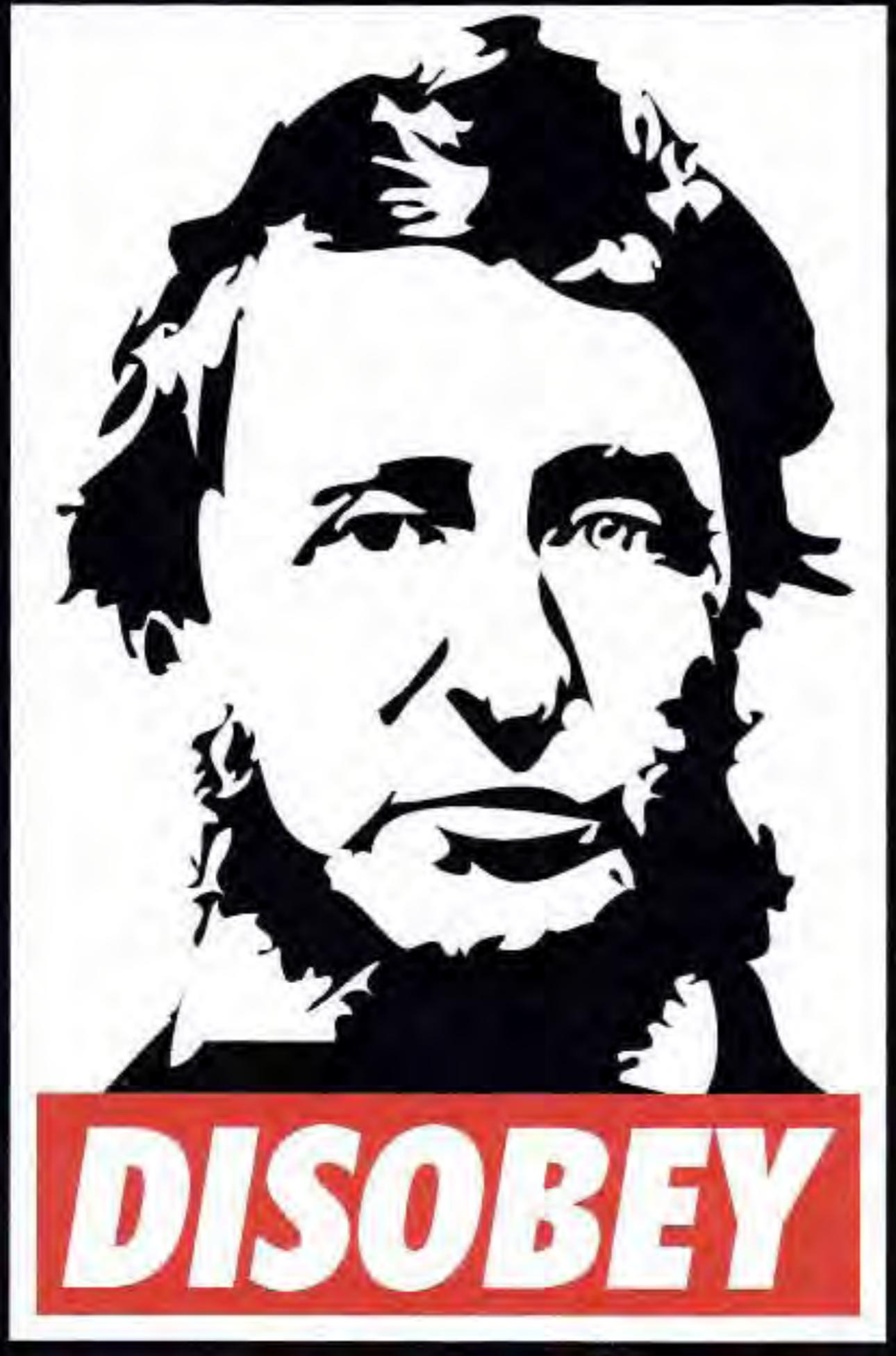




# Don't Fuck It Up!



Zoz



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*

```

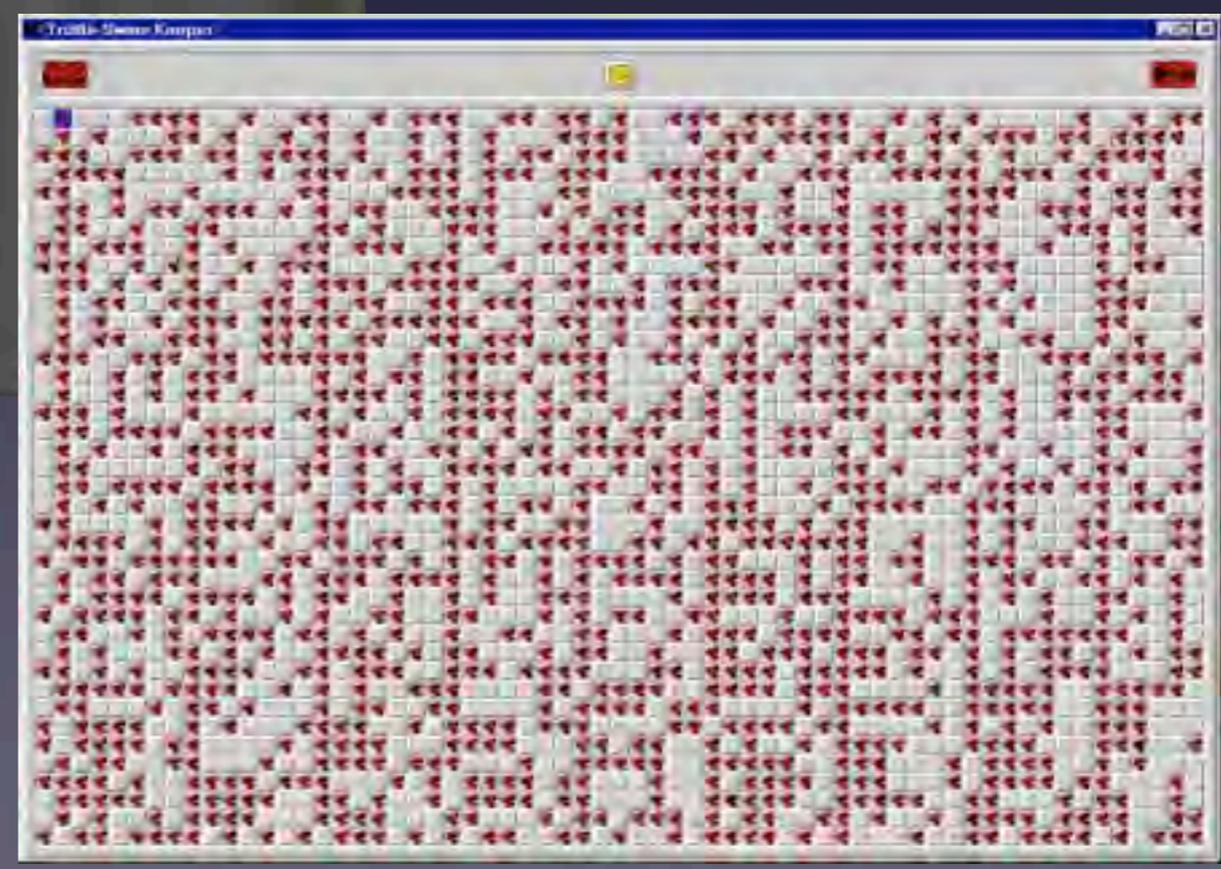
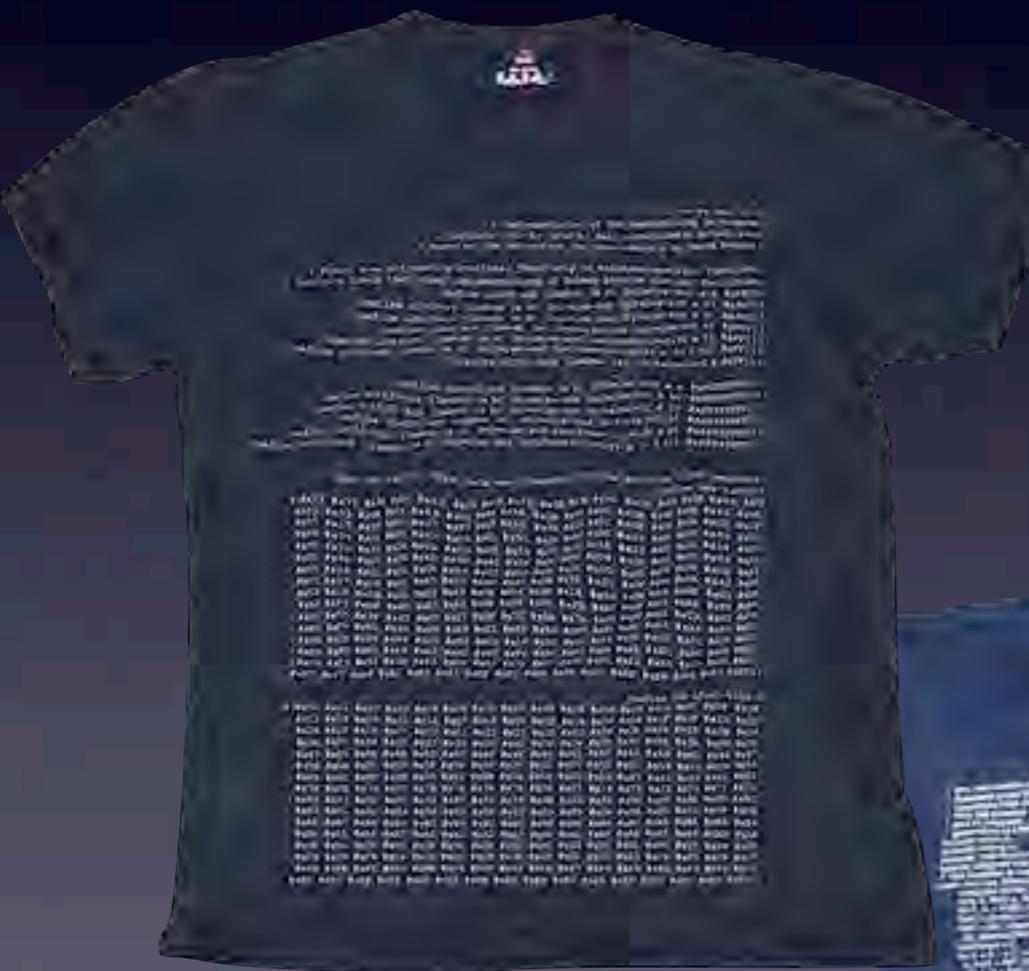
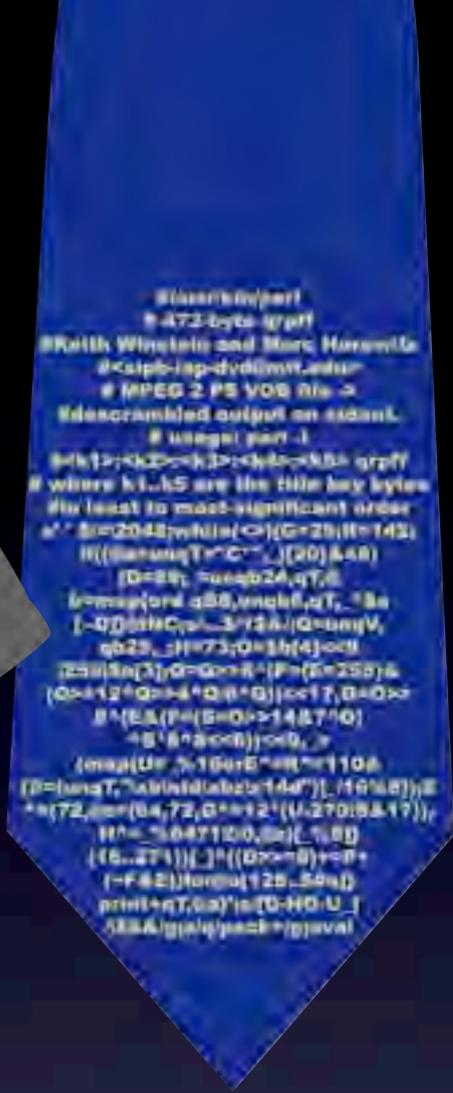
DVDlogo.c
/*
 * efdtt.c Author: Charles M. Hannun <root@ihack.net>
 * Thanks to Phil Carmody <fatphil@asdf.org> for additional tweaks.
 * DVD-logo shaped version by Alex Bowley <alex@hyperspeed.org>
 * Usage is: cat title-key scrambled.vob | efdtt >clear.vob
 */

#define m(l)(x[l]*s[l+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]88+20] /1684 --1 )int
l=m( 1)17 *256 +m(0) 8,k =m(2)
0,j= m(4) 17* m(3) 9*k* 2-k88
*s,s =0,c =-26;for (s[y] --16;
--c;] *-2)a= a*2*14 1,l=l /2*1&l
<<26;for(j= 127; ++j<n;c=0)
y)
c

++y=i*1/8*i>>4*i>>12,
i=i>>8*y<<17,a*=a>>14,y=a*a*8*a<<6,a=a
>>8*y<<8,k=s[j],k =*7No-'G_'216*(k
47)+2**cr3afw6v;*k>>/n.**(k>>4)+2*k*257/
8,s[j]=k*(k&k*2434)+6*c-y
}}

```





# Spy Eye v1.3

Encryption key (for config):

smthrandomkey

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 v3.07w1**

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:

\* Mutex name:



Make config & get build



419eater.com



FUCK IT UP

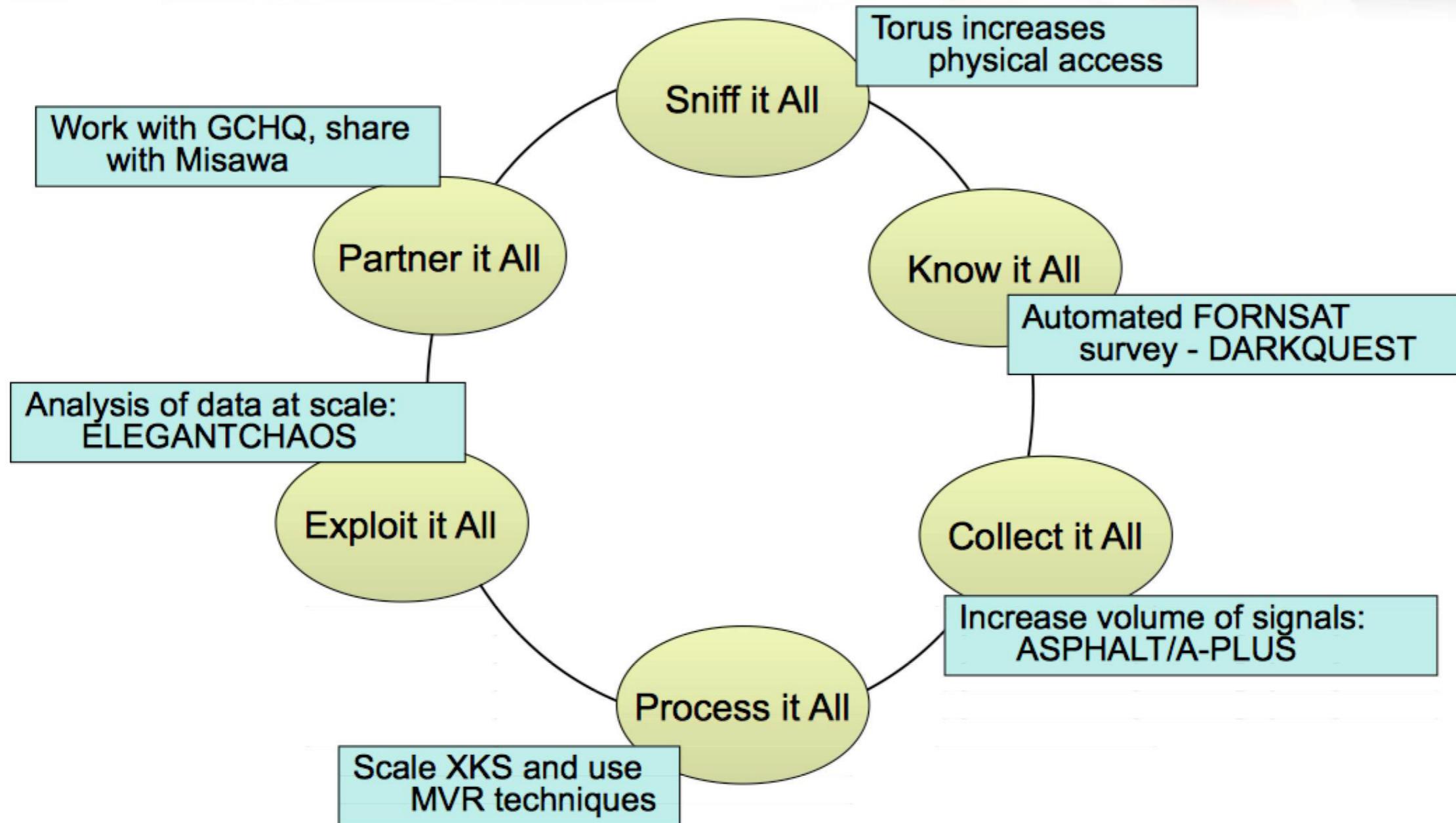


**NSA** ILLEGAL  
SPYING  
BELOW

[StandAgainstSpying.org](http://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.ioos.gov](http://www.ioos.gov)

## The OPSEC Process:

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



THINK ABOUT IT... ALL THE TIME!



## 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



Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
158	50.727396000	10.1.10.233	224.0.0.176	IAPP	128	Announce Response(1) (version=1)
159	50.728072000	10.1.10.233	224.0.0.176	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 _amb.
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

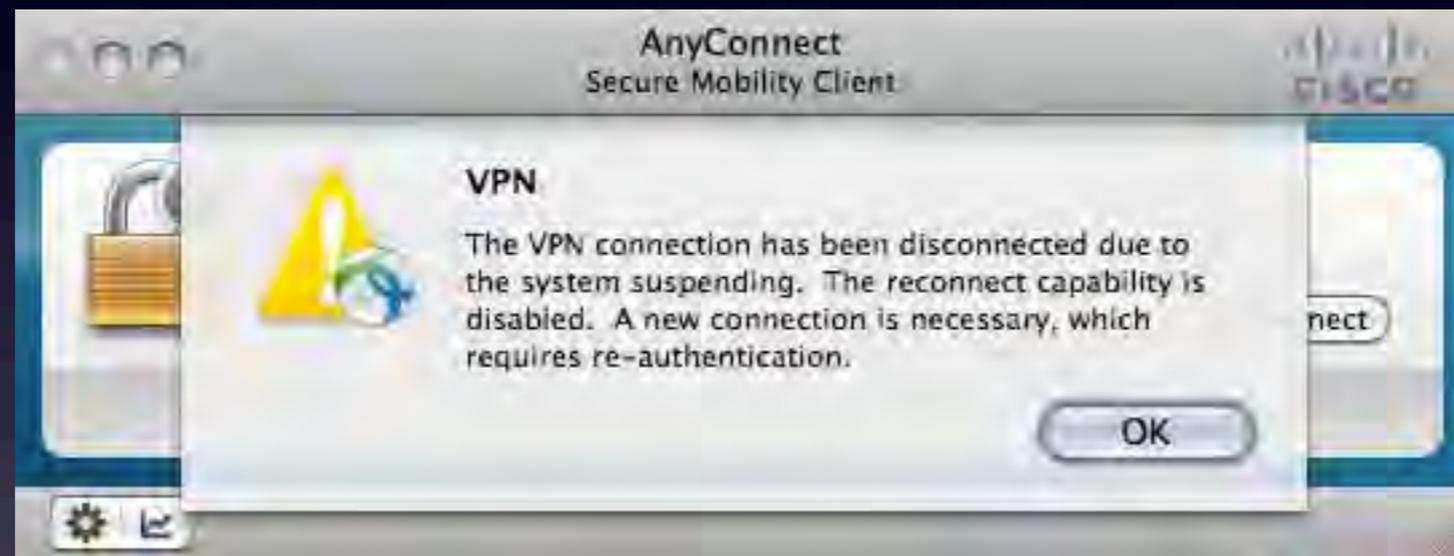
Frame 21: 60 bytes on wire (480 bits) captured (480 bits) on interface 0

```

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 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0010	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

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

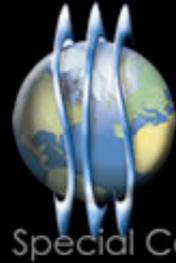


```
% killall -STOP Mail thunderbird Google Safari Firefox Adium Dropbox
% killall -CONT Mail thunderbird Google Safari Firefox Adium Dropbox
```

# 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**



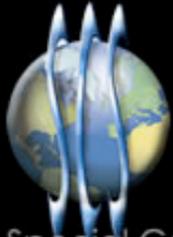
Special Collection Service

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

# 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?

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



Special Collection Service

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

# SCS Opportunities





# Private Networks are Important

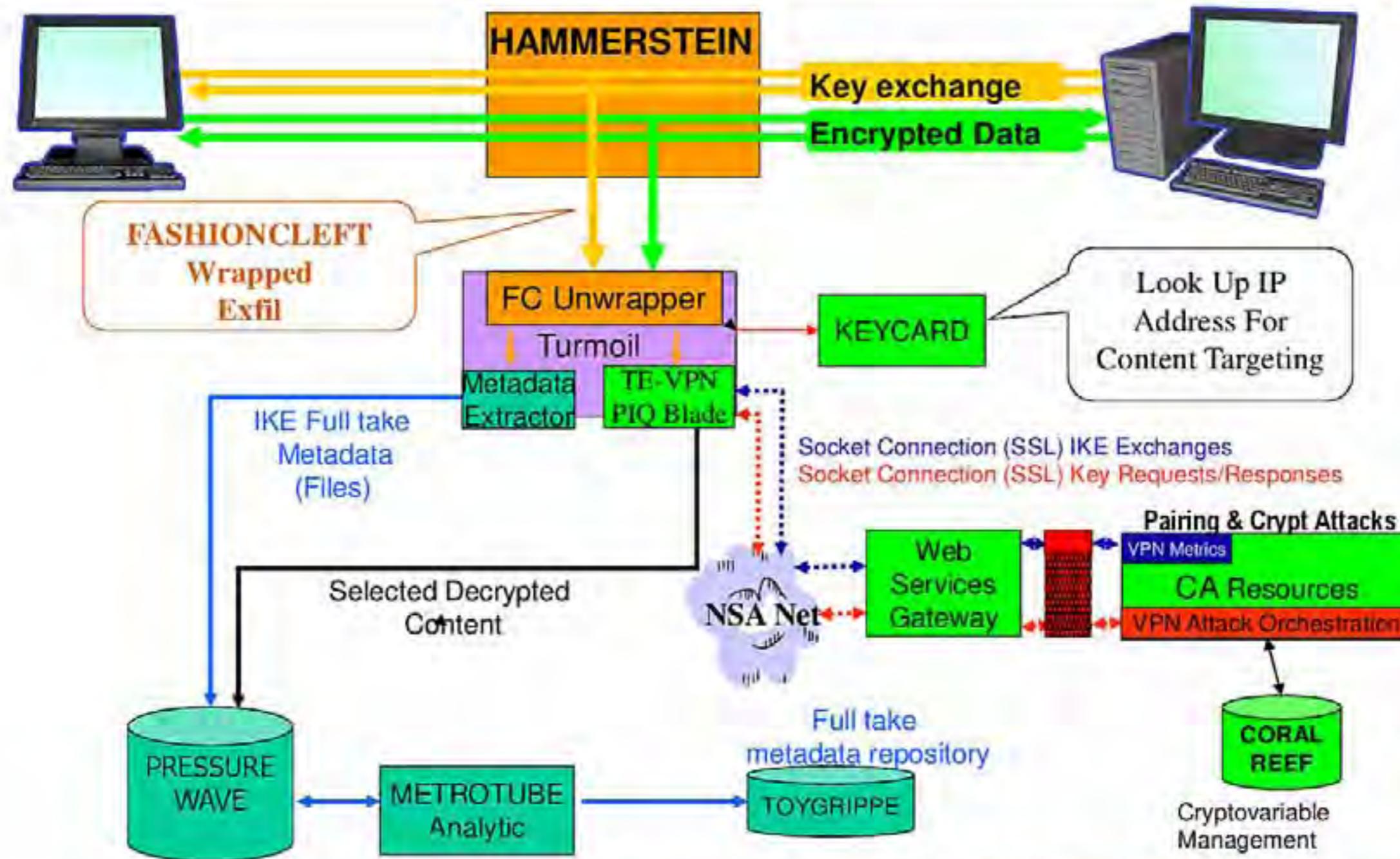
- Many targets use private networks.

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:

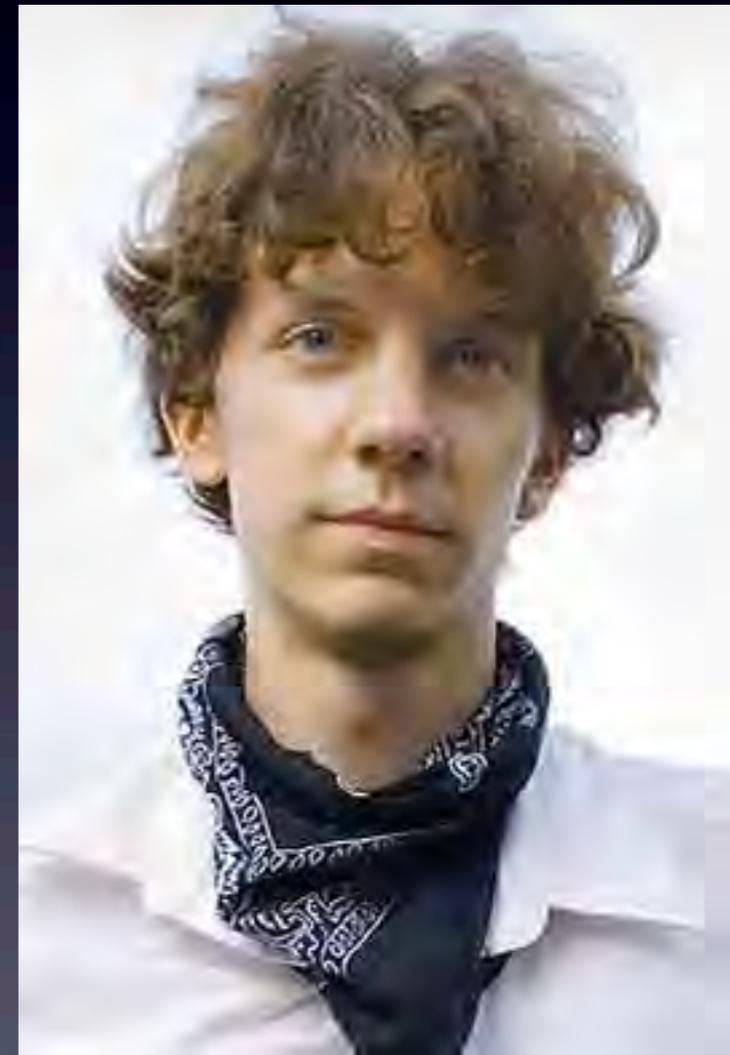
PPTP Broken As Of



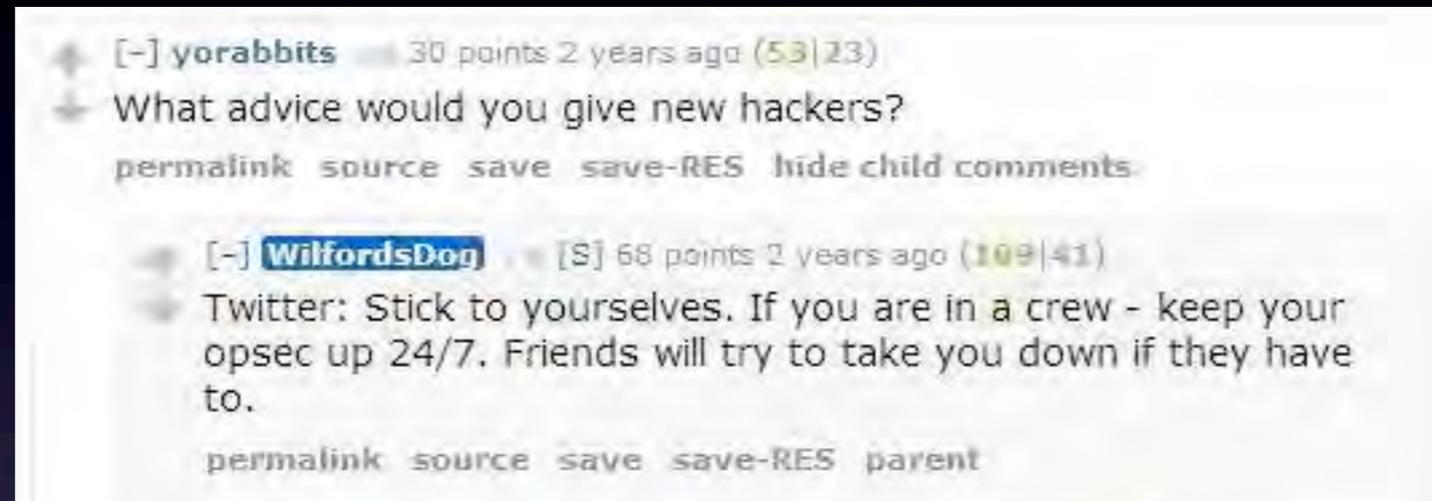
Don't Fuck It Up  
When You Use



# Case Study: LulzSec/AntiSec

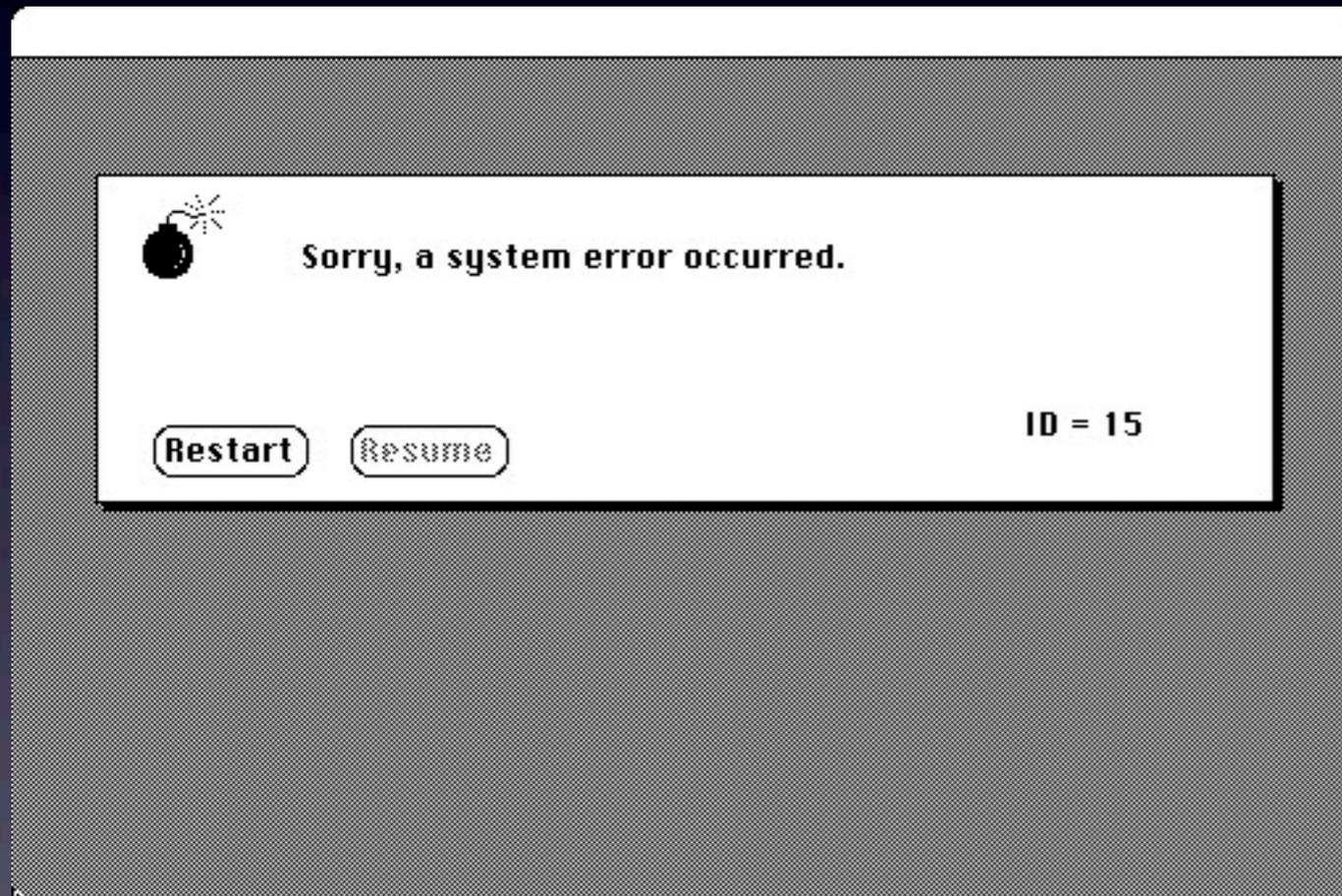


# Moral:



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

# Case Study: Harvard Bomb Hoax



# 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... (1)

- 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.

## Analytics:

### Goes In/ta Goes Outta/Low Latency (5/7/30)

- 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)

## Analytics: Cookie Leakage (11/1/50)

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

## Exploitation: QUANTUM (11/1/50)

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

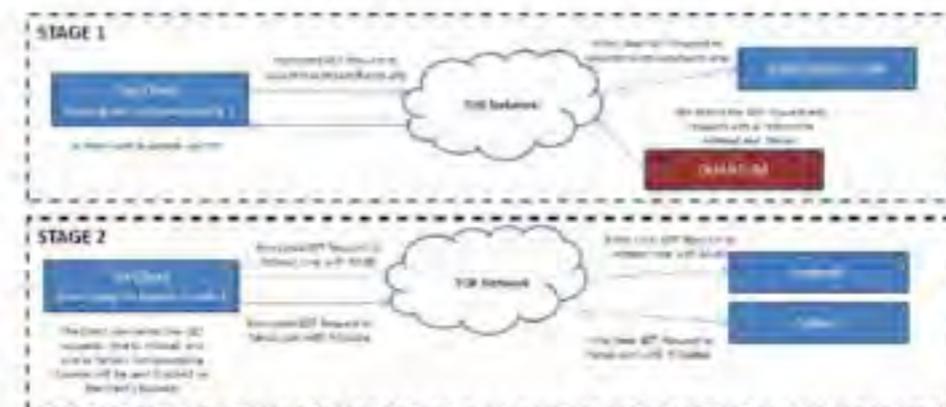


Figure 4: A diagram of how the QUANTUM exploit technique works.

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

## (C//REL) Types of IAT – Advanced Open Source Multi-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* us
  - (S//REL) Still the King of high secure, low latency Internet Anonymity
    - (S//REL) There are no contenders for the throne in waiting



TOP SECRET//COMINT REL TO USA,FVEY

TOP SECRET//SI//REL TO USA,FVEY  
(S//REL) *Tor* Project and friends Recent Activity



# Tails

the amnesic incognito live system

- (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/torproject_visit')=http_host('www.torproject.org')
  and not(xff_cc('US' OR 'GB' OR 'CA' OR 'AU' OR 'NZ'));
```

```
// 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
```

```
// 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/' | 0++
  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::define_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 FLAG = "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"] = FLAG;
      DB.apply();
    }
    xks::fire_fingerprint("anonymizer/tor/directory/bridge");
  }
  return true;
  )];
```

```
// END_DEFINITION
```

# Case Study: Silk Road/DPR



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



# What Fucked It Up?

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

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

WHERE CAN YOU FIND THE BEST WEB DEVELOPERS FOR YOUR TEAM?

CAREERS 2.0

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

```
25 curl - 'http://[hidden]([ip]wamp).onion/'  
Sch = 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, CURLOPT_PROXY_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

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

## anonymous market online?

#1386085 · 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](http://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: 🐼 🐼 🐼

IT pro needed for venture backed bitcoin startup  
October 31, 2011, 09:08:23 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 [resubright@gmail.com](mailto:resubright@gmail.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.



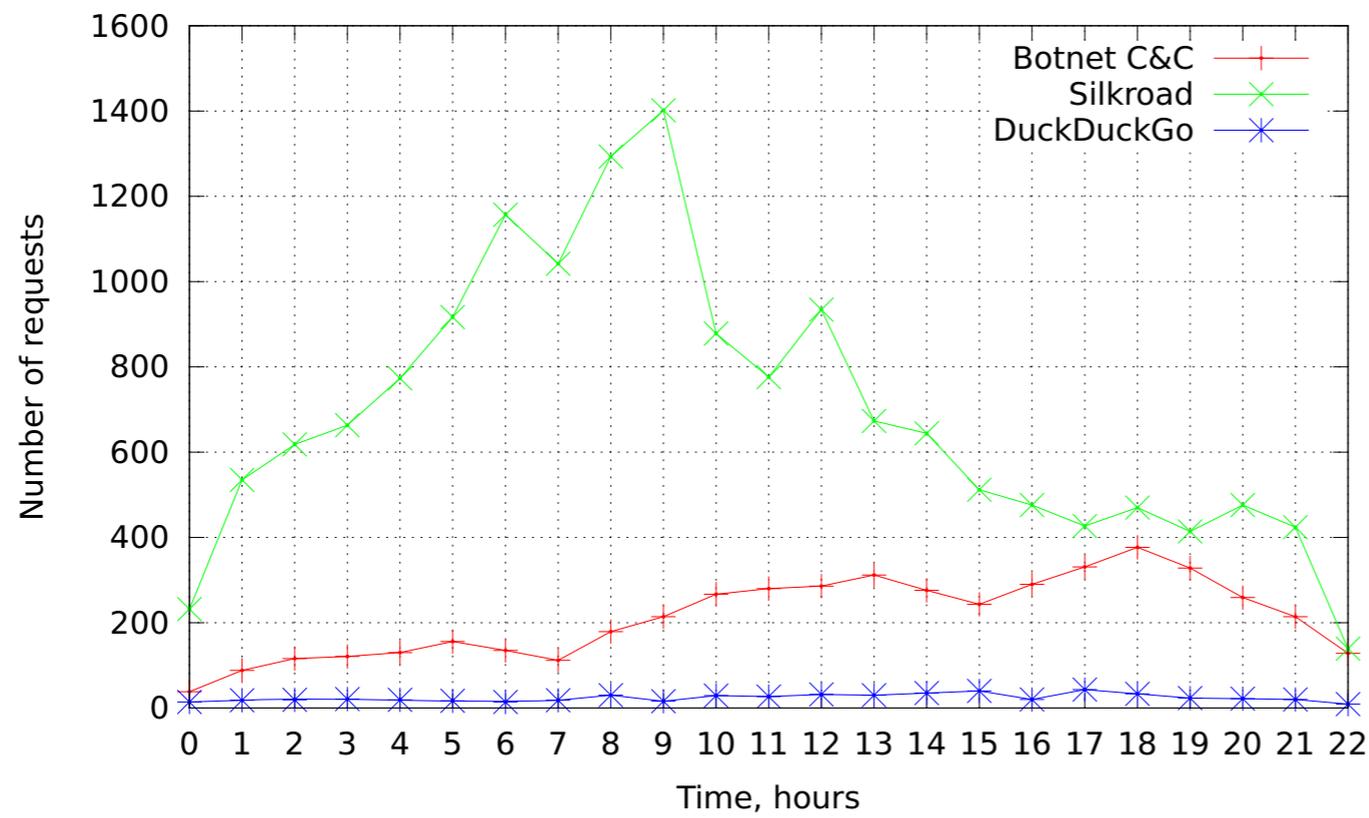


Figure 4. Hidden service descriptor request rate during one day.

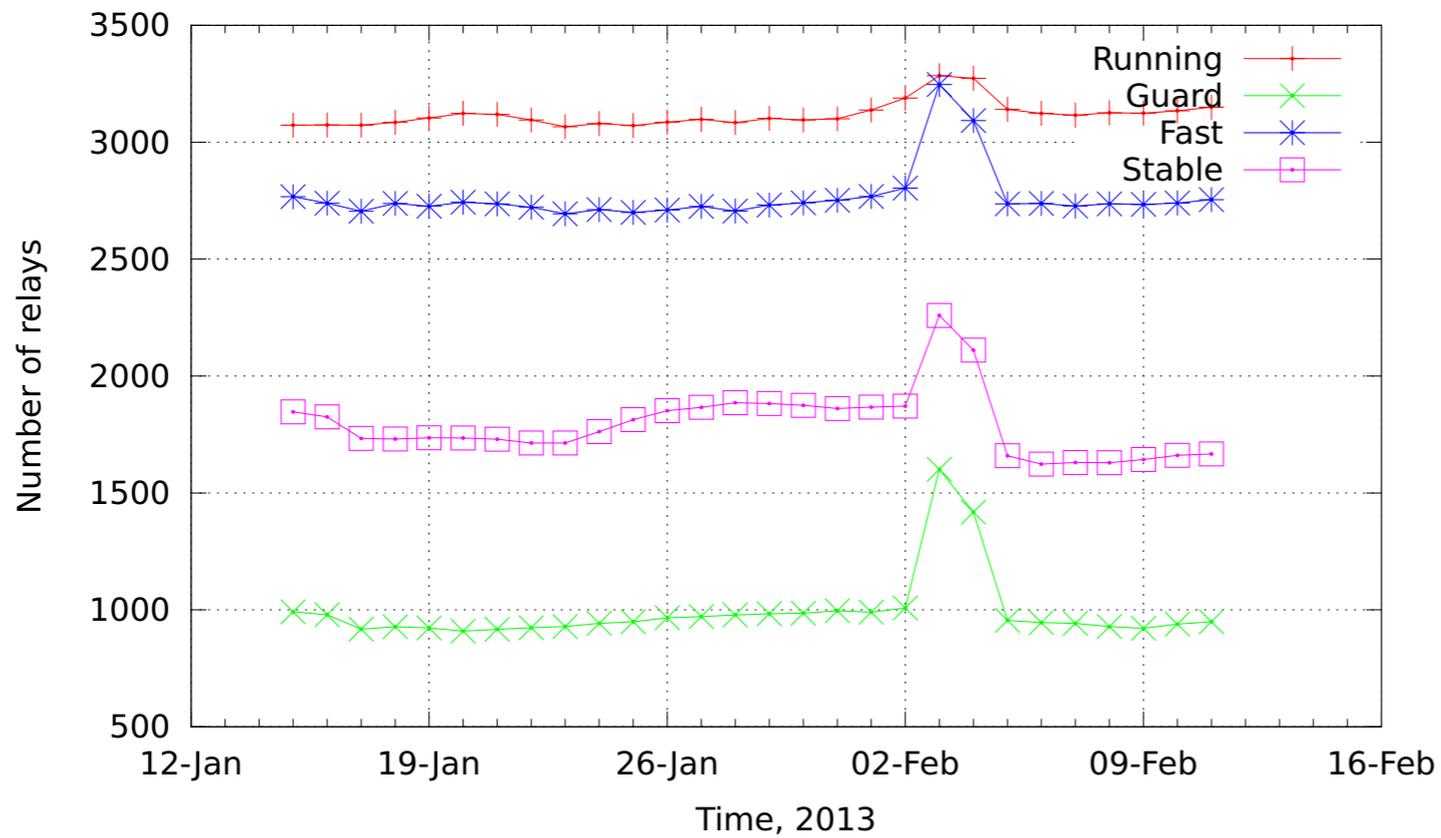


Figure 6. Increase in the number of Guard nodes.

## Technical Analysis: Hidden Services

(TS//SI)

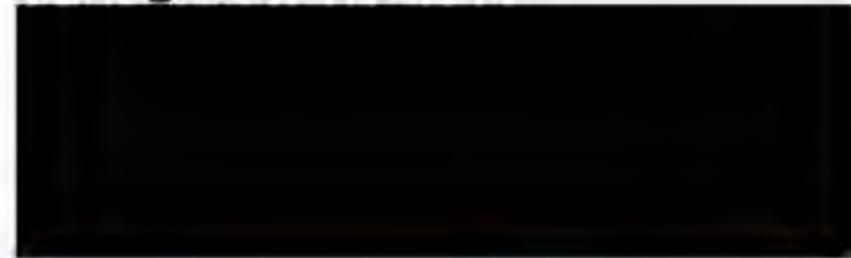
What do we know about Hidden Services?

- 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

(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.



TOP SECRET STRAP1 COMINT  
 The maximum classification allowed on GCWiki is **TOP SECRET STRAP1 COMINT**. Click to report inappropriate content.  
 For GCWiki help contact: [Support page](#)

# 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



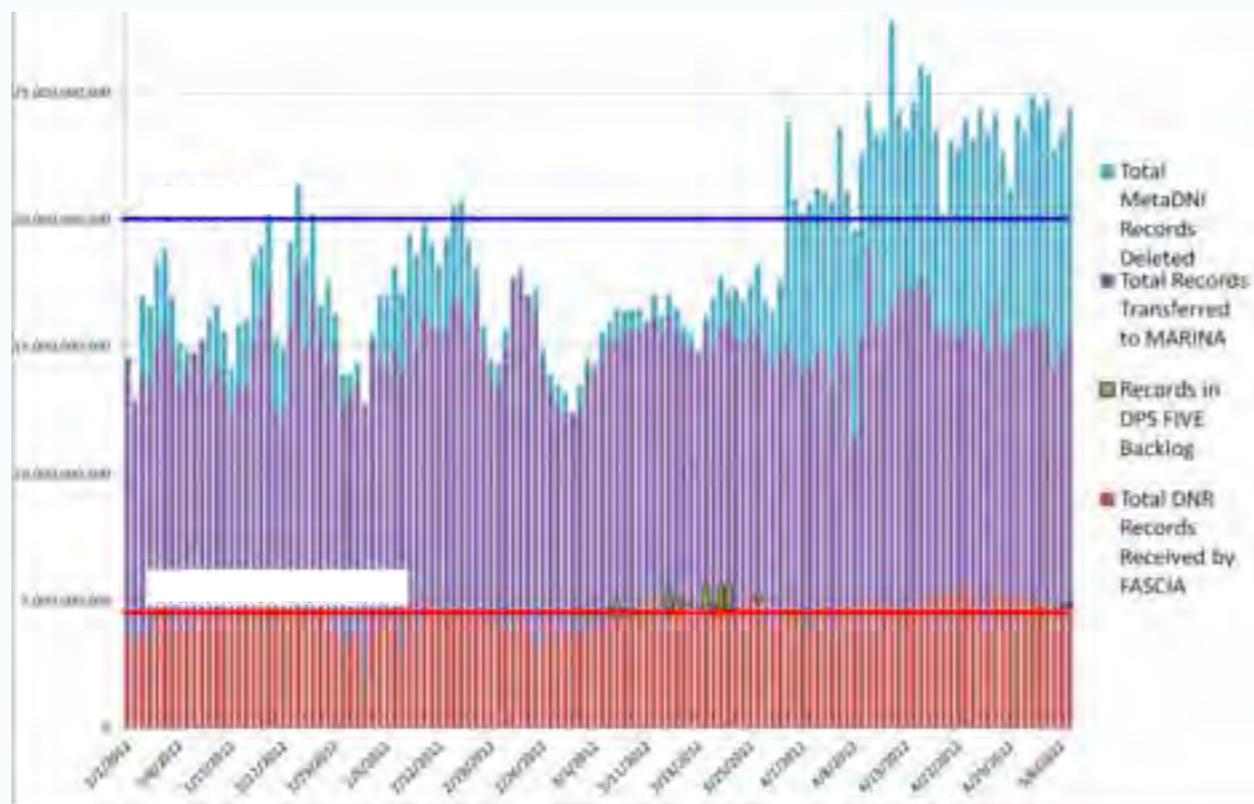
<b>ALLIUM ARCH</b>	JTRIG UIA via the Tor network.	OPERATIONAL	JTRIG Infrastructure Team <a href="#">✉</a>
<b>ASTRAL PROJECTION</b>	Remote GSM secure covert internet proxy using TOR hidden services.	OPERATIONAL	JTRIG Infrastructure Team <a href="#">✉</a>
<b>NUT ALLERGY</b>	JTRIG Tor web browser - Sandbox IE replacement and FRUIT BOWL sub-system	PILOT	JTRIG Infrastructure Team <a href="#">✉</a>
<b>BUMBLEBEE DANCE</b>	JTRIG Operational VM/TOR architecture	OPERATIONAL	JTRIG Infrastructure Team <a href="#">✉</a>
<b>SILVER SPECTER</b>	Allows batch Nmap scanning over TOR		JTRIG Software Developers <a href="#">✉</a> In Development
<b>SHADOWCAT</b>	End-to-End encrypted access to a VPS over SSH using the TOR network		JTRIG OSO <a href="#">✉</a>

# 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	<b>PDDG</b>

## (U) Converged Analysis of Smartphone Devices

Identification/Processing/Tasking –  
All in a day's work



## Golden Nugget!

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

What can we get?



## Targeting

Targeting both Telephony and DNI systems

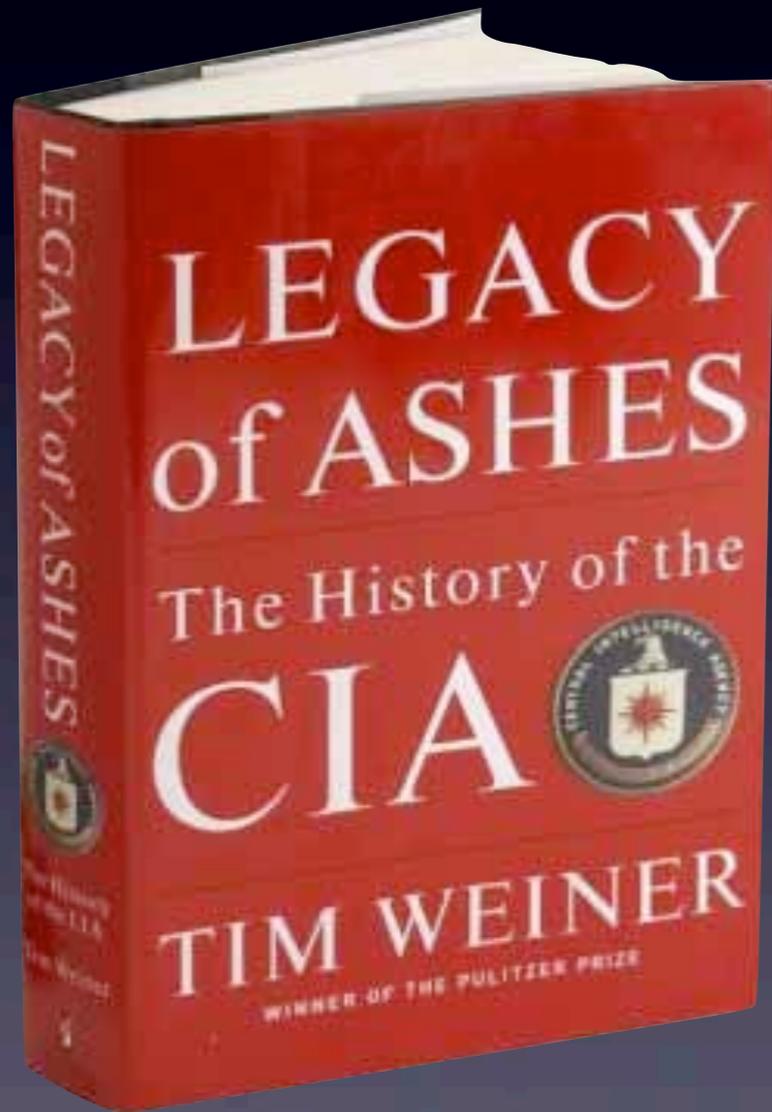
- Call Logs
- SMS
- SIM Card Leads
- Email address
- IMEI/IMSI
- Unique Identifiers
- Blackberry PINS



## 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

# 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



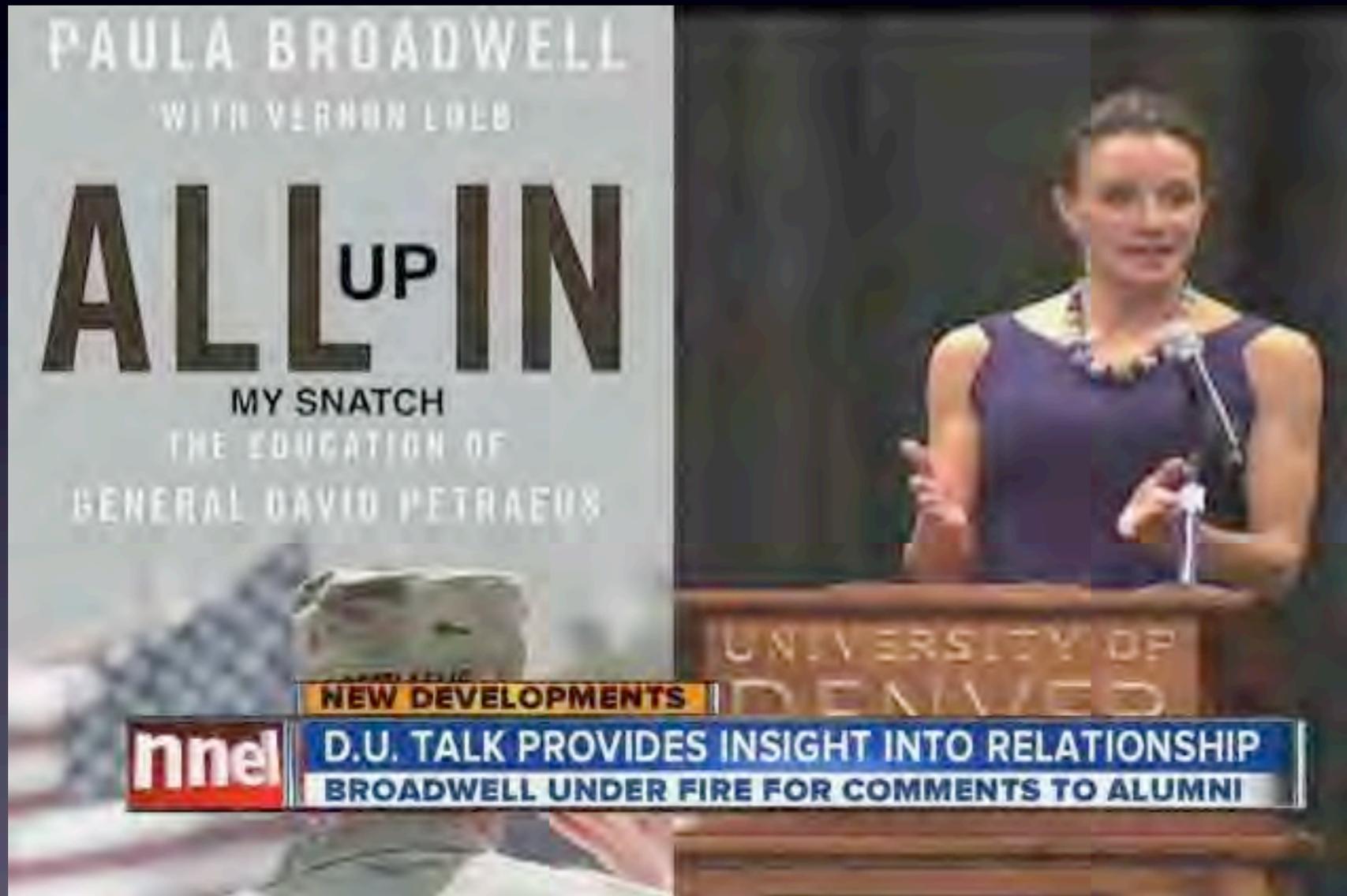
# Don't Fuck It Up When You Use Messaging

- 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 SO Principle

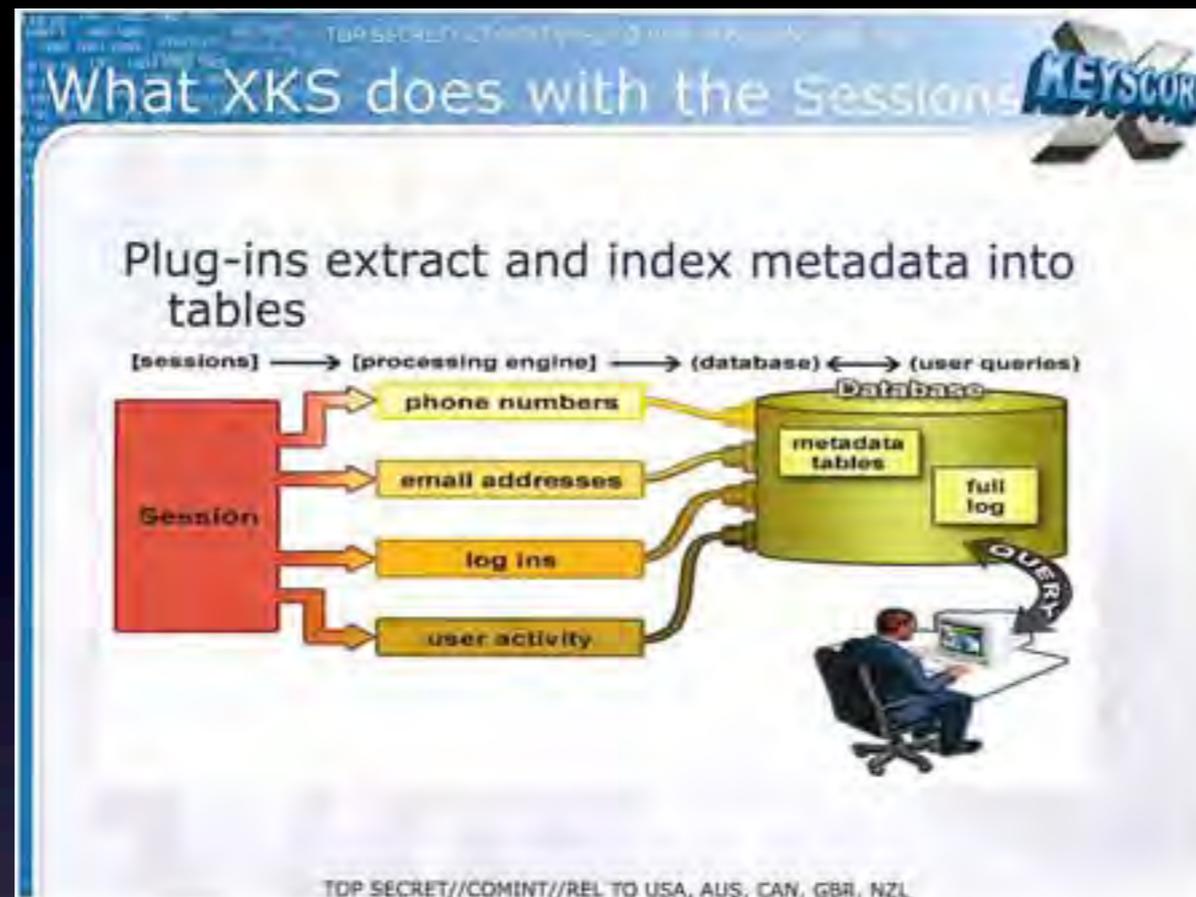


Threadworm in sheep intestine

# 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?"

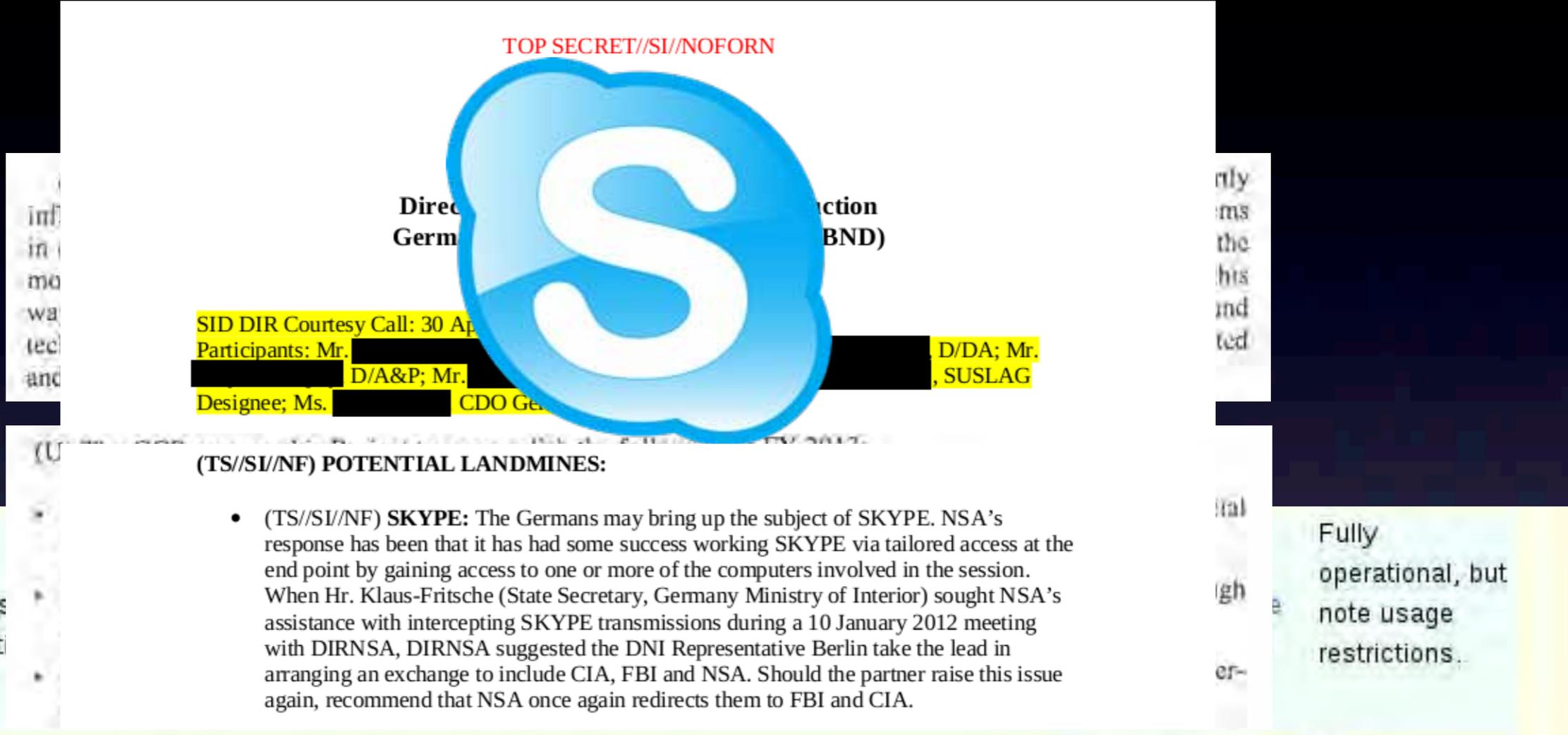
# Common Broken/Compromised Services



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

# Common Broken/Compromised Services

TOP SECRET//SI//NOFORN



Directorate of National Security (BND)

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

(U) (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 s 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.)

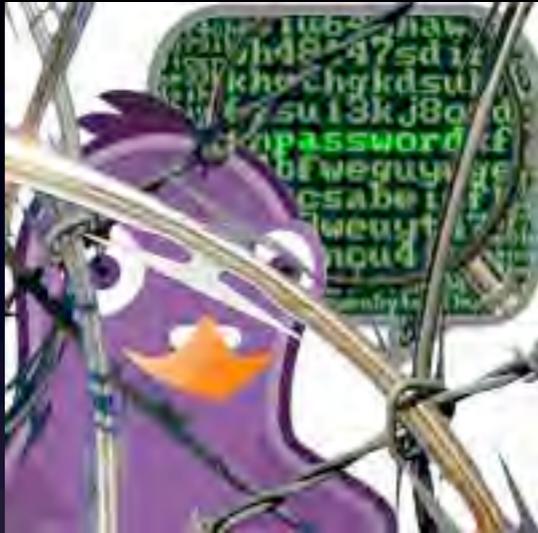
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

## 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
  - 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?
- We Need More:
  - Auditing
  - Steganography



# Stylometrics: Don't Fuck It Up

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



# 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//COMINT//REL TO USA, FVEY

## The Challenge

Collection is outpacing our ability to ingest, process and store to the “norms” to which we have become accustomed.

- 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

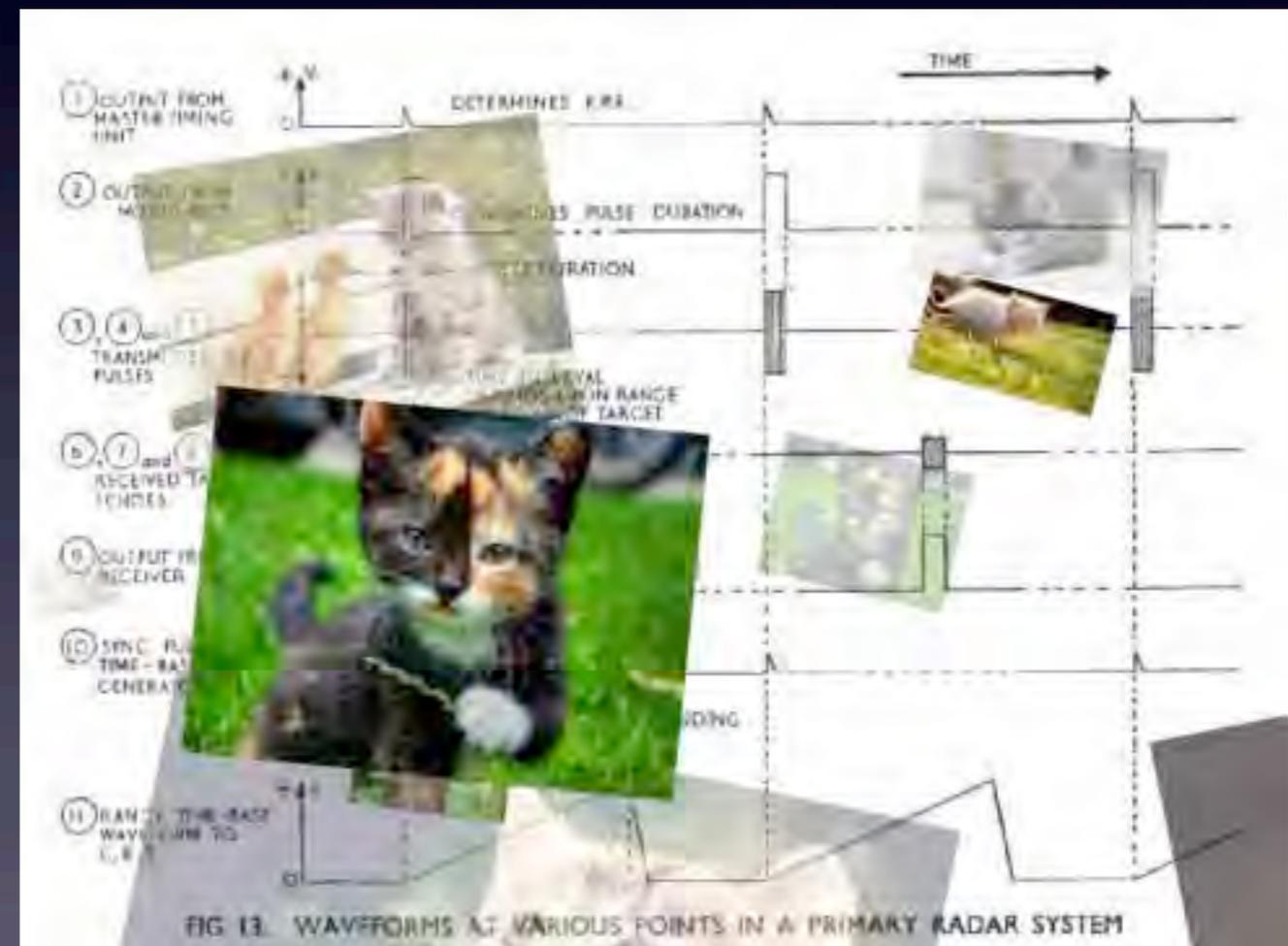
27. Unfortunately, there are issues with undesirable images within the data. It would appear that a surprising number of people use webcam conversations to show intimate parts of their body to the other person. Also, the fact that the Yahoo software allows more than one person to view a webcam stream 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> HAHAAHAHA  
<@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
```

<sup>9</sup> 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



