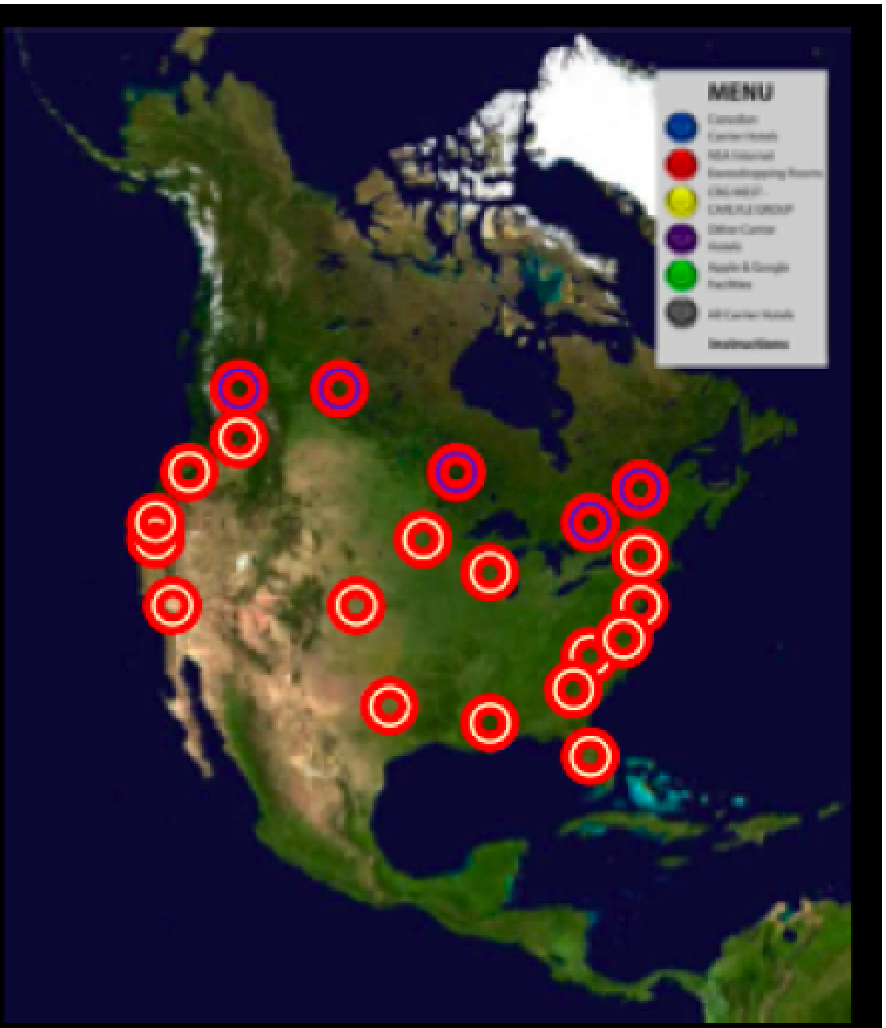
IXmaps.ca

Interactively mapping NSA surveillance points in the internet “cloud”



Andrew Clement,[1] Nancy Paterson,[1,2] David Phillips[1]

[1] Faculty of Information, University of Toronto

[2] Ontario College of Art and Design

Overview

- NSA warrantless surveillance
- Internet routing
- Mapping packet paths
- Outting the NSA sites
- Future work

Background

- Much is going on ‘inside’ the internet, but out of sight, that should concern users and policy advocates:
  - **Surveillance (e.g.**
    - **Eavesdropping by the NSA and other security agencies)**
    - Deep packet inspection (DPI) by ISPs/carriers
  - Discriminatory traffic management and blockage
  - Excessive energy consumption
  - Oligopolistic and anti competitive business practices
- There is relatively little critical research into, or public understanding of, internet backbone structure and operation
- Prevailing metaphors, such as ‘dumb core/ intelligent edges’ and ‘cloud computing’, obscure important insights and possibilities for action

Research ambitions

- Make visible to users interesting internet backbone/core phenomena related to everyday usage
  - e.g. NSA surveillance, DPI, Carrier Hotel ownership, energy (in)efficiency, …
- Promote an understanding of the internet core amenable to public policy engagement
- Develop a research tool for conducting critical internet backbone investigations, and for presenting findings publically
- Enroll others (users, activists, researchers) in building the database of internet sites of interest

NSA Warrantless Surveillance

2005/6: Mark Klein, AT&T whistleblower:

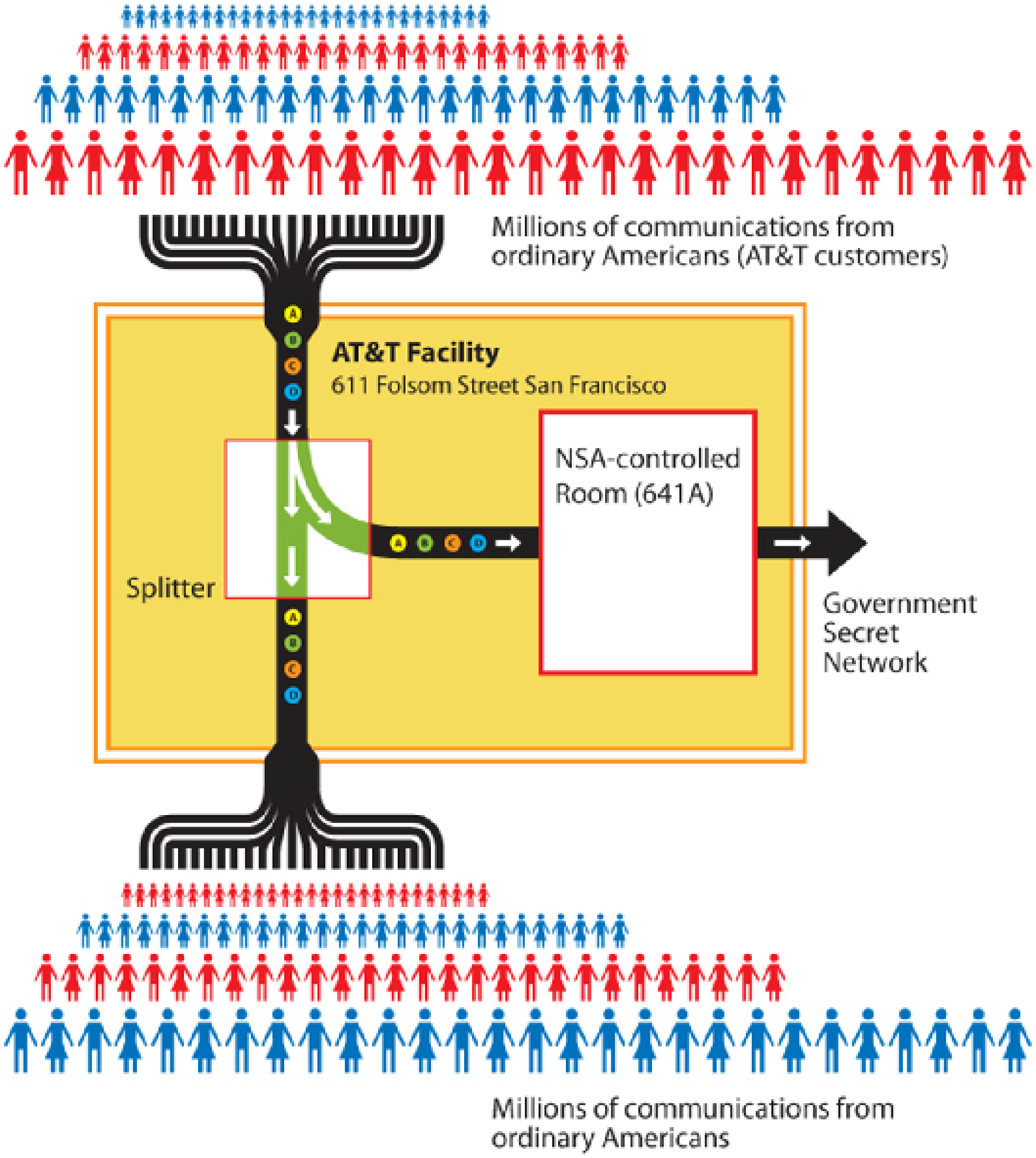
- Installation of “Splitter room” at 611 Folsom St, San Francisco at the request of National Security Agency
- 40+ court cases against US government, AT&T, Verizon/MCI, BellSouth, Sprint & Cingular
- Estimated 15-20 splitter sites in US (Bamford, 2008)

2008 July: Foreign Intelligence Surveillance Act amended giving telecom carriers immunity from prosecution

2010 March 31: Judge Walker finds “N.S.A. Wiretaps Were Illegal" (NYT), rejects “state secrets privilege”

EFF's view:

Intercepting Communications at AT&T Folsom Street Facility



Millions of communications from ordinary Americans (AT&T customers)

AT&T Facility
611 Folsom Street San Francisco

Splitter

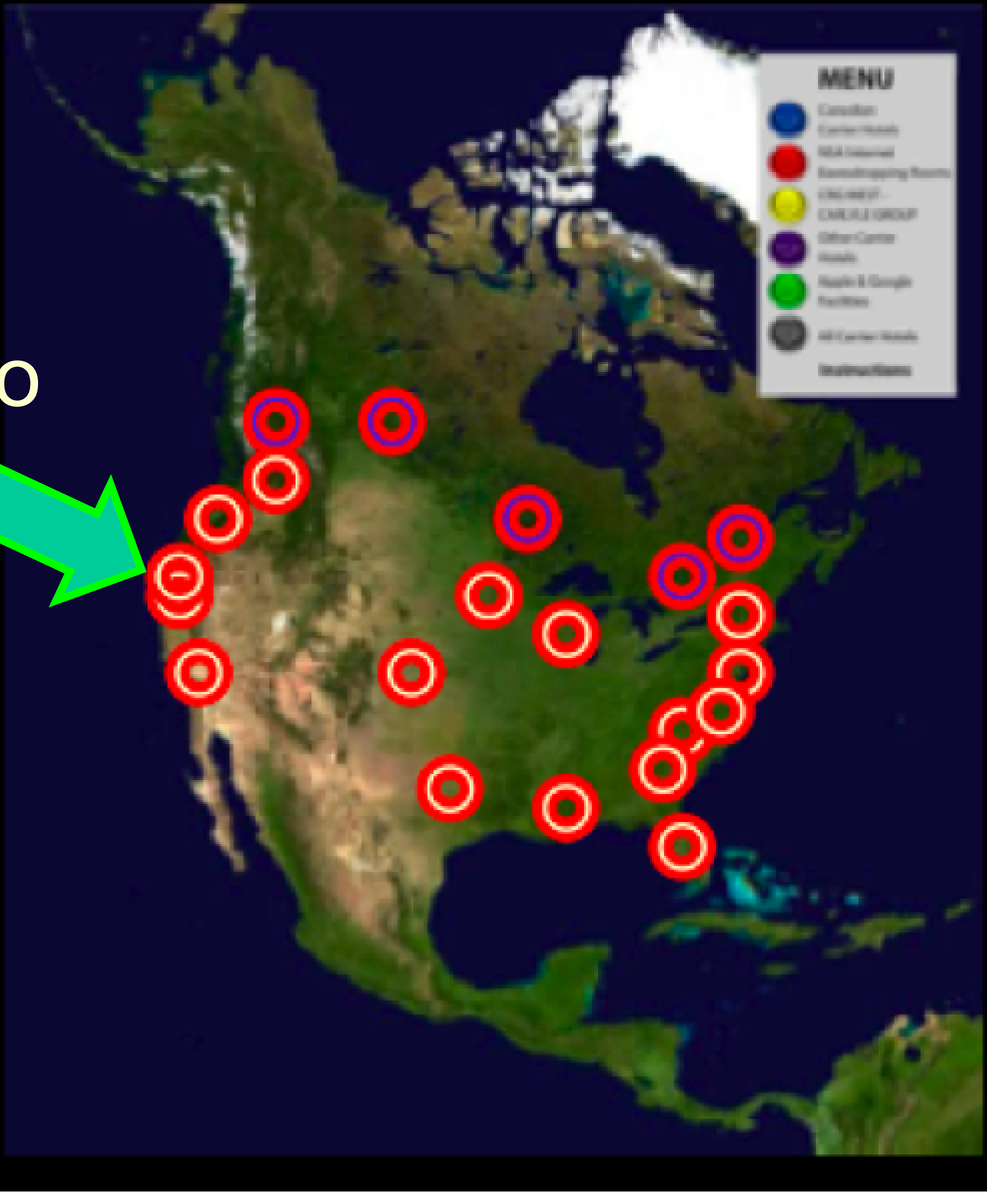
NSA-controlled Room (641A)

Government Secret Network

Millions of communications from ordinary Americans

Suspected splitter sites

611 Folsom
Street,
San Francisco



Internet routing basics

To: Mom@herISP.com

Msg: Hi Mom! love, Son

Internet routing basics – DNS lookup

To: Mom@herISP.com

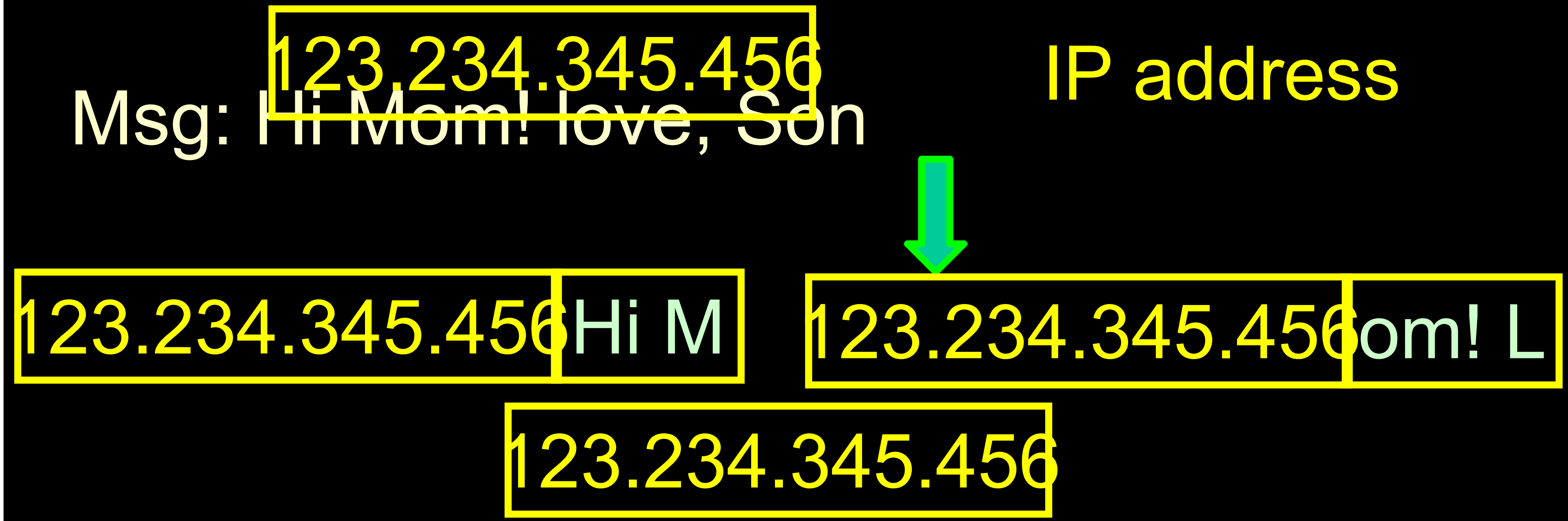
123.234.345.456

IP address

Msg: Hi Mom! love, Son

Internet routing basics – packets

To: Mom@herISP.com



Msg: Hi Mom! love, Son

123.234.345.456

IP address

123.234.345.456 Hi M

123.234.345.456 om! L

123.234.345.456

These packets are transferred from one router to another until they reach their destination

Each intermediate router has its own unique IP address

Generating Traceroutes via IXmaps

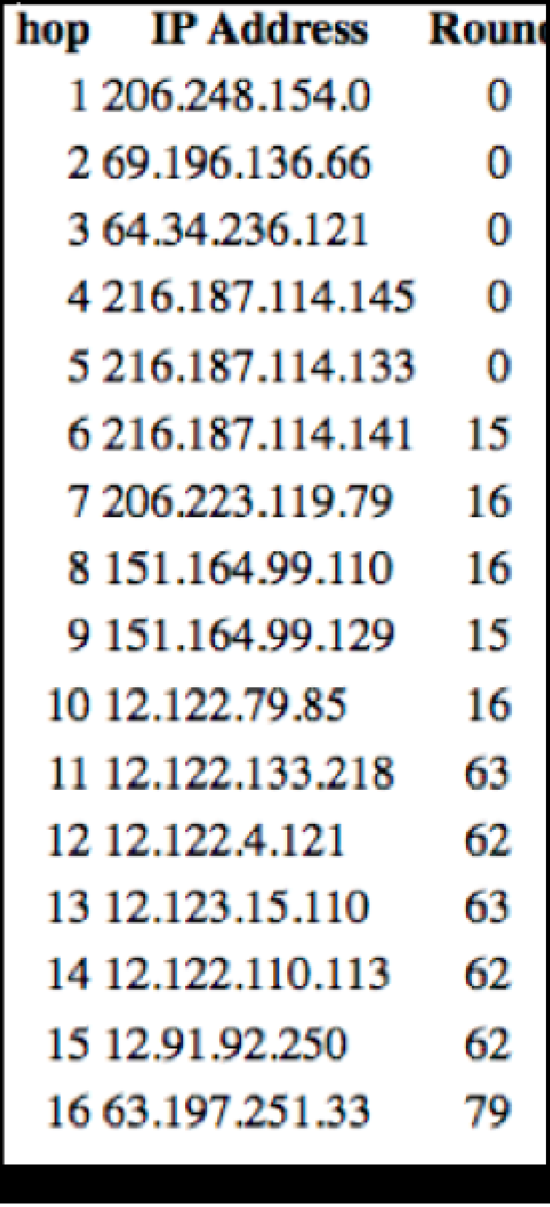
Building a database of traceroutes in NA

- TRgen installable software – ‘crowd sourcing’
- Destination address collections
  - Universities on the NA periphery e.g. http://ucsd.edu
  - Sites near 611 Folsom Street e.g. http://sfai.edu
  - User chosen
- Immediate storage in the IXmaps.ca database

Current status: ~30 contributors, ~3000 traceroutes

+ Internet exchange points (IXPs) aka carrier hotels
  e.g. location, NSA, ownership, carriers, …

Trace route – basic (TR#1859)

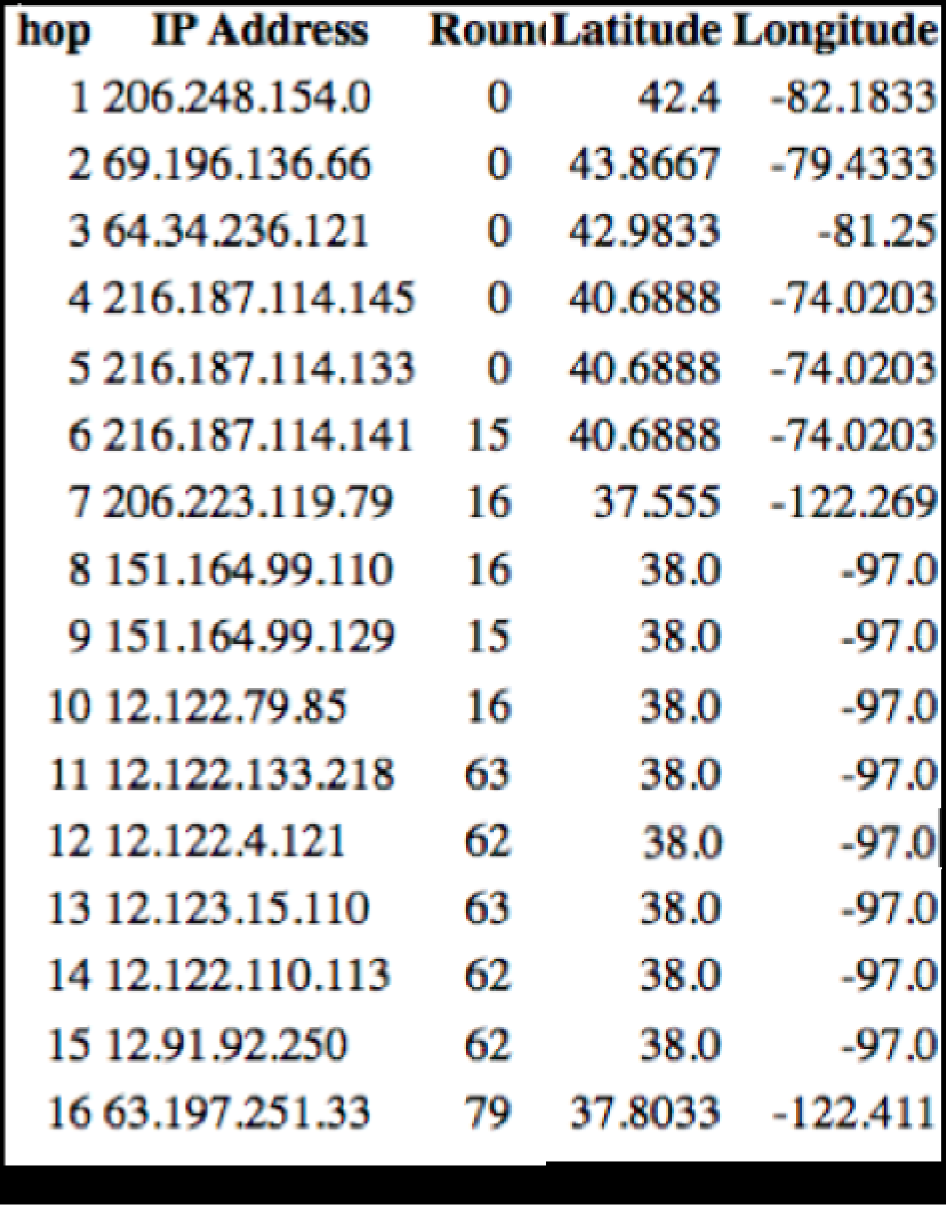


hop	IP Address	Roun
1	206.248.154.0	0
2	69.196.136.66	0
3	64.34.236.121	0
4	216.187.114.145	0
5	216.187.114.133	0
6	216.187.114.141	15
7	206.223.119.79	16
8	151.164.99.110	16
9	151.164.99.129	15
10	12.122.79.85	16
11	12.122.133.218	63
12	12.122.4.121	62
13	12.123.15.110	63
14	12.122.110.113	62
15	12.91.92.250	62
16	63.197.251.33	79

Toronto home

San Francisco
Art Institute

Trace route + Lat/Long (Maxmind)



hop	IP Address	Roun	Latitude	Longitude
1	206.248.154.0	0	42.4	-82.1833
2	69.196.136.66	0	43.8667	-79.4333
3	64.34.236.121	0	42.9833	-81.25
4	216.187.114.145	0	40.6888	-74.0203
5	216.187.114.133	0	40.6888	-74.0203
6	216.187.114.141	15	40.6888	-74.0203
7	206.223.119.79	16	37.555	-122.269
8	151.164.99.110	16	38.0	-97.0
9	151.164.99.129	15	38.0	-97.0
10	12.122.79.85	16	38.0	-97.0
11	12.122.133.218	63	38.0	-97.0
12	12.122.4.121	62	38.0	-97.0
13	12.123.15.110	63	38.0	-97.0
14	12.122.110.113	62	38.0	-97.0
15	12.91.92.250	62	38.0	-97.0
16	63.197.251.33	79	37.8033	-122.411

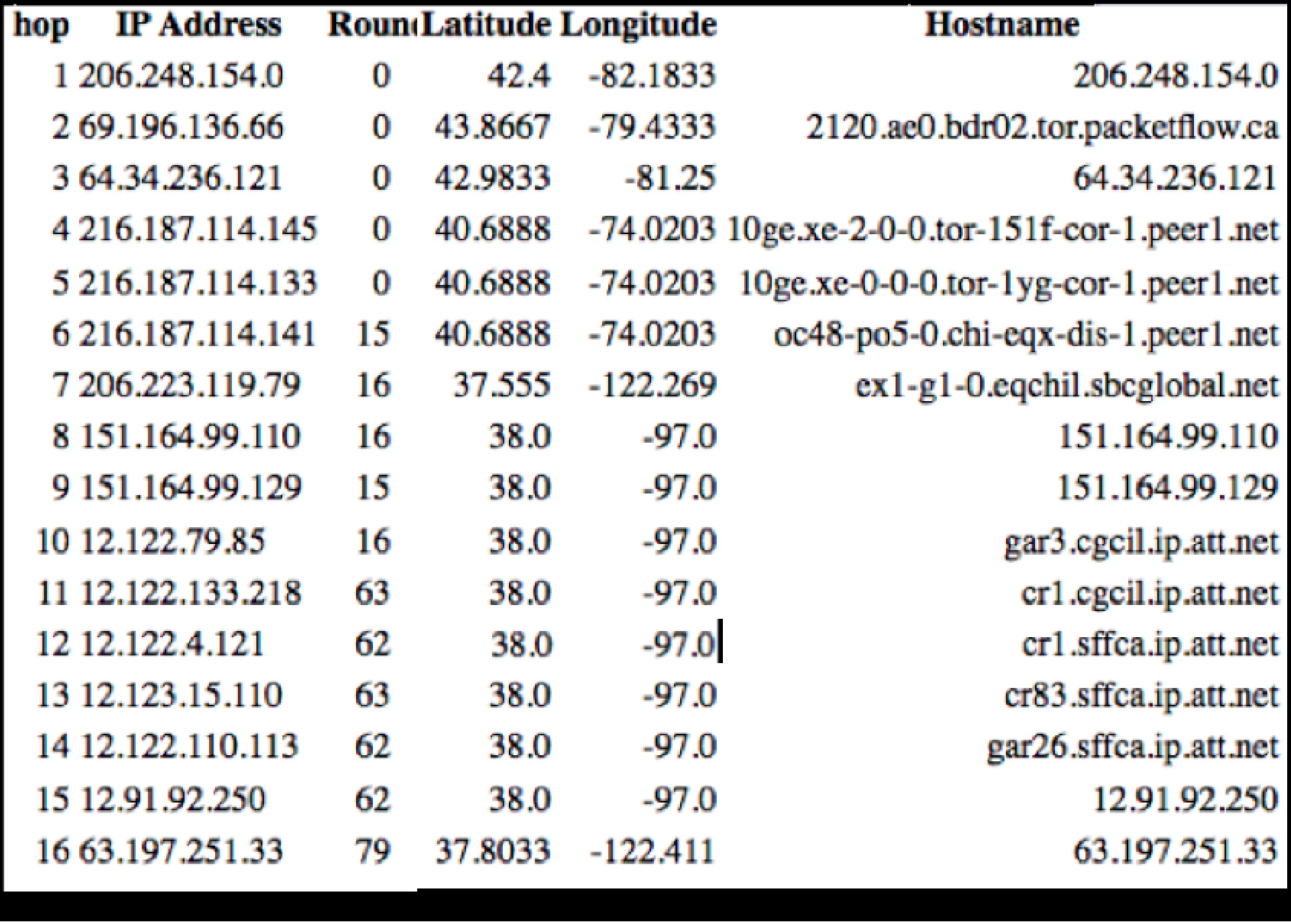
Toronto home OK

? ? ?

? ? ?

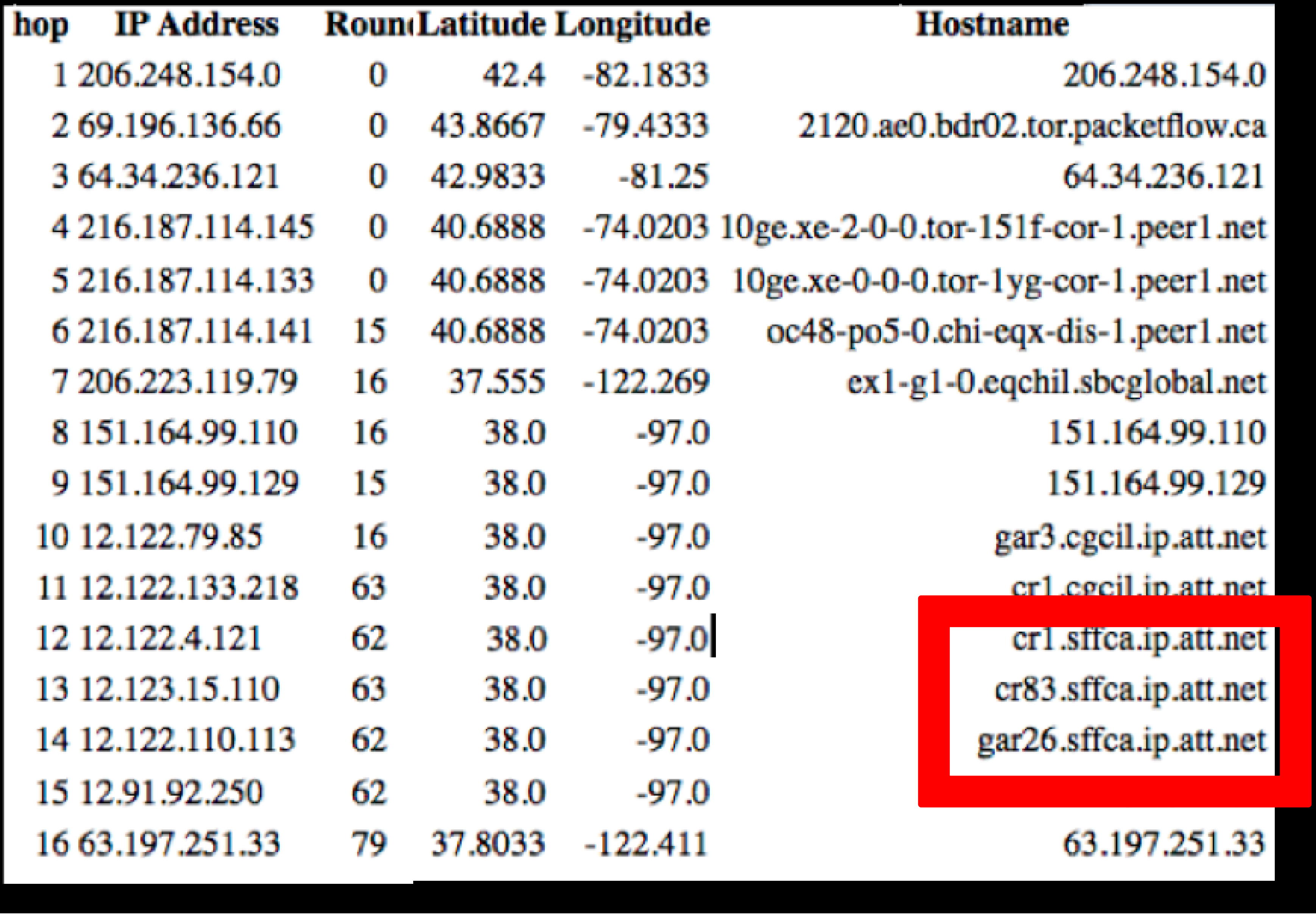
San Francisco
Art Institute OK

Trace route with Lat/Long + URLs



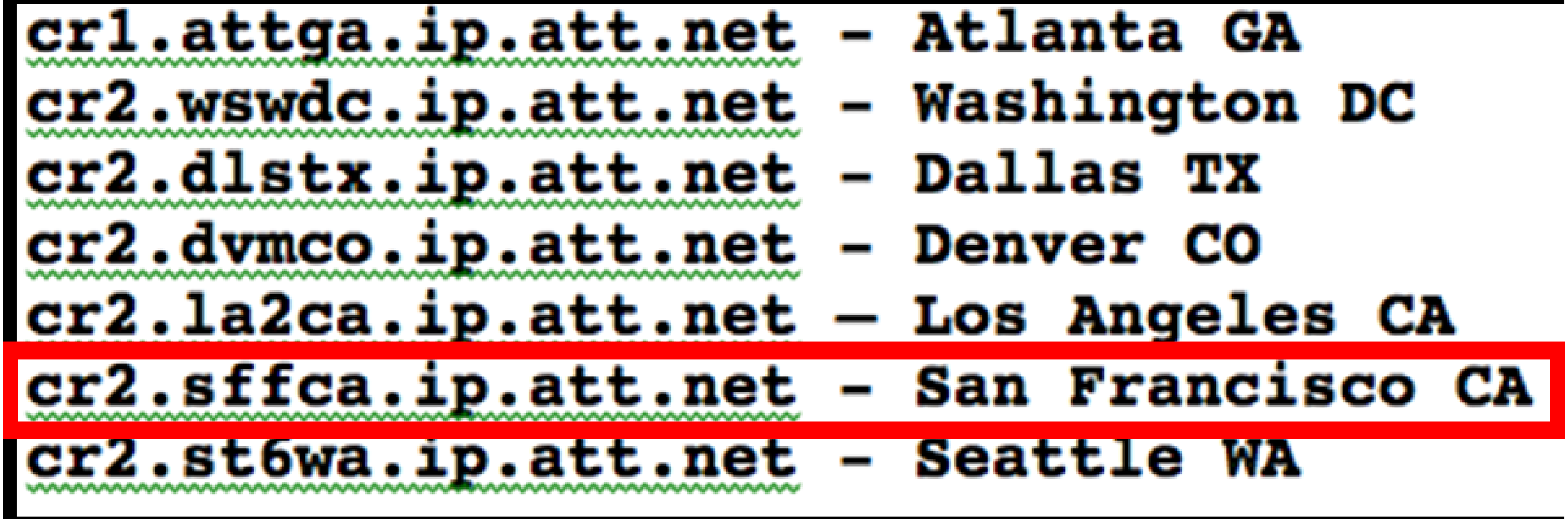
hop	IP Address	Roun	Latitude	Longitude	Hostname
1	206.248.154.0	0	42.4	-82.1833	206.248.154.0
2	69.196.136.66	0	43.8667	-79.4333	2120.ae0.bdr02.tor.packetflow.ca
3	64.34.236.121	0	42.9833	-81.25	64.34.236.121
4	216.187.114.145	0	40.6888	-74.0203	10ge.xe-2-0-0.tor-151f-cor-1.peer1.net
5	216.187.114.133	0	40.6888	-74.0203	10ge.xe-0-0-0.tor-1yg-cor-1.peer1.net
6	216.187.114.141	15	40.6888	-74.0203	oc48-po5-0.chi-eqx-dis-1.peer1.net
7	206.223.119.79	16	37.555	-122.269	ex1-g1-0.eqchil.sbcglobal.net
8	151.164.99.110	16	38.0	-97.0	151.164.99.110
9	151.164.99.129	15	38.0	-97.0	151.164.99.129
10	12.122.79.85	16	38.0	-97.0	gar3.cgcil.ip.att.net
11	12.122.133.218	63	38.0	-97.0	cr1.cgcil.ip.att.net
12	12.122.4.121	62	38.0	-97.0	cr1.sffca.ip.att.net
13	12.123.15.110	63	38.0	-97.0	cr83.sffca.ip.att.net
14	12.122.110.113	62	38.0	-97.0	gar26.sffca.ip.att.net
15	12.91.92.250	62	38.0	-97.0	12.91.92.250
16	63.197.251.33	79	37.8033	-122.411	63.197.251.33

Trace route with Lat/Long + URLs



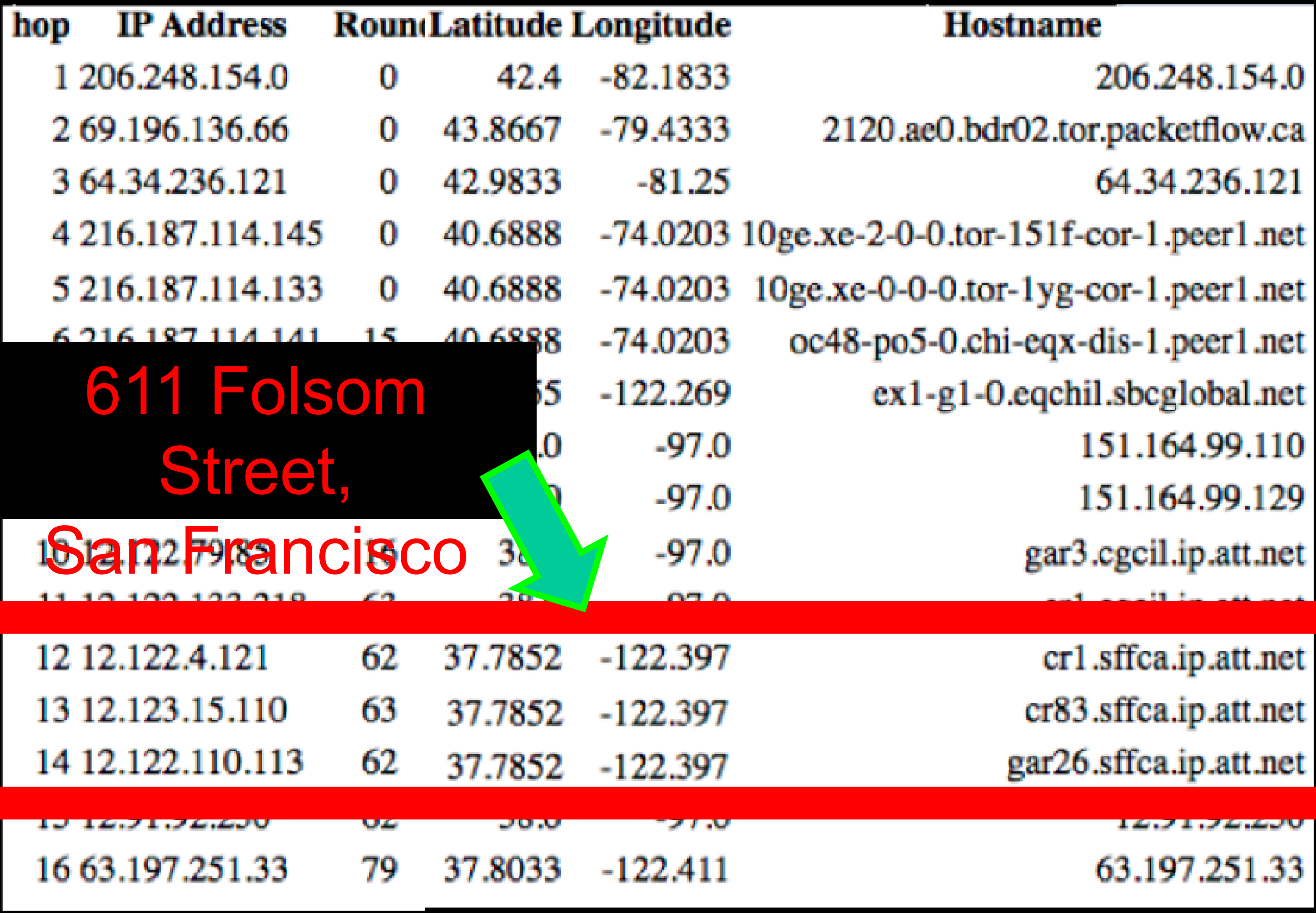
hop	IP Address	Roun	Latitude	Longitude	Hostname
1	206.248.154.0	0	42.4	-82.1833	206.248.154.0
2	69.196.136.66	0	43.8667	-79.4333	2120.ae0.bdr02.tor.packetflow.ca
3	64.34.236.121	0	42.9833	-81.25	64.34.236.121
4	216.187.114.145	0	40.6888	-74.0203	10ge.xe-2-0-0.tor-151f-cor-1.peer1.net
5	216.187.114.133	0	40.6888	-74.0203	10ge.xe-0-0-0.tor-1yg-cor-1.peer1.net
6	216.187.114.141	15	40.6888	-74.0203	oc48-po5-0.chi-eqx-dis-1.peer1.net
7	206.223.119.79	16	37.555	-122.269	ex1-g1-0.eqchil.sbcglobal.net
8	151.164.99.110	16	38.0	-97.0	151.164.99.110
9	151.164.99.129	15	38.0	-97.0	151.164.99.129
10	12.122.79.85	16	38.0	-97.0	gar3.cgcil.ip.att.net
11	12.122.133.218	63	38.0	-97.0	cr1.cgcil.ip.att.net
12	12.122.4.121	62	38.0	-97.0	cr1.sffca.ip.att.net
13	12.123.15.110	63	38.0	-97.0	cr83.sffca.ip.att.net
14	12.122.110.113	62	38.0	-97.0	gar26.sffca.ip.att.net
15	12.91.92.250	62	38.0	-97.0	
16	63.197.251.33	79	37.8033	-122.411	63.197.251.33

AT&T Core routers?



```
cr1.attga.ip.att.net - Atlanta GA
cr2.wswdc.ip.att.net - Washington DC
cr2.dlstx.ip.att.net - Dallas TX
cr2.dvmco.ip.att.net - Denver CO
cr2.la2ca.ip.att.net — Los Angeles CA
cr2.sffca.ip.att.net - San Francisco CA
cr2.st6wa.ip.att.net - Seattle WA
```

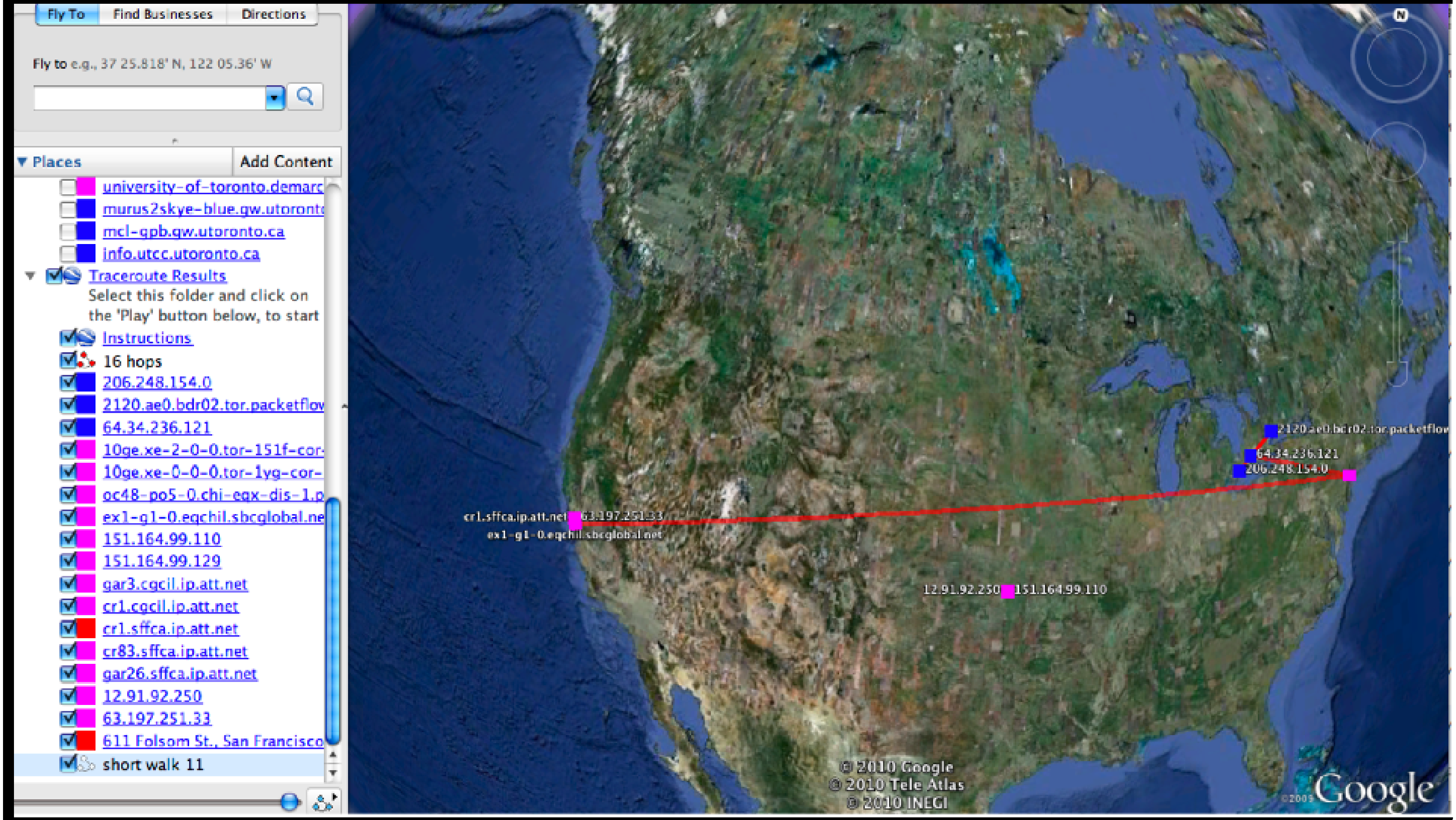
Trace route with Lat/Long updated



611 Folsom Street, San Francisco

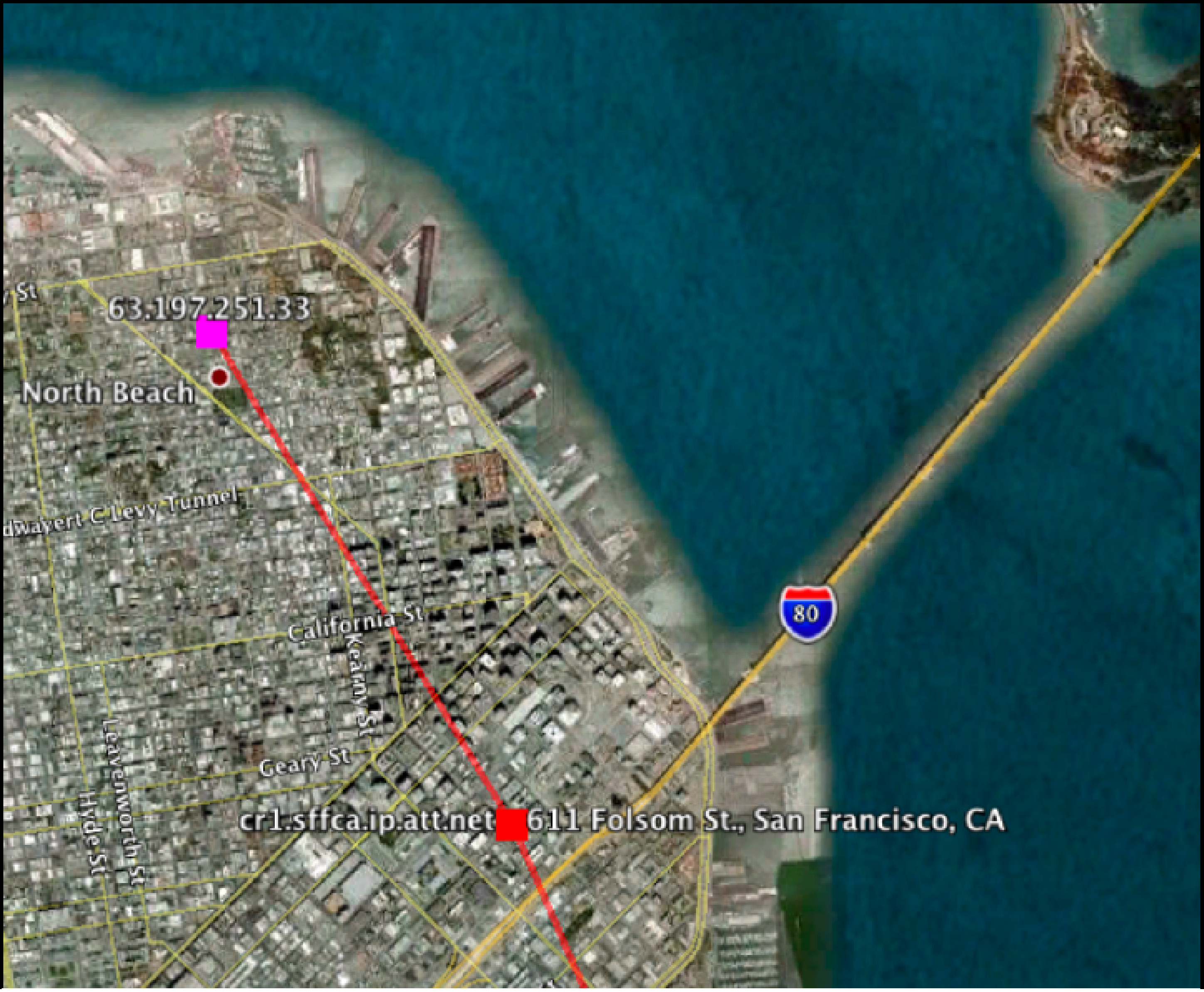
hop	IP Address	Roun	Latitude	Longitude	Hostname
1	206.248.154.0	0	42.4	-82.1833	206.248.154.0
2	69.196.136.66	0	43.8667	-79.4333	2120.ae0.bdr02.tor.packetflow.ca
3	64.34.236.121	0	42.9833	-81.25	64.34.236.121
4	216.187.114.145	0	40.6888	-74.0203	10ge.xe-2-0-0.tor-151f-cor-1.peer1.net
5	216.187.114.133	0	40.6888	-74.0203	10ge.xe-0-0-0.tor-1yg-cor-1.peer1.net
6	216.187.114.141	15	40.6888	-74.0203	oc48-po5-0.chi-eqx-dis-1.peer1.net
[illegible]	[illegible]	[illegible]	[illegible]	-122.269	ex1-g1-0.eqchil.sbcglobal.net
[illegible]	[illegible]	[illegible]	[illegible]	-97.0	151.164.99.110
[illegible]	[illegible]	[illegible]	[illegible]	-97.0	151.164.99.129
10	[illegible]	[illegible]	[illegible]	-97.0	gar3.cgcil.ip.att.net
11	12.122.122.218	62	[illegible]	-97.0	cr1.cgcil.ip.att.net
12	12.122.4.121	62	37.7852	-122.397	cr1.sffca.ip.att.net
13	12.123.15.110	63	37.7852	-122.397	cr83.sffca.ip.att.net
14	12.122.110.113	62	37.7852	-122.397	gar26.sffca.ip.att.net
15	[illegible]	62	38.0	-97.0	[illegible]
16	63.197.251.33	79	37.8033	-122.411	63.197.251.33

Google Earth rendering of TR#1859

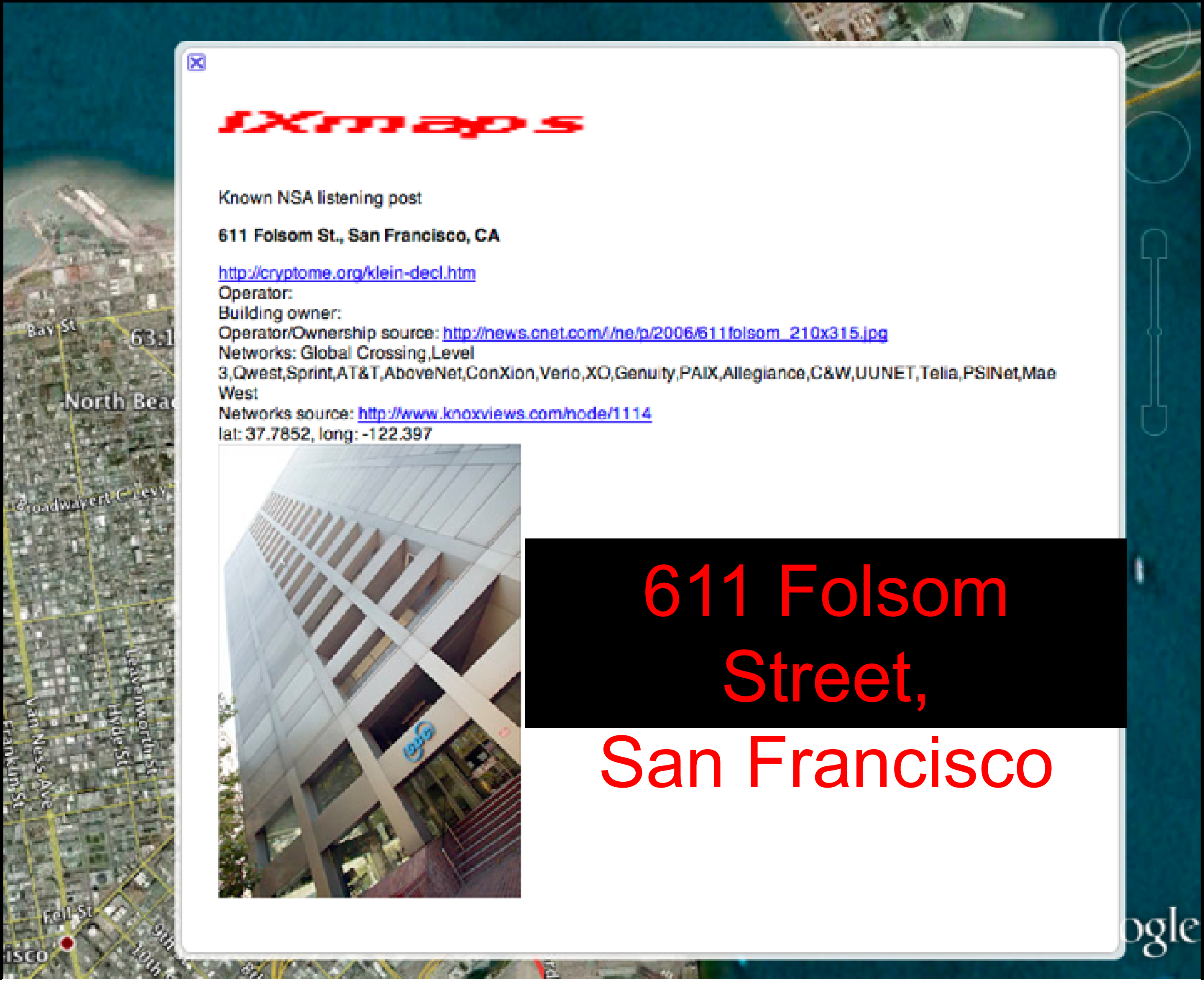


- □ 🟪 university-of-toronto.demarc
- □ 🟦 murus2skye-blue.gw.utoront
- □ 🟦 mcl-gpb.gw.utoronto.ca
- □ 🟦 info.utcc.utoronto.ca
- ☑ Traceroute Results
  Select this folder and click on the 'Play' button below, to start
  - ☑ Instructions
  - ☑ 16 hops
  - ☑ 🟦 206.248.154.0
  - ☑ 🟦 2120.ae0.bdr02.tor.packetflow
  - ☑ 🟦 64.34.236.121
  - ☑ 🟪 10ge.xe-2-0-0.tor-151f-cor-
  - ☑ 🟪 10ge.xe-0-0-0.tor-1yg-cor-
  - ☑ 🟪 oc48-po5-0.chi-eqx-dis-1.p
  - ☑ 🟪 ex1-g1-0.eqchil.sbcglobal.ne
  - ☑ 🟪 151.164.99.110
  - ☑ 🟪 151.164.99.129
  - ☑ 🟪 gar3.cgcil.ip.att.net
  - ☑ 🟪 cr1.cgcil.ip.att.net
  - ☑ 🟥 cr1.sffca.ip.att.net
  - ☑ 🟪 cr83.sffca.ip.att.net
  - ☑ 🟪 gar26.sffca.ip.att.net
  - ☑ 🟪 12.91.92.250
  - ☑ 🟪 63.197.251.33
  - ☑ 🟥 611 Folsom St., San Francisco
- ☑ short walk 11

Google Earth rendering of TR#1859



Google Earth rendering of TR#1859



Known NSA listening post

611 Folsom St., San Francisco, CA

http://cryptome.org/klein-decl.htm
Operator:
Building owner:
Operator/Ownership source: http://news.cnet.com/i/ne/p/2006/611folsom_210x315.jpg
Networks: Global Crossing,Level 3,Qwest,Sprint,AT&T,AboveNet,ConXion,Verio,XO,Genuity,PAIX,Allegiance,C&W,UUNET,Telia,PSINet,Mae West
Networks source: http://www.knoxviews.com/node/1114
lat: 37.7852, long: -122.397

611 Folsom Street,
San Francisco

Room 641A at 611 Folsom Street

Future work

- Working prototype as proof of concept:
  - The internet is not a “cloud”, but a very specific, material infrastructure of deeply entangled socio-technical relationships
- Build data base of:
  - NSA sites
  - DPI sites and policies
  - Ownership of the “cloud”
  - Energy consumption
- Evidence of individual ‘harm’ in NSA court cases?
- Cyber-surveillance - international research workshop, May 2011, Toronto

http://IXmaps.ischool.utoronto.ca

Acknowledgements

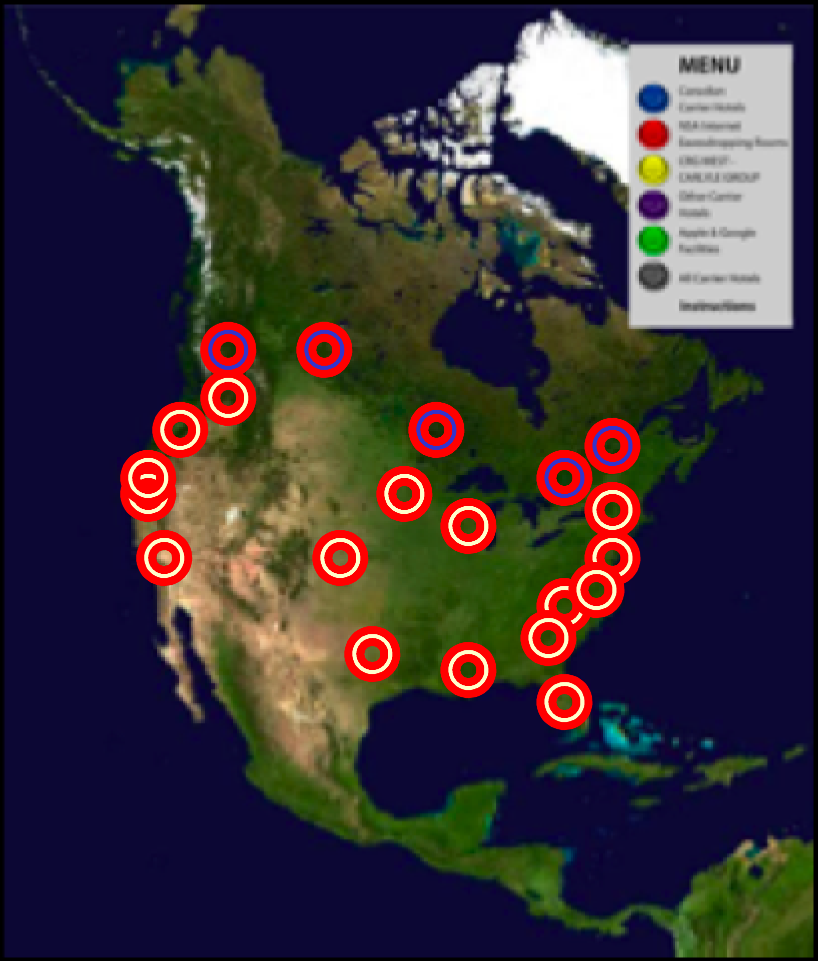
Funded by SSHRC ITST grant

Affiliated with:

- The New Transparency: Surveillance and Social Sorting, SSHRC MCRI grant , and
- Information Policy Research Program

http://iprp.ischool.utoronto.ca/

Suspected splitter sites


MENU
Canadian Carrier Hotels
NSA Internet Eavesdropping Rooms
CRG WEST - CARLYLE GROUP
Other Carrier Hotels
Apple & Google Facilities
All Carrier Hotels
Instructions