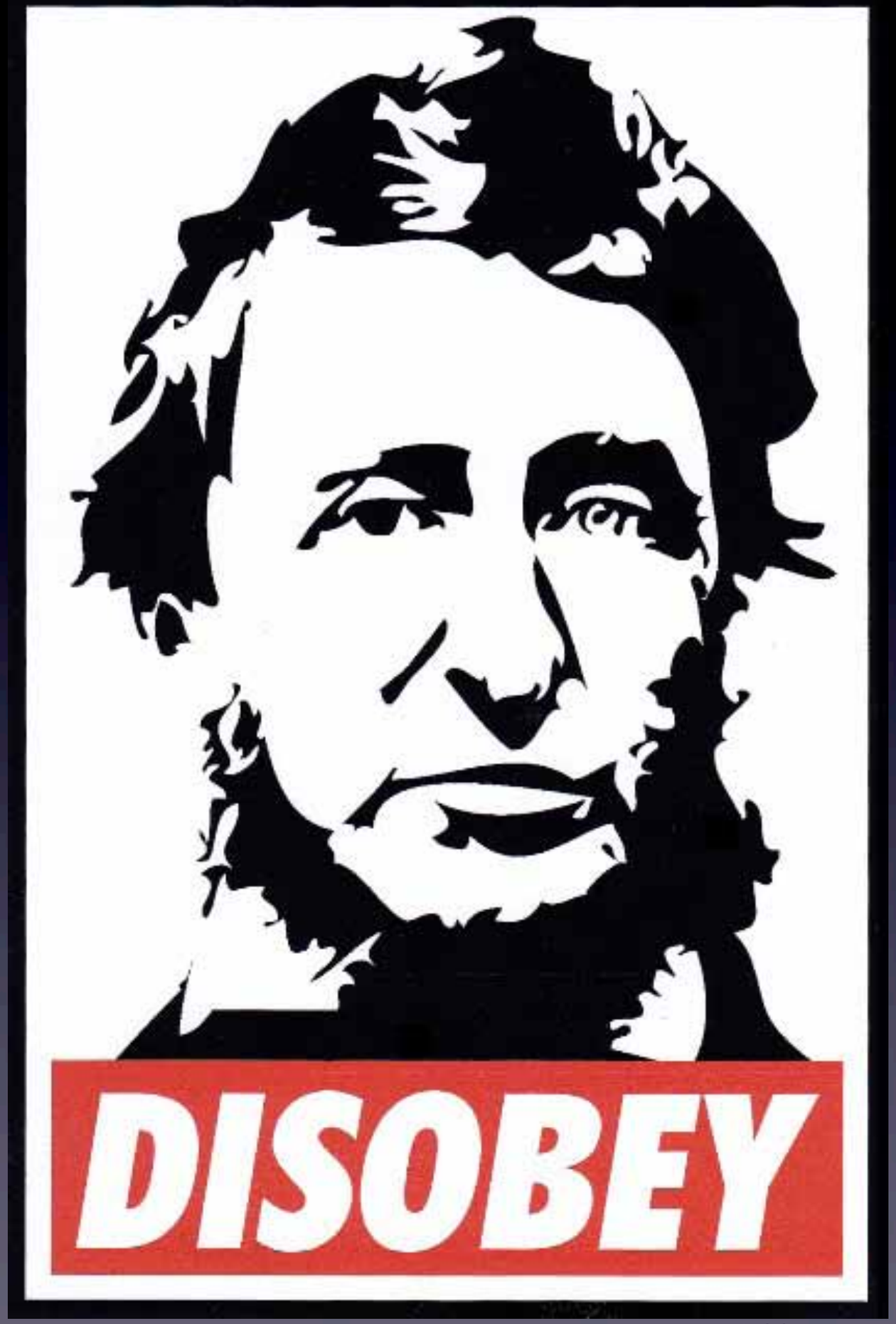
Don’t Fuck It Up!

Zoz

DISOBEY



jackdawsart.com

Unjust laws exist: shall we be content to obey them, or shall we endeavor to amend them, and obey them until we have succeeded, or shall we transgress them at once?

—Henry David Thoreau, *Civil Disobedience*

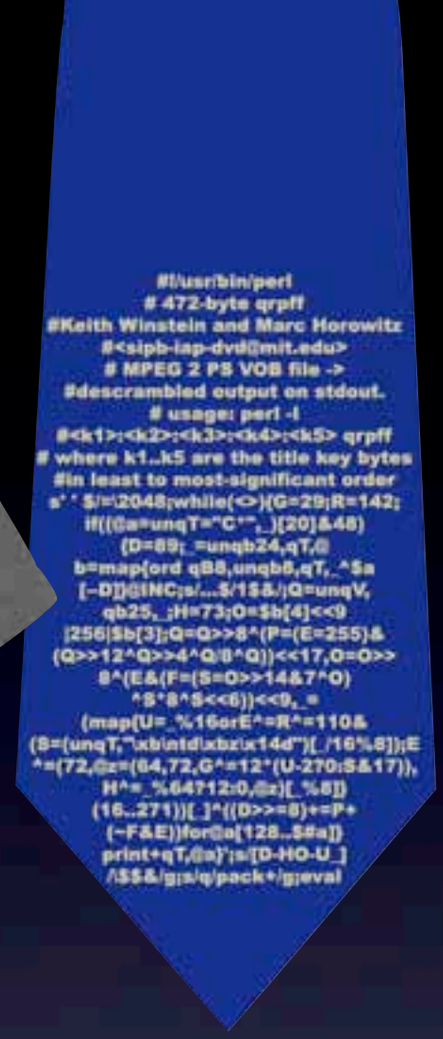
DVDlogo.c

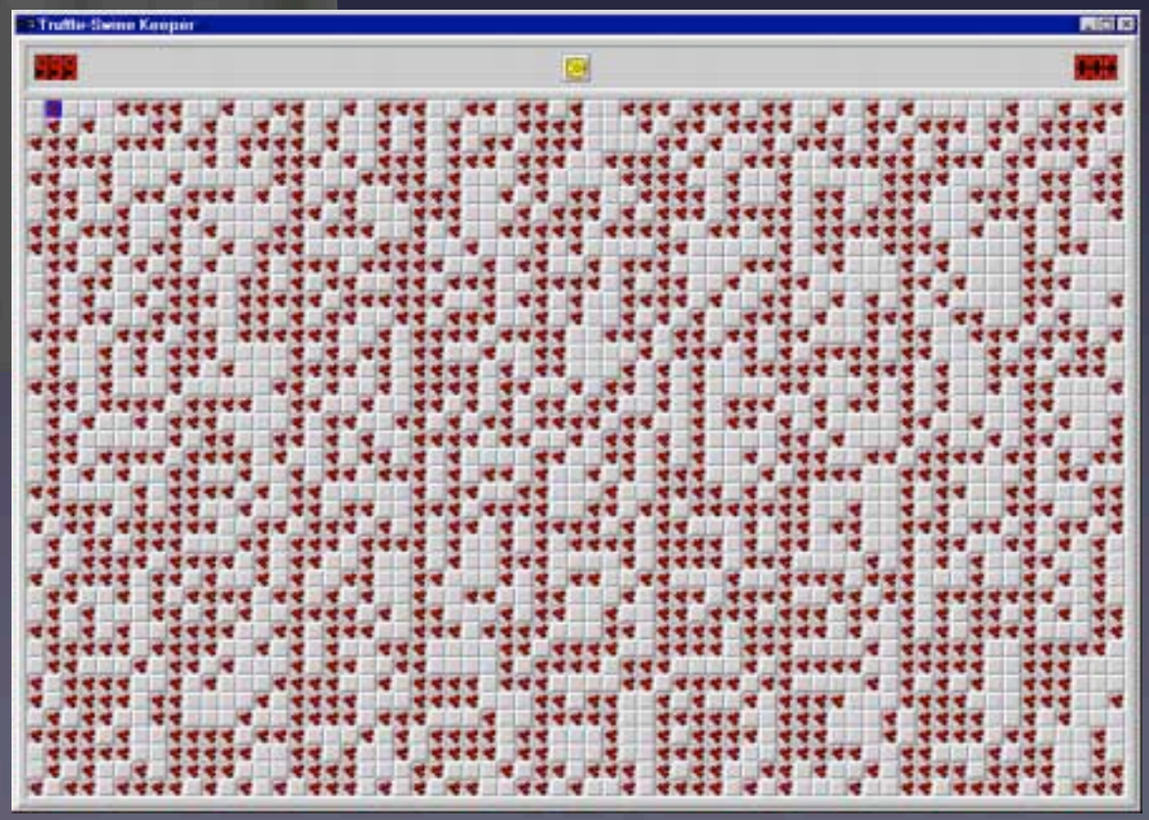
```
/*      efdtt.c     Author:  Charles M. Hannum <root@ihack.net>                */
/*                                                                             */
/*      Thanks to Phil Carmody <fatphil@asdf.org> for additional tweaks.       */
/*                                                                             */
/*      DVD-logo shaped version by Alex Bowley <alex@hyperspeed.org>           */
/*                                                                             */
/*      Usage is:  cat title-key scrambled.vob | efdtt >clear.vob              */

#define m(i)(x[i]^s[i+84])<<

                unsigned char x[5]      ,y,s[2048];main(
                n){for( read(0,x,5     );read(0,s ,n=2048
                      ); write(1   ,s,n)          )if(s
               [y=s      [13]%8+20]  /16%4  --1      ){int
               i=m(      1)17  ^256 +m(0)   8,k      =m(2)
               0,j=      m(4)   17^ m(3)   9^k*     2-k%8
               ^8,s      =0,c    =26;for   (s[y]    --16;
              --c;j  *=2)s=     s*2^i&    1,i=i /2^j&1
              <<24;for(j=        127;     ++j<n;c=c>
                                 y)
                                 c

                    +=y=i^i/8^i>>4^i>>12,
                  i=i>>8^y<<17,s^=s>>14,y=s^s*8^s<<6,s=s
                >>8^y<<9,k=s[j],k                ="7No-'C_\216"[k
                &7]+2^"cr3sfw6v;*k+>/n."[k>>4]*2^k*257/
                     8,s[j]=k^(k&k*2&34)*6^c+-y
                                 ;}}
```





SpyEye Builder v1.3.34 [ ]

Spy Eye v1.3

Encryption key *(for config)*: smthrandomkey timestamp: 0xD66CD983

Clear cookies every startup *(IE, FF)*:
Delete non-exportable certificates:
Don't send http-reports:

Anti-Rapport:
FF webinjects:
Opera formgrabber:
Chrome formgrabber:

Compress build by **UPX v3.07w**:

Make build without **ZLIB** support
*(SpyEye may use zlib for unpacking gzip or deflate content at **FF** webinjects ... so, this option can save 15-16 KB)*:

Make **LITE**-config
(without webinjects, plugins & screenshots):

• EXE name : Recycle.Bin

• Mutex name : SystemService

Make config & get build


WITH LOVE FROM FELLO
GOAT LOVERS
419eater.com


HANDS OFF
MY INTERNET?
THE INTERNET
TOOL OF THE PEOPLE
DO YOU REALLY WANT
YOUR GOVERNMENT
TO CONTROL IT?


WHEN YOU DOWNLOAD
INTERNET PORN.
YOU'RE JERKING
OFF WITH HITLER!
Kosmetiktücher

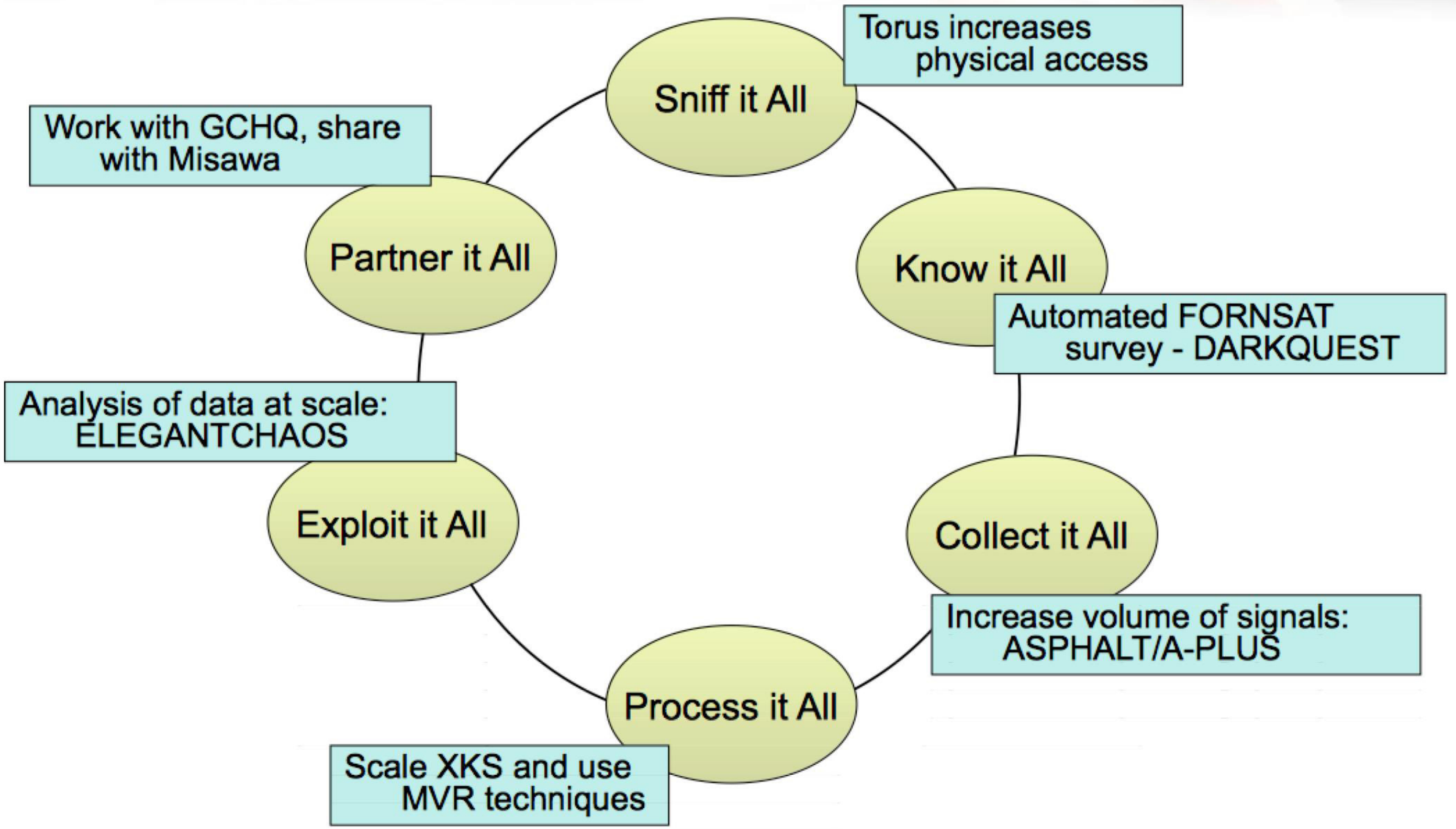

FUCK IT UP

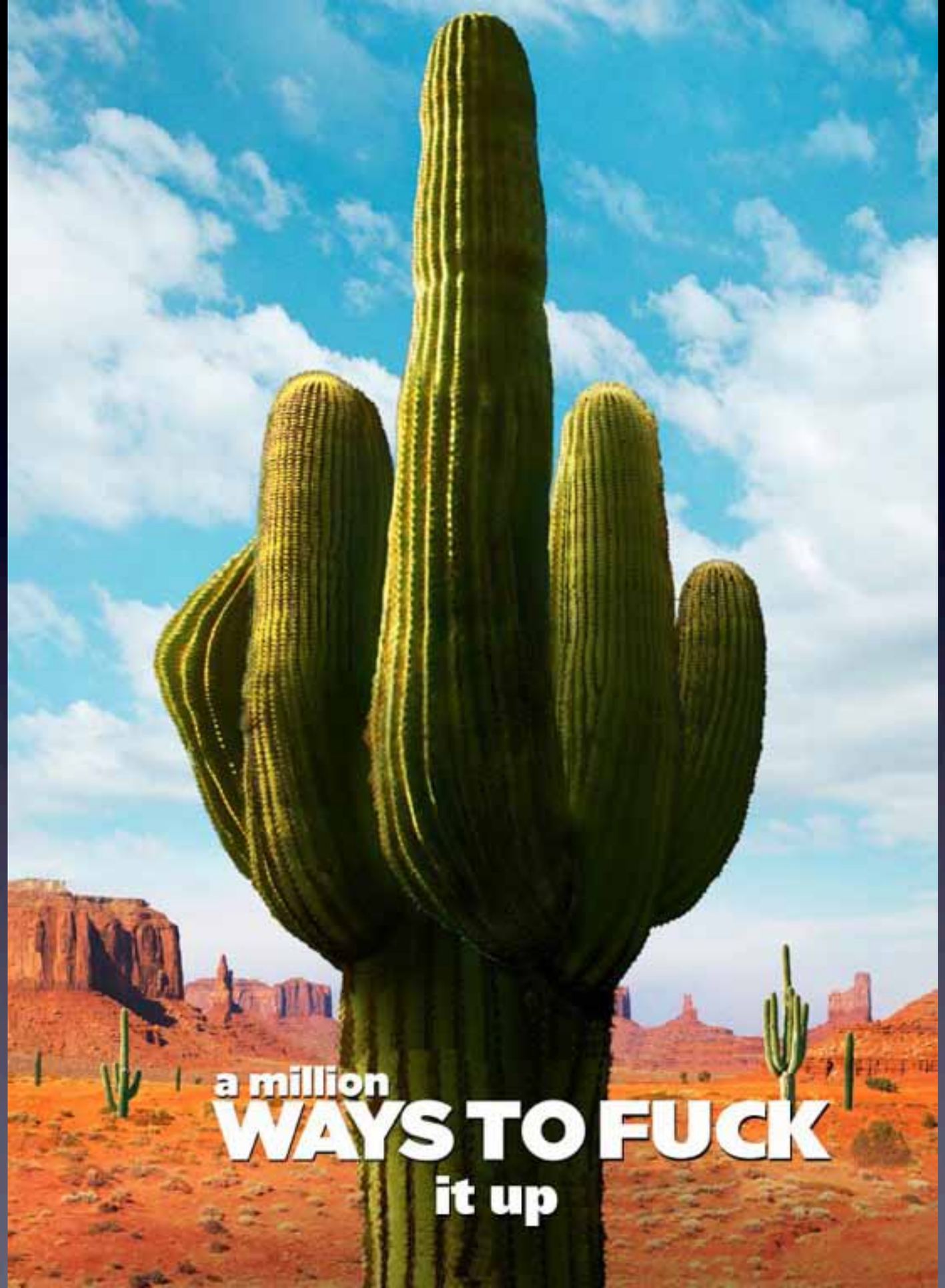
"On the Internet, nobody knows you're a dog."

On the Internet, everyone knows you like ASCII Goatse.


NSA
ILLEGAL
SPYING
BELOW
StandAgainstSpying.org
GREENPEACE

New Collection Posture




a million
WAYS TO FUCK
it up

Tradecraft

Perceptual Biases Expectations Resistance Ambiguities	**Biases In Evaluating Evidence** Consistency Missing Information Discredited Evidence
Biases In Estimating Probabilities Availability Anchoring Overconfidence	**Biases In Perceiving Causality** Rationality Attribution

Tradecraft

- Key Assumptions Check
- Quality Of Information Check
- Contrarian Techniques
- Devil's Advocacy
- High Impact/Low Probability
- "What If?" Analysis
- Red Team

OPSEC

ENEMY EARS are listening

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.

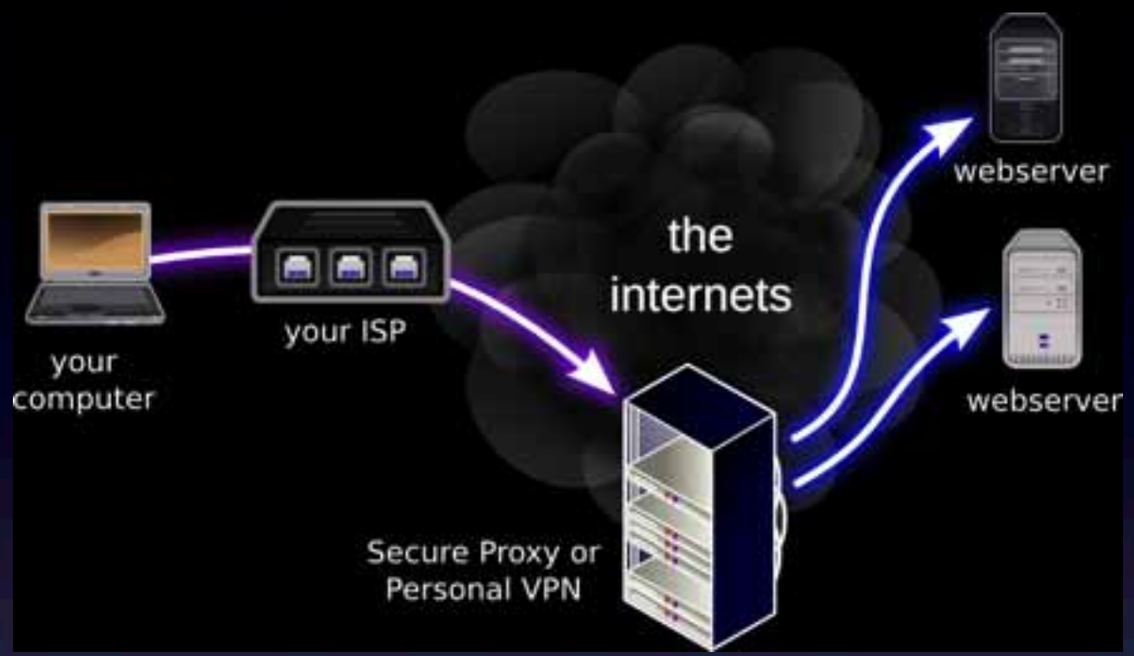
The 7 Deadly Fuckups

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

WARNING

Keep hands away from jet.

Don’t Fuck It Up When You Use A VPN



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

*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

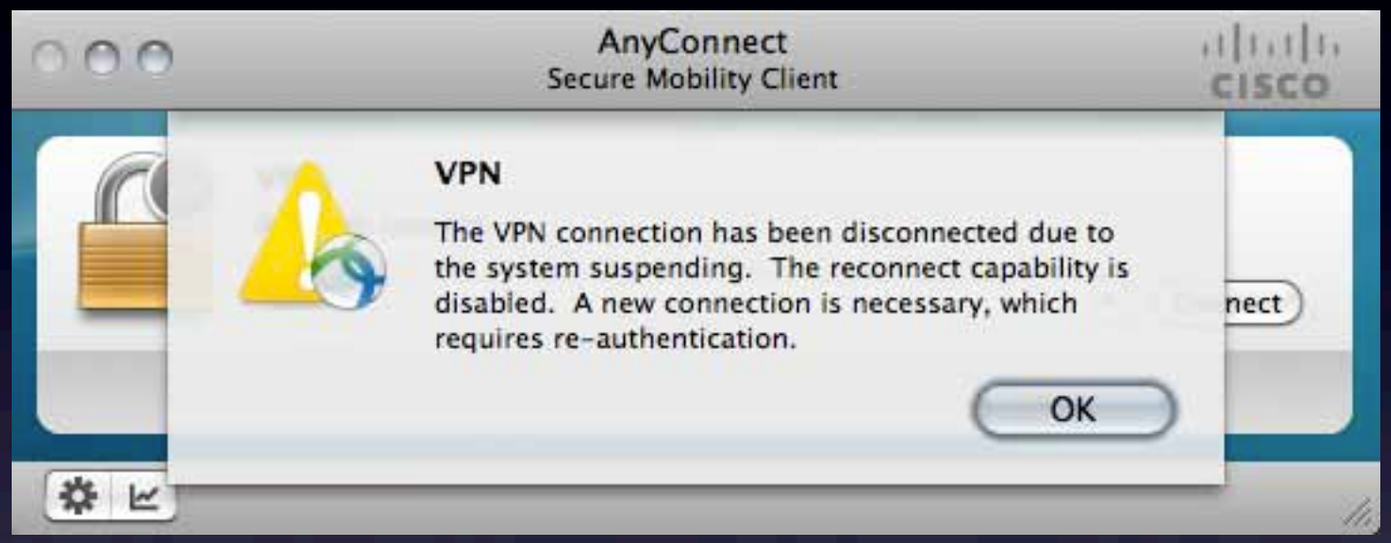
No.	Time	Source	Destination	Protocol	Length	Info
158	50.727396000	10.1.10.233	224.0.1.76	IAPP	128	Announce Response(1) (version=1)
159	50.728072000	10.1.10.233	224.0.1.76	IAPP	128	Announce Response(1) (version=1)
161	51.617440000	10.1.10.15	224.0.0.251	MDNS	147	Standard query response 0x0000 TXT
162	51.779381000	10.1.10.12	224.0.0.251	MDNS	194	Standard query 0x0000 PTR _afpovertcp._tcp.local, "QM" question PTR _smb.
165	52.668754000	10.1.10.15	224.0.0.251	MDNS	147	Standard query response 0x0000 TXT
166	53.788231000	10.1.10.34	10.1.10.255	BJNP	60	Scanner Command: Discover
167	53.788236000	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	156	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  ff ff ff ff ff ff 00 23  df 7c 62 8c 08 00 45 00   .......# .|b...E.
0010  00 2c 30 af 00 00 40 11  20 f0 0a 01 0a 22 0a 01   .,0...@. .....".
0020  0a ff d2 15 21 a4 00 18  54 50 42 4e 4a 42 02 01   ....!... TPBNJB..
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

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

```
Write failed: Permission denied
[Vomitose:~] zoz%
```




```
% 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
%
```

Technology Detection

- Show me all the VPN startups in country X, and give me the data so I can decrypt and discover the users
  - These events are easily browsable in XKEYSCORE
    - No strong-selector
  - XKEYSCORE extracts and stores authoring information for many major document types – can perform a retrospective survey to trace the document origin since metadata is typically kept for up to 30 days
  - No other system performs this on raw unselected bulk traffic, data volumes prohibit forwarding

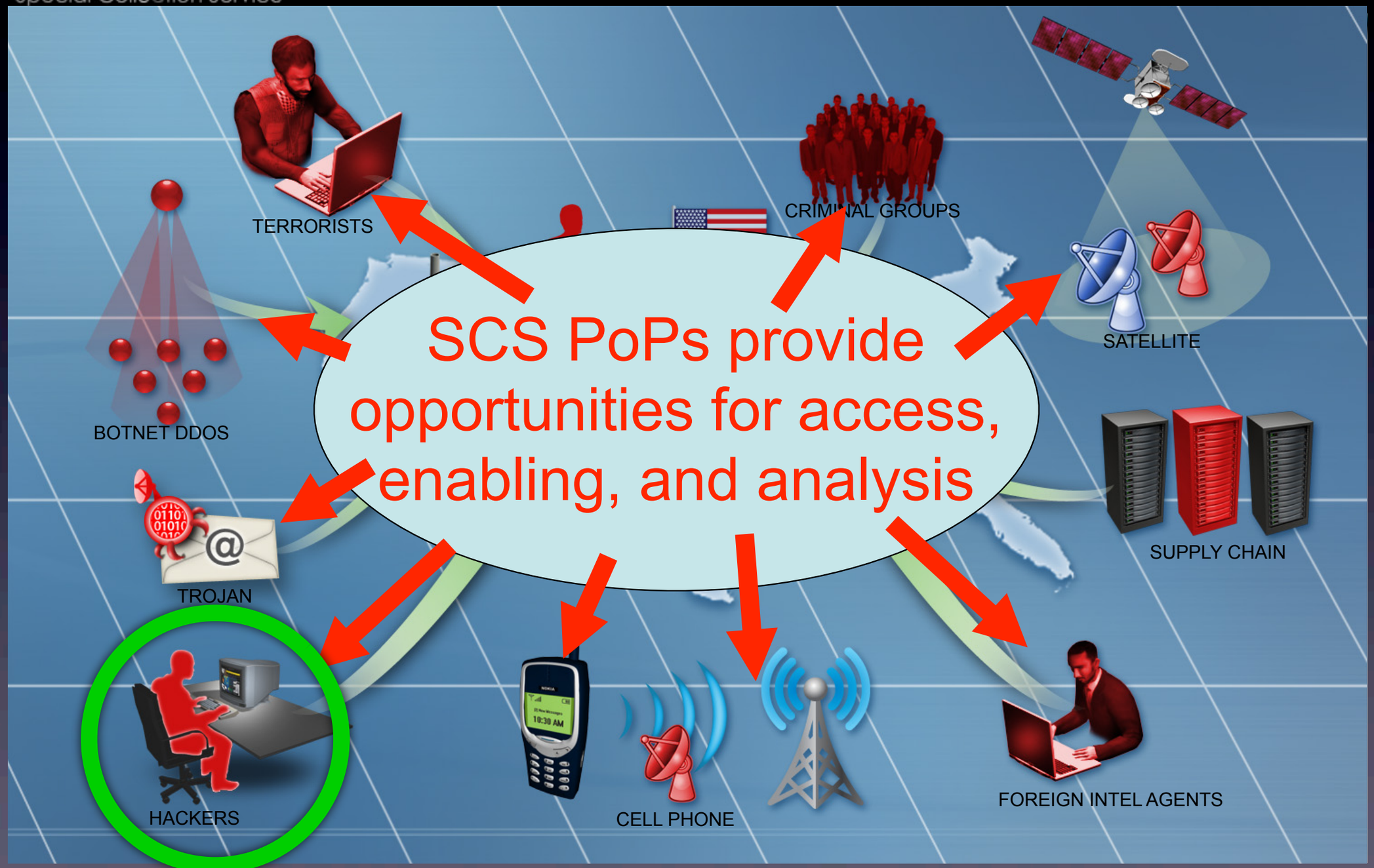
Special Collection Service

CES/SSC/AAD VPN "Surge"

- Main Goal:
  - To evaluate SCS VPN access and analysis to determine better methods of identifying and exploiting networks of interest.
- Two Focuses:
  - What can we do with VPN data that is already ingested into the system?
    - Find better methods of reporting VPN stats and exploitation determinations from CES back to SSC and site.
  - Are there methods to better identify and survey VPN's to provide CES the data they need?
    - Can we leverage MIRROR, DARKQUEST, PANOPLY survey information to quickly identify and report the presence of VPN's in surveyed signals?
    - Can we use BIRDWATCHER or other means to automatically resurvey for key exchanges and obtain paired collect?

Special Collection Service

SCS Opportunities



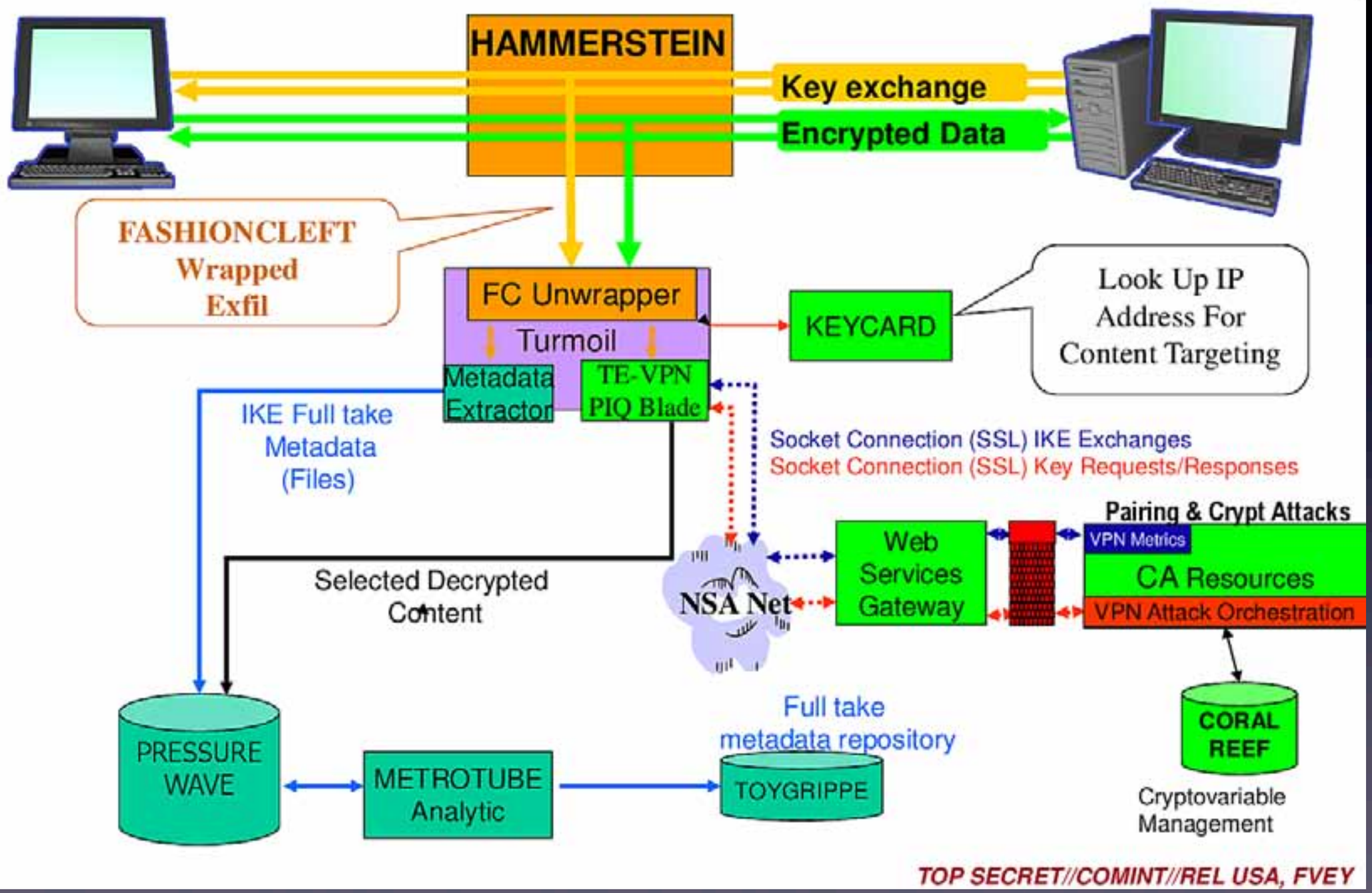
Private Networks are Important

- Many targets use private networks.

Google infrastructure	SWIFT Network
REDACTED	REDACTED
REDACTED	Gazprom
Aeroflot	REDACTED
French MFA	REDACTED
Warid Telecom	Petrobras
REDACTED	REDACTED

- Evidence in Survey: 30%-40% of traffic in BLACKPEARL has at least one endpoint private.

APEX VPN Exploitation



Remember:

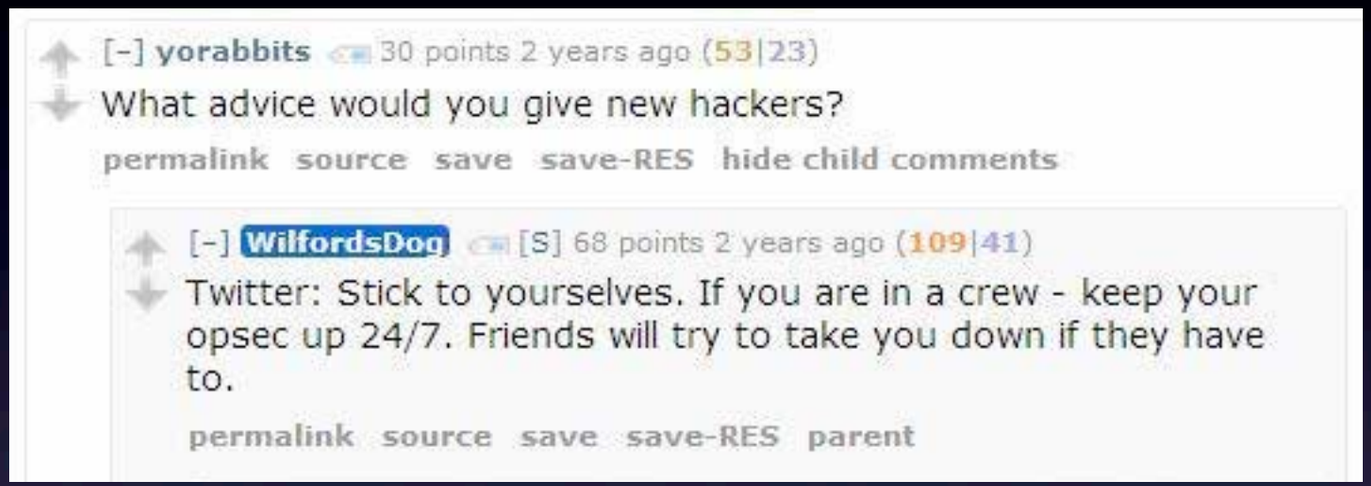
PPTP Broken As Of

Don’t Fuck It Up When You Use

Case Study: LulzSec/AntiSec

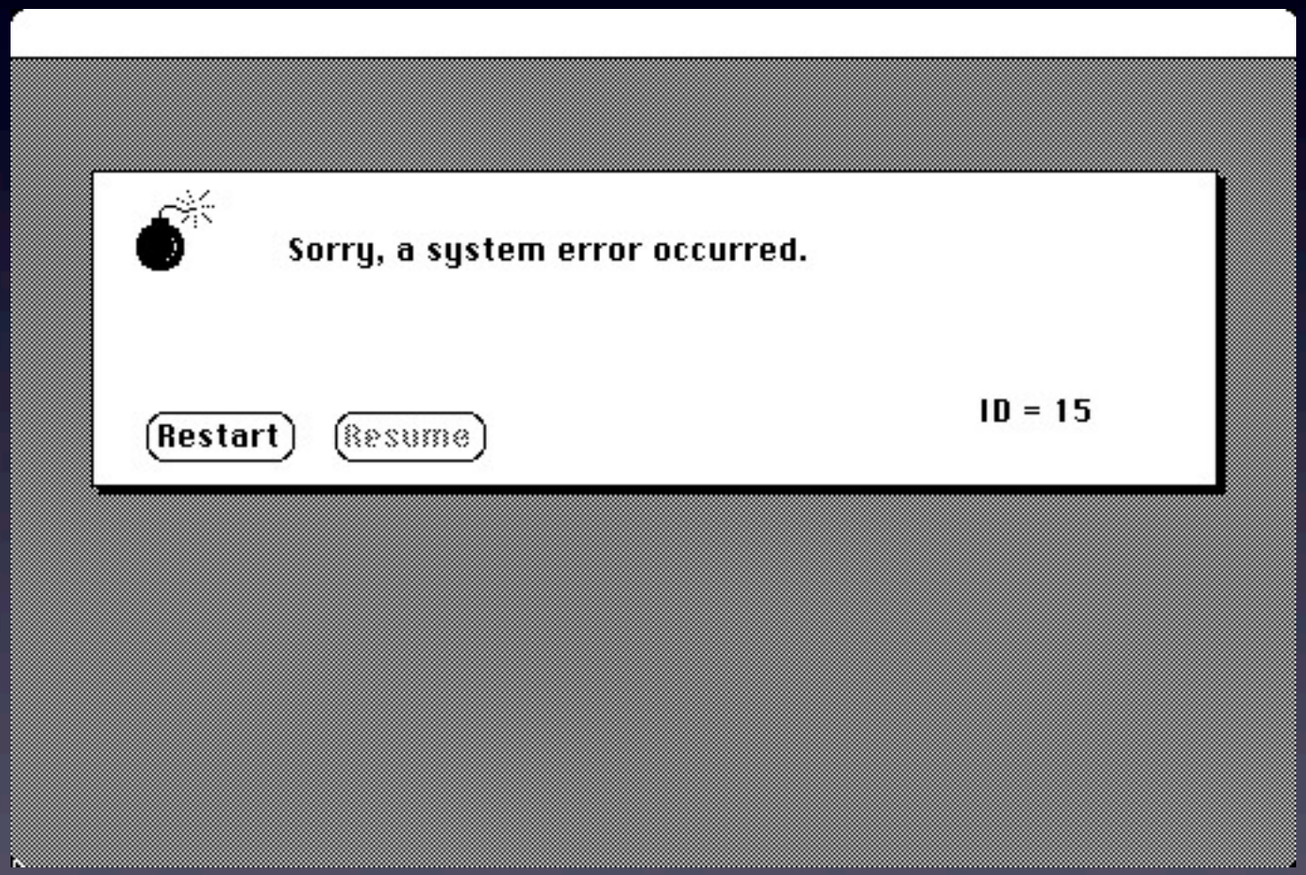

IRC WITHOUT TOR...
...NOT EVEN ONCE

Moral:



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

Case Study: Harvard Bomb Hoax



WHAT AIN'T NO COUNTRY I EVER HEARD OF

THEY SPEAK OPSEC IN WHAT?

What Fucked It Up?

- Harvard Network Registration
- Outgoing Traffic Logs
- Pervasive Surveillance Microcosm
- Moral:
  - Key Assumptions Check
  - High Impact/Low Probability Analysis
  - Bridge Relays
  - Traffic Analysis Preparation

(TS//SI//REL) Fingerprinting TOR

(TS//SI//REL) BuildID gives a timestamp for when the Firefox release was built

20121024073032

Year Month Day Hour Min Sec

(TS//SI//REL) tbb-firefox's BuildID:

0

(TS//SI//REL) Fingerprinting TOR

- (TS//SI//REL) TorButton cares about TOR users being indistinguishable from TOR users
- (TS//SI//REL) We only care about TOR users versus non-TOR users
- (TS//SI//REL) Thanks to TorButton, it's easy!

(TS//SI//REL) Exploiting TOR

- (TS//SI//REL) tbb-firefox is barebones
  - Flash is a no-no
  - NoScript addon pre-installed…
    …but not enabled by default!
  - TOR explicitly advises against using any addons or extensions other than TorButton and NoScript
- (TS//SI//REL) Need a native Firefox exploit

(TS//SI//REL) Exploiting TOR

- (TS//SI//REL) ERRONEOUSINGENUITY
  - Commonly known as ERIN
  - First native Firefox exploit in a long time
  - Only works against 13.0-16.0.2
- (TS//SI//REL) EGOTISTICALGOAT
  - Commonly known as EGGO
  - Configured for 11.0-16.0.2…
    …but the vulnerability also exists in 10.0!

Tor Stinks… (U)

- We will never be able to de-anonymize all Tor users all the time.
- With manual analysis we can de-anonymize a **very small fraction** of Tor users, however, **no** success de-anonymizing a user in response to a TOPI request/on demand.

[redacted]

Analytics: Cookie Leakage (TS//SI)

Use cookies to identify Tor users when they are not using Tor

- Current: preliminary analysis shows that some cookies "survive" Tor use. Depends on how target is using Tor (Torbutton/Tor Browser Bundle clears out cookies).
- Goal: test with cookies **associated** with CT targets
  - Idea: what if we seeded cookies to a target?
  - Investigate Evercookie persistence

Analytics:

Goes Inta Goes Outta/Low Latency (S//SI)

Find possible alternative accounts for a target: look for connections to Tor, from the target's suspected country, near time of target's activity.

- Current: GCHQ has working version (QUICKANT). R has alpha tested NSA's version. NSA's version produced no obvious candidate selectors.
- Goal: Figure out if QUICKANT works, compare methodologies. Gathering data for additional tests of NSA's version (consistent, random and heavy user)

Exploitation: QUANTUM (TS//SI)

- QUANTUM to degrade/deny/disrupt Tor access?
- QUANTUMCOOKIE – forces clients to divulge stored cookies.

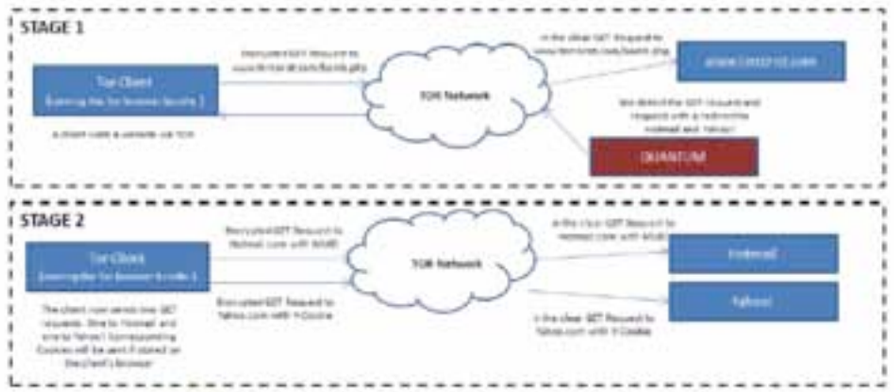


Figure 4 A diagram of how the QUANTUM Survey / Cookie technique works

(C//REL) Types of IAT – Advanced Open Source M[illegible] Hop

- (S//REL) Open Source Multi-Hop Networks
  - (S//REL) *Tor*
    - (S//REL) Very widely used worldwide
    - (S//REL) Open Source
      - (S//REL) Active Development
      - (S//REL) Mitigates Threats
    - (S//REL) Very Secure
    - (S//REL) Low enough latency for most *TCP* u[illegible]
    - (S//REL) Still the King of high secure, low latency Internet Anonymity
      - (S//REL) There are no contenders for the throne in waiting

(S//REL) *Tor* Project and friends Recent Activity

- (S//

– to use!

–

–

–

– (S//REL) *Tails*: Complete Bootable OS on CD for anonymity – includes *Tor*

- (S//REL) Adds Severe CNE misery to equation
- (S//SI//REL) Has been discussed by CT targets

```
// START_DEFINITION
/**
 * Fingerprint Tor authoritative directories enacting the directory protocol.
 */
fingerprint('anonymizer/tor/node/authority') = $tor_authority
  and ($tor_directory or preappid(/anonymizer\/tor\/directory/));
// END_DEFINITION
```

```
// START_DEFINITION
/*
Global Variable for Tor foreign directory servers. Searching for potential Tor
clients connecting to the Tor foreign directory servers on ports 80 and 443.
*/

$tor_foreign_directory_ip = ip('193.23.244.244' or '194.109.206.212' or
'86.59.21.38' or '213.115.239.118' or '212.112.245.170') and port ('80' or
'443');
// END_DEFINITION

// START_DEFINITION
/*
this variable contains the 3 Tor directory servers hosted in FVEY countries.
Please do not update this variable with non-FVEY IPs. These are held in a
separate variable called $tor_foreign_directory_ip. Goal is to find potential
Tor clients connecting to the Tor directory servers.
*/
$tor_fvey_directory_ip = ip('128.31.0.39' or '216.224.124.114' or
'208.83.223.34') and port ('80' or '443');
// END_DEFINITION
```

```
// START_DEFINITION
/*
The fingerprint identifies sessions visiting the Tor Project website from
non-fvey countries.
*/
fingerprint('anonymizer/tor/torpoject_visit')=http_host('www.torproject.org')
and not(xff_cc('US' OR 'GB' OR 'CA' OR 'AU' OR 'NZ'));
// END_DEFINITION
```

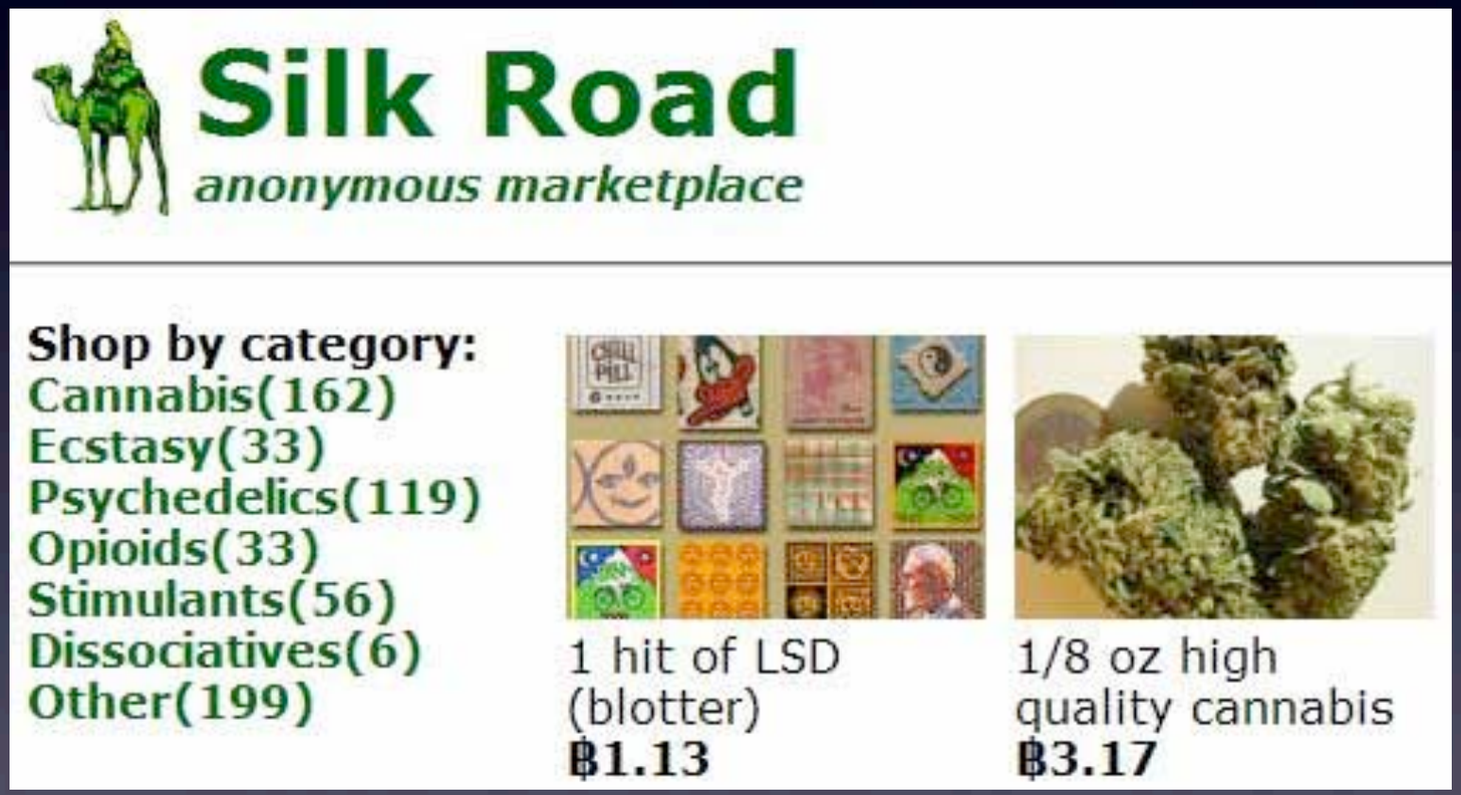
```
// START_DEFINITION
requires grammar version 5
/**
 * Identify clients accessing Tor bridge information.
 */
fingerprint('anonymizer/tor/bridge/tls') =
ssl_x509_subject('bridges.torproject.org') or
ssl_dns_name('bridges.torproject.org');

/**
 * Database Tor bridge information extracted from confirmation emails.
 */
fingerprint('anonymizer/tor/bridge/email') =
email_address('bridges@torproject.org')
  and email_body('https://bridges.torproject.org/' : c++
  extractors: {{
    bridges[] = /bridge\s([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}):?([0-9
]{2,4}?[^0-9])/;
  }}
  init: {{
    xks::undefine_name("anonymizer/tor/torbridges/emailconfirmation");
  }}
  main: {{
    static const std::string SCHEMA_OLD = "tor_bridges";
    static const std::string SCHEMA_NEW = "tor_routers";
    static const std::string FLAGS = "Bridge";
    if (bridges) {
      for (size_t i=0; i < bridges.size(); ++i) {
        std::string address = bridges[i][0] + ":" + bridges[i][1];
        DB[SCHEMA_OLD]["tor_bridge"] = address;
        DB.apply();
        DB[SCHEMA_NEW]["tor_ip"] = bridges[i][0];
        DB[SCHEMA_NEW]["tor_port_or"] = bridges[i][1];
        DB[SCHEMA_NEW]["tor_flags"] = FLAGS;
        DB.apply();
      }
      xks::fire_fingerprint("anonymizer/tor/directory/bridge");
    }
    return true;
  }});
// END_DEFINITION
```

```
// START_DEFINITION
/*
These variables define terms and websites relating to the TAILs (The Amnesic
Incognito Live System) software program, a comsec mechanism advocated by
extremists on extremist forums.
*/

$TAILS_terms=word('tails' or 'Amnesiac Incognito Live System') and word('linux'
or ' USB ' or ' CD ' or 'secure desktop' or ' IRC ' or 'truecrypt' or ' tor ');
$TAILS_websites=('tails.boum.org/') or ('linuxjournal.com/content/linux*');
// END_DEFINITION
```

Case Study: Silk Road/DPR



What Fucked It Up?

stackoverflow Questions Tags Tour Users

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?

25 6

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
```

Jump to first unread post Pages: 1

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

anonymous market online? NEW
#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...

Post Extras:

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

altoid
Member
Activity: 48
Ignore

IT pro needed for venture backed bitcoin startup
October 11, 2011, 08:06:22 PM #1

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.

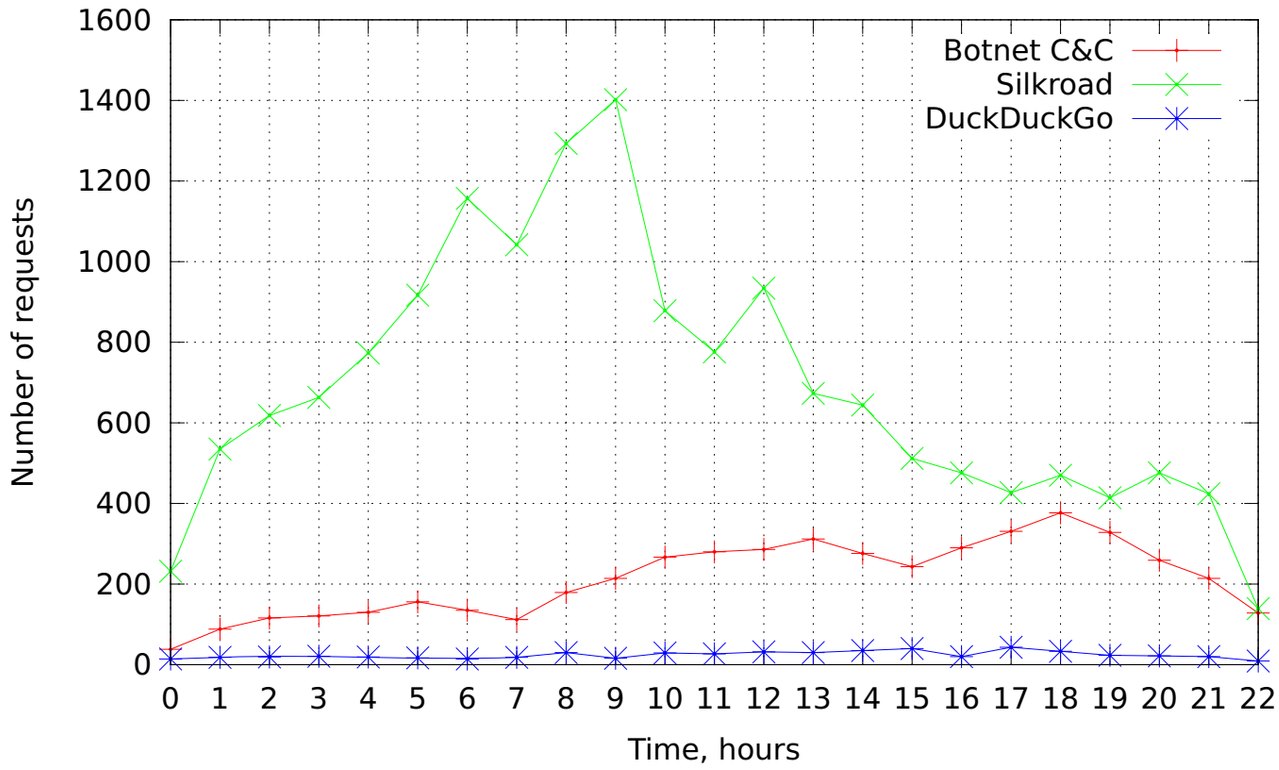


Figure 4. Hidden service descriptor request rate during one day.

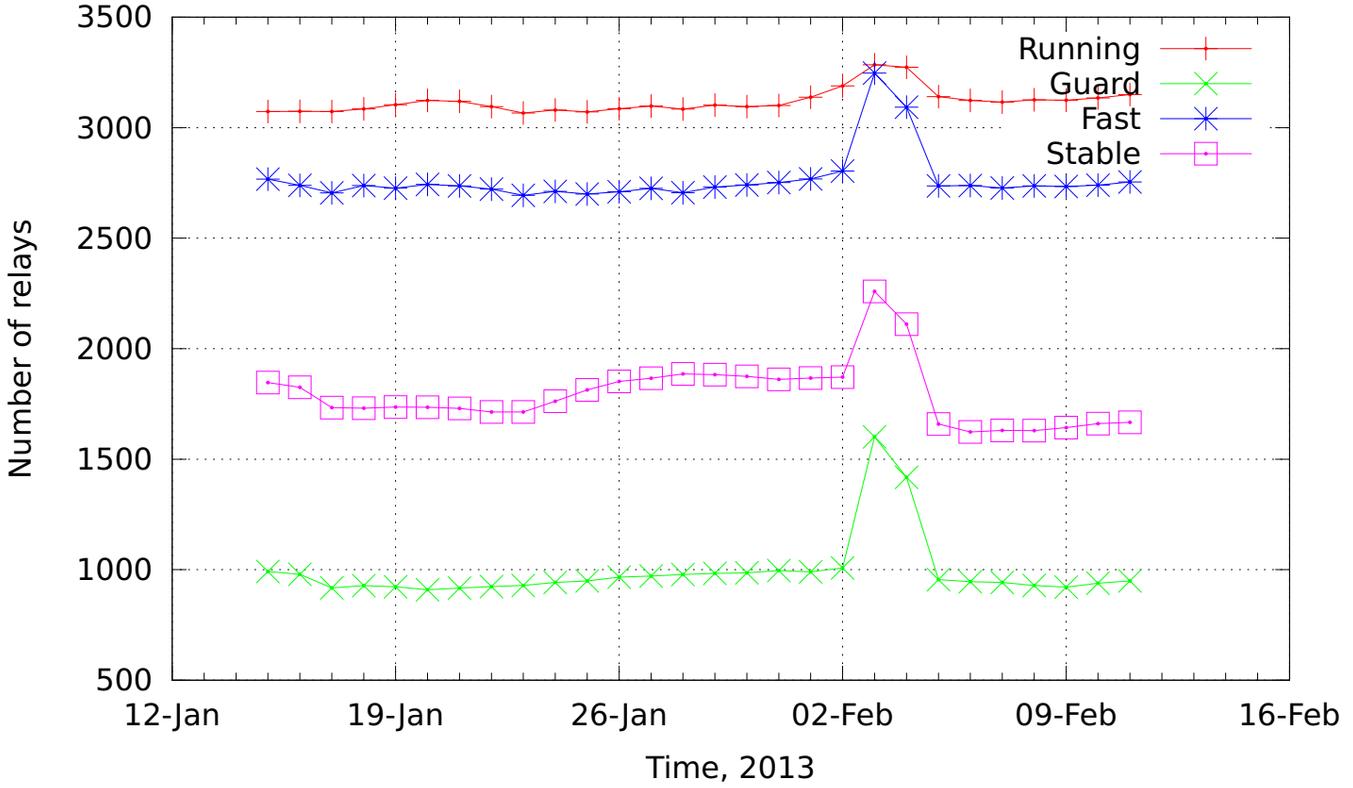


Figure 6. Increase in the number of Guard nodes.

Biryukov, Pustogarov, Weinmann:
Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization, 2013

Technical Analysis: Hidden Services

(TS//SI)

What do we know about Hidden Services?

- Current: No effort by NSA, some DSD and GCHQ work on ONIONBREATH.
- Goal:
  - Harvest and enumerate .onion URLs
  - Identify similar HS based on referrer fields
  - Distinguish HS from normal Tor clients

Technical Analysis: torservers.net (TS//SI)

Investigate the Amazon AWS cloud instances of Tor servers. How are IPs allocated and reassigned once bandwidth limit is reached? Impact on RONIN's ability to detect nodes?

- Current: GCHQ set up Tor nodes on the AWS cloud during REMATION II.

[redacted]

JTRIG tools and techniques

(Redirected from JTRIG CITD - Covert Internet Technical Development)

navigation

- Main Page
- Help Pages
- Wikipedia Mirror
- Ask Me About...
- Random page
- Recent changes
- Report a Problem
- Contacts
- GCWeb

search

Overview | **JTRIG Capabilities** | Contacts

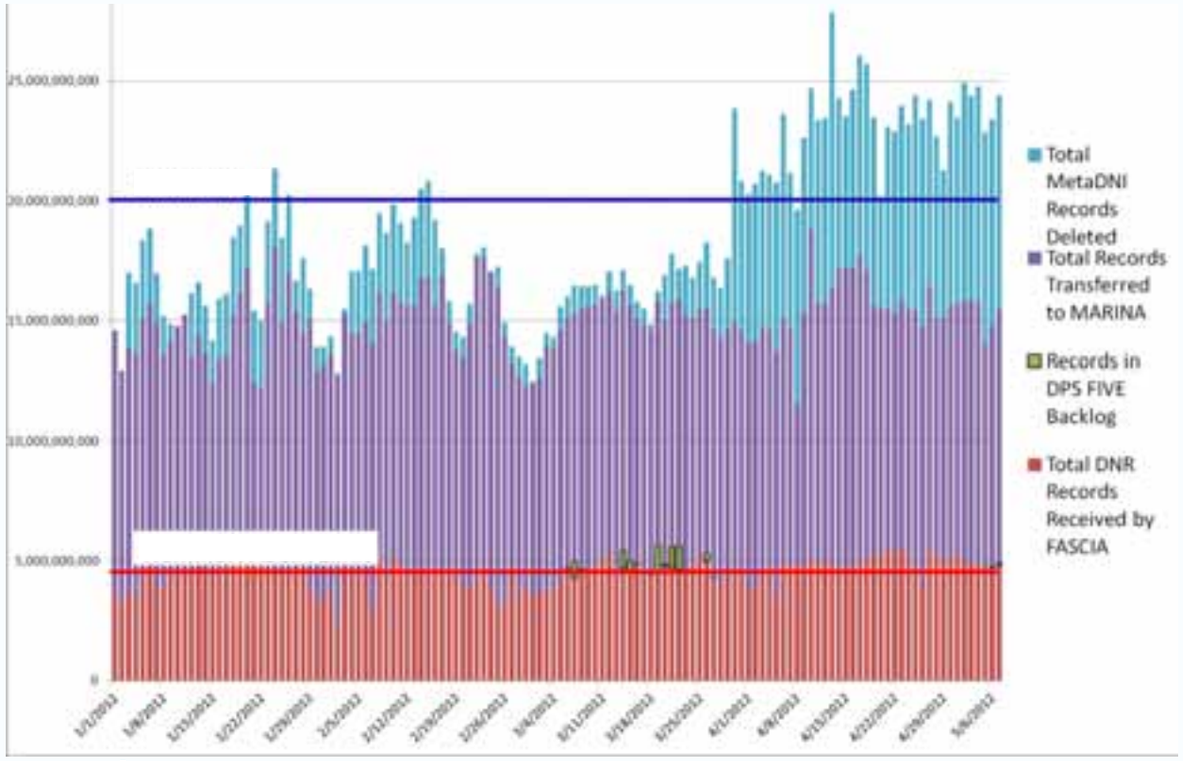
[edit] JTRIG tools

ALLIUM ARCH	JTRIG UIA via the Tor network.	OPERATIONAL	JTRIG Infrastructure Team
ASTRAL PROJECTION	Remote GSM secure covert internet proxy using TOR hidden services.	OPERATIONAL	JTRIG Infrastructure Team
FRUIT BOWL	CERBERUS UIA Replacement and new tools infrastructure – Primary Domain for Generic User/Tools Access and TOR split into 3 sub-systems.	DESIGN	JTRIG Infrastructure Team
NUT ALLERGY	JTRIG Tor web browser - Sandbox IE replacement and FRUIT BOWL sub-system	PILOT	JTRIG Infrastructure Team
BUMBLEBEE DANCE	JTRIG Operational VM/TOR architecture	OPERATIONAL	JTRIG Infrastructure Team
SILVER SPECTER	Allows batch Nmap scanning over TOR	JTRIG Software Developers	In Development
SHADOWCAT	End-toEnd encrypted access to a VPS over SSH using the TOR network	JTRIG OSO	

Don't Fuck It Up When You Use The Phone

- 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

Example of Current Volumes and Limits



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

(U) Converged Analysis of Smartphone Devices

Identification/Processing/Tasking –

All in a day's work

[redacted]

Golden Nugget!

Perfect Scenario – Target uploading photo to a social media site taken with a mobile device.

What can we get?

User Activity Leads

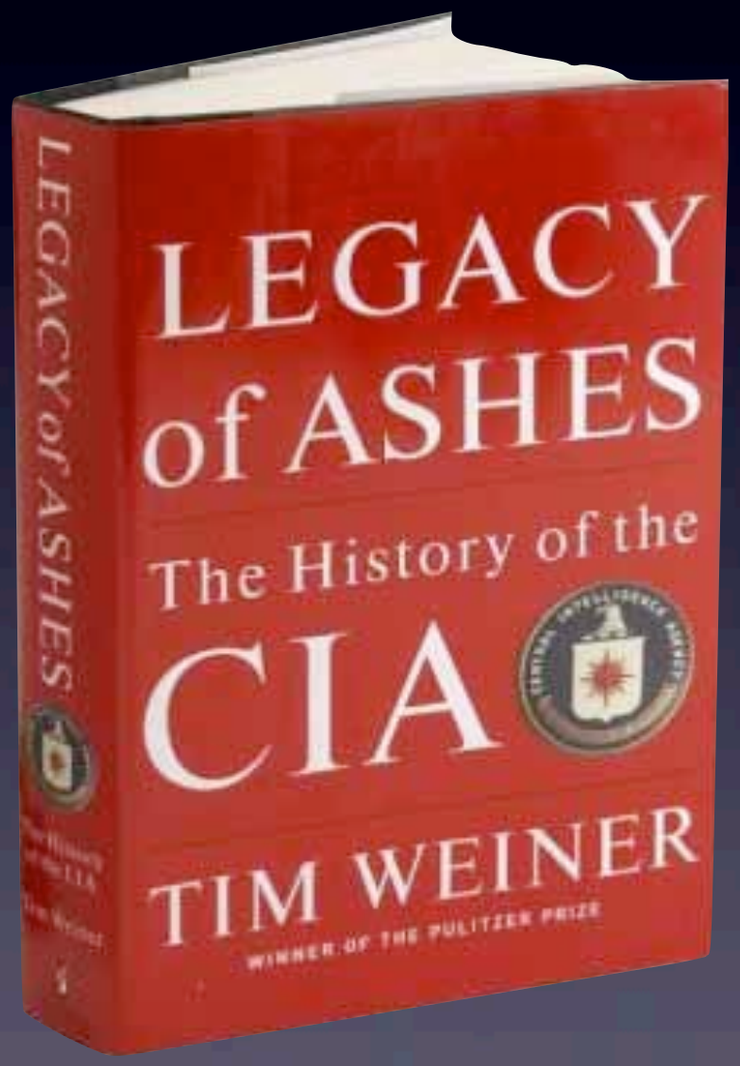
- Examine settings of phone as well as service providers for geo-location; specific to a certain region
- Networks connected
- Websites visited
- Buddy Lists
- Documents Downloaded
- Encryption used and supported
- User Agents

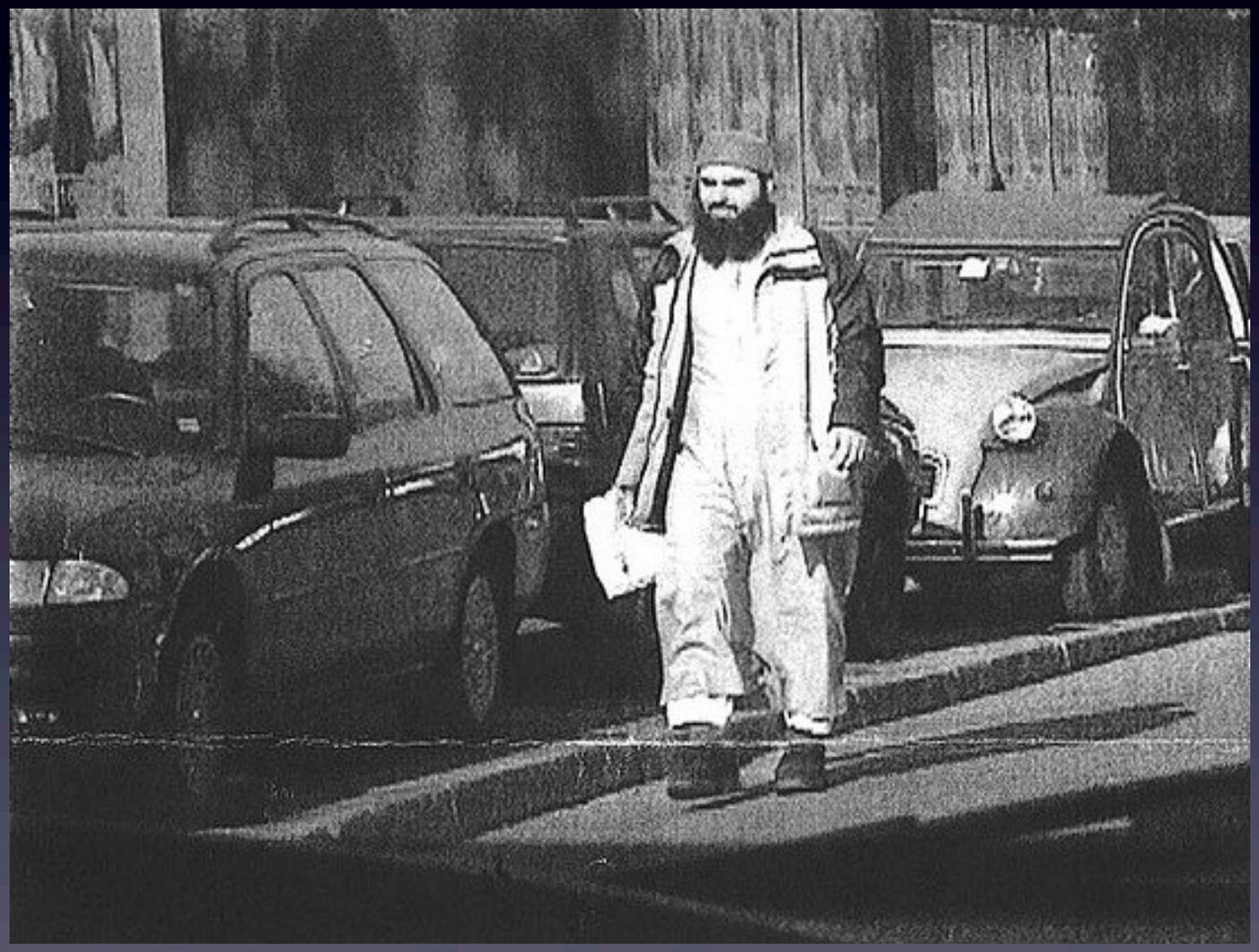
Targeting

Targeting both Telephony and DNI systems

- Call Logs
- SMS
- SIM Card Leads
- Email address
- IMEI/IMSI
- Unique Identifiers
- Blackberry PINS

Case Study: CIA/Abu Omar





OCD OPSEC:

Using A Burner Phone Without Fucking It Up

- DO:
  - Advance Purchase
  - Register Far Away
  - Lie To Phone Companies
  - Stay Dumb
  - Remove Battery
  - Fake Contacts
  - Minimize Use
  - Move & Switch
  - Falsify Call Network
  - Purpose Equipment
  - Thou Shalt Always Kill

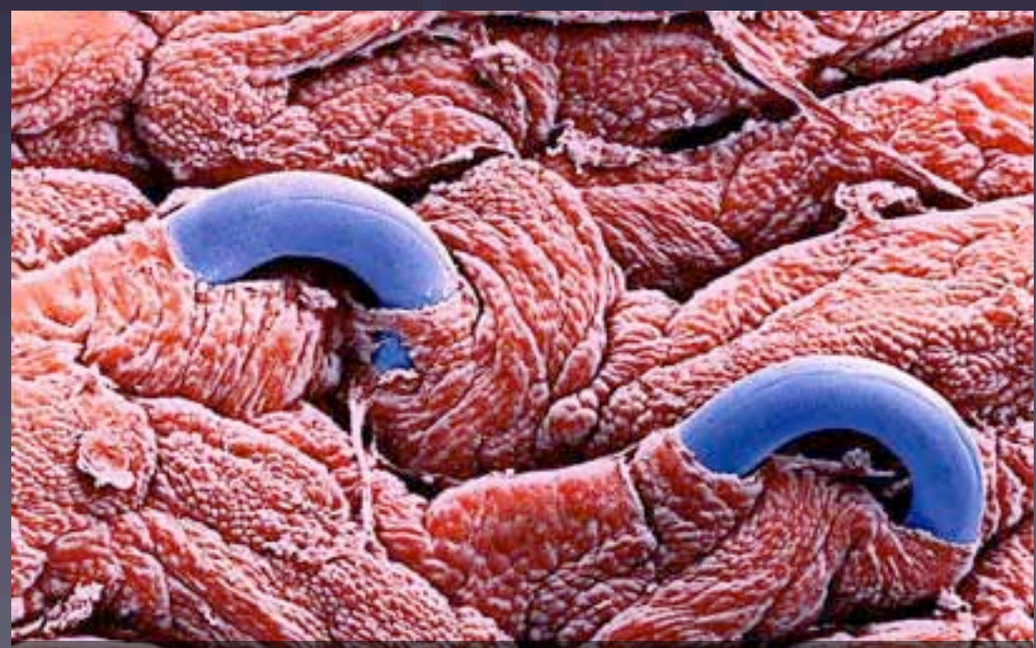
OCD OPSEC:

Using A Burner Phone Without Fucking It Up

- DON'T EVER:
  - Co-Localize
  - Co-Activate
  - Co-Contact
  - Store Real Data
  - Match Entry/Exit
  - Bridge Online Metadata

Don't Fuck It Up When You Use Messaging

- After All These Years, E-Mail Still Sucks
  - Spam Fighting Aids Tracking
  - Webmail Using HTTP
  - Weak Server-Side Storage
  - Encrypted Content Not Metadata
  - Insecure Client-Side Logging
  - Bad Retention Habits
  - Google
- And IM Is Not Much Better
- Psycho Ex Principle



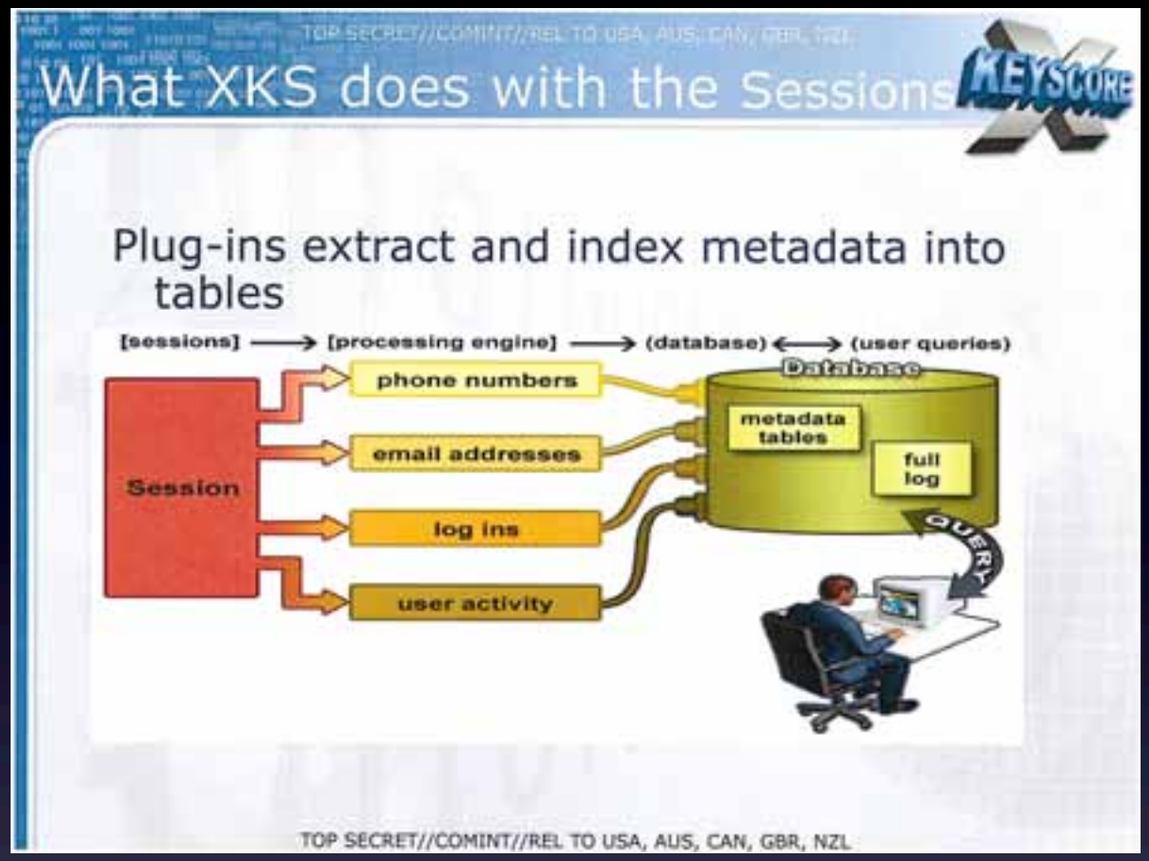
Threadworm in sheep intestine

SECURITY BY OBSCURITY DOESN'T WORK

TELL THAT TO THESE GUYS

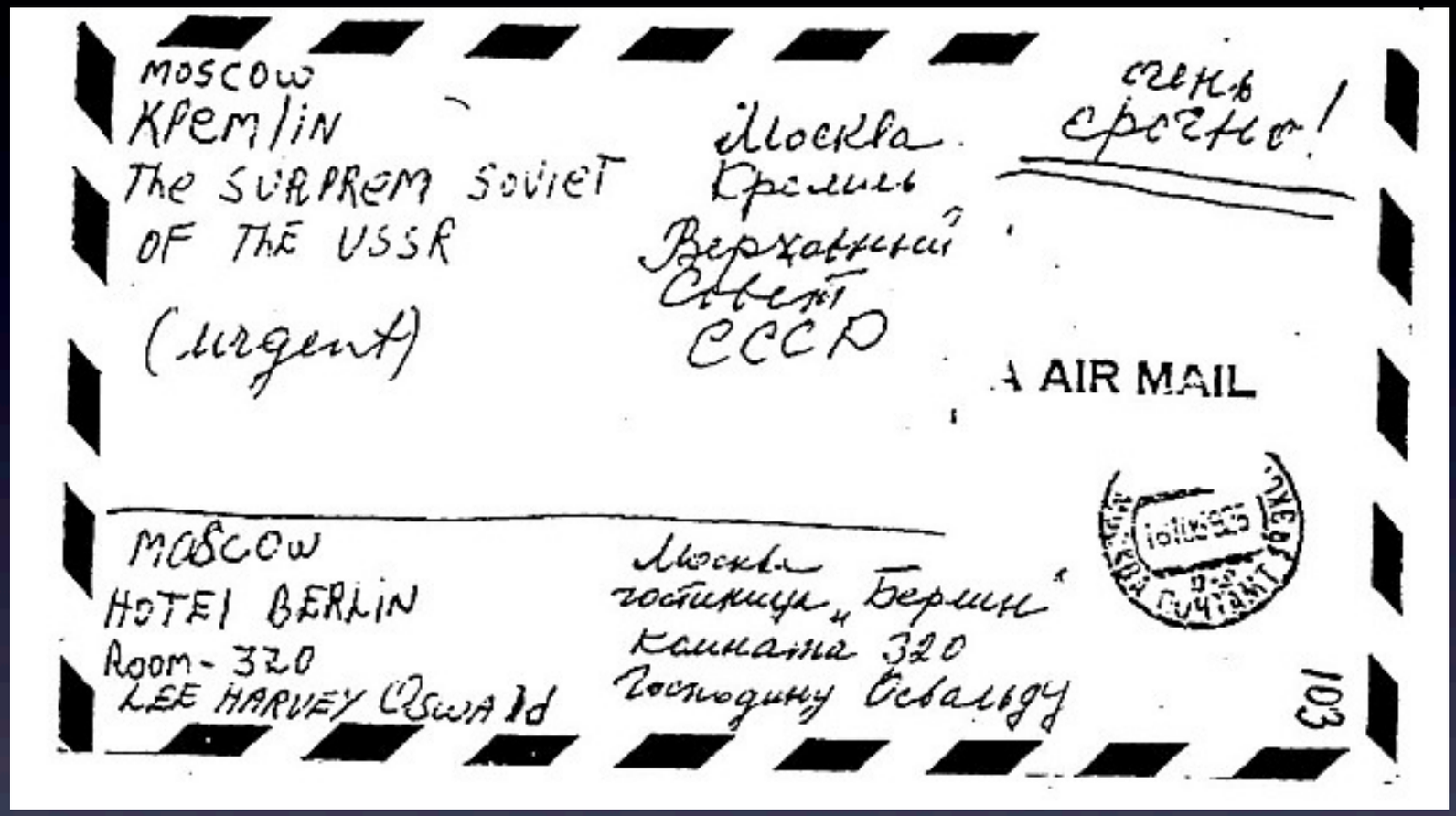
Case Study: CIA/Petraeus

What Fucked It Up?



- Technique Already Identified & Compromised
- Pervasive Surveillance Designed To Expose Exactly This Type Of Access Correlation
- Deleted Things Aren't
- Understand & Manage Insecure Channels
  - Quality Of Information Check, "What If?"

Common Broken/Compromised Services



- Commercial Webmail
  - Run Your Own Mailserver
  - Metadata's Still A Bitch

Common Broken/Compromised Services

TOP SECRET//SI//NOFORN

Direc… …ction
Germ… …BND)

SID DIR Courtesy Call: 30 Ap…
Participants: Mr. [redacted] D/DA; Mr. [redacted] D/A&P; Mr. [redacted], SUSLAG Designee; Ms. [redacted] CDO Ge…

(TS//SI//NF) POTENTIAL LANDMINES:

- (TS//SI//NF) **SKYPE:** The Germans may bring up the subject of SKYPE. NSA's response has been that it has had some success working SKYPE via tailored access at the end point by gaining access to one or more of the computers involved in the session. When Hr. Klaus-Fritsche (State Secretary, Germany Ministry of Interior) sought NSA's assistance with intercepting SKYPE transmissions during a 10 January 2012 meeting with DIRNSA, DIRNSA suggested the DNI Representative Berlin take the lead in arranging an exchange to include CIA, FBI and NSA. Should the partner raise this issue again, recommend that NSA once again redirects them to FBI and CIA.

MINIATURE HERO	Active … bidirect…	Fully operational, but note usage restrictions.

- Skype
  - PRISM, SIGINT Enabling, JTRIG, Forced "Upgrades", Pre-MS EOL
  - Fuck Skype

Common Broken/Compromised Services

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

Why are we interested in HTTP?

- Almost all web-browsing uses HTTP:
  - Internet surfing
  - Webmail (Yahoo/Hotmail/Gmail/etc.)
  - OSN (Facebook/MySpace/etc.)
  - Internet Searching (Google/Bing/etc.)
  - Online Mapping (Google Maps/Mapquest/etc.)

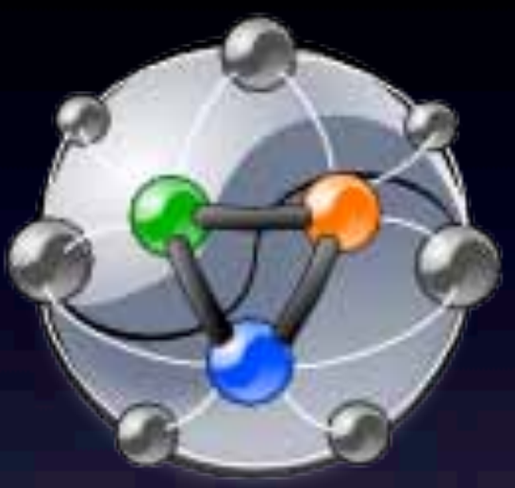
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

XKS HTTP Activity Search

Another common query is analysts who want to see all traffic from a given IP address (or IP addresses) to a specific website.

- Many Chats
  - Let's Just Assume IRC Is All Collected
    - Why Not Grab 6667 Like 80?
    - TLS Only Protects You To The Server
    - QUANTUMBOT
  - GChat's "Off The Record" Isn't The Same As OTR
  - That First OTR Message

What Might Not Be Completely Fucked



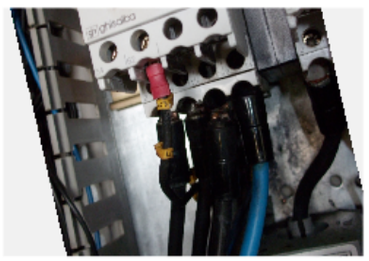
- Some OTR Implementations (But Which Ones?)
- Cryptocat?
- Bitmessage?
- Retroshare?
- We Need More:
  - Auditing
  - Steganography

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

Steganography:
Hiding In Plain Sight

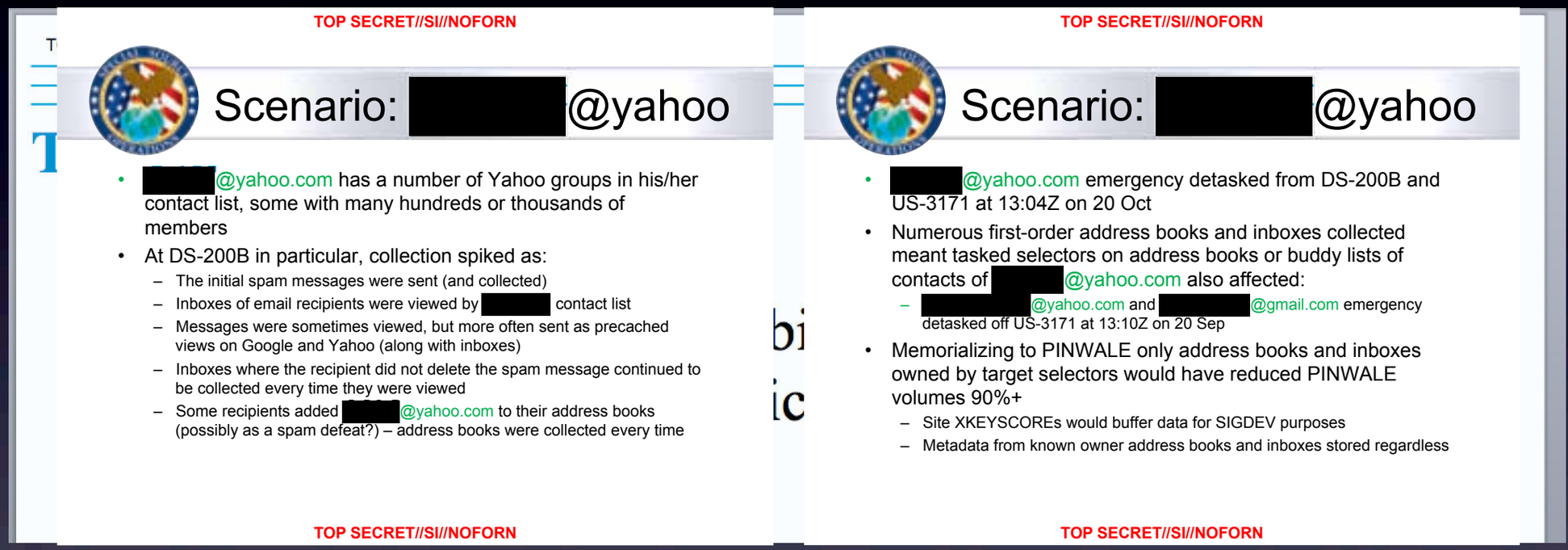
(U) Analytics for Targets in Europe

- (C//FVEY) OPSEC Savvy Targets
  - "…most terrorists stop thru Europe"
- (TS//FVEY) Use advanced techniques
  - Steganography
    - Forensics or Analytics on front end
  - Encryption
    - Takes time and has "black hole" issue
- (TS//SI//FVEY) Reliance on "special" collection
  - GCHQ and FAA
  - Problems processing w/r to TS



TOP SECRET//SI//REL USA, FVEYS

Steganography:
Hiding In Plain Sight



TOP SECRET//SI//NOFORN

Scenario: [redacted]@yahoo

- [redacted]@yahoo.com has a number of Yahoo groups in his/her contact list, some with many hundreds or thousands of members
- At DS-200B in particular, collection spiked as:
  - The initial spam messages were sent (and collected)
  - Inboxes of email recipients were viewed by [redacted] contact list
  - Messages were sometimes viewed, but more often sent as precached views on Google and Yahoo (along with inboxes)
  - Inboxes where the recipient did not delete the spam message continued to be collected every time they were viewed
  - Some recipients added [redacted]@yahoo.com to their address books (possibly as a spam defeat?) – address books were collected every time

TOP SECRET//SI//NOFORN

TOP SECRET//SI//NOFORN

Scenario: [redacted]@yahoo

- [redacted]@yahoo.com emergency detasked from DS-200B and US-3171 at 13:04Z on 20 Oct
- Numerous first-order address books and inboxes collected meant tasked selectors on address books or buddy lists of contacts of [redacted]@yahoo.com also affected:
  - [redacted]@yahoo.com and [redacted]@gmail.com emergency detasked off US-3171 at 13:10Z on 20 Sep
- Memorializing to PINWALE only address books and inboxes owned by target selectors would have reduced PINWALE volumes 90%+
  - Site XKEYSCOREs would buffer data for SIGDEV purposes
  - Metadata from known owner address books and inboxes stored regardless

TOP SECRET//SI//NOFORN

- Reported But Docs Not Released:
  - P2P Traffic High Volume/Low Value
  - GCHQ TEMPORA Minimizes, 30% Ingest Reduction
  - Need To Hide In This Flood

Steganography:
Hiding In Plain Sight

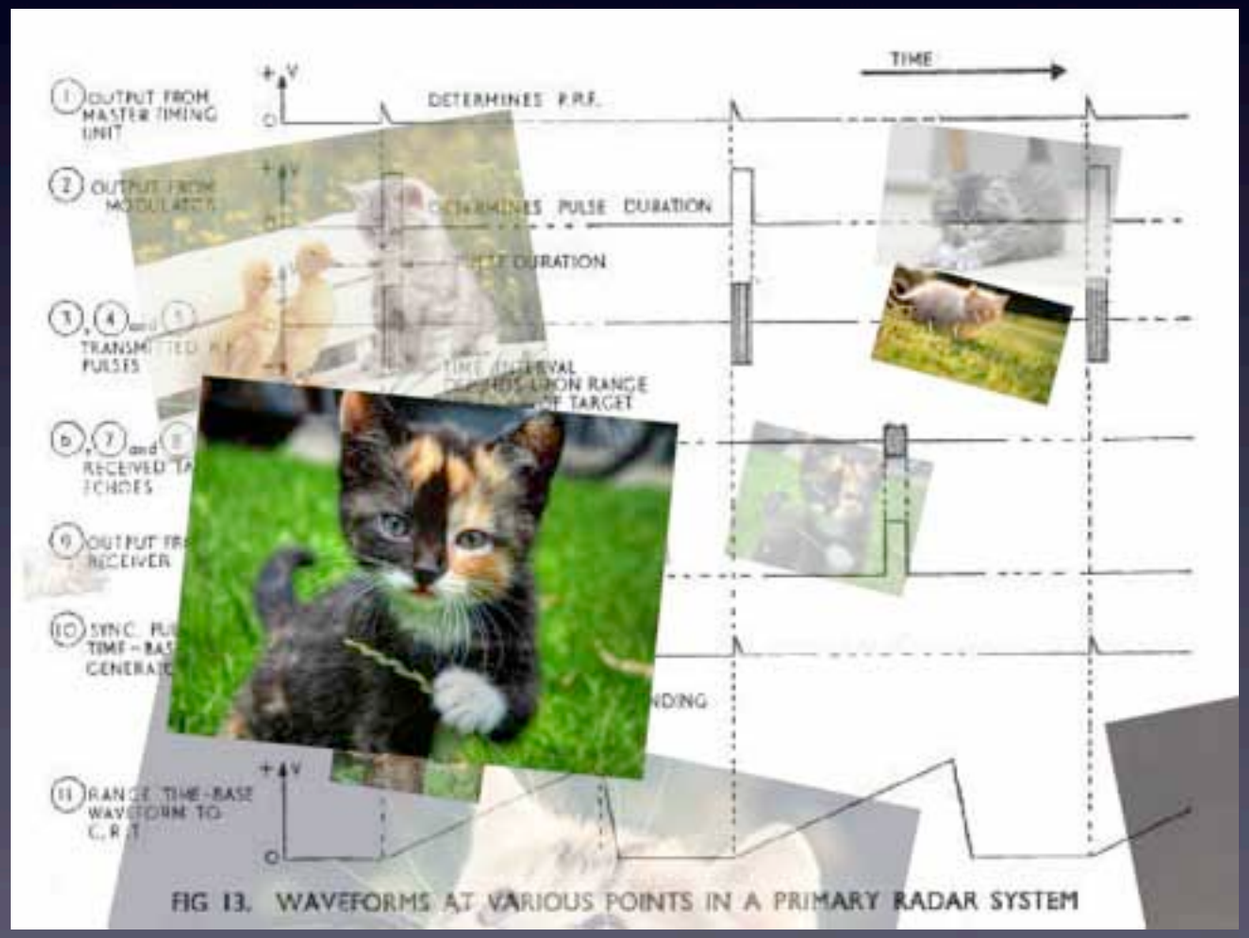
27. Unfortunately, there are issues with undesirable images within the data. It would appear that a surprising number of people use webcam conversations to show intimate parts of their body to the other person. Also, the fact that the Yahoo software allows more than one person to view a webcam stream without necessarily sending a reciprocal stream means that it appears sometimes to be used for broadcasting pornography.

28. A survey was conducted, taking a single image from each of 323 user ids. 23 (7.1%) of those images contained undesirable nudity. From this we can infer that the true proportion of undesirable images in Yahoo webcam is $7.1\% \pm 3.7\%$ with confidence 95%.

[edit] Potentially Undesirable Images

We use face detection to try to censor material which may be offensive but this does not work perfectly so you should read the following before using OPTIC NERVE:

- It is possible to handle and display undesirable images. There is no perfect ability to censor material which may be offensive. Users who may feel uncomfortable about such material are advised not to open them.
- You are reminded that under GCHQ's offensive material policy, the dissemination of offensive material is a disciplinary offence.
- Retrieval of or reference to such material should be avoided; see IB 150 for guidance on dealing with offensive material



H4x0rz: Lose The Ego

<CW-1> you mother fuckers are going to get me raied ["raided," i.e., arrested]
<CW-1> HAHAHAAHA
<@sup_g> we put out 30k cards, the it.stratfor.com dump, and another statement
<@sup_g> dude it's big..
<CW-1> raided
<CW-1> if I get raided anarchaos your job is to cause havok in my honor
<CW-1> <3
<CW-1> sup_g:
<@sup_g> it shall be so

[9] For example, in a chat with the defendant on or about December 26, 2011, discussed in greater detail below, CW-1 referred to the defendant as both "sup_g" and "anarchaos." The defendant responded to both aliases. In a chat with CW-1 over Jabber on or about November 6, 2011, the defendant, using the alias "yohoho," told CW-1 "k im sup_g," that is, identifying himself as both "yohoho" and "sup_g."

- Burner Rules For IDs
- IRL Identity Real And Separate
- Know & Compartmentalize Pseudonyms
- Cred Is Another Enemy
- Really Burn Them, No Really

Don't Fuck It Up, And After You Do:

- Contingency Planning
- Plausible Deniability
- Adversary Capability
- Seek Advice In Advance
  - Support Those Who Provide It
- Good Luck & Never Surrender To Obedience


DANGER
FREE
Wi Fi

Stylometrics: Don't Fuck It Up

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