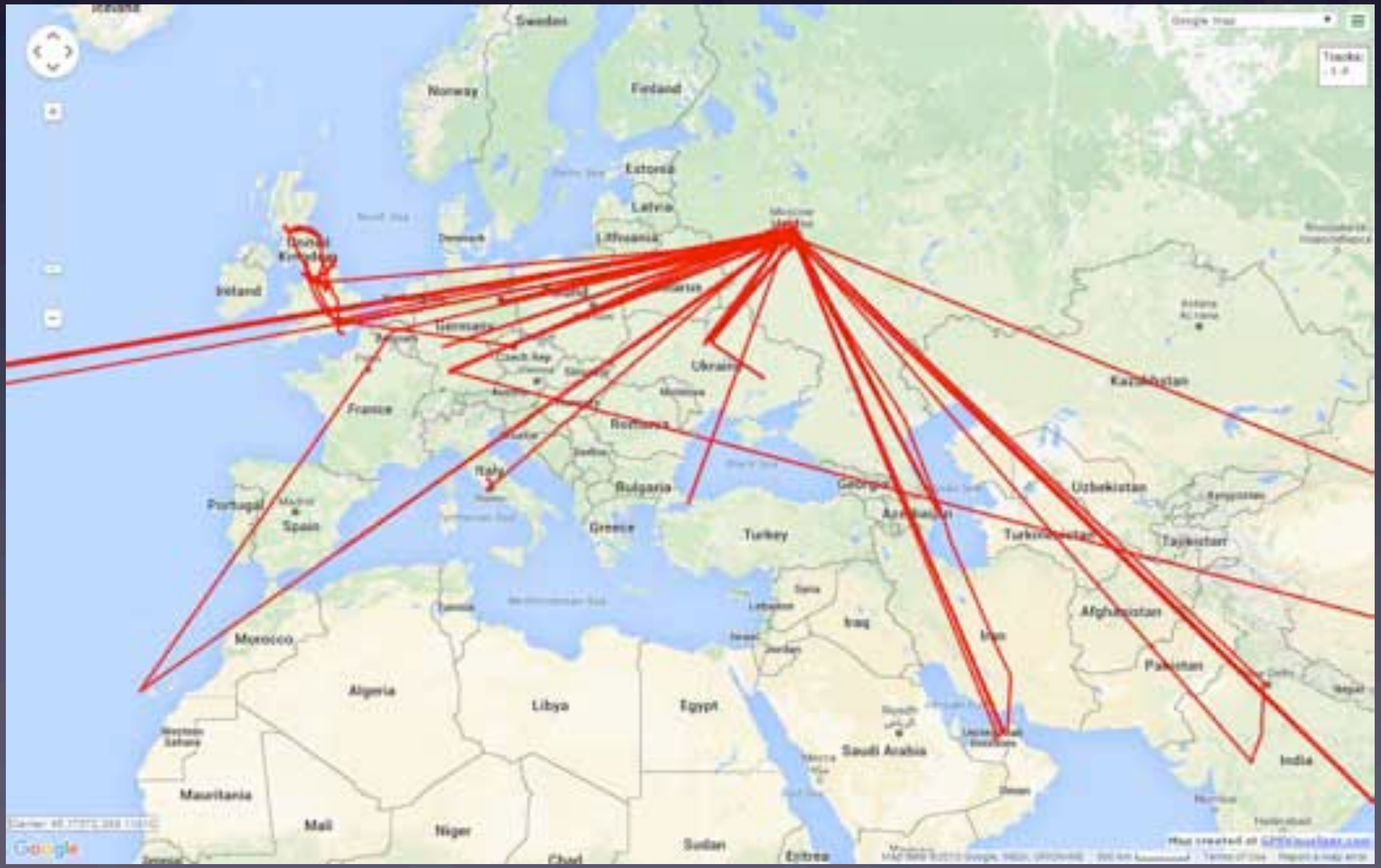
On the Internet, everyone knows you like ASCII Goatse.

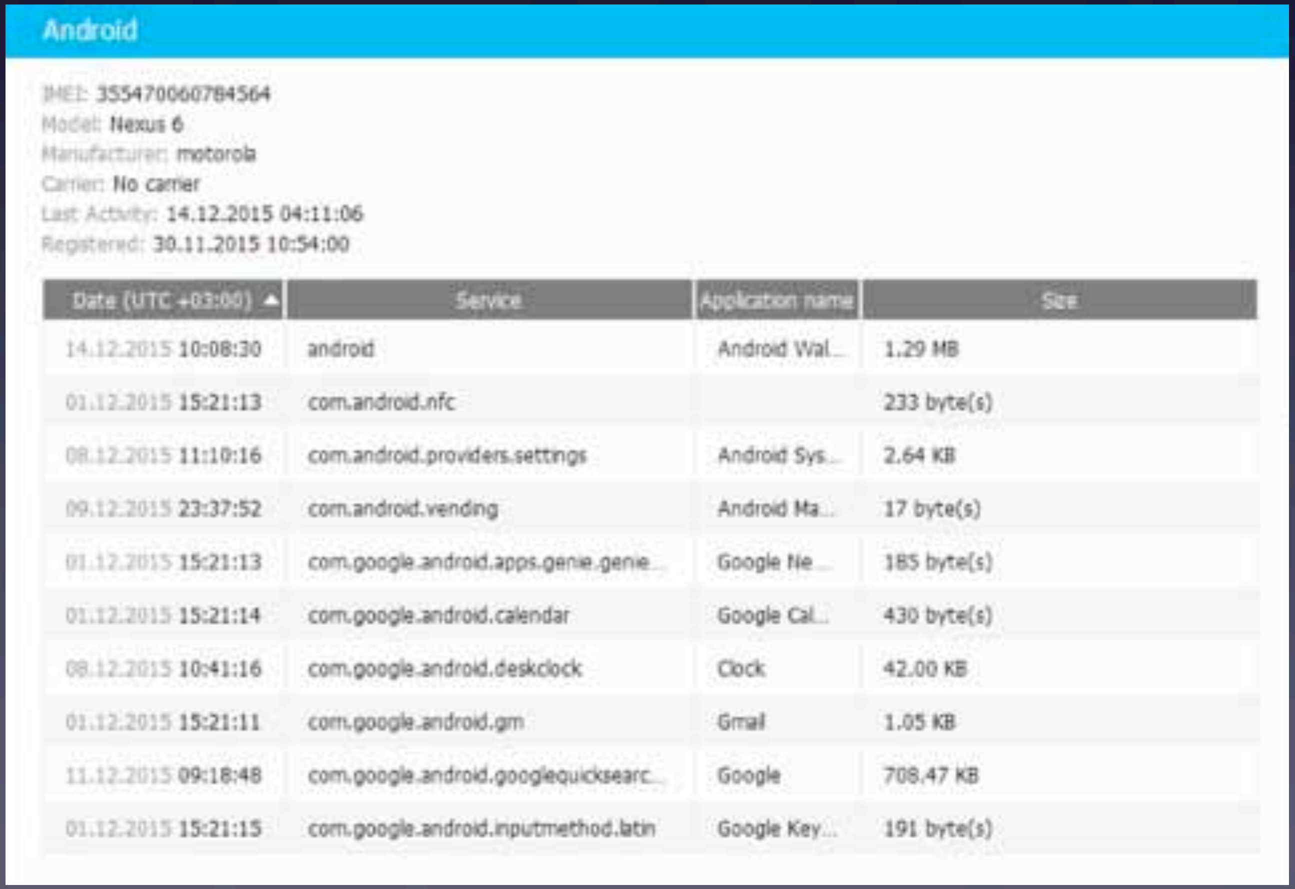
What Google Tracks

- Searches
- Things you type into the search bar
- Links clicked following a search
- Videos watched on YouTube

What Google Tracks

- Browser fingerprint
- Location history
- Mobile device information including IMEIs



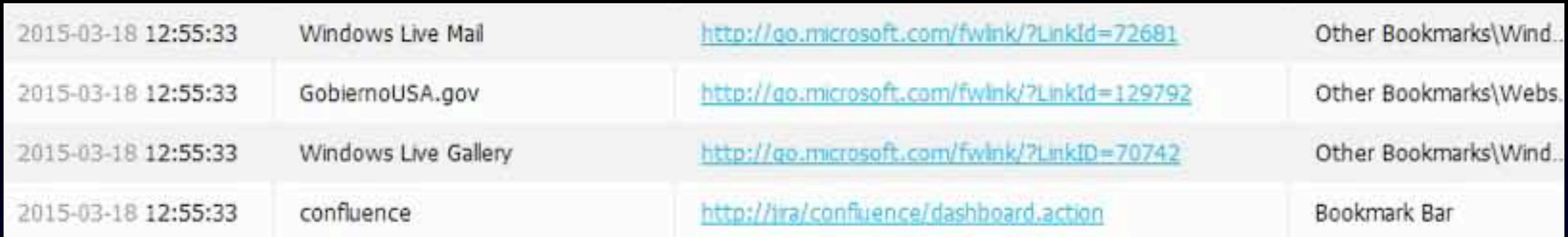


Android

IMEI: 355470060784564
Model: Nexus 6
Manufacturer: motorola
Carrier: No carrier
Last Activity: 14.12.2015 04:11:06
Registered: 30.11.2015 10:54:00

Date (UTC +03:00) ▲	Service	Application name	Size
14.12.2015 10:08:30	android	Android Wal...	1.29 MB
01.12.2015 15:21:13	com.android.nfc		233 byte(s)
08.12.2015 11:10:16	com.android.providers.settings	Android Sys...	2.64 KB
09.12.2015 23:37:52	com.android.vending	Android Ma...	17 byte(s)
01.12.2015 15:21:13	com.google.android.apps.genie.genie...	Google Ne...	185 byte(s)
01.12.2015 15:21:14	com.google.android.calendar	Google Cal...	430 byte(s)
08.12.2015 10:41:16	com.google.android.deskclock	Clock	42.00 KB
01.12.2015 15:21:11	com.google.android.gm	Gmail	1.05 KB
11.12.2015 09:18:48	com.google.android.googlequicksearc...	Google	708.47 KB
01.12.2015 15:21:15	com.google.android.inputmethod.latin	Google Key...	191 byte(s)

What Google Tracks



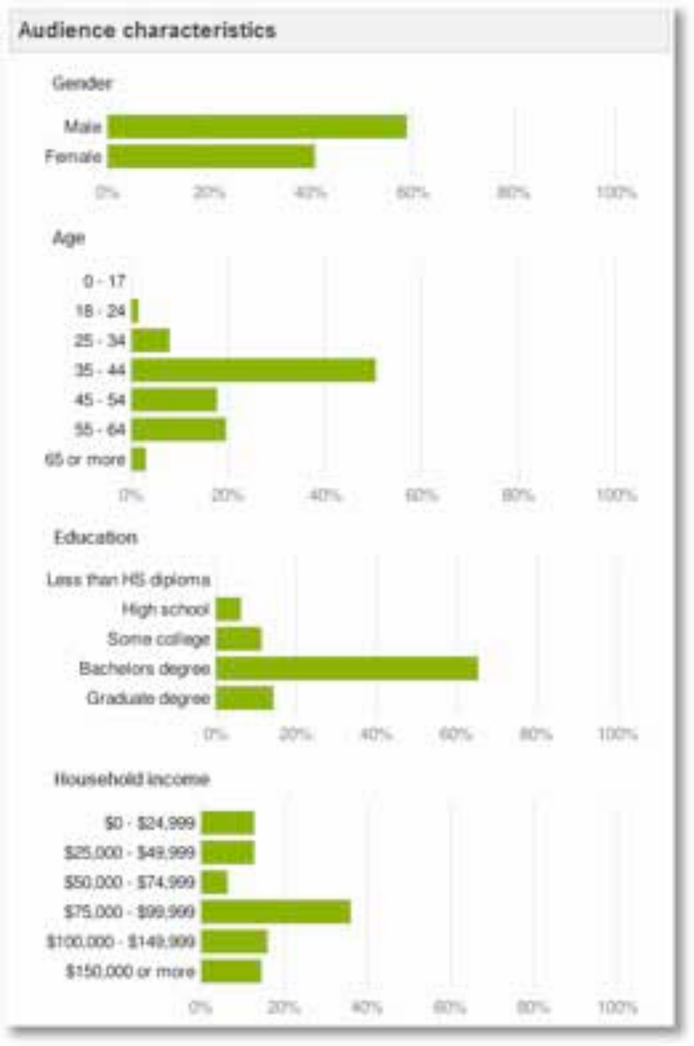
2015-03-18 12:55:33	Windows Live Mail	http://go.microsoft.com/fwlink/?LinkId=72681	Other Bookmarks\Wind..
2015-03-18 12:55:33	GobiernoUSA.gov	http://go.microsoft.com/fwlink/?LinkId=129792	Other Bookmarks\Webs.
2015-03-18 12:55:33	Windows Live Gallery	http://go.microsoft.com/fwlink/?LinkID=70742	Other Bookmarks\Wind..
2015-03-18 12:55:33	confluence	http://jira/confluence/dashboard.action	Bookmark Bar

- If you use Google tools (e.g. Chrome):
  - Browsing history
  - Bookmarks
  - Passwords
  - Credit card data and purchase history
  - Travel data including airline tickets
  - Hotel stays and car rentals

What Google Tracks

- If you use Google services:
  - All your e-mail
  - Photos and videos you have taken
  - Contacts
  - Notes
  - Hangouts conversations

What Google Tracks



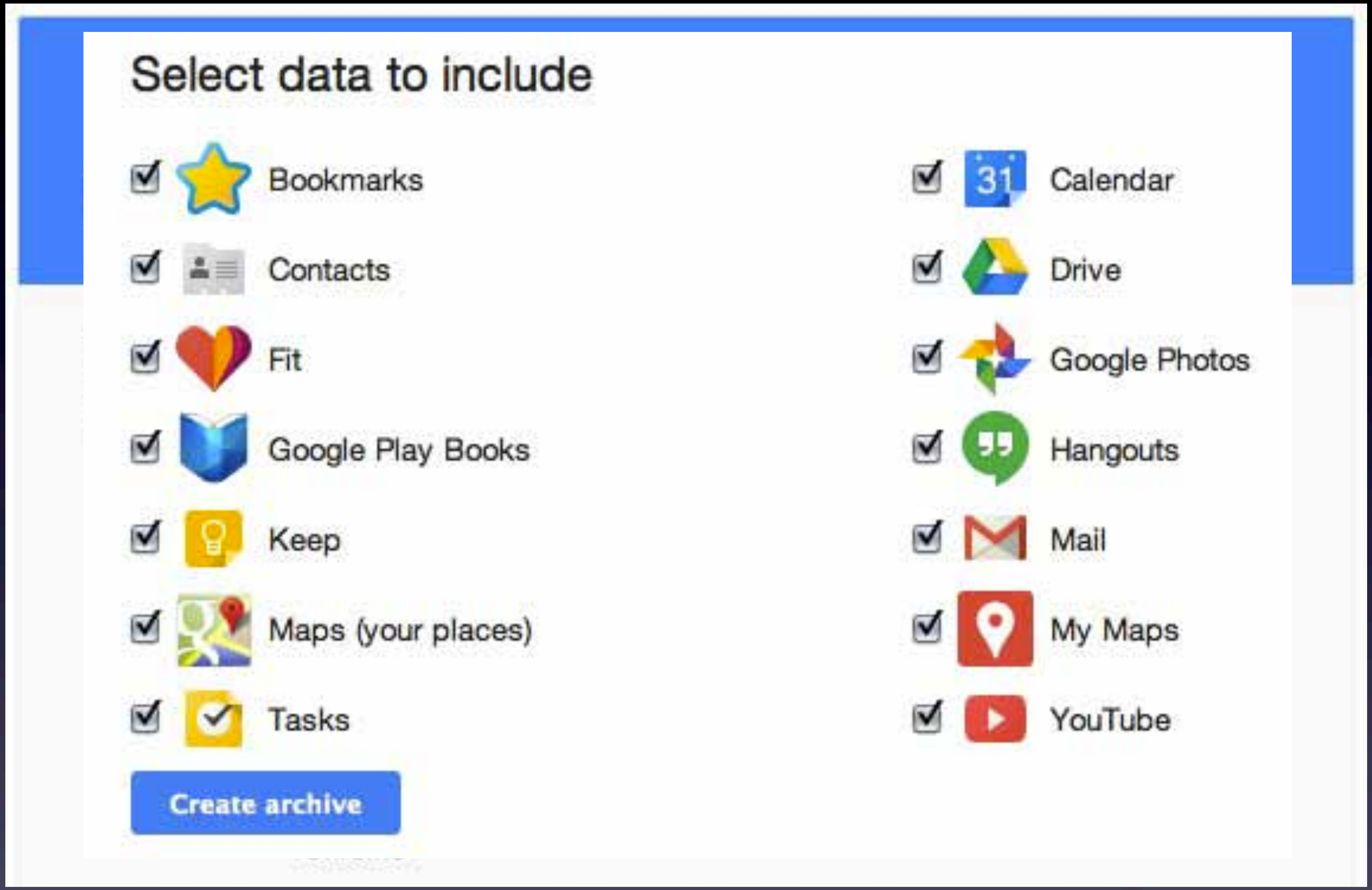
- Your inferred profile for targeted ads
- And more!

What Google Tracks

- Searches
- Things you type into the search bar
- Links clicked following a search
- Videos watched on YouTube
- Browser fingerprint
- Location history
- Mobile device information including IMEIs
- If you use Google tools (e.g. Chrome):
    - Browsing history
    - Bookmarks
    - Passwords
    - Credit card data and purchase history
    - Travel data including airline tickets
    - Hotel stays and car rentals
- If you use Google services:
    - Photos and videos you have taken
    - Contacts
    - Notes
    - Hangouts conversations
- Your inferred profile for targeted ads
- And more!

Google can also trivially correlate multiple accounts belonging to the same user.

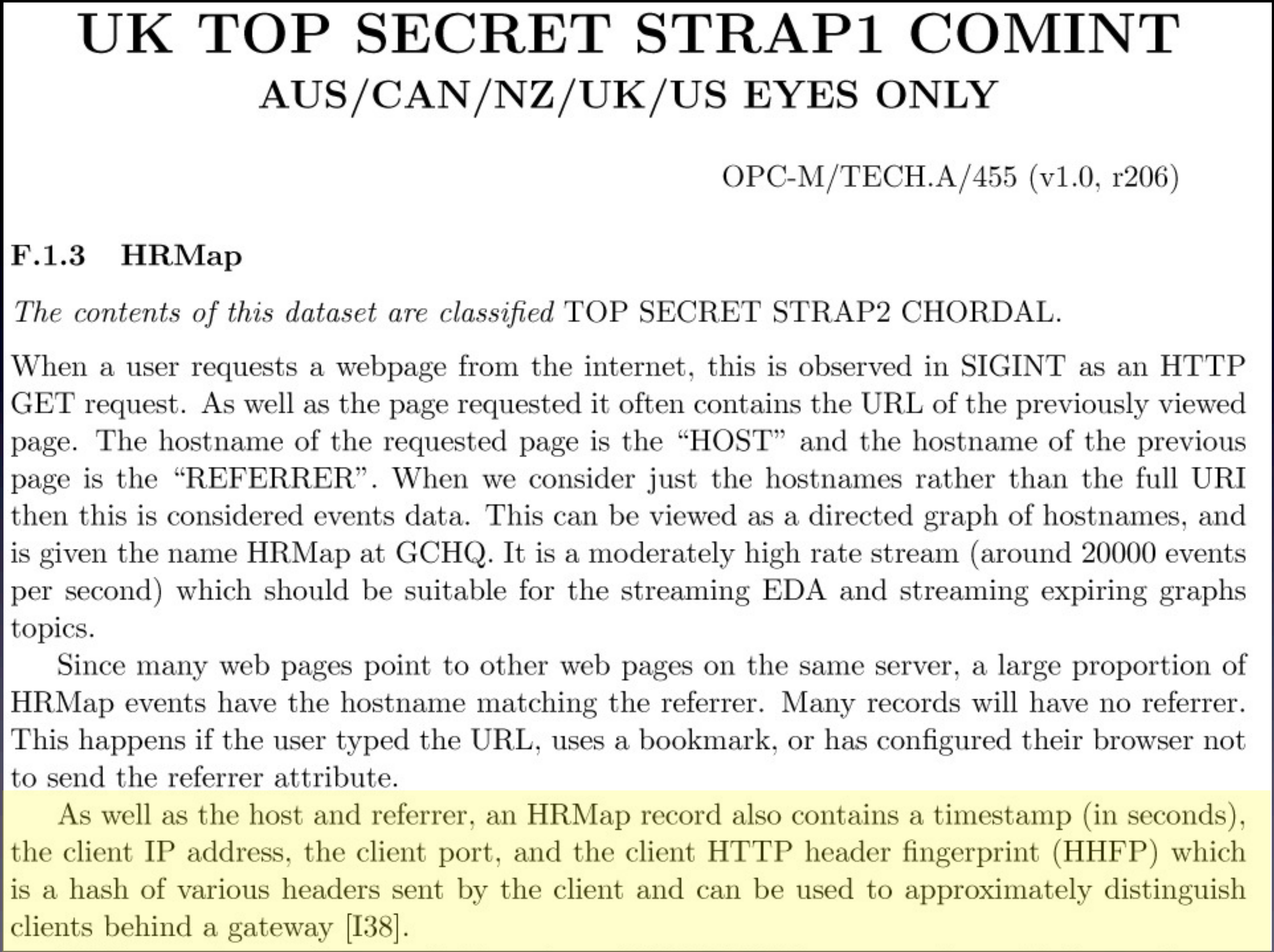
Google's Data Store



Select data to include

- ☑ Bookmarks
- ☑ Contacts
- ☑ Fit
- ☑ Google Play Books
- ☑ Keep
- ☑ Maps (your places)
- ☑ Tasks
- ☑ Calendar
- ☑ Drive
- ☑ Google Photos
- ☑ Hangouts
- ☑ Mail
- ☑ My Maps
- ☑ YouTube

- Can retrieve some with Google Takeout
- Google notifies on account access, but:
  - Developer tools can access without notification
  - Auth keys can be stolen by malware and used to access without notification



UK TOP SECRET STRAP1 COMINT

AUS/CAN/NZ/UK/US EYES ONLY

OPC-M/TECH.A/455 (v1.0, r206)

F.1.3 HRMap

The contents of this dataset are classified TOP SECRET STRAP2 CHORDAL.

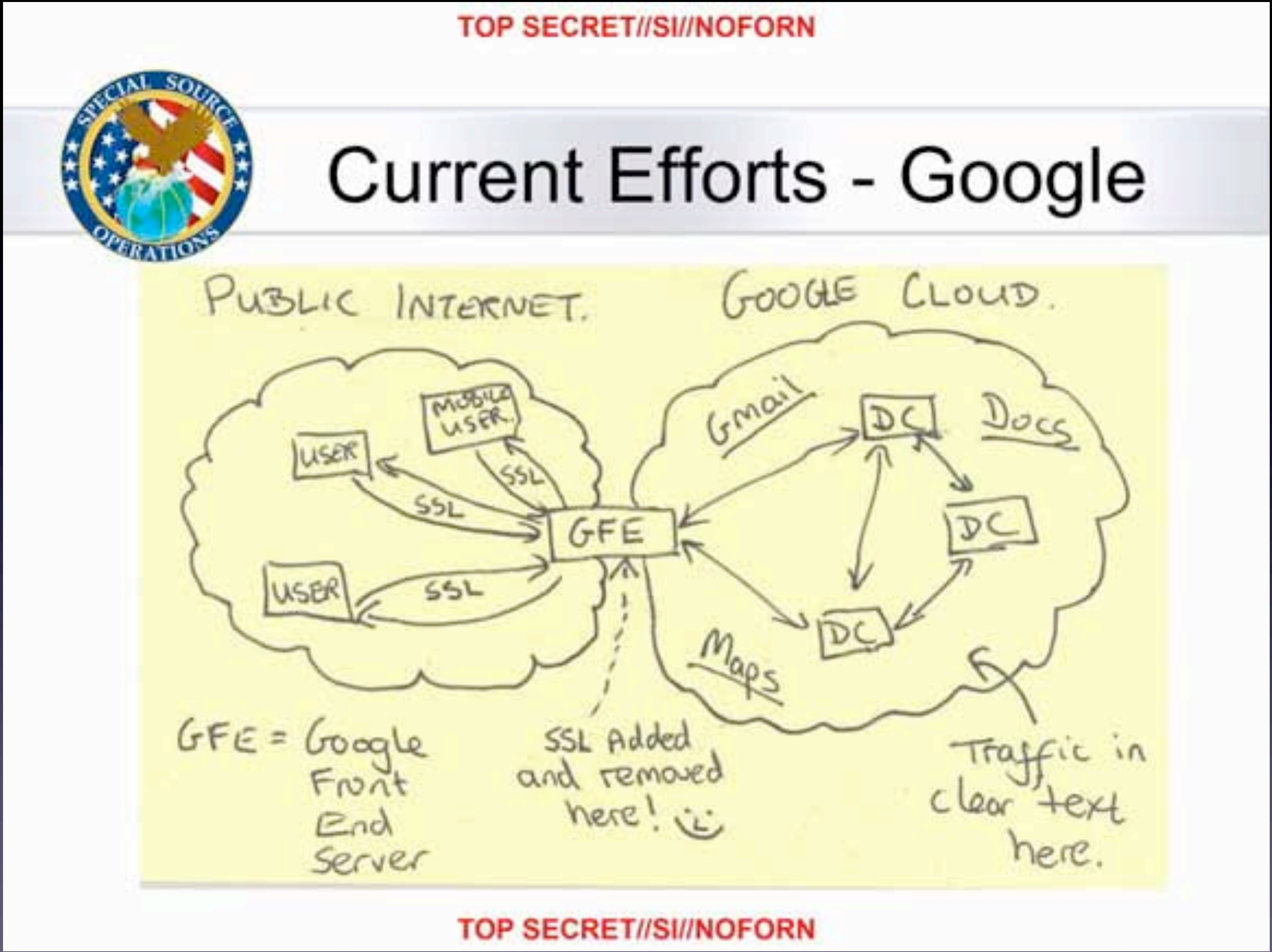
When a user requests a webpage from the internet, this is observed in SIGINT as an HTTP GET request. As well as the page requested it often contains the URL of the previously viewed page. The hostname of the requested page is the "HOST" and the hostname of the previous page is the "REFERRER". When we consider just the hostnames rather than the full URI then this is considered events data. This can be viewed as a directed graph of hostnames, and is given the name HRMap at GCHQ. It is a moderately high rate stream (around 20000 events per second) which should be suitable for the streaming EDA and streaming expiring graphs topics.

Since many web pages point to other web pages on the same server, a large proportion of HRMap events have the hostname matching the referrer. Many records will have no referrer. This happens if the user typed the URL, uses a bookmark, or has configured their browser not to send the referrer attribute.

As well as the host and referrer, an HRMap record also contains a timestamp (in seconds), the client IP address, the client port, and the client HTTP header fingerprint (HHFP) which is a hash of various headers sent by the client and can be used to approximately distinguish clients behind a gateway [I38].

TOP SECRET//SI//NOFORN

Current Efforts - Google


PUBLIC INTERNET.
GOOGLE CLOUD.
MOBILE USER.
USER
USER
SSL
SSL
SSL
GFE
Gmail
DC
Docs
DC
DC
Maps
GFE = Google Front End Server
SSL Added and removed here! ☺
Traffic in clear text here.

TOP SECRET//SI//NOFORN

What Facebook Tracks

Zuck: Yeah so if yo nyone at Harvard

Zuck: Just ask.

Zuck: I have over 4 ddresses, SNS

[Redacted Friend' manage that one?

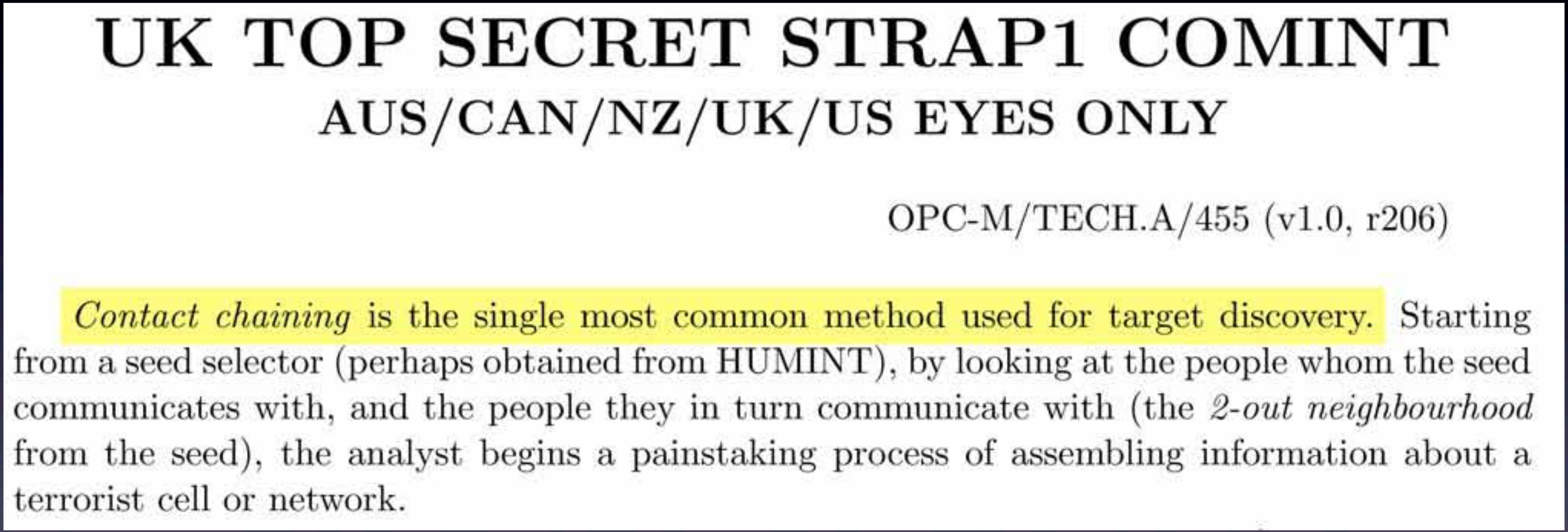
Zuck: People

Zuck: I dor

Zuck: Th

Zuck: Dum

- Everything you do on Facebook
  - Including messages written but not sent
- Many things you browse not on Facebook
  - Via ‘Like’ button tracking
- 2011: tracking cookies from facebook.com even for non-users
- 2012: emotional contagion experiment
- From late 2014: cross-device tracking via Atlas
  - Facebook/Instagram ad tracking program



UK TOP SECRET STRAP1 COMINT

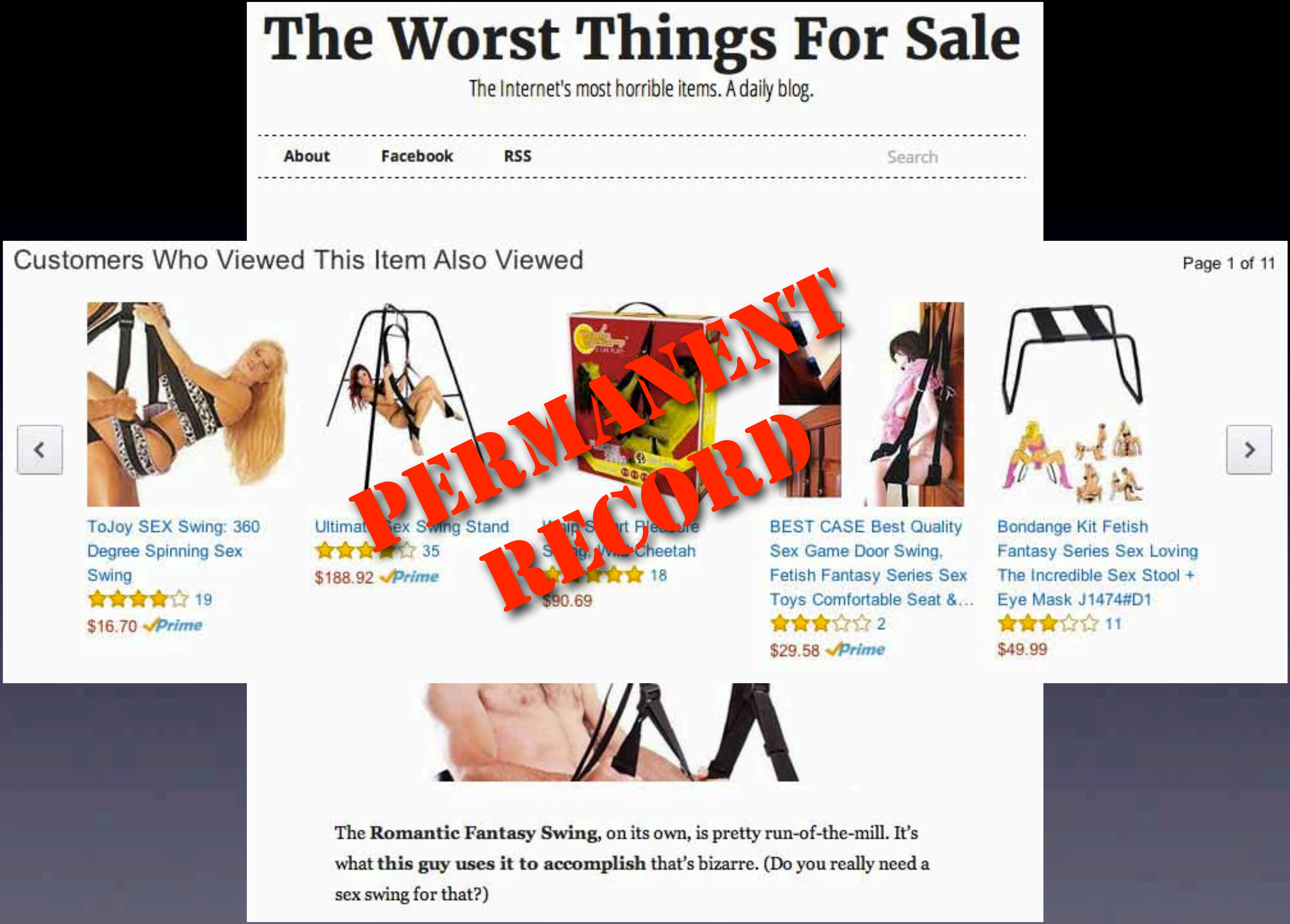
AUS/CAN/NZ/UK/US EYES ONLY

OPC-M/TECH.A/455 (v1.0, r206)

Contact chaining is the single most common method used for target discovery. Starting from a seed selector (perhaps obtained from HUMINT), by looking at the people whom the seed communicates with, and the people they in turn communicate with (the *2-out neighbourhood* from the seed), the analyst begins a painstaking process of assembling information about a terrorist cell or network.

What Big E-Commerce Tracks

- Every item you’ve ever looked at
  - Whether logged in or not
- Purchases and purchasing habits
- What you’re willing to pay for items
- Product reviews
- Detailed, predictive ad targeting profiles



The Worst Things For Sale

The Internet's most horrible items. A daily blog.

Customers Who Viewed This Item Also Viewed

Page 1 of 11

ToJoy SEX Swing: 360 Degree Spinning Sex Swing
★★★★☆ 19
$16.70 ✓Prime

Ultimate Sex Swing Stand
★★★★☆ 35
$188.92 ✓Prime

Whip Smart Pleasure Swing, Wild Cheetah
★★★★★ 18
$90.69

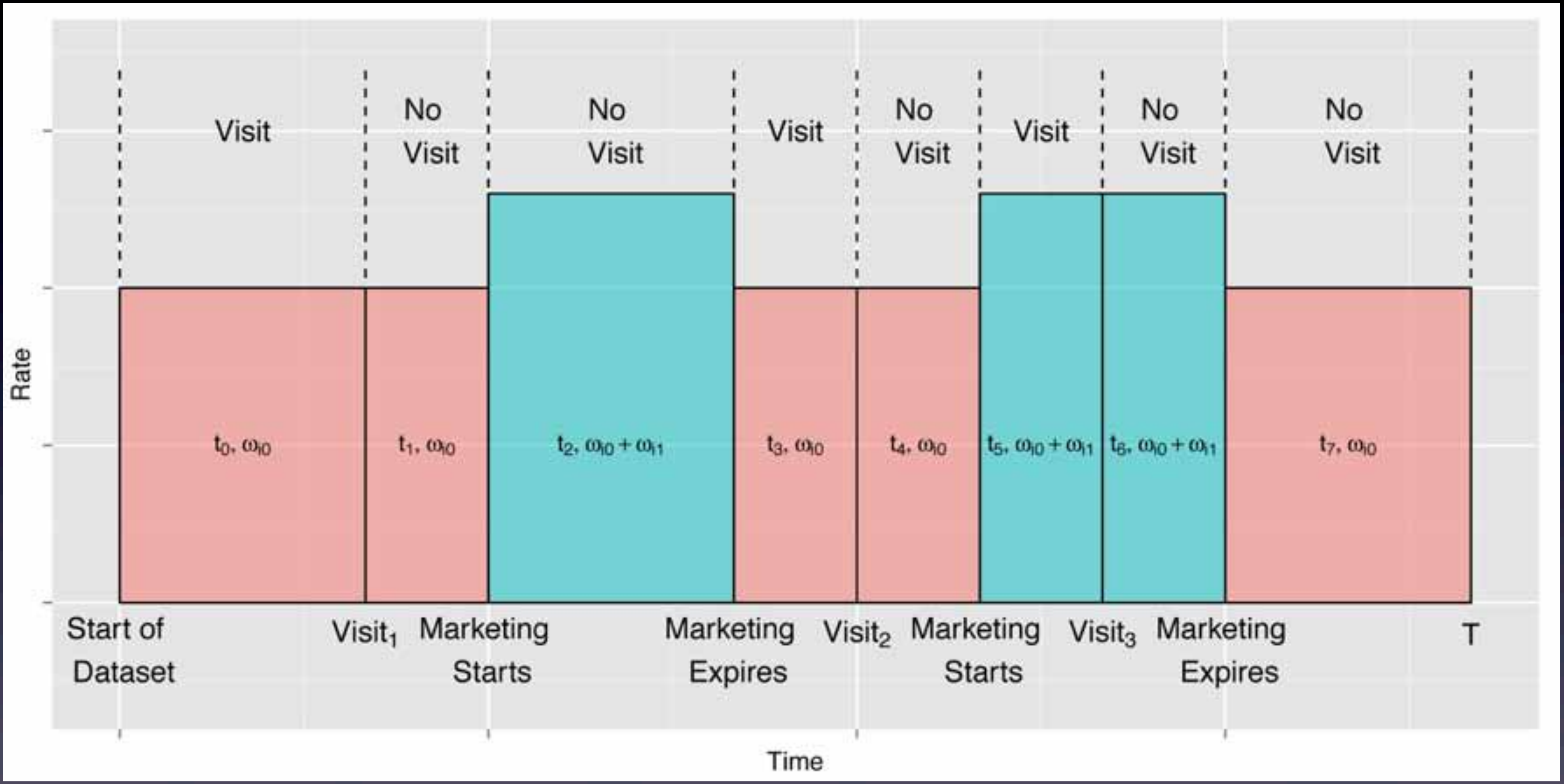
BEST CASE Best Quality Sex Game Door Swing, Fetish Fantasy Series Sex Toys Comfortable Seat &...
★★★☆☆ 2
$29.58 ✓Prime

Bondange Kit Fetish Fantasy Series Sex Loving The Incredible Sex Stool + Eye Mask J1474#D1
★★★☆☆ 11
$49.99

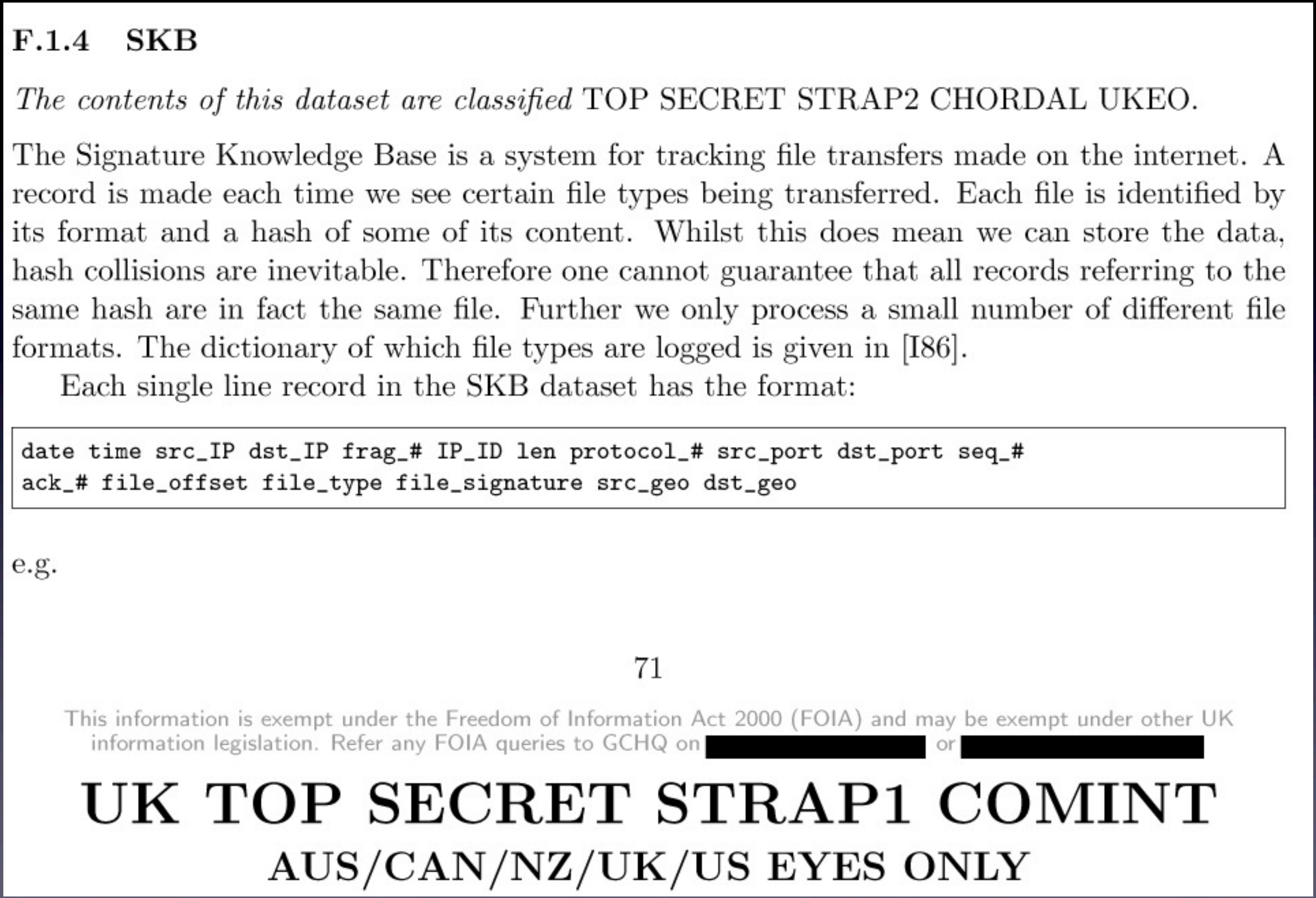
PERMANENT RECORD

The **Romantic Fantasy Swing**, on its own, is pretty run-of-the-mill. It's what **this guy uses it to accomplish** that's bizarre. (Do you really need a sex swing for that?)

E-Commerce Deanonymization



Novak, Feit, Jensen, Bradlow:
Bayesian Imputation for
Anonymous Visits in CRM Data,
December 2015



F.1.4 SKB

The contents of this dataset are classified TOP SECRET STRAP2 CHORDAL UKEO.

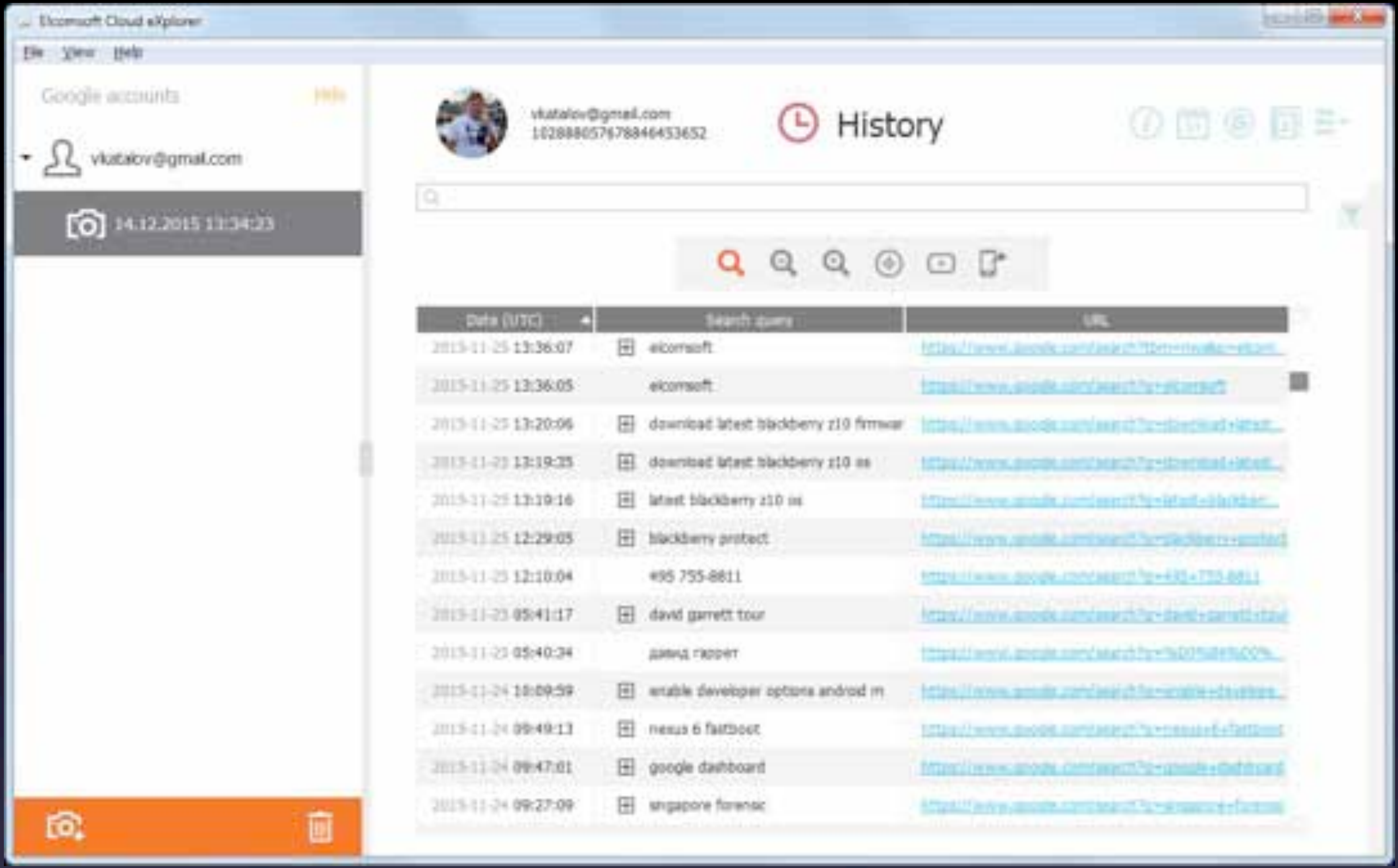
The Signature Knowledge Base is a system for tracking file transfers made on the internet. A record is made each time we see certain file types being transferred. Each file is identified by its format and a hash of some of its content. Whilst this does mean we can store the data, hash collisions are inevitable. Therefore one cannot guarantee that all records referring to the same hash are in fact the same file. Further we only process a small number of different file formats. The dictionary of which file types are logged is given in [I86].

Each single line record in the SKB dataset has the format:

```
date time src_IP dst_IP frag_# IP_ID len protocol_# src_port dst_port seq_#
ack_# file_offset file_type file_signature src_geo dst_geo
```

e.g.

Vulnerabilities

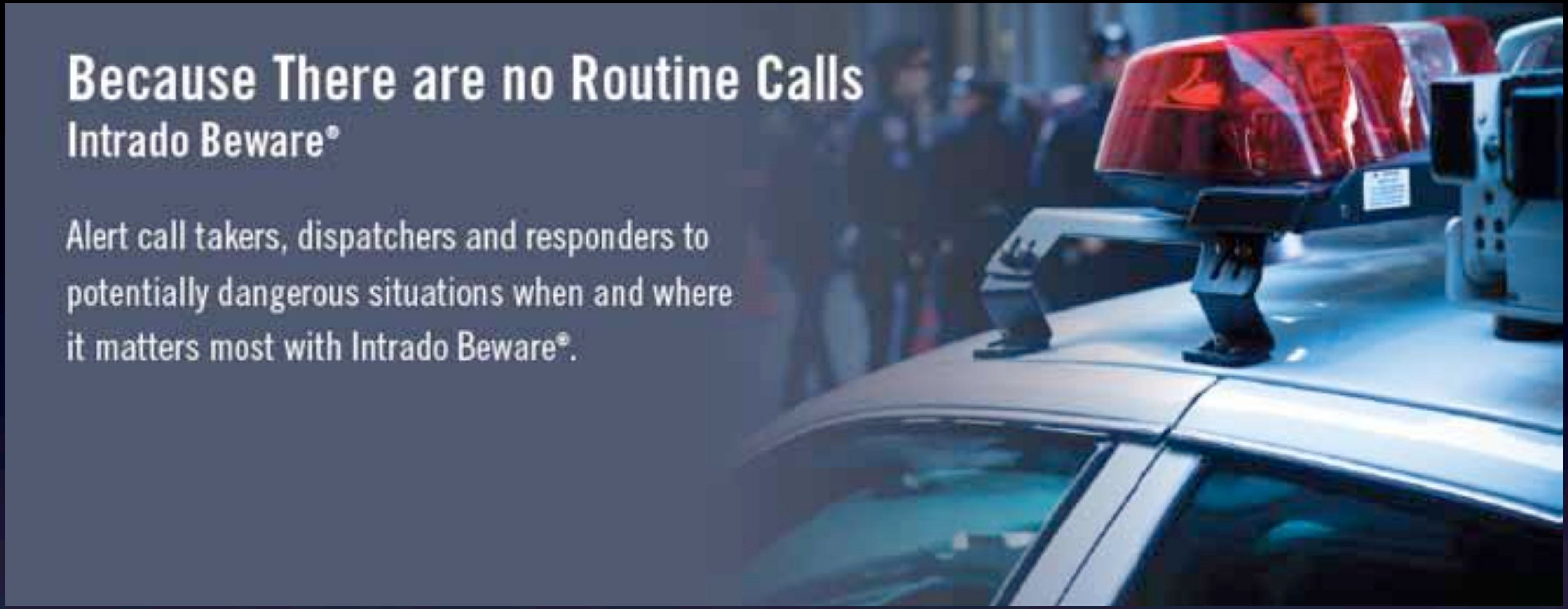


Date (UTC)	Search query	URL
2015-11-25 13:36:07	elcomsoft	[illegible]
2015-11-25 13:36:05	elcomsoft	https://www.google.com/search?q=elcomsoft
2015-11-25 13:20:06	download latest blackberry z10 firmwar	https://www.google.com/search?q=download+latest…
2015-11-25 13:19:35	download latest blackberry z10 os	https://www.google.com/search?q=download+latest…
2015-11-25 13:19:16	latest blackberry z10 os	https://www.google.com/search?q=latest+blackber…
2015-11-25 12:29:05	blackberry protect	https://www.google.com/search?q=blackberry+protect
2015-11-25 12:10:04	+495 755-8811	https://www.google.com/search?q=+495+755-8811
2015-11-23 05:41:17	david garrett tour	https://www.google.com/search?q=david+garrett+tour
2015-11-23 05:40:34	давид гаррет	https://www.google.com/search?q=%D0%B4%D0%…
2015-11-24 10:09:59	enable developer options android m	https://www.google.com/search?q=enable+develope…
2015-11-24 09:49:13	nexus 6 fastboot	https://www.google.com/search?q=nexus+6+fastboot
2015-11-24 09:47:01	google dashboard	https://www.google.com/search?q=google+dashboard
2015-11-24 09:27:09	singapore forensic	https://www.google.com/search?q=singapore+forensic

Elcomsoft Cloud eXplorer

- Information is available for purchase
- Commercially available forensic tools can get it
- Can be leveraged by MITM & man-on-the-side attacks
  - e.g. QUANTUM, Great Cannon
- OSINT: spearphishing enabler
- Psych profiling, pattern of life/network graph analysis

Profiling Tools



Because There are no Routine Calls

Intrado Beware®

Alert call takers, dispatchers and responders to potentially dangerous situations when and where it matters most with Intrado Beware®.

- Data mining & inference tools
  - Police first, then who?
- Integrate data & assign “threat level”:
  - Public & commercial databases
  - Deep web
  - Social media
- Black box: weightings unknown
  - Unpredictable results for you

Resisting Surveillance

- There is no reclaiming data once given up
  - Protect the truth from storage
  - Corrupt storage with falsehoods

OPSEC

You never know who's on the wires!
BE CAREFUL
WHAT YOU SAY

THE BOTTOM LINE ON OPSEC;

We all have information that the Bad Guys need to hurt us. We don't want them to get it. The OPSEC process helps us to look at our world through the eyes of an adversary and to develop measures in order to deny them. Get it?

The Interagency
OPSEC Support Staff
www.ioss.gov

The OPSEC Process:

1. Identify Critical Info
2. Analyze Threats
3. Analyze Vulnerabilities
4. Assess the Risks
5. Apply Countermeasures

5 STEPS... 1 MINDSET

WHAT IS OPERATIONS SECURITY?
Operations Security, or OPSEC, is a risk management methodology used to deny an adversary information concerning our intentions and capabilities by identifying, controlling, and protecting critical information associated with the planning and execution of a mission.

The 7 Deadly OPSEC Sins

- Overconfidence
- Trust
- Perceived Insignificance
- Guilt By Association
- Packet Origin
- Cleartext
- Documentation

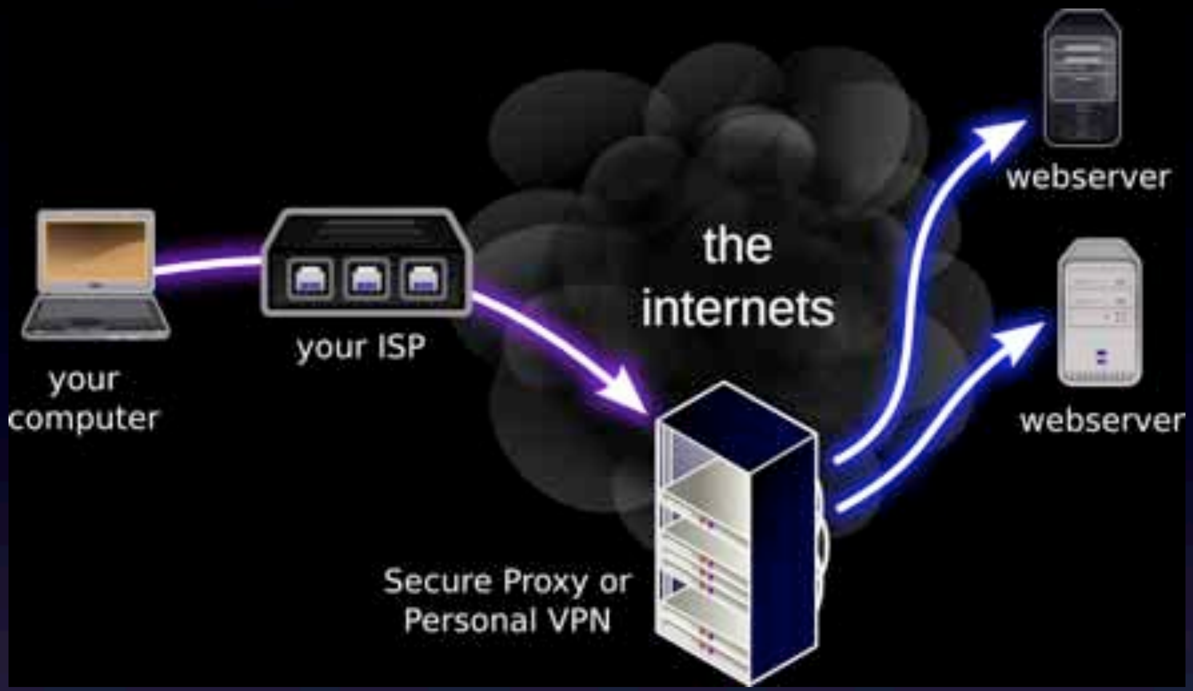
⚠ **WARNING**

Keep hands away from jet.

Basic Tools

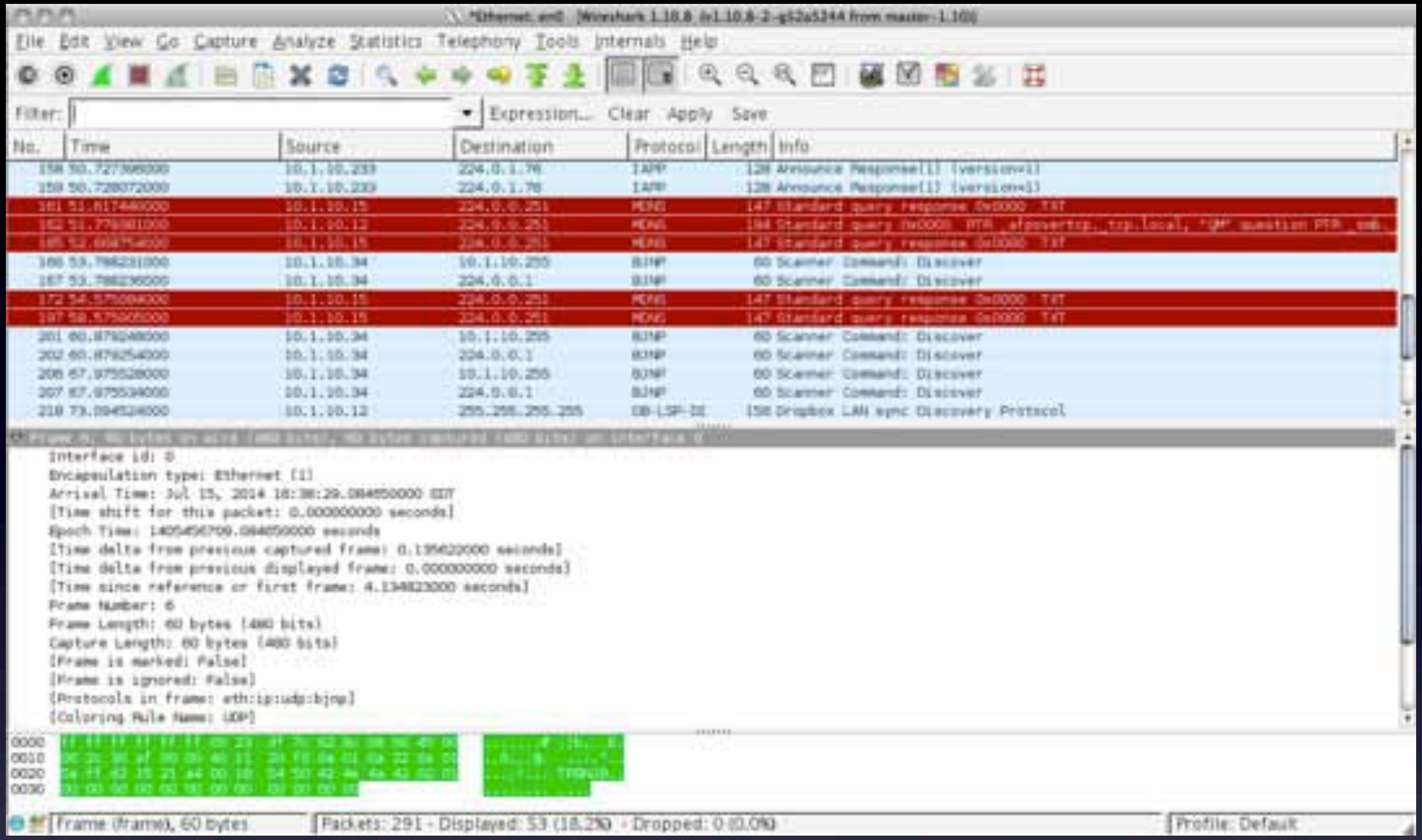
- Ad Blocking
  - AdBlockPlus, GlimmerBlocker etc
  - /etc/hosts: http://someonewhocares.org/hosts/
- Bug Sweeping, Descripting, XSR
  - Ghostery (turn off data sharing)
  - NoScript, RequestPolicy, µMatrix (Mozilla)
  - Privacy Badger
- HTTPS Everywhere
- Search Proxying
  - e.g. search.disconnect.me
- Fake your user-agent string
- Clear browser data frequently

VPNs



- Traffic Encryption
- Location Obfuscation
- Request Concealment
    - ...Depending On Listener Location
    - ...Depending On Provider

VPN Failure Modes


*Ethernet: en0 [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

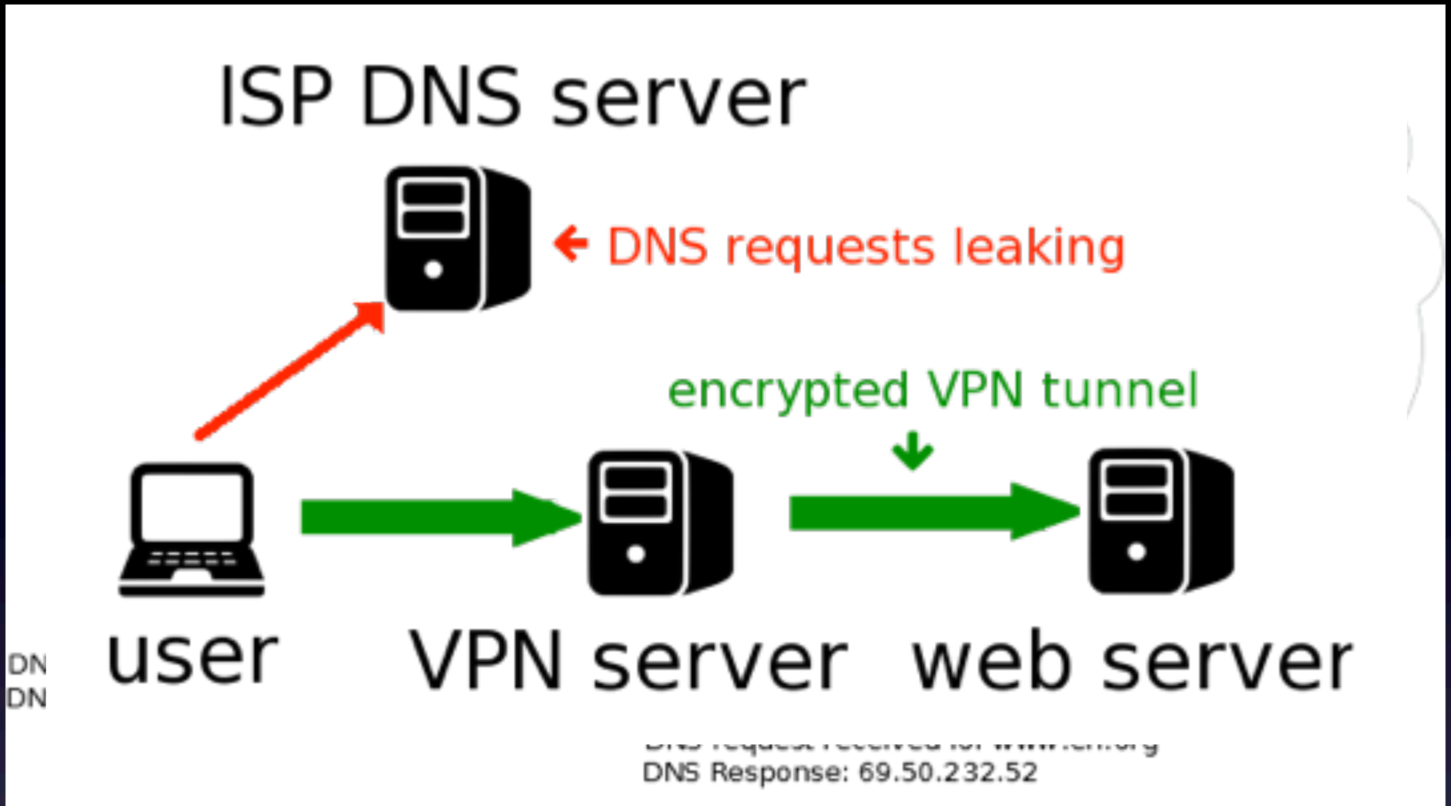
```
No.  Time              Source        Destination      Protocol  Length Info
 158 50.727366000      10.1.10.233   224.0.1.76       IAPP      128 Announce Response(1) (version=1)
 159 50.728072000      10.1.10.233   224.0.1.76       IAPP      128 Announce Response(1) (version=1)
 161 51.817440000      10.1.10.15    224.0.0.251      MDNS      147 Standard query response 0x0000  TXT
 162 51.776981000      10.1.10.12    224.0.0.251      MDNS      184 Standard query 0x0000  PTR _afpovertcp._tcp.local, "QM" question PTR _smb.
 165 52.658754000      10.1.10.15    224.0.0.251      MDNS      147 Standard query response 0x0000  TXT
 166 53.786231000      10.1.10.34    10.1.10.255      BJNP       60 Scanner Command: Discover
 167 53.786236000      10.1.10.34    224.0.0.1        BJNP       60 Scanner Command: Discover
 172 54.575084000      10.1.10.15    224.0.0.251      MDNS      147 Standard query response 0x0000  TXT
 197 58.575905000      10.1.10.15    224.0.0.251      MDNS      147 Standard query response 0x0000  TXT
 201 60.879248000      10.1.10.34    10.1.10.255      BJNP       60 Scanner Command: Discover
 202 60.879254000      10.1.10.34    224.0.0.1        BJNP       60 Scanner Command: Discover
 206 67.975528000      10.1.10.34    10.1.10.255      BJNP       60 Scanner Command: Discover
 207 67.975534000      10.1.10.34    224.0.0.1        BJNP       60 Scanner Command: Discover
 218 73.094524000      10.1.10.12    255.255.255.255  DB-LSP-DI 158 Dropbox LAN sync Discovery Protocol
```

```
Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
    Interface id: 0
    Encapsulation type: Ethernet (1)
    Arrival Time: Jul 15, 2014 16:38:29.084650000 EDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1405456709.084650000 seconds
    [Time delta from previous captured frame: 0.135622000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 4.134823000 seconds]
    Frame Number: 6
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:udp:bjnp]
    [Coloring Rule Name: UDP]
0000  [illegible]
0010  [illegible]
0020  [illegible]
0030  [illegible]
```

Frame (frame), 60 bytes | Packets: 291 · Displayed: 53 (18.2%) · Dropped: 0 (0.0%) | Profile: Default

- Leaks
  - IPv6 leaks
  - DNS leaks
  - WebRTC leaks
  - “Port Fail” port forwarding leak
- Protocol vulnerabilities
- User error

DNS Leaks



- Exposure methods:
  - DNS queries go to default ISP DNS
  - ISP implements transparent DNS proxy
- Remedy:
  - Set static IP properties before VPN connection
  - After connecting, flush DNS resolver cache
  - Remove DNS settings for primary interface
  - Test for DNS leaks
  - After disconnecting, restore DNS settings & flush DNS resolver cache

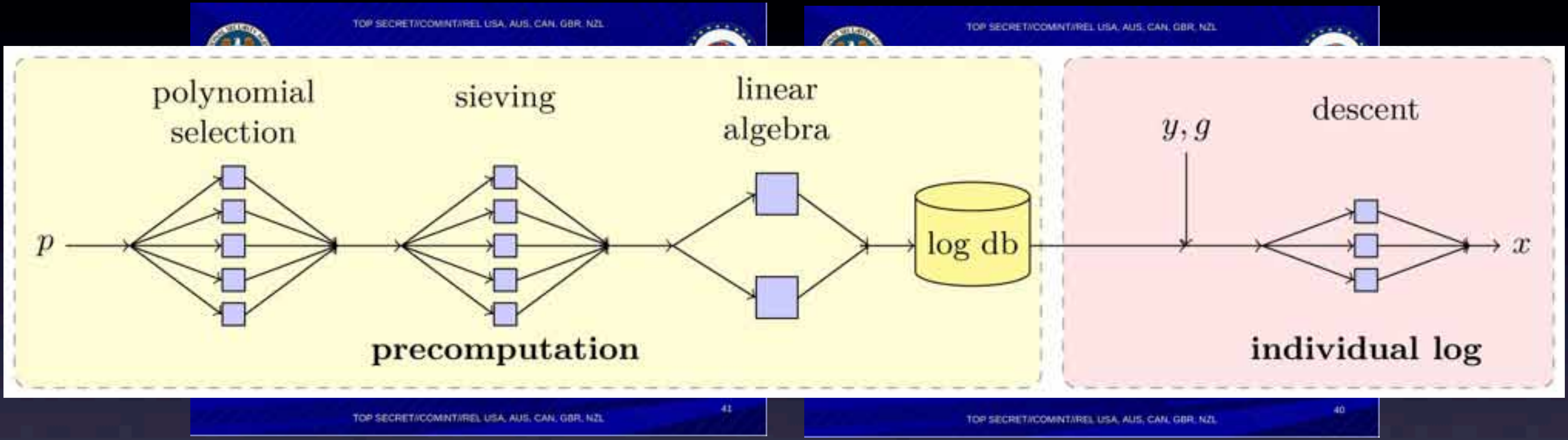
WebRTC Leaks

- Voice/Video/PTP in browser
- Firefox/Chrome/Opera/Android/iOS
- Javascript can send UDP request to STUN server via all available interfaces
- Cannot be blocked reliably with browser plugins
- Remedy:
  - Set firewall rules to enforce all traffic over VPN

“Port Fail”

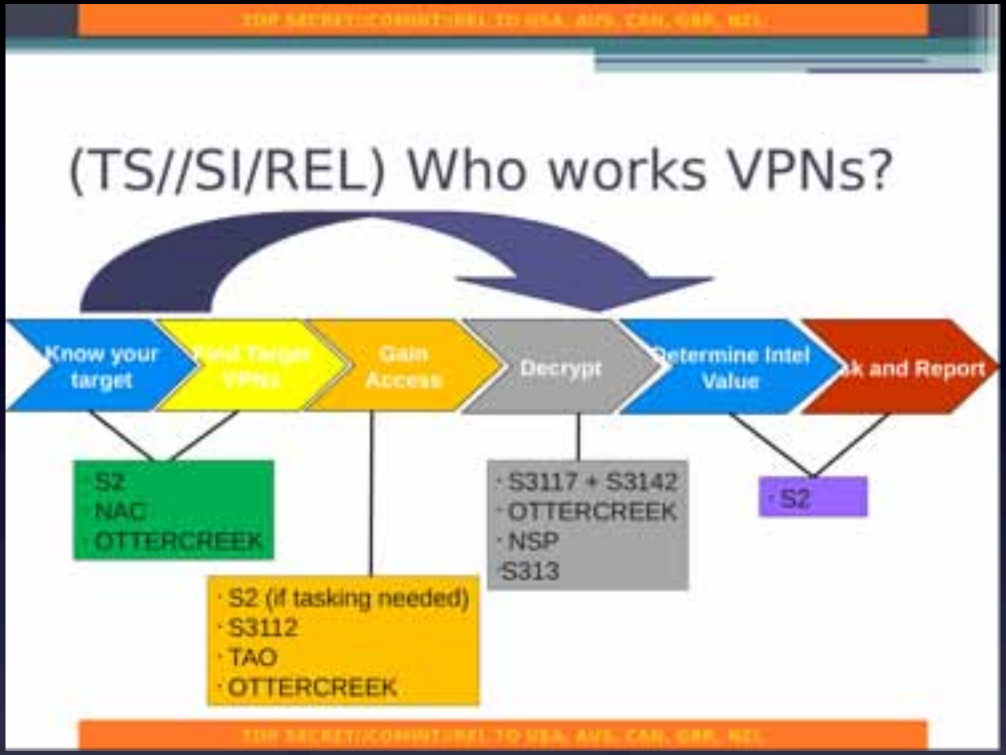
- Attacker has account at same VPN provider and ability to set up port forwarding at exit IP
- Forward a port, and trick target into connecting to it
- Target’s default route to VPN provider will cause it to make direct connection, exposing real IP
- Remedy:
  - Ensure VPN provider does not permit port forwarding for others or separates incoming/exit IPs

Protocol Vulnerabilities


TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL
TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL
polynomial selection
sieving
linear algebra
p
log db
y, g
descent
x
precomputation
individual log
41
TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL
40
TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL

- PPTP vulnerable to masses via CloudCrack since 2012
- IPsec IKE vulnerable to NSA via passive and active means since at least 2009 (100,000 decrypts/hr in 2011)
- 2015: NSA precompute attack on 1024-bit Diffie-Helman key exchange all but confirmed

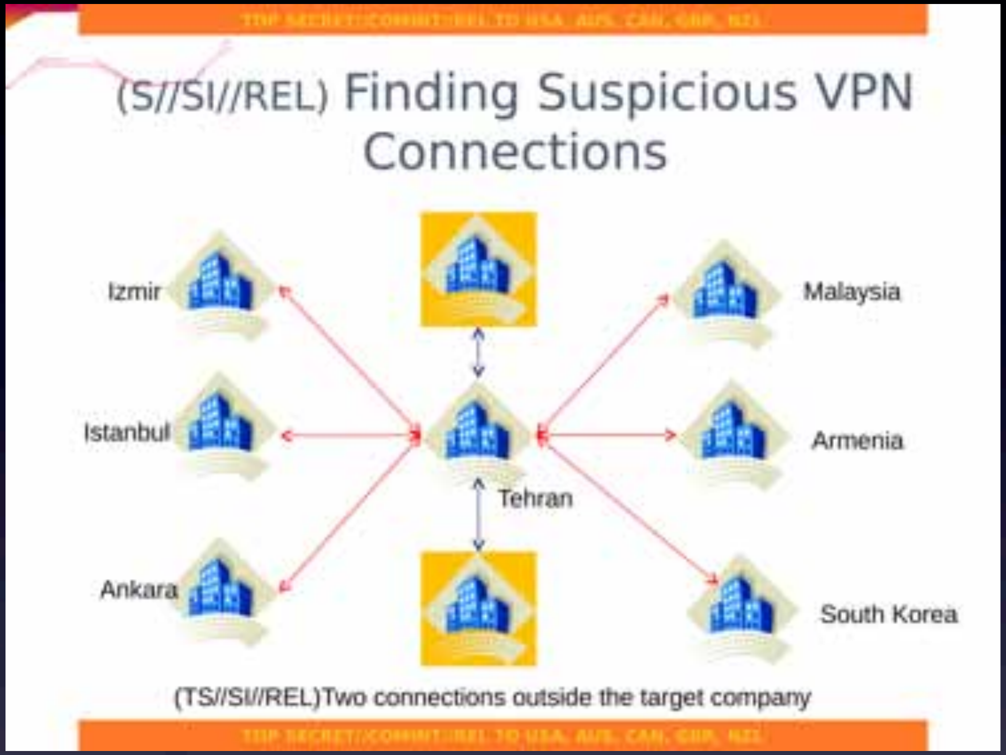
Mitigation



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

(TS//SI/REL) Who works VPNs?

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

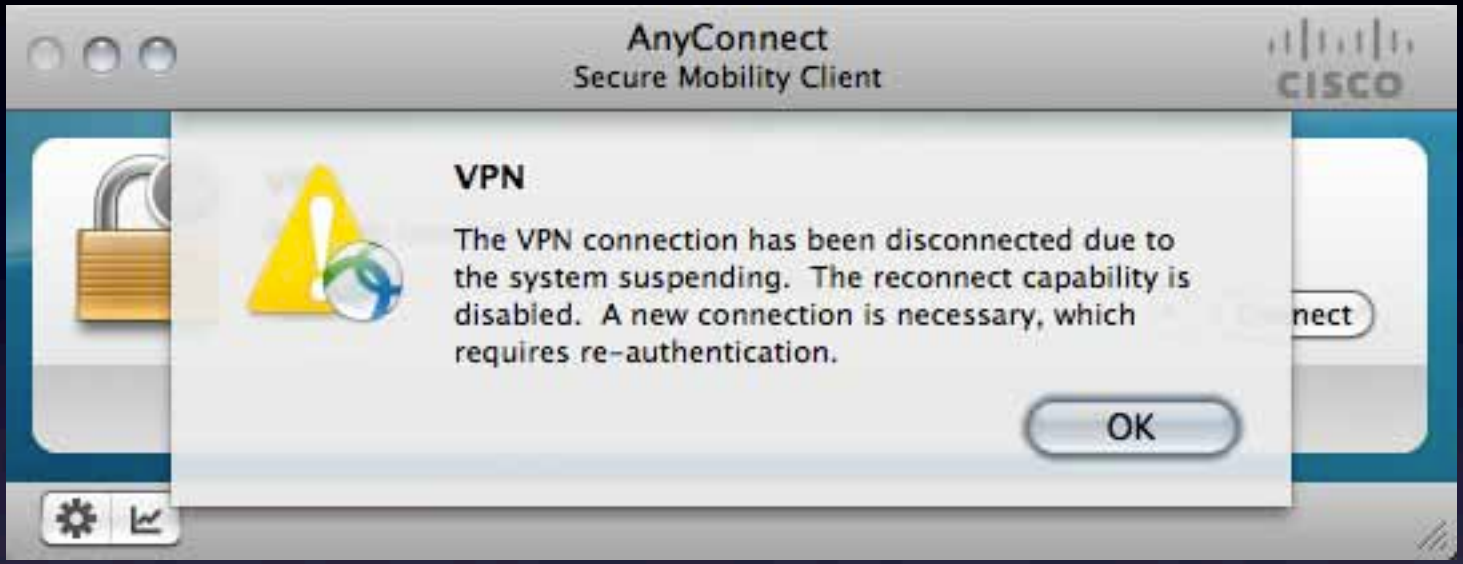
(S//SI//REL) Finding Suspicious VPN Connections

(TS//SI//REL)Two connections outside the target company

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

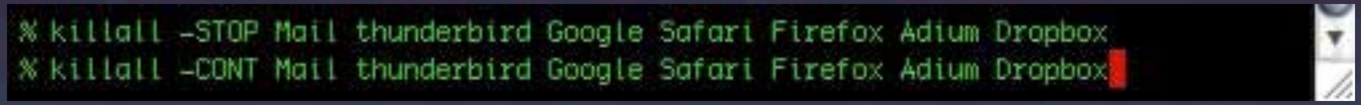
- IPsec:
  - Always use Perfect Forward Secrecy
  - Avoid Pre Shared Keys
- OpenVPN:
  - 2048-bit EC-DHE
  - Generate fresh prime groups
- Harden your SSH too

Be Careful Out & About

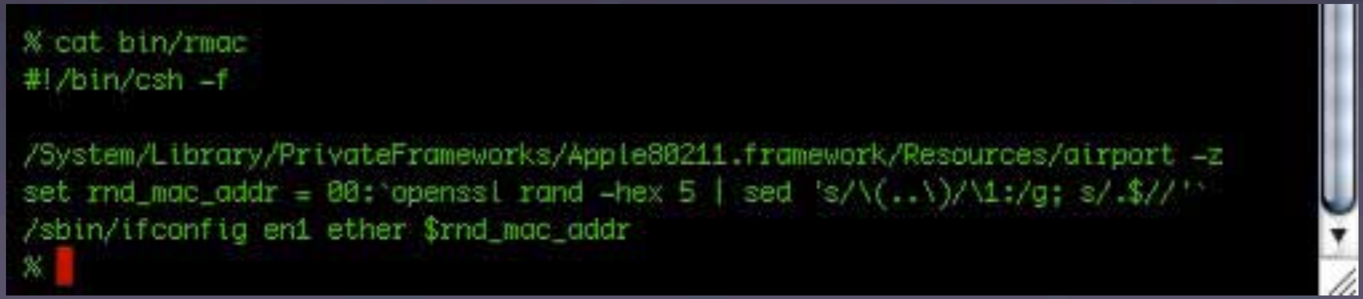


VPN

The VPN connection has been disconnected due to the system suspending. The reconnect capability is disabled. A new connection is necessary, which requires re-authentication.



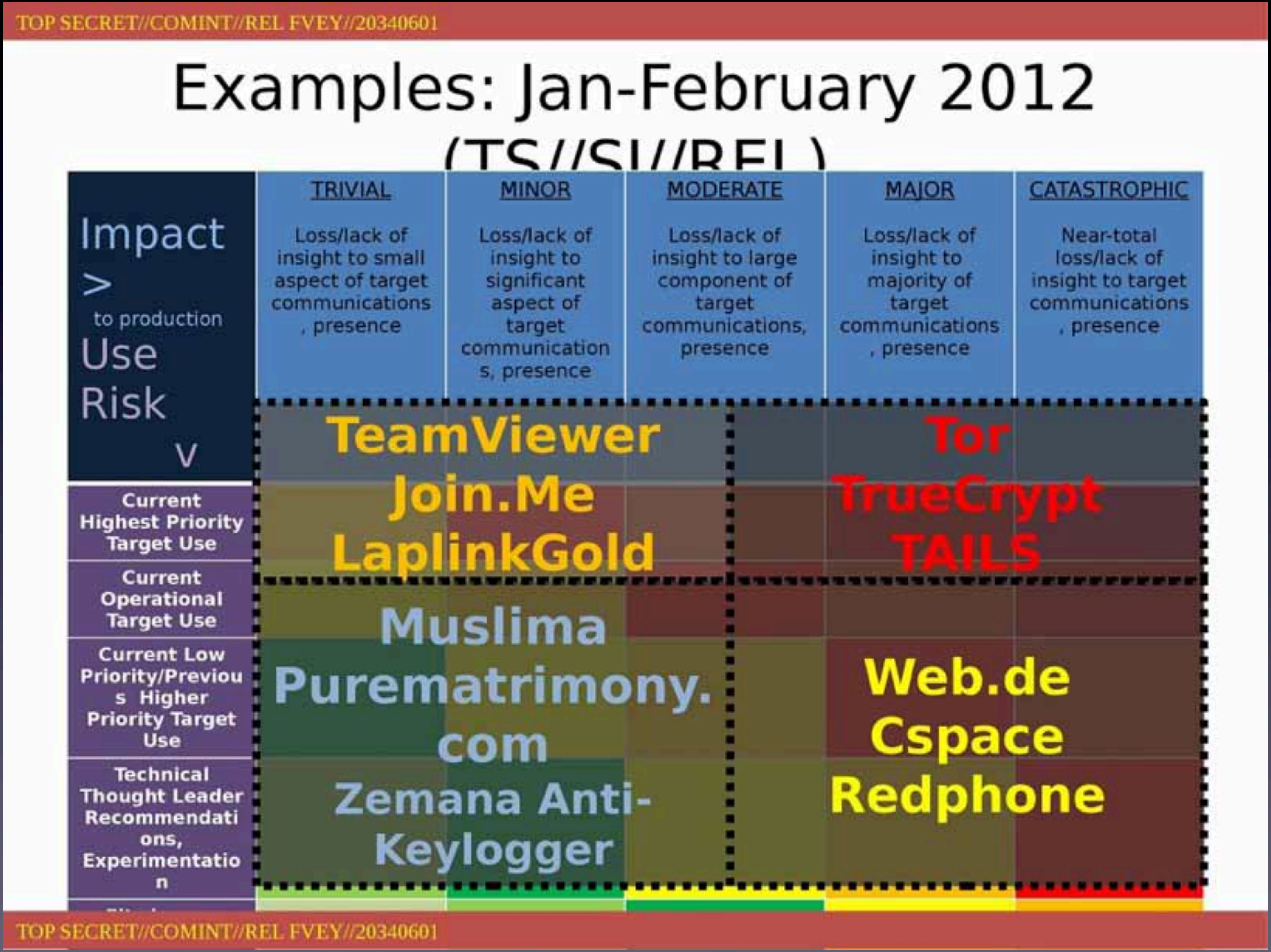
```
% killall -STOP Mail thunderbird Google Safari Firefox Adium Dropbox
% killall -CONT Mail thunderbird Google Safari Firefox Adium Dropbox
```



```
% cat bin/rmac
#!/bin/csh -f

/System/Library/PrivateFrameworks/Apple80211.framework/Resources/airport -z
set rnd_mac_addr = 00:`openssl rand -hex 5 | sed 's/\(..\)/\1:/g; s/.$//'`
/sbin/ifconfig en1 ether $rnd_mac_addr
%
```

Using Anonymity Tools



TOP SECRET//COMINT//REL FVEY//20340601

Examples: Jan-February 2012 (TS//SI//REL)

Impact > to production Use Risk v	TRIVIAL	MINOR	MODERATE	MAJOR	CATASTROPHIC
	Loss/lack of insight to small aspect of target communications, presence	Loss/lack of insight to significant aspect of target communications, presence	Loss/lack of insight to large component of target communications, presence	Loss/lack of insight to majority of target communications, presence	Near-total loss/lack of insight to target communications, presence
Current Highest Priority Target Use					
Current Operational Target Use					
Current Low Priority/Previous Higher Priority Target Use					
Technical Thought Leader Recommendations, Experimentation					

TeamViewer
Join.Me
LaplinkGold

Tor
TrueCrypt
TAILS

Muslima
Purematrimony.com
Zemana Anti-Keylogger

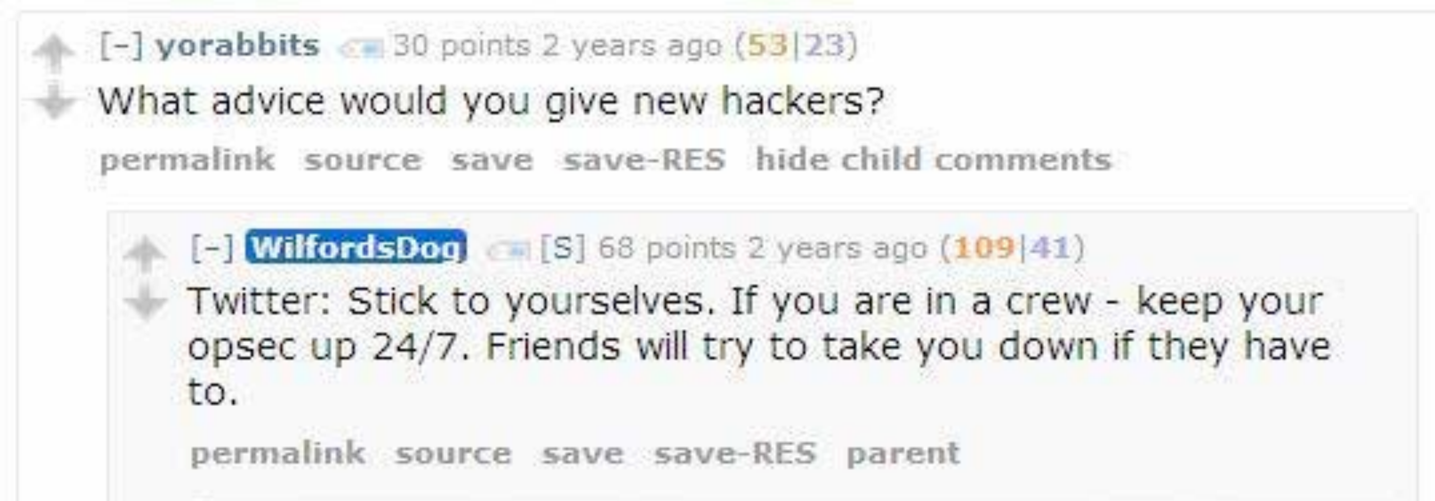
Web.de
Cspace
Redphone

TOP SECRET//COMINT//REL FVEY//20340601

Case Study: LulzSec/AntiSec

IRC WITHOUT TOR...
...NOT EVEN ONCE

Moral:



[-] yorabbits 30 points 2 years ago (53|23)

What advice would you give new hackers?

permalink source save save-RES hide child comments

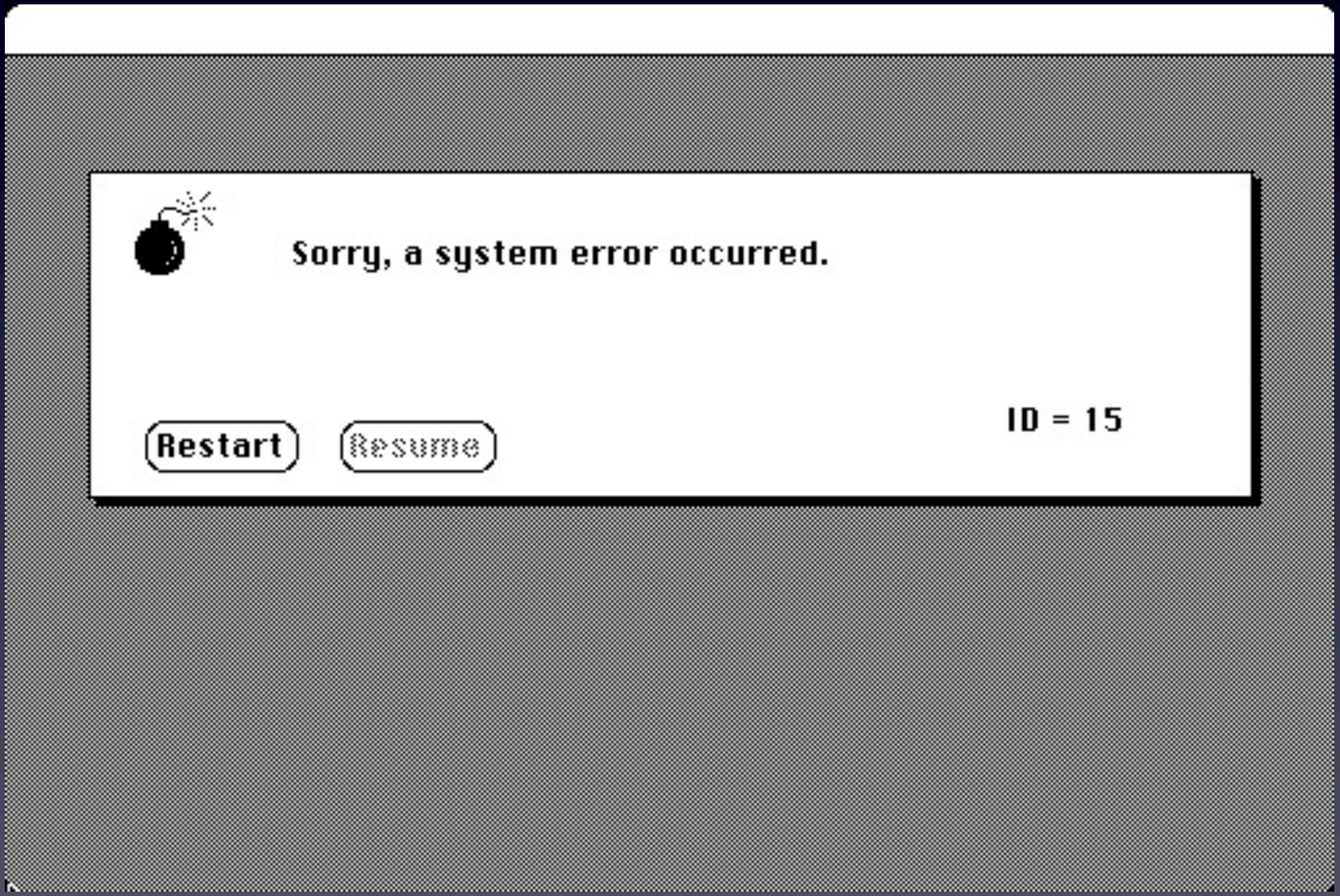
[-] WilfordsDog [S] 68 points 2 years ago (109|41)

Twitter: Stick to yourselves. If you are in a crew - keep your opsec up 24/7. Friends will try to take you down if they have to.

permalink source save save-RES parent

- Don’t Fail Unsafe With Tor
- Always Check What You’re Exposing
- OPSEC Is 24/7

Case Study: Harvard Bomb Hoax



Sorry, a system error occurred.

ID = 15

What Messed It Up?

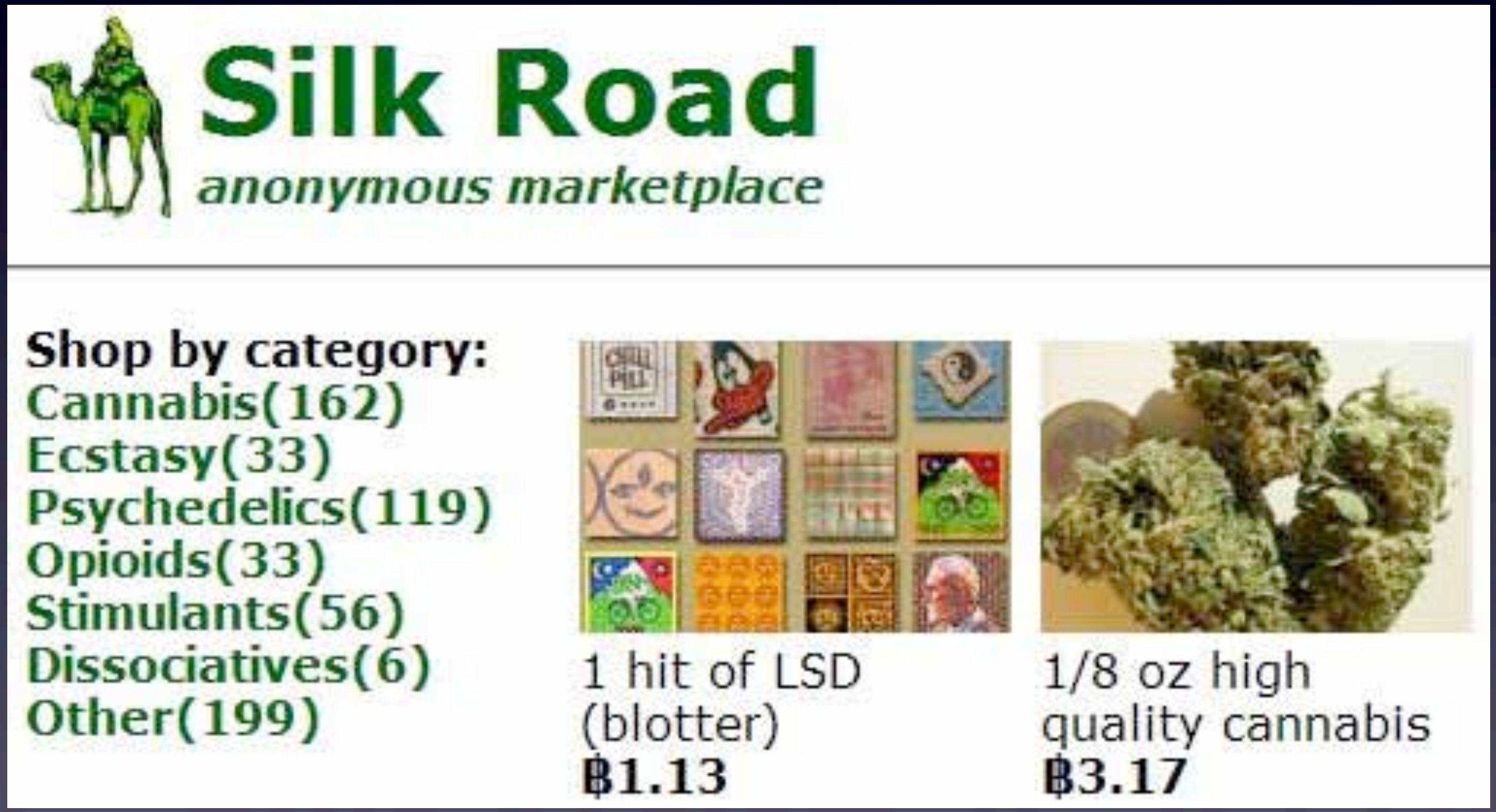
- Harvard Network Registration
- Outgoing Traffic Logs
- Pervasive Surveillance Microcosm
  - Corporate Parallels
- Moral:
  - Bridge Relays
  - Traffic Analysis Preparation

TransUnion

EQUIFAX

Experian

Case Study: Silk Road/DPR



Silk Road

anonymous marketplace

Shop by category:

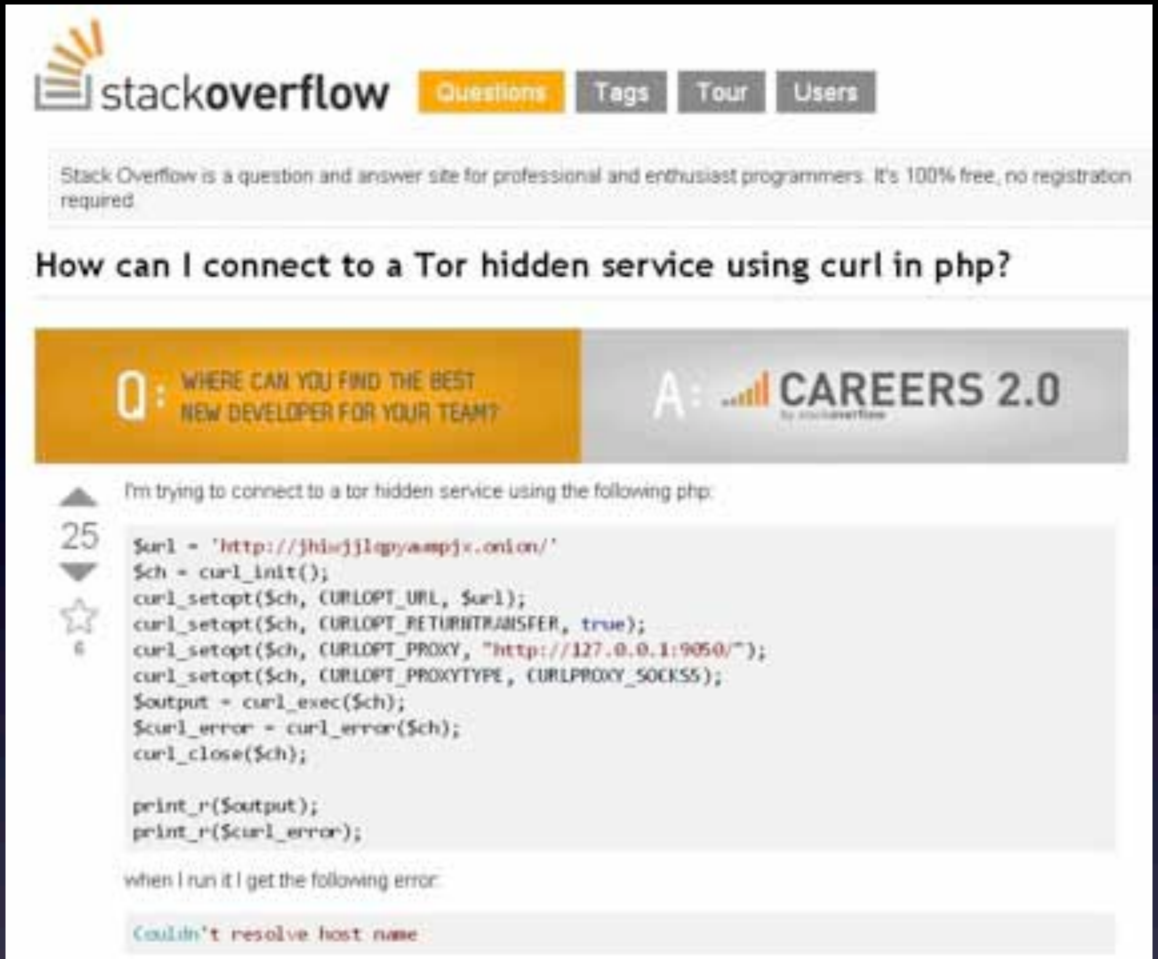
Cannabis(162)
Ecstasy(33)
Psychedelics(119)
Opioids(33)
Stimulants(56)
Dissociatives(6)
Other(199)

1 hit of LSD (blotter)
฿1.13

1/8 oz high quality cannabis
฿3.17

THIS HIDDEN SITE HAS BEEN SEIZE
by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administra

What Messed It Up?



Stack Overflow is a question and answer site for professional and enthusiast programmers. It's 100% free, no registration required.

How can I connect to a Tor hidden service using curl in php?

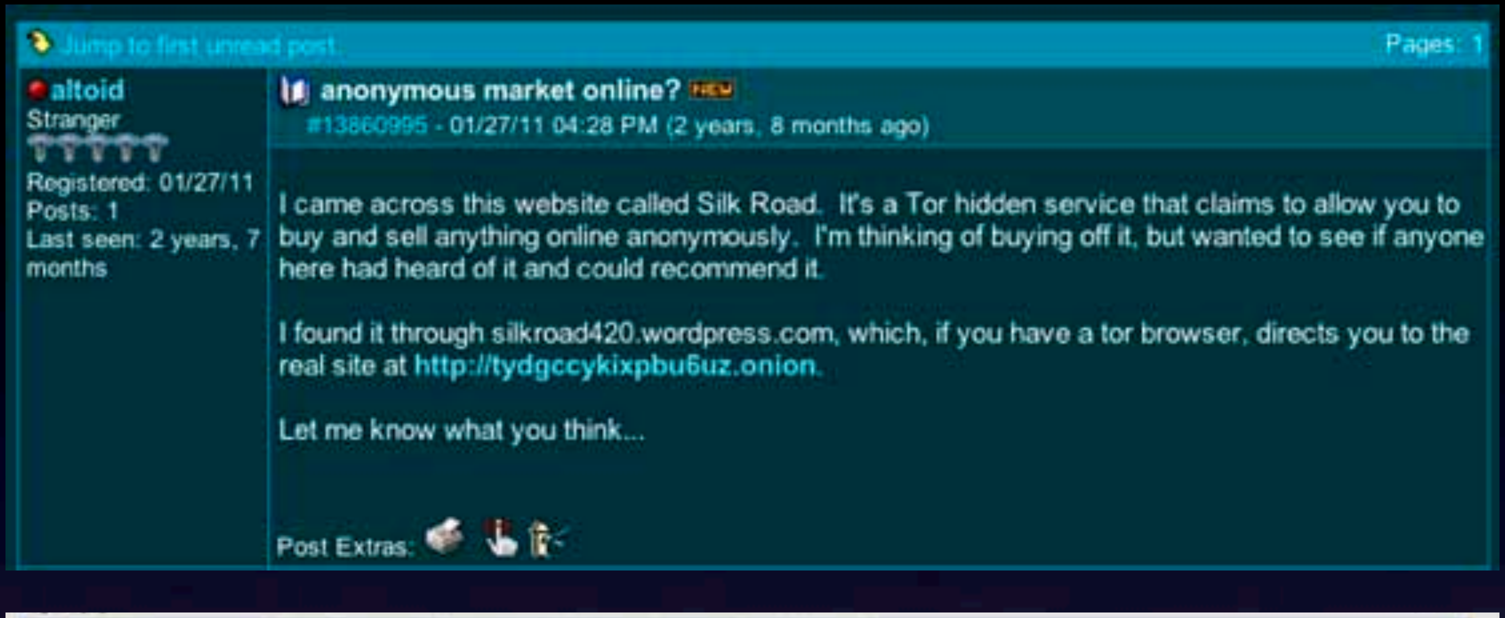
I'm trying to connect to a tor hidden service using the following php:

```
$url = 'http://jhiwjjlqpyawmpjx.onion/'
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $url);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_PROXY, "http://127.0.0.1:9050/");
curl_setopt($ch, CURLOPT_PROXYTYPE, CURLPROXY_SOCKS5);
$output = curl_exec($ch);
$curl_error = curl_error($ch);
curl_close($ch);

print_r($output);
print_r($curl_error);
```

when I run it I get the following error:

```
Couldn't resolve host name
```



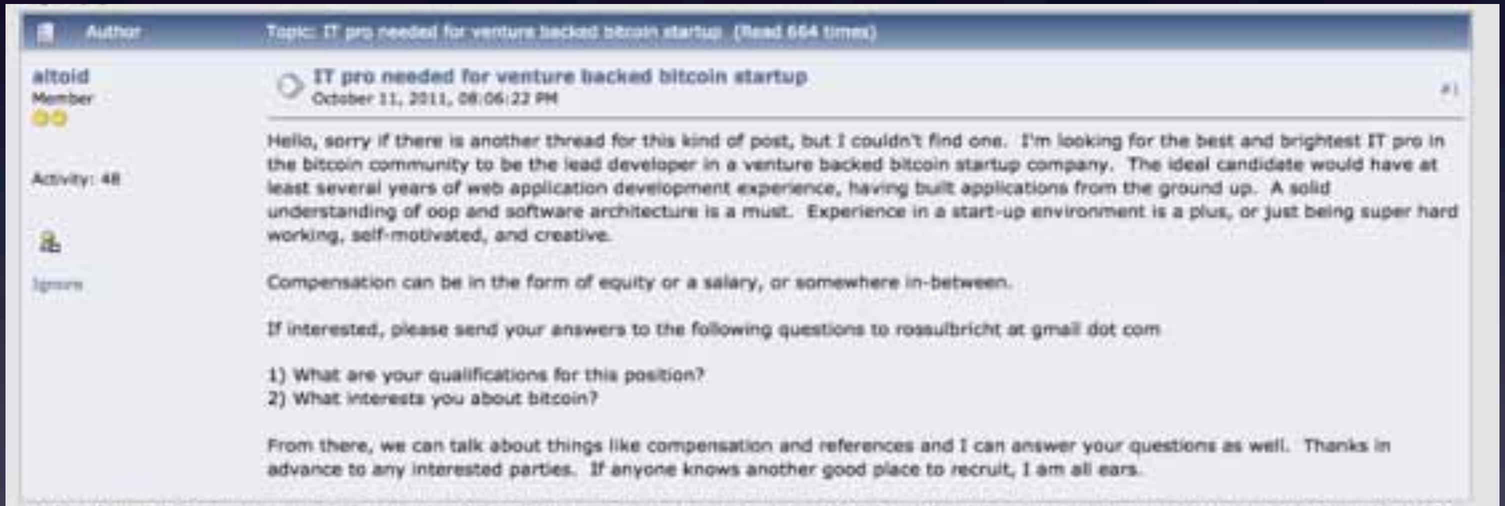
altoid
Stranger
Registered: 01/27/11
Posts: 1
Last seen: 2 years, 7 months

anonymous market online?
#13860995 - 01/27/11 04:28 PM (2 years, 8 months ago)

I came across this website called Silk Road. It's a Tor hidden service that claims to allow you to buy and sell anything online anonymously. I'm thinking of buying off it, but wanted to see if anyone here had heard of it and could recommend it.

I found it through silkroad420.wordpress.com, which, if you have a tor browser, directs you to the real site at http://tydgccykixpbu6uz.onion.

Let me know what you think...


Author
Topic: IT pro needed for venture backed bitcoin startup (Read 664 times)
#1
Ignore

altoid
Member
Activity: 48

IT pro needed for venture backed bitcoin startup
October 11, 2011, 08:06:22 PM

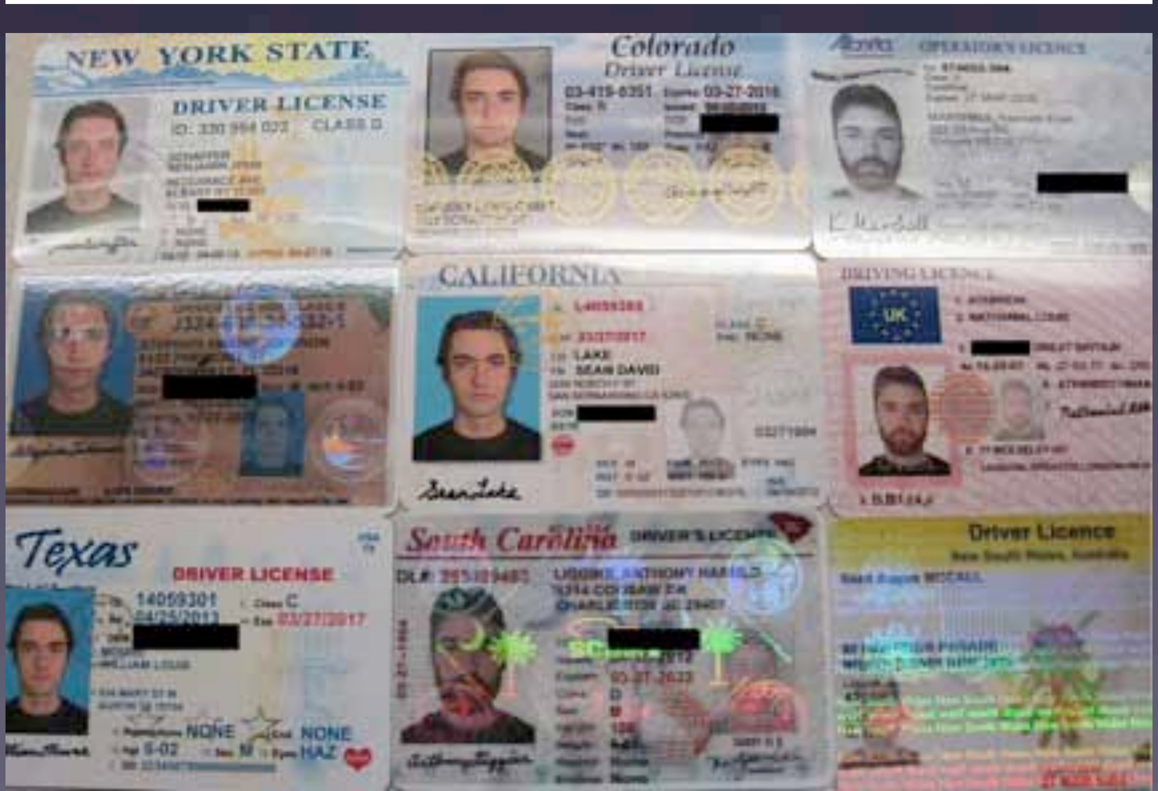
Hello, sorry if there is another thread for this kind of post, but I couldn't find one. I'm looking for the best and brightest IT pro in the bitcoin community to be the lead developer in a venture backed bitcoin startup company. The ideal candidate would have at least several years of web application development experience, having built applications from the ground up. A solid understanding of oop and software architecture is a must. Experience in a start-up environment is a plus, or just being super hard working, self-motivated, and creative.

Compensation can be in the form of equity or a salary, or somewhere in-between.

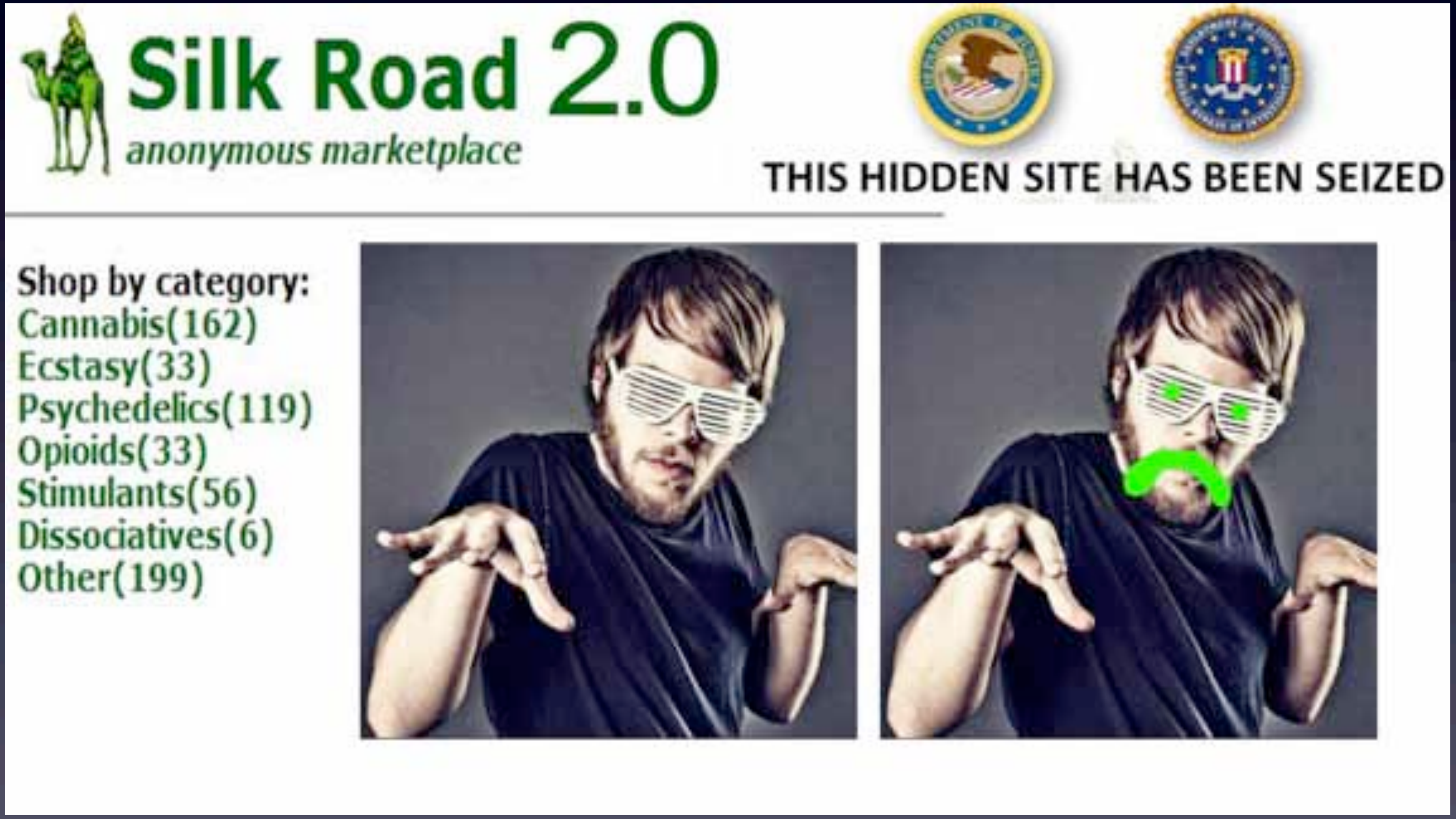
If interested, please send your answers to the following questions to rossulbricht at gmail dot com

1) What are your qualifications for this position?
2) What interests you about bitcoin?

From there, we can talk about things like compensation and references and I can answer your questions as well. Thanks in advance to any interested parties. If anyone knows another good place to recruit, I am all ears.



Case Study: Operation Onymous



Silk Road 2.0

anonymous marketplace

THIS HIDDEN SITE HAS BEEN SEIZED

Shop by category:

Cannabis(162)

Ecstasy(33)

Psychedelics(119)

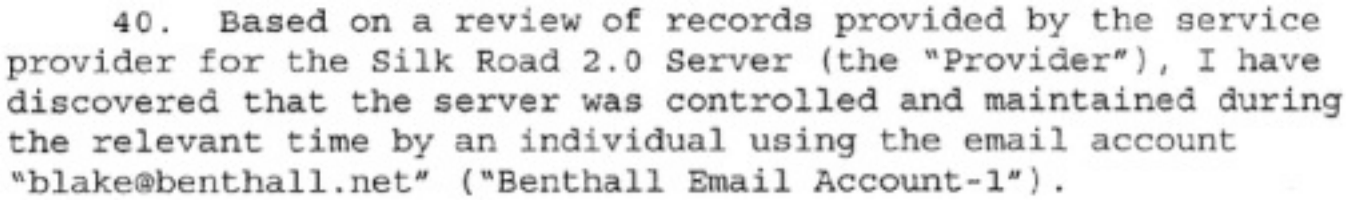
Opioids(33)

Stimulants(56)

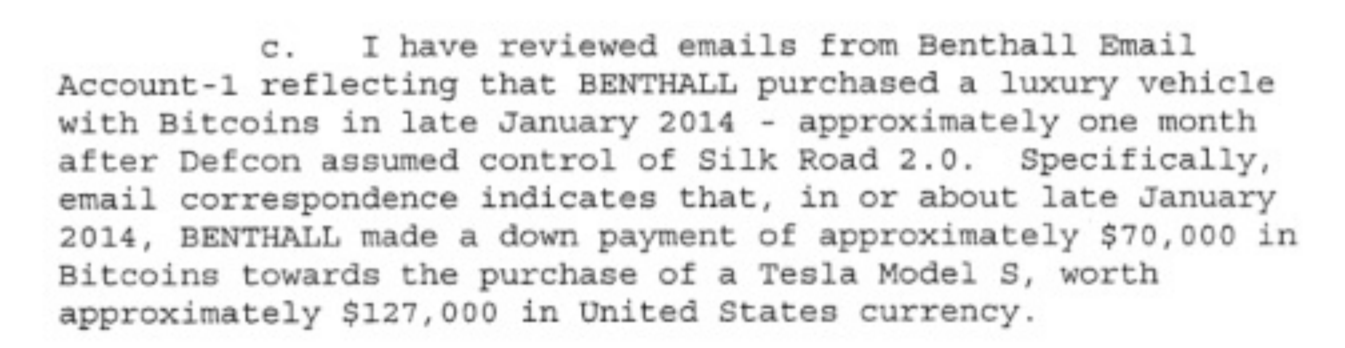
Dissociatives(6)

Other(199)

What Messed It Up?

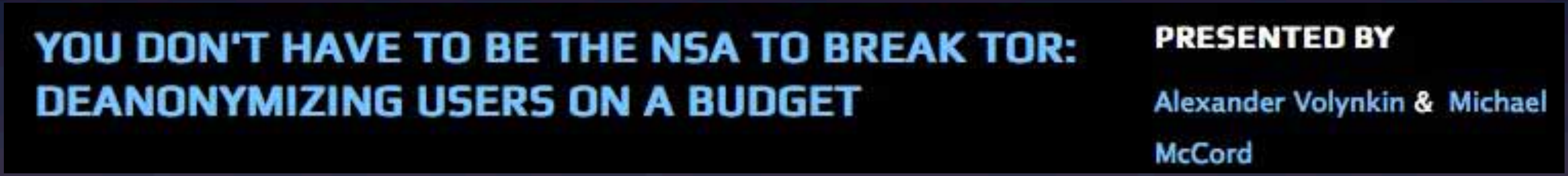


40. Based on a review of records provided by the service provider for the Silk Road 2.0 Server (the "Provider"), I have discovered that the server was controlled and maintained during the relevant time by an individual using the email account "blake@benthall.net" ("Benthall Email Account-1").



c. I have reviewed emails from Benthall Email Account-1 reflecting that BENTHALL purchased a luxury vehicle with Bitcoins in late January 2014 - approximately one month after Defcon assumed control of Silk Road 2.0. Specifically, email correspondence indicates that, in or about late January 2014, BENTHALL made a down payment of approximately $70,000 in Bitcoins towards the purchase of a Tesla Model S, worth approximately $127,000 in United States currency.

black hat USA 2014



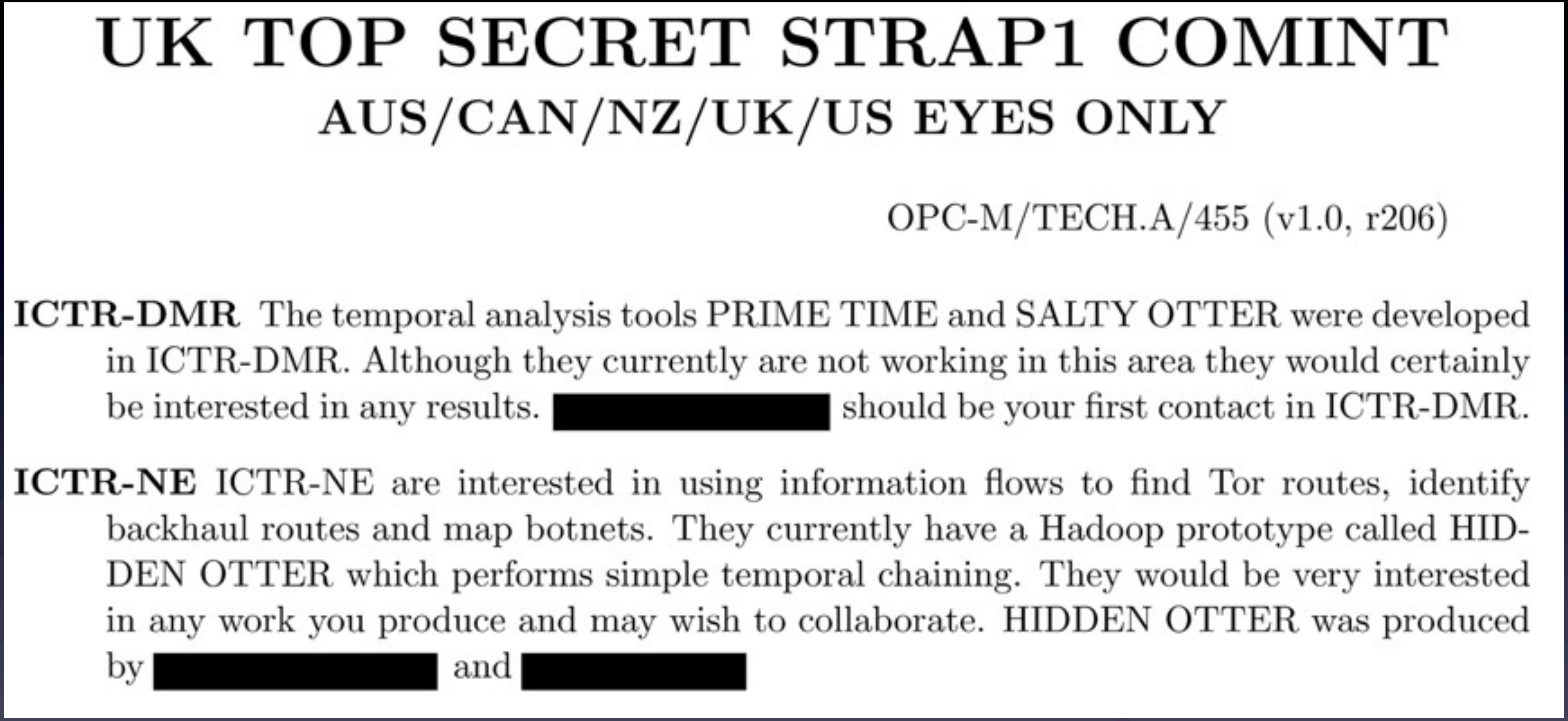
YOU DON'T HAVE TO BE THE NSA TO BREAK TOR: DEANONYMIZING USERS ON A BUDGET

PRESENTED BY

Alexander Volynkin & Michael McCord

- Attacking relays active January 30 – July 4
- Stained Tor protocol headers
  - Allows retroactive deanonymization
- Waited to get HSDir & Entry Guard flags
  - Injected covert message between them to deanonymize HSs
- Fixed July 2014

Low Latency Is A Compromise



UK TOP SECRET STRAP1 COMINT

AUS/CAN/NZ/UK/US EYES ONLY

OPC-M/TECH.A/455 (v1.0, r206)

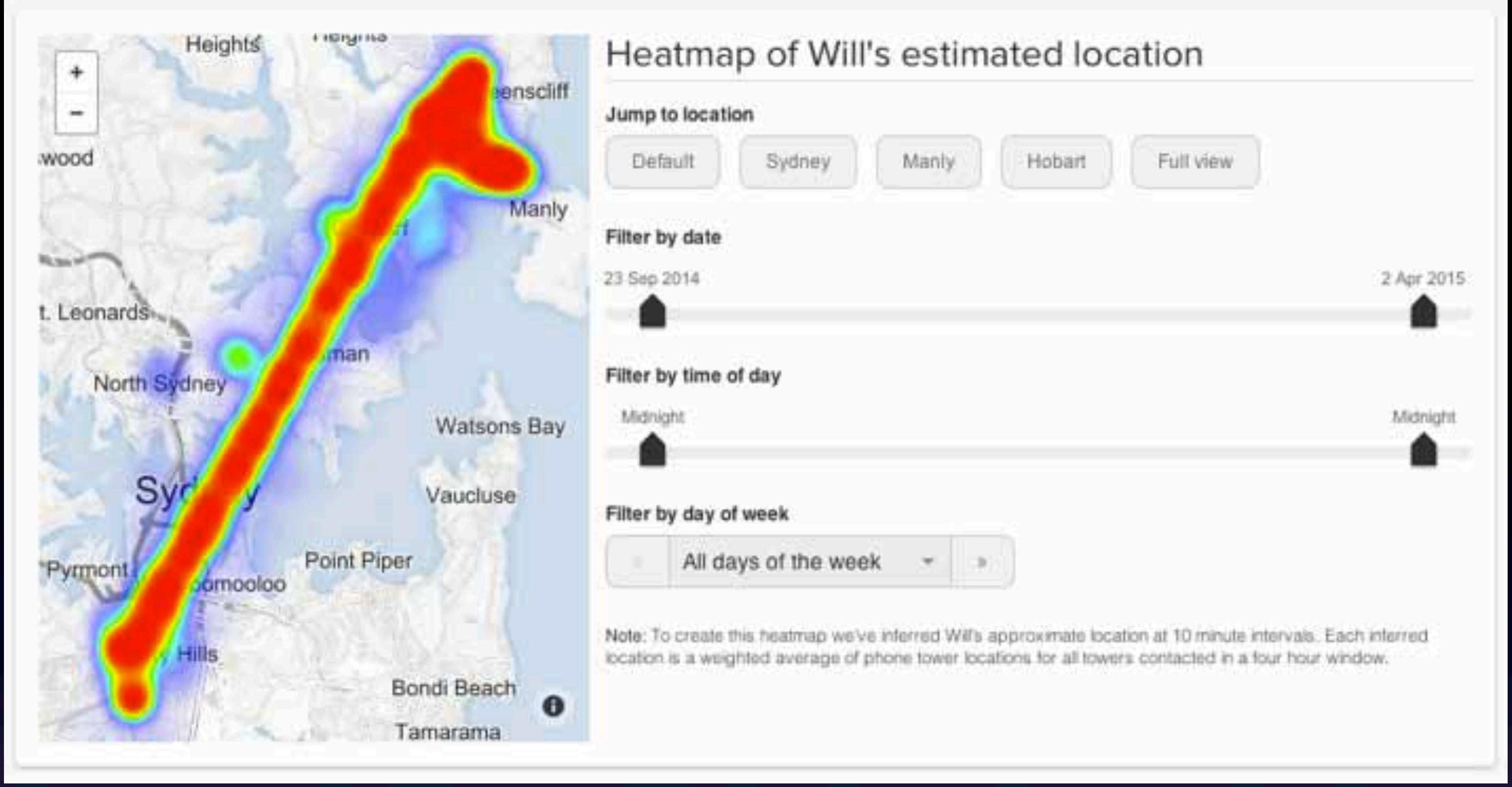
ICTR-DMR The temporal analysis tools PRIME TIME and SALTY OTTER were developed in ICTR-DMR. Although they currently are not working in this area they would certainly be interested in any results. [redacted] should be your first contact in ICTR-DMR.

ICTR-NE ICTR-NE are interested in using information flows to find Tor routes, identify backhaul routes and map botnets. They currently have a Hadoop prototype called HIDDEN OTTER which performs simple temporal chaining. They would be very interested in any work you produce and may wish to collaborate. HIDDEN OTTER was produced by [redacted] and [redacted]

- Timing/Traffic Correlation attacks and temporal graph methods will always be possible
- Plan accordingly

Living With Your Personal Snitch

- How Does Your Phone Betray You? Let Me Count The Ways...
  - Metadata
  - Location
  - Contacts
  - Networks
  - Unique Identifiers
  - Cookies
  - Searches
  - Weak Crypto
  - Repeated Access
  - Autoconnect (Pineapple's BFF)
  - Apps
  - Pattern Of Life



Heatmap of Will's estimated location

Jump to location

Default | Sydney | Manly | Hobart | Full view

Filter by date

23 Sep 2014 — 2 Apr 2015

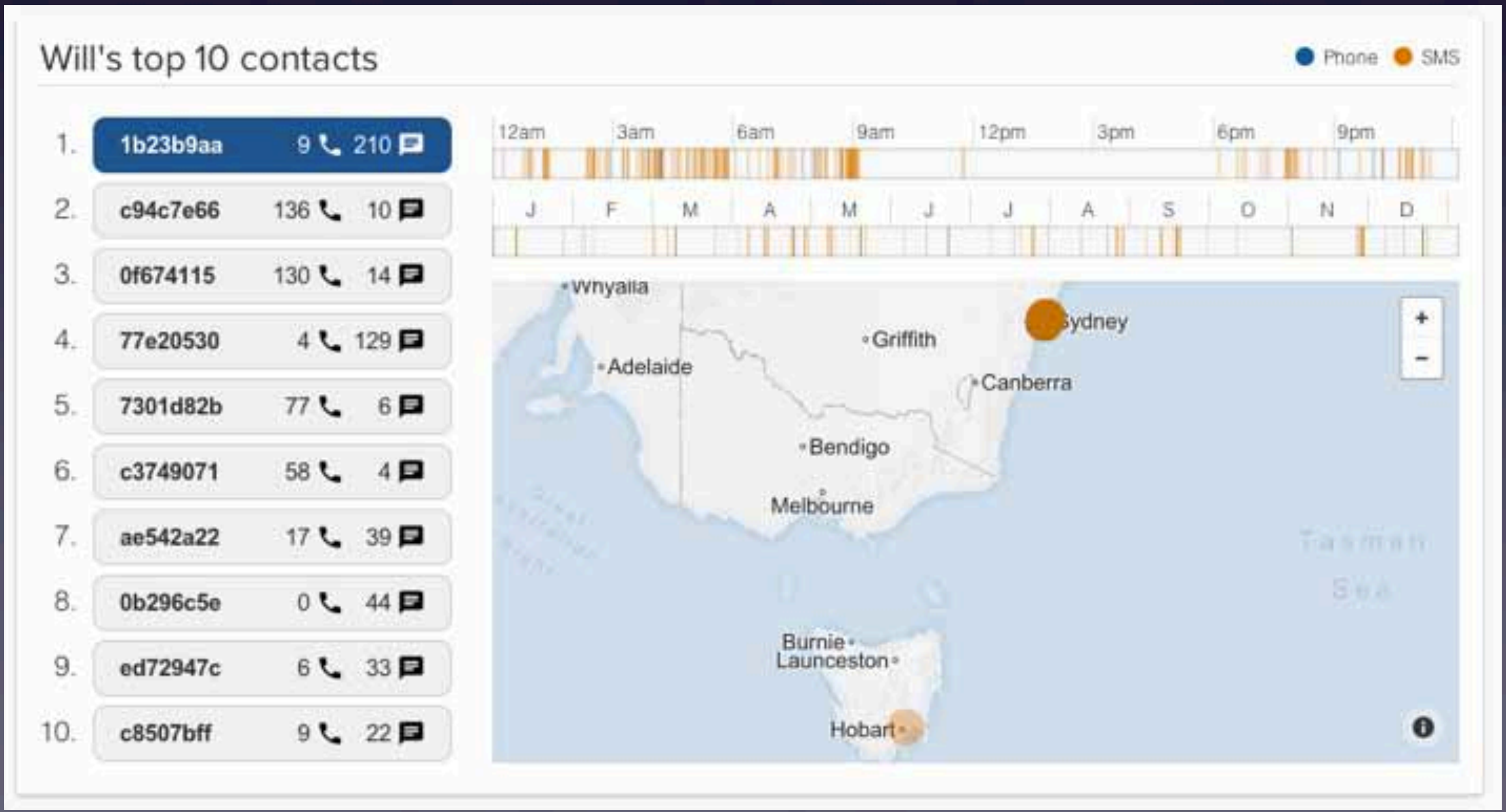
Filter by time of day

Midnight — Midnight

Filter by day of week

All days of the week

Note: To create this heatmap we've inferred Will's approximate location at 10 minute intervals. Each inferred location is a weighted average of phone tower locations for all towers contacted in a four hour window.



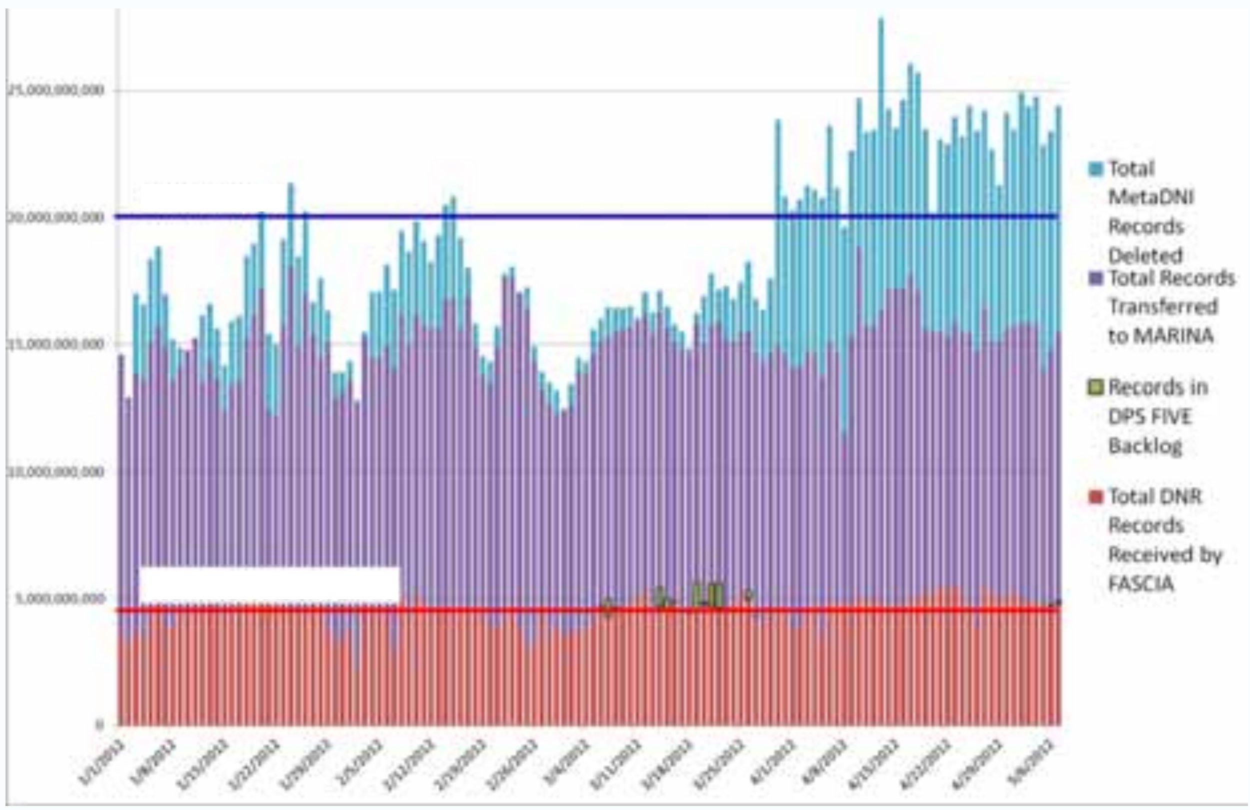
Will's top 10 contacts

● Phone ● SMS

		☎	SMS
1.	1b23b9aa	9	210
2.	c94c7e66	136	10
3.	0f674115	130	14
4.	77e20530	4	129
5.	7301d82b	77	6
6.	c3749071	58	4
7.	ae542a22	17	39
8.	0b296c5e	0	44
9.	ed72947c	6	33
10.	c8507bff	9	22

TOP SECRET//COMINT//REL TO USA, FVEY

Example of Current Volumes and Limits



TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

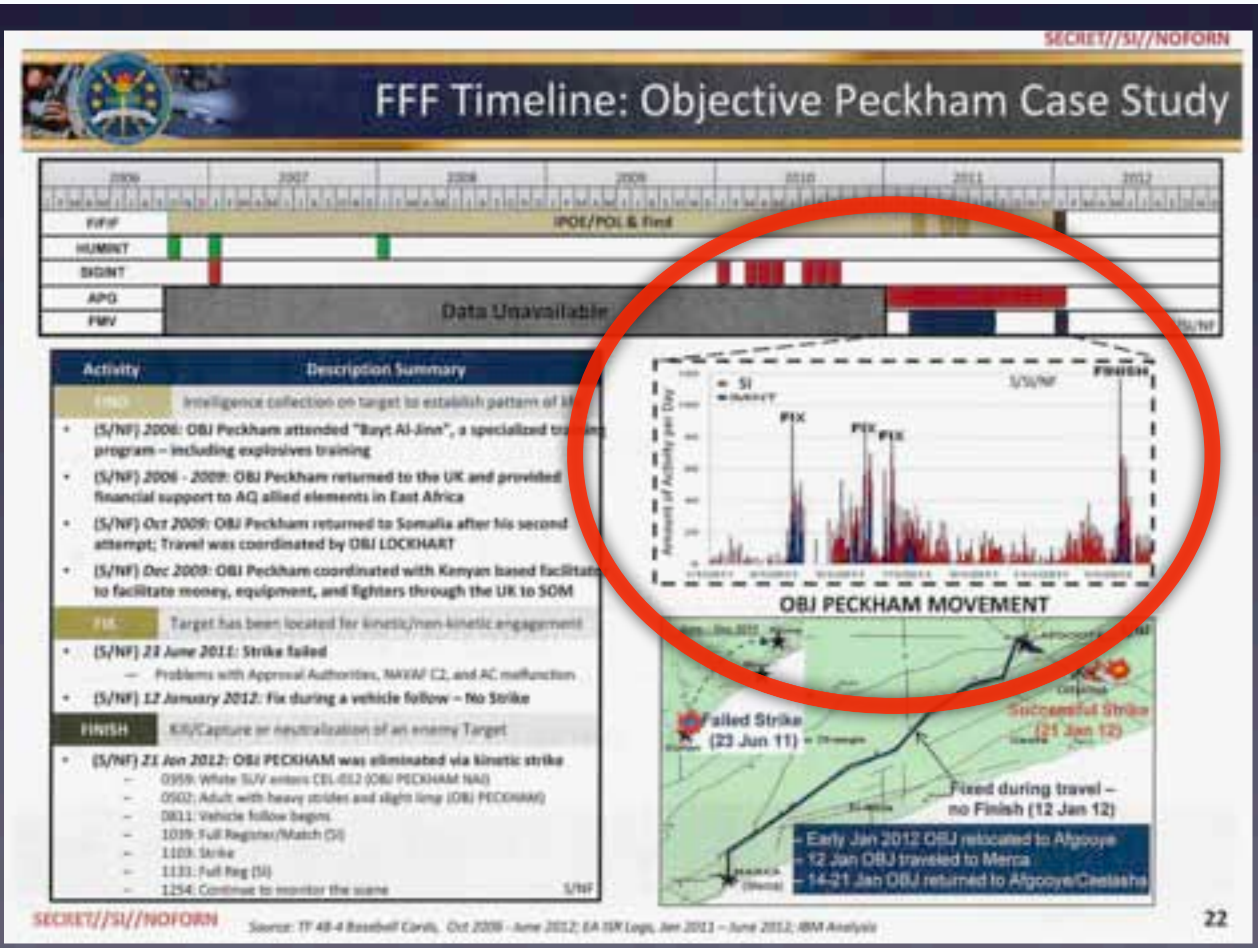
Dupe Methodology

Compare records within various time windows that share identical selectors and locations, specifically:

LAC	CellID	VLR	DesigChannelID
IMEI	ESN	IMSI	MIN
TMSI	MDN	CLI	ODN
MSISDN	RegFMID	CdFMID	CgFMID
RegGID	CdGID	RegIID	Kc
CdIID	CgIID	MSRN	Rand
Sres	Opcode	RQ1	XR1
Q_CK1	Q_IK1	AU1	NewPTMSI
OSME	DSME	RTMSI	PDP_Address
TEID	TLLI	PTMSI	PDDG

TOP SECRET//COMINT//REL TO USA, FVEY

“We kill people based on metadata.”
--NSA/CIA Director Michael Hayden



SECRET//SI//NOFORN

FFF Timeline: Objective Peckham Case Study

2006
2007
2008
2009
2010
2011
2012
F/F/F
HUMINT
SIGINT
APG
FMV
IPOE/POL & Find
Data Unavailable
S//NF

Activity	Description Summary
FIND	Intelligence collection on target to establish pattern of li

- (S/NF) *2006*: OBJ Peckham attended "Bayt Al-Jinn", a specialized training program – including explosives training
- (S/NF) *2006 - 2009*: OBJ Peckham returned to the UK and provided financial support to AQ allied elements in East Africa
- (S/NF) *Oct 2009*: OBJ Peckham returned to Somalia after his second attempt; Travel was coordinated by OBJ LOCKHART
- (S/NF) *Dec 2009*: OBJ Peckham coordinated with Kenyan based facilitat to facilitate money, equipment, and fighters through the UK to SOM

FIX	Target has been located for kinetic/non-kinetic engagement

- (S/NF) *23 June 2011*: Strike failed
  - Problems with Approval Authorities, NAVAF C2, and AC malfunction
- (S/NF) *12 January 2012*: Fix during a vehicle follow – No Strike

FINISH	Kill/Capture or neutralization of an enemy Target

- (S/NF) *21 Jan 2012*: OBJ PECKHAM was eliminated via kinetic strike
  - 0359: White SUV enters CEL-012 (OBJ PECKHAM NAI)
  - 0502: Adult with heavy strides and slight limp (OBJ PECKHAM)
  - 0811: Vehicle follow begins
  - 1039: Full Register/Match (SI)
  - 1103: Strike
  - 1131: Full Reg (SI)
  - 1254: Continue to monitor the scene

S/NF

OBJ PECKHAM MOVEMENT

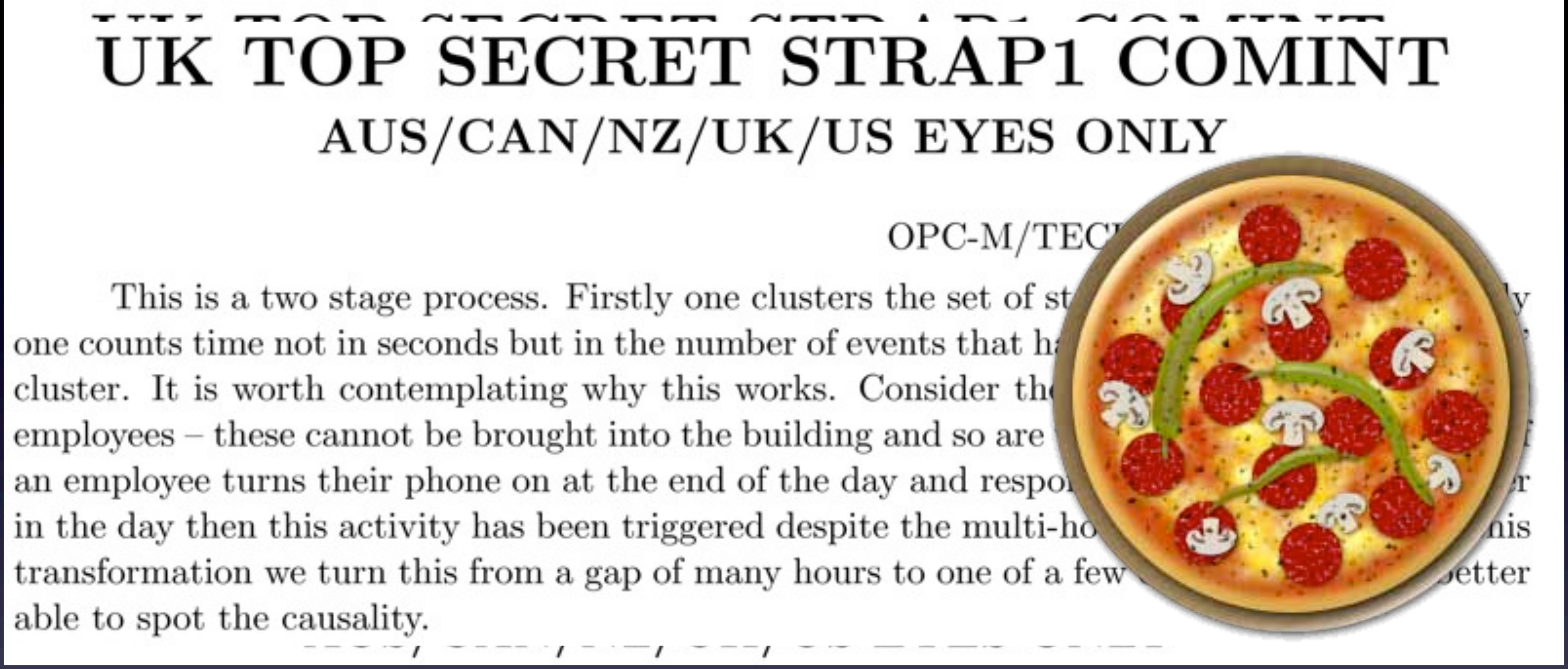
Afgooye
Failed Strike (23 Jun 11)
Successful Strike (21 Jan 12)
Fixed during travel – no Finish (12 Jan 12)
MARKA (Merca)

- Early Jan 2012 OBJ relocated to Afgooye
- 12 Jan OBJ traveled to Merca
- 14-21 Jan OBJ returned to Afgooye/Ceelasha

SECRET//SI//NOFORN

Source: TF 48-4 Baseball Cards, Oct 2009 – June 2012; EA ISR Logs, Jan 2011 – June 2012; IBM Analysis

From Phone To Target



UK TOP SECRET STRAP1 COMINT

AUS/CAN/NZ/UK/US EYES ONLY

OPC-M/TEC

This is a two stage process. Firstly one clusters the set of st y
one counts time not in seconds but in the number of events that h
cluster. It is worth contemplating why this works. Consider th
employees – these cannot be brought into the building and so are
an employee turns their phone on at the end of the day and respo r
in the day then this activity has been triggered despite the multi-ho his
transformation we turn this from a gap of many hours to one of a few etter
able to spot the causality.

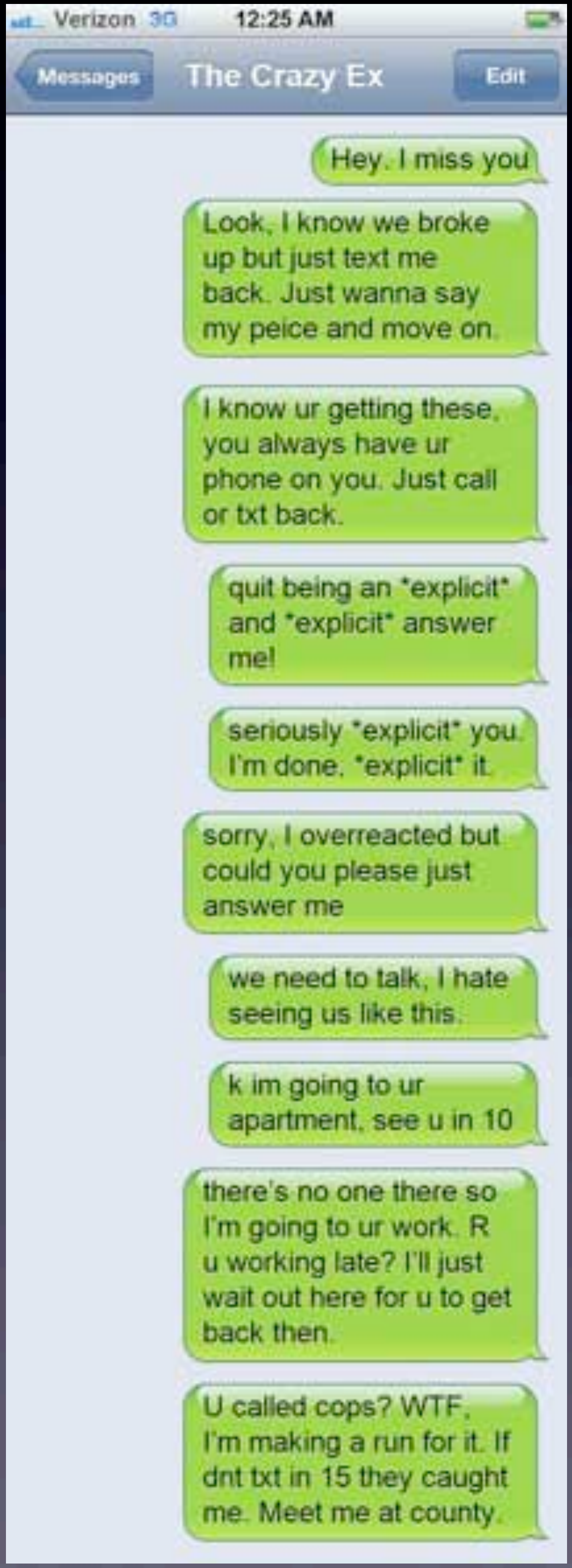
- Network analysis:
  - Beware closed loops
  - Falsify network without "pizza nodes"
- Metadata analysis is primarily temporal
  - Manage latency and apparent causality

Phone Alternative

- Unavoidable phone compromises:
  - Cell tower tracking
  - IMSI catcher interception
  - Baseband/SIM vulns
- iPod Touch:
  - No Android
  - Turn off iCloud backup
  - Comms:
    - VPN
    - Signal (Redphone/TextSecure)
    - ChatSecure/Tor (experimental), Wickr

Messaging

- After All These Years, E-Mail Still Sucks
  - Spam Fighting Aids Tracking
  - Non-TLS Mail Still Abounds
  - Link Encryption Only, Weak Server-Side Storage
  - End-to-end Encrypted Content Not Metadata
  - Insecure Client-Side Logging
  - Bad Retention Habits
  - Google
- Psycho Ex Principle



Hey. I miss you

Look, I know we broke up but just text me back. Just wanna say my peice and move on.

I know ur getting these, you always have ur phone on you. Just call or txt back.

quit being an *explicit* and *explicit* answer me!

seriously *explicit* you. I'm done. *explicit* it.

sorry, I overreacted but could you please just answer me

we need to talk, I hate seeing us like this.

k im going to ur apartment, see u in 10

there's no one there so I'm going to ur work. R u working late? I'll just wait out here for u to get back then.

U called cops? WTF. I'm making a run for it. If dnt txt in 15 they caught me. Meet me at county.

Secure Messaging Alternatives

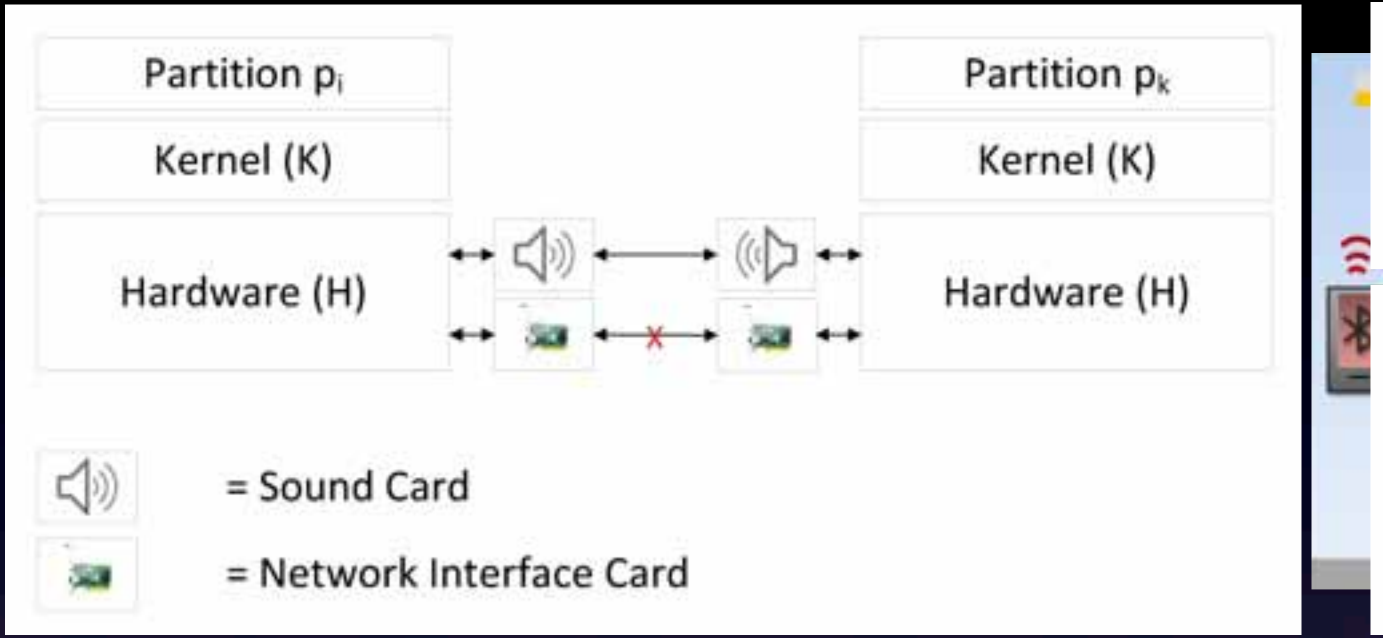
- OTR Jabber
- Ricochet
- Cryptocat
- Bitmessage
- Retroshare
- We Need More:
  - Auditing
  - Steganography

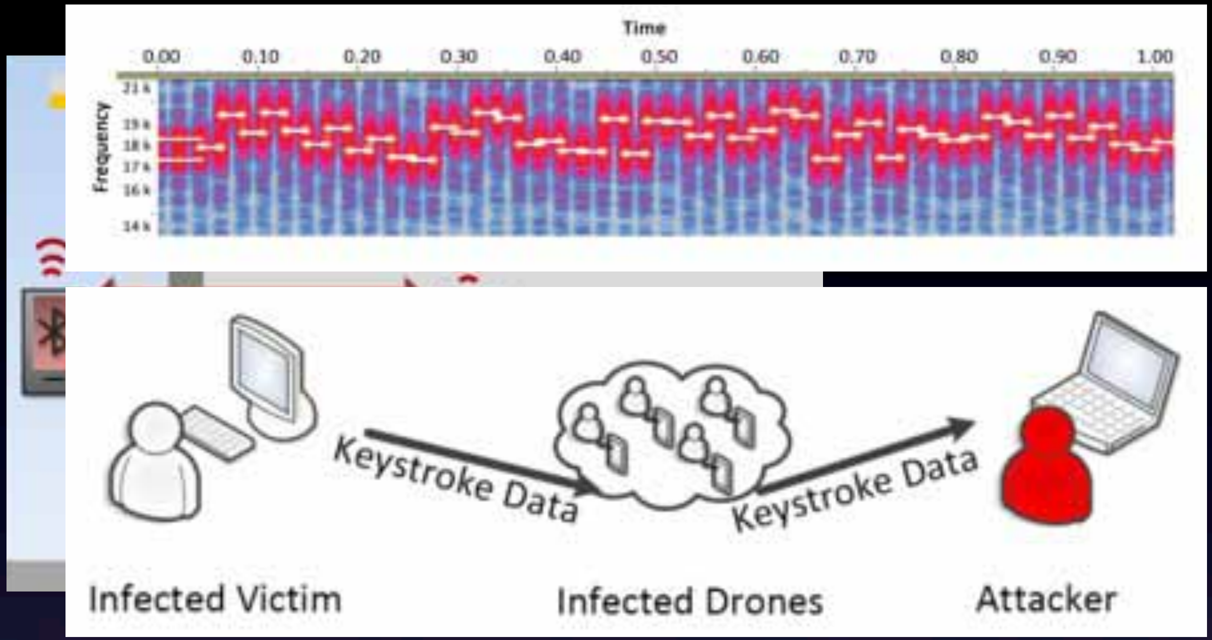
So what if I’m a glasshole? You are too.

Stylometrics

- Resist Providing A Corpus
- Obfuscate
  - Machine Translate
- Imitate
- Alpha Tools: JStylo/Anonymouth

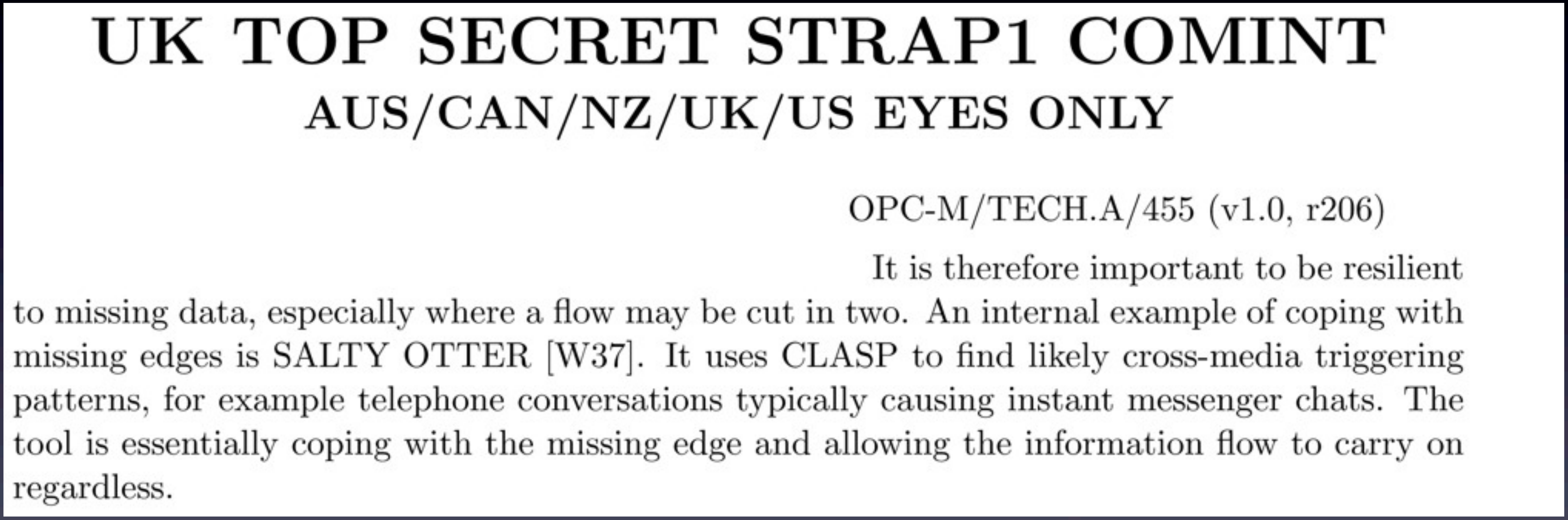
Spy Malware Goes Mainstream





Hanspach & Goetz: *On Covert Acoustical Mesh Networks In Air*, 2013

- 2010: Acoustic airgap-jumping malware theorized
- 2012: Flame state-sponsored espionage malware identified, jumps airgap with Bluetooth
- 2013: Fraunhofer demonstrates POC of covert acoustical mesh networks
  - Including acoustical multi-hop keylogger
- 2014: SilverPush develops ultrasonic "audio beacons" embedded in ads to enable cross-device tracking



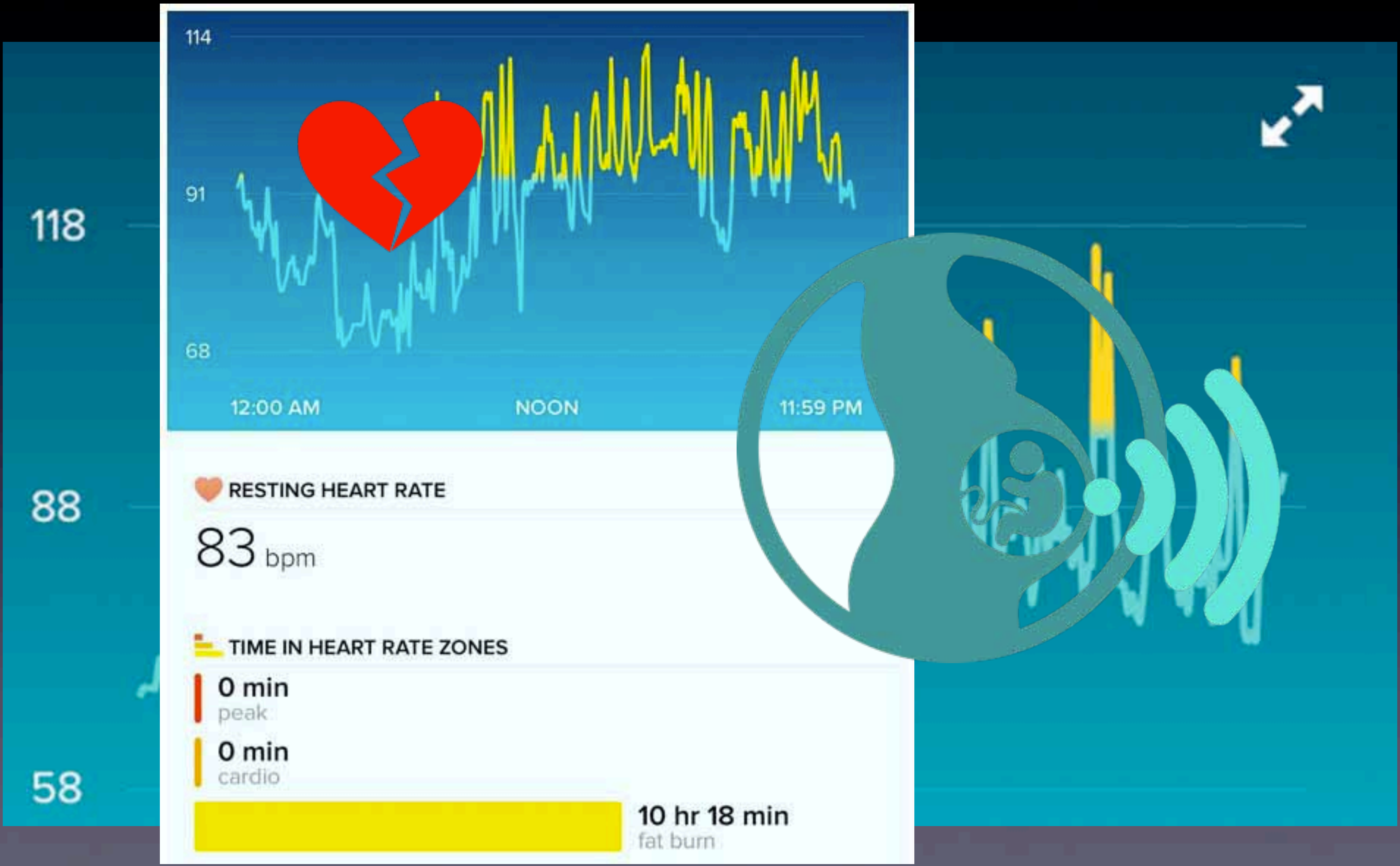
UK TOP SECRET STRAP1 COMINT

AUS/CAN/NZ/UK/US EYES ONLY

OPC-M/TECH.A/455 (v1.0, r206)

It is therefore important to be resilient to missing data, especially where a flow may be cut in two. An internal example of coping with missing edges is SALTY OTTER [W37]. It uses CLASP to find likely cross-media triggering patterns, for example telephone conversations typically causing instant messenger chats. The tool is essentially coping with the missing edge and allowing the information flow to carry on regardless.

Beware New Data Sources



RESTING HEART RATE

83 bpm

TIME IN HEART RATE ZONES

0 min
peak

0 min
cardio

10 hr 18 min
fat burn

Digital surveillance is a public-private partnership

OPSEC is 24/7