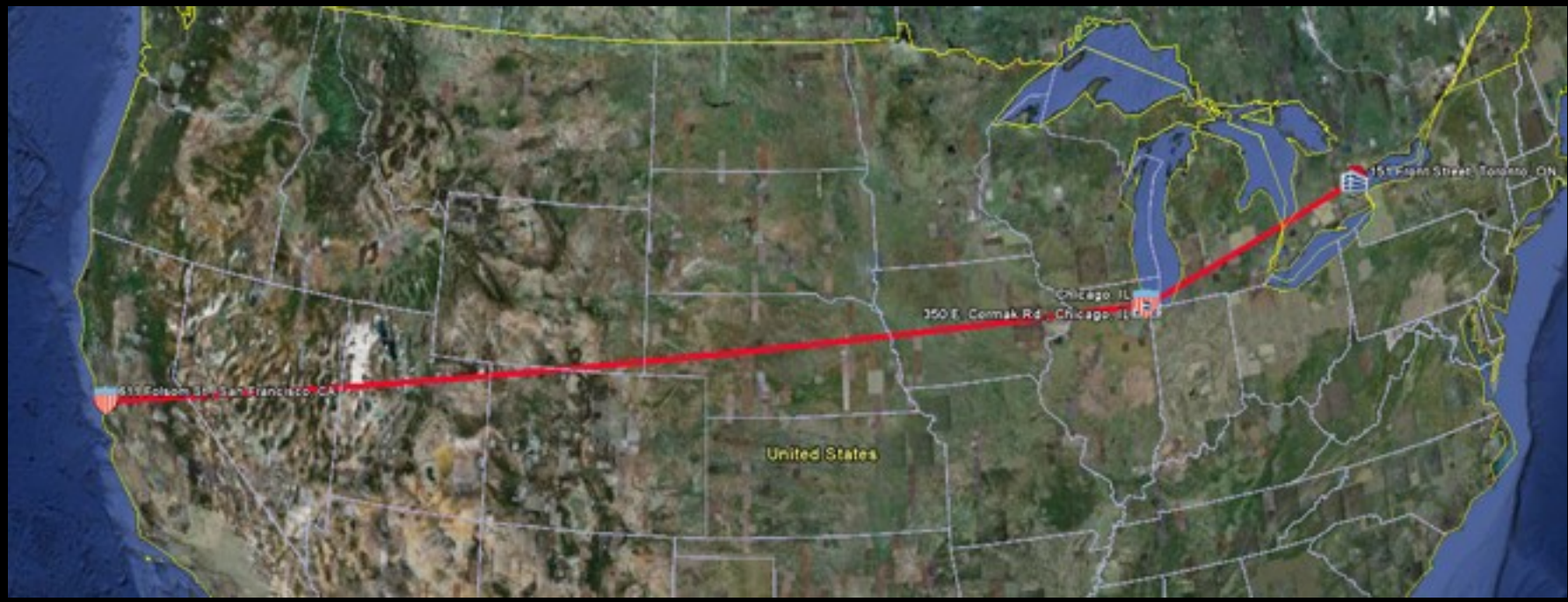
IXmaps

Tracking your Information Packets Over the Net, Through Exchange Points and Across Borders



Andrew Clement (U of T),
Colin McCann (U of T),
Gabby Resch (U of T),
Erik Stewart (Independent)

iConference
Culture ♦ Design ♦ Society
Hosted by the
Faculty of Information
University of Toronto
February 10, 2012

Today's Workshop

1. Enable attendees to learn about internet traceroute visualization, and in particular how they can use the IXmaps.ca mapping service to see where their packets travel, discovering information about ‘interesting’ points and internet policy issues along the way.
2. Enroll contributors in the collaborative expansion and refinement of the IXmaps.ca database of traceroutes, backbone router locations, and internet exchange point facts.

We hope to foster an enthusiastic cohort of informed individuals interested in collaboratively shedding light on the inner workings of the internet and contributing to the value and utility of the IXmaps tool.

Agenda

1. Introductions (10 mins)
2. Motivations – backbone surveillance, network sovereignty (10mins)
3. Traceroutes and geolocating backbone routers (10 mins)
4. Traceroutes, visualization, IXmaps generation of TRs (30 mins)
5. Policy implications (20 mins)
6. Wrapup: staying in touch (10 mins)

Motivations

Background

- There is popular tendency to regard the internet core as an immaterial, virtual, placeless 'cloud' where much happens, but without wider interest or concern.
- The IXmaps research project seeks to dispel this myth by revealing the internet core’s political, geographical and physical concreteness.
- It does this by illuminating for users the routes their packets take through the internet core along with the related issues - e.g. surveillance, ownership, network sovereignty, etc.

'Inside' the Internet

- Much is going on ‘inside’ the internet, but out of sight, that should concern users and public interest policy advocates:
  - Surveillance (e.g. eavesdropping by the NSA and other national security agencies)
  - Deep packet inspection (DPI) by ISPs/carriers
  - Discriminatory traffic management and blockage
  - Reach, reachability & (de-)peering
  - Cross-border flows (national “network sovereignty” issue)
  - Oligopolistic and anti-competitive business practices
  - Energy (over) consumption…
- ‘Cloud computing’ as a metaphor obscures important insights and possibilities for action

IXmaps Description

- IXmaps allows users to explore geographic visualizations of the routes taken by their information requests over the internet - presenting information about internet exchange points along the way. Data packet routes and switching sites are shown using Google Earth.
- The IXmaps project relies on voluntary user contributions to its database, mainly through the installation of TRgen, a modified version of a common Traceroute analysis program.

What is a traceroute?

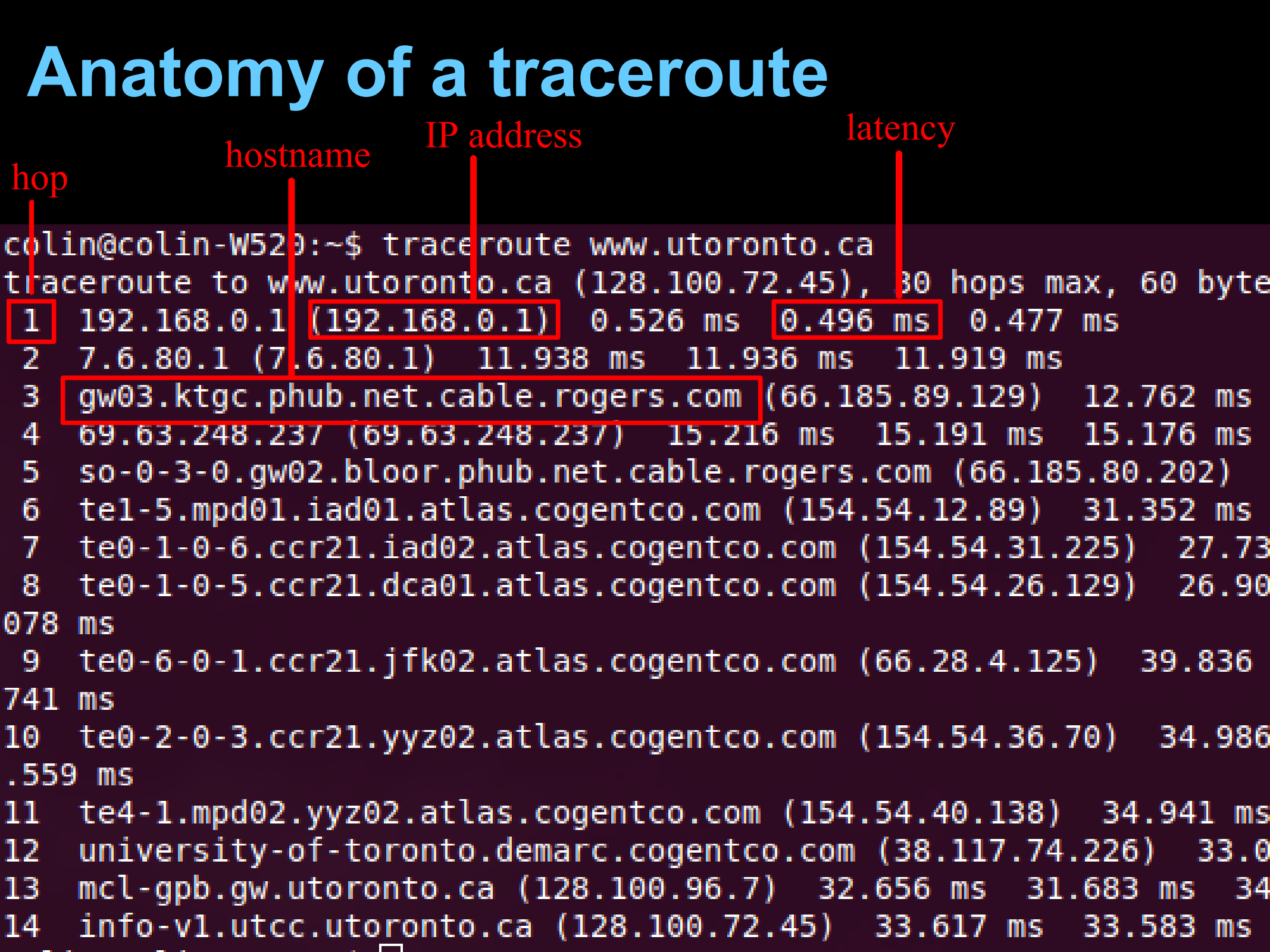
- traceroute is a cross-platform network analysis tool, which shows the steps that data packets take to reach a target URL

- To run, open a terminal and type:

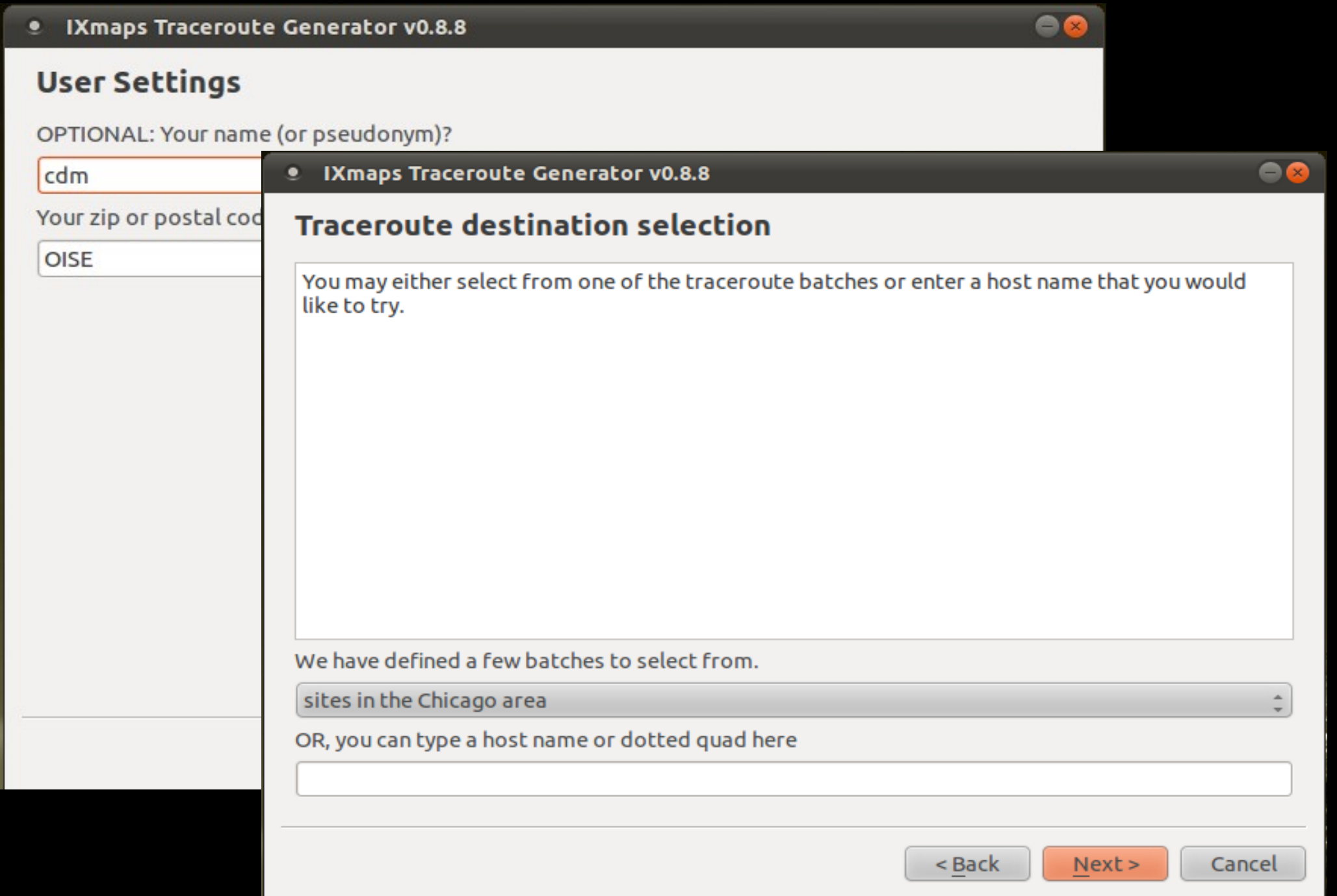
Mac – traceroute google.ca
Windows – tracert google.ca
Linux – traceroute google.ca

- Def'n: IP address – a number assigned to each device in a computer network, i.e. 172.168.4.28

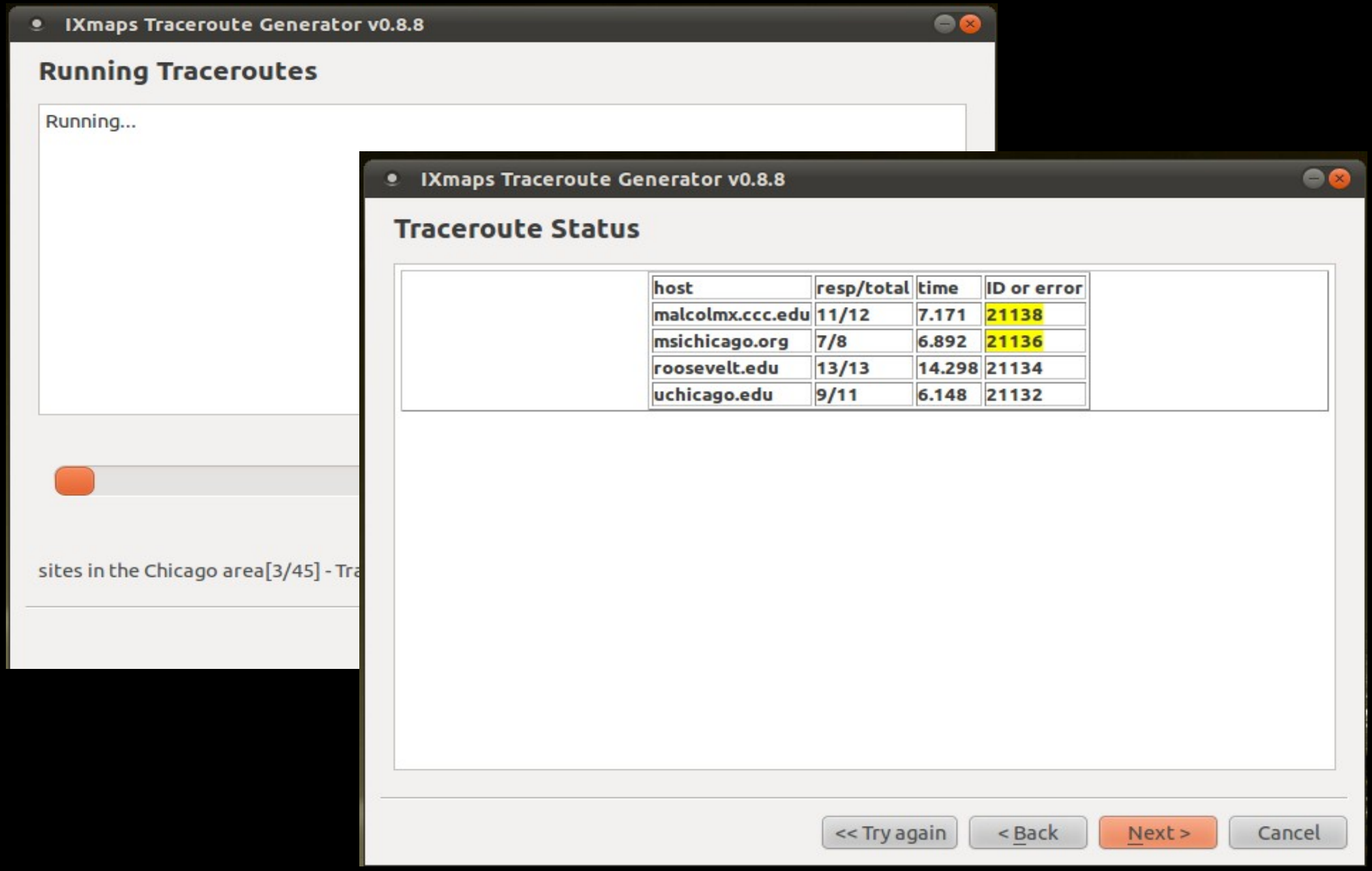
Anatomy of a traceroute



TRgen in action



TRgen in action (cont'd)



TRgen and the IXmaps website

Traceroute detail

Traceroute id: **7598**
origin: **M4L** destination: **Toronto ON** (www.utoronto.ca [128.100.72.45])
submitter: gbby_lville submitted: 2011-10-05 23:23

Open in GoogleEarth

Hop	IP Address	Min. Latency	Carrier	Location	GeoPrecision	Hostname
1	7.5.140.0	8	not listed by Maxmind	unknown	Maxmind	7.5.140.0
2	66.185.89.201	10	ROGERS-CABLE - Rogers Cable Communications Inc.	unknown	Maxmind	66.185.89.201
3	69.63.252.222	10	ROGERS-CABLE - Rogers Cable Communications Inc.	unknown	Maxmind	69.63.252.222
4	69.63.248.141	20	ROGERS-CABLE - Rogers Cable Communications Inc.	Chicago IL	city level	69.63.248.141
5	154.54.10.229	22	Cogent	Chicago IL	city level	te0-3-0-1.ccr21.ord03.atlas.cogentco.com
6	154.54.2.93	22	Cogent	Chicago IL	city level	te1-1.mpd01.ord01.atlas.cogentco.com
7	154.54.27.250	22	Cogent	Toronto ON	city level	te8-1.mpd01.yyz02.atlas.cogentco.com
8	154.54.43.173	22	Cogent	Toronto ON	city level	te0-2-0-0.ccr22.yyz02.atlas.cogentco.com
9	154.54.40.166	23	Cogent	Toronto ON	city level	te4-2.mpd02.yyz02.atlas.cogentco.com
10	38.117.74.226	23	Cogent	Toronto ON	building level	university-of-toronto.demarc.cogentco.com
11	128.100.96.7	23	University of Toronto	Toronto ON	building level	mcl-gpb.gw.utoronto.ca
12	128.100.72.45	40	University of Toronto	Toronto ON	building level	info-v1.utcc.utoronto.ca

Legend

- NSA: Known NSA listening facility in the city
- NSA: Suspected NSA listening facility in the city
- Hotel: Carrier hotel exchange point

Geolocation of routers

- www.maxmind.com
- Free GeoLite service claims to locate “over 99.5% on a country level and 79% on a city level”
- Edge routers vs core routers

IXmaps geolocation methods - hostnames

```
colin@colin-W520:~$ traceroute www.utoronto.ca
traceroute to www.utoronto.ca (128.100.72.45), 30 hops max, 60 byte
 1  192.168.0.1 (192.168.0.1)  0.526 ms  0.496 ms  0.477 ms
 2  7.6.80.1 (7.6.80.1)  11.938 ms  11.936 ms  11.919 ms
 3  gw03.ktgc.phub.net.cable.rogers.com (66.185.89.129)  12.762 ms
 4  69.63.248.237 (69.63.248.237)  15.216 ms  15.191 ms  15.176 ms
 5  so-0-3-0.gw02.bloor.phub.net.cable.rogers.com (66.185.80.202)
 6  te1-5.mpd01.iad01.atlas.cogentco.com (154.54.12.89)  31.352 ms
 7  te0-1-0-6.ccr21.iad02.atlas.cogentco.com (154.54.31.225)  27.73
 8  te0-1-0-5.ccr21.dca01.atlas.cogentco.com (154.54.26.129)  26.90
078 ms
 9  te0-6-0-1.ccr21.jfk02.atlas.cogentco.com (66.28.4.125)  39.836
741 ms
10  te0-2-0-3.ccr21.yyz02.atlas.cogentco.com (154.54.36.70)  34.986
.559 ms
11  te4-1.mpd02.yyz02.atlas.cogentco.com (154.54.40.138)  34.941 ms
12  university-of-toronto.demarc.cogentco.com (38.117.74.226)  33.0
13  mcl-gpb.gw.utoronto.ca (128.100.96.7)  32.656 ms  31.683 ms  34
14  info-v1.utcc.utoronto.ca (128.100.72.45)  33.617 ms  33.583 ms
```

IXmaps geolocation methods - latency

Traceroute detail

Traceroute id: **7598**
origin: **M4L** destination: **Toronto ON** (www.utoronto.ca [128.100.72.45])
submitter: gbby_lville submitted: 2011-10-05 23:23

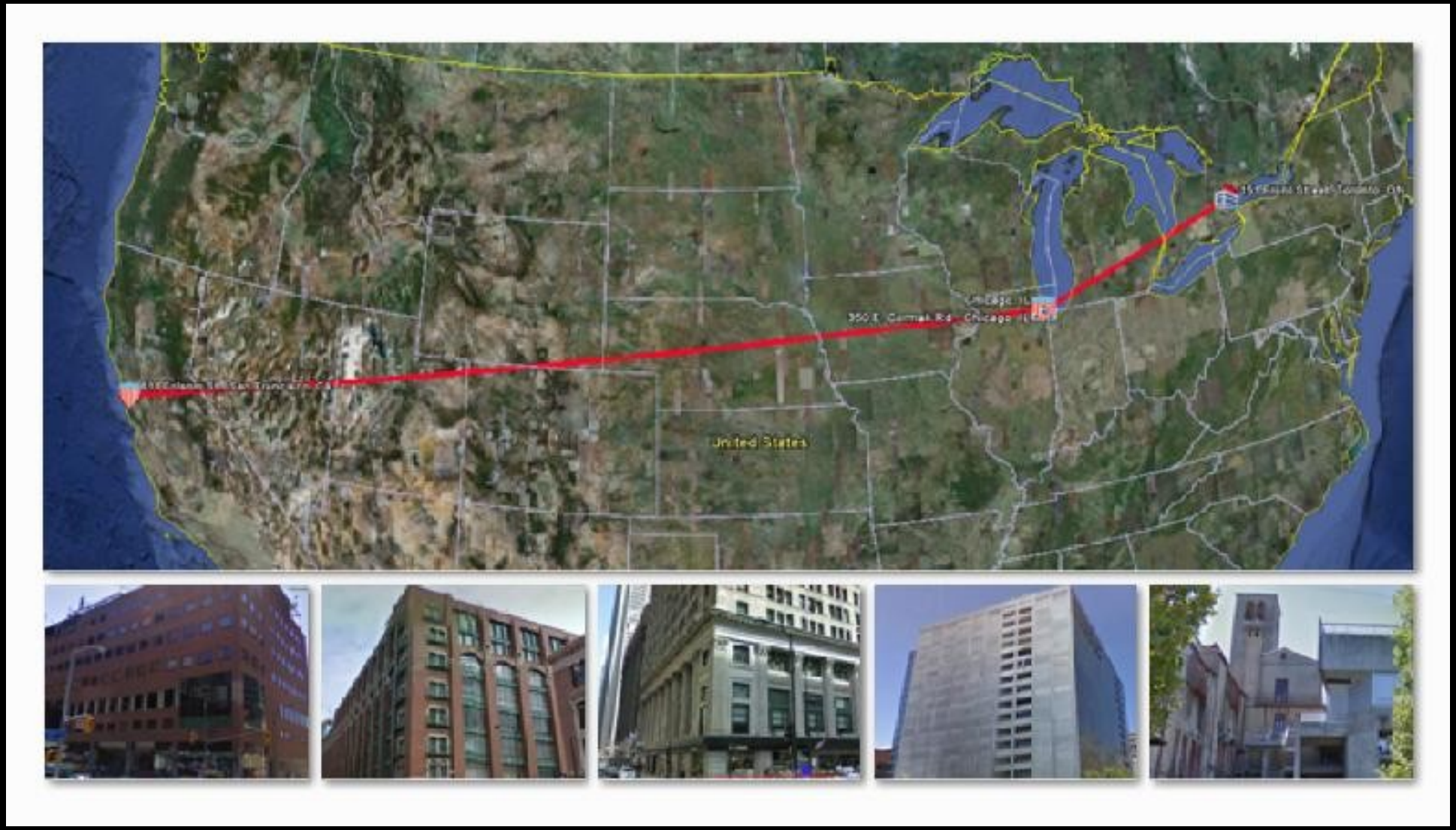
Open in GoogleEarth

Hop	IP Address	Min. Latency	Carrier	Location	GeoPrecision	Hostname
1	7.5.140.0	8	not listed by Maxmind	unknown	Maxmind	7.5.140.0
2	66.185.89.201	10	ROGERS-CABLE - Rogers Cable Communications Inc.	unknown	Maxmind	66.185.89.201
3	69.63.252.222	10	ROGERS-CABLE - Rogers Cable Communications Inc.	unknown	Maxmind	69.63.252.222
4	69.63.248.141	20	ROGERS-CABLE - Rogers Cable Communications Inc.		city level	69.63.248.141
5	154.54.10.229	22	Cogent	Chicago IL	city level	te0-3-0-1.ccr21.ord03.atlas.cogentco.com
6	154.54.2.93	22	Cogent	Chicago IL	city level	te1-1.mpd01.ord01.atlas.cogentco.com
7	154.54.27.250	22	Cogent	Toronto ON	city level	te8-1.mpd01.yyz02.atlas.cogentco.com
8	154.54.43.173	22	Cogent	Toronto ON	city level	te0-2-0-0.ccr22.yyz02.atlas.cogentco.com
9	154.54.40.166	23	Cogent	Toronto ON	city level	te4-2.mpd02.yyz02.atlas.cogentco.com
10	38.117.74.226	23	Cogent	Toronto ON	building level	university-of-toronto.demarc.cogentco.com
11	128.100.96.7	23	University of Toronto	Toronto ON	building level	mcl-gpb.gw.utoronto.ca
12	128.100.72.45	40	University of Toronto	Toronto ON	building level	info-v1.utcc.utoronto.ca

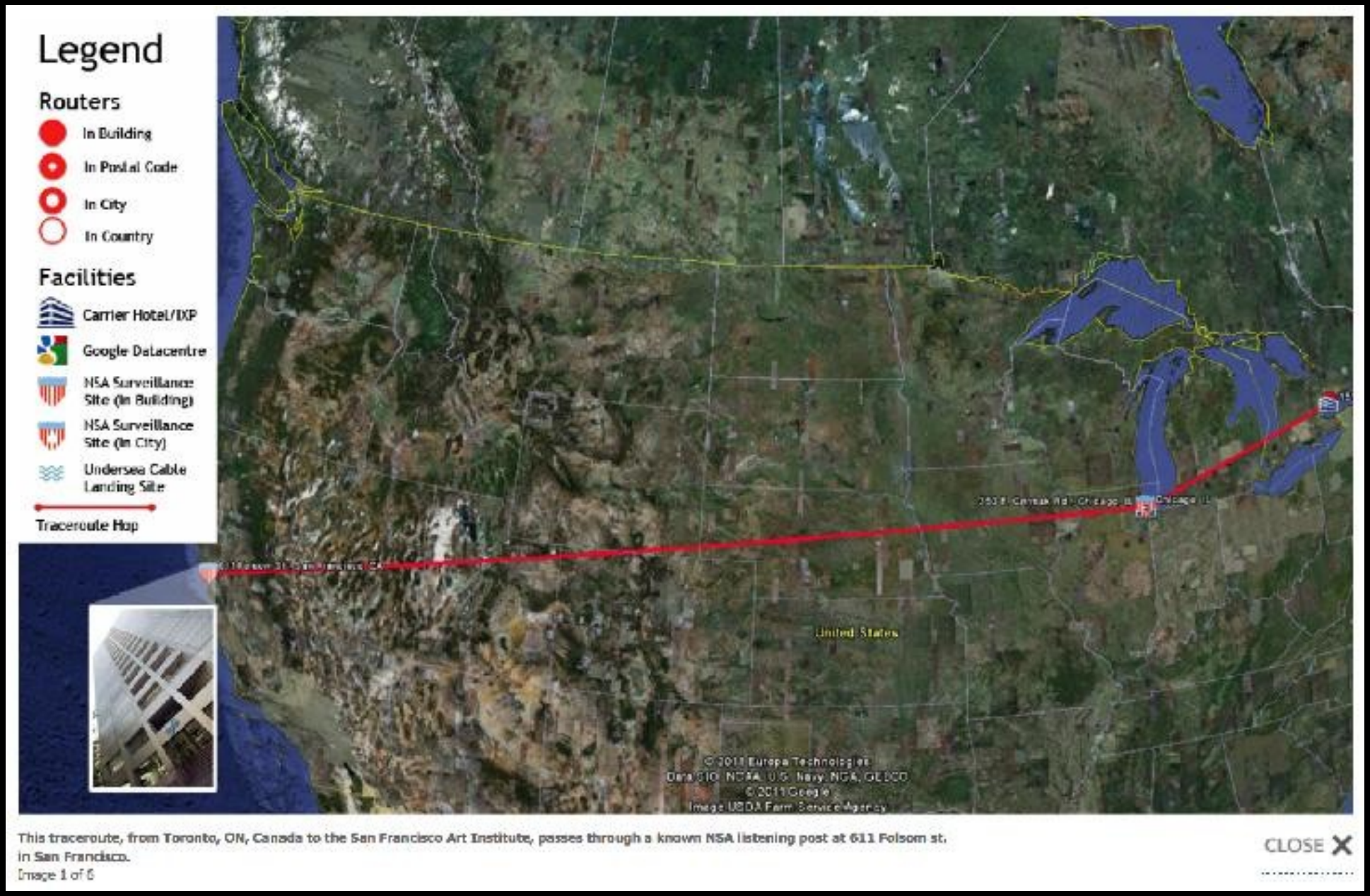
IXmaps.ca – visualizing internet routing

- Crowd-sourced traceroute generation across North America
- Google Earth mash-up
  - Traceroutes, internet exchange points (IXPs), carrier hotels, “interesting” site info

The Internet is not a cloud!



Toronto > San Francisco (TR1859)



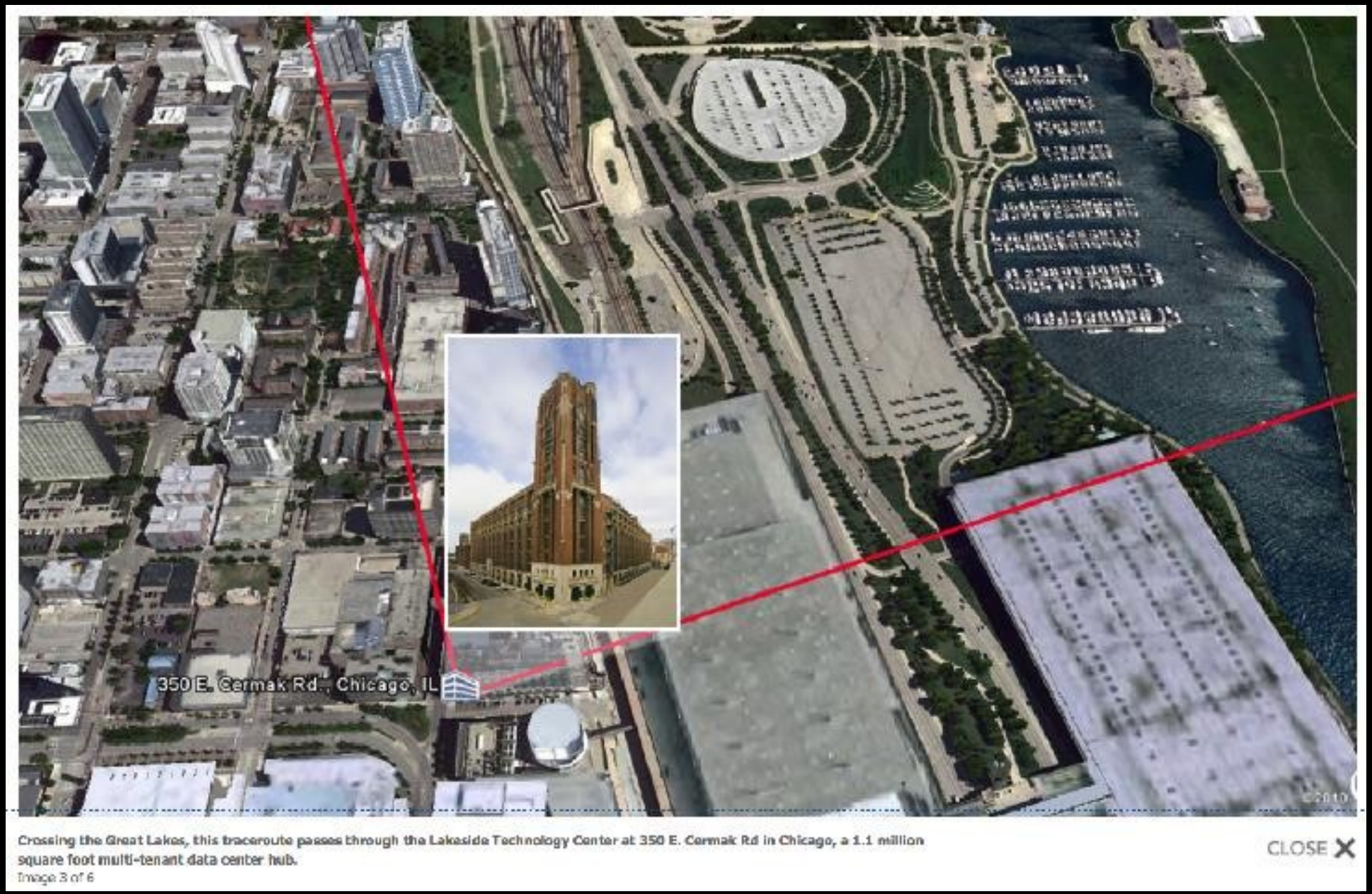
Toronto: 151 Front Street

Originating in Toronto, this traceroute passes through 151 Front Street, a major carrier hotel that houses over 100 telecommunications companies, and is Canada's premier telecommunications hub.

Image 2 of 5

CLOSE

Chicago: 350E Cermak Rd.

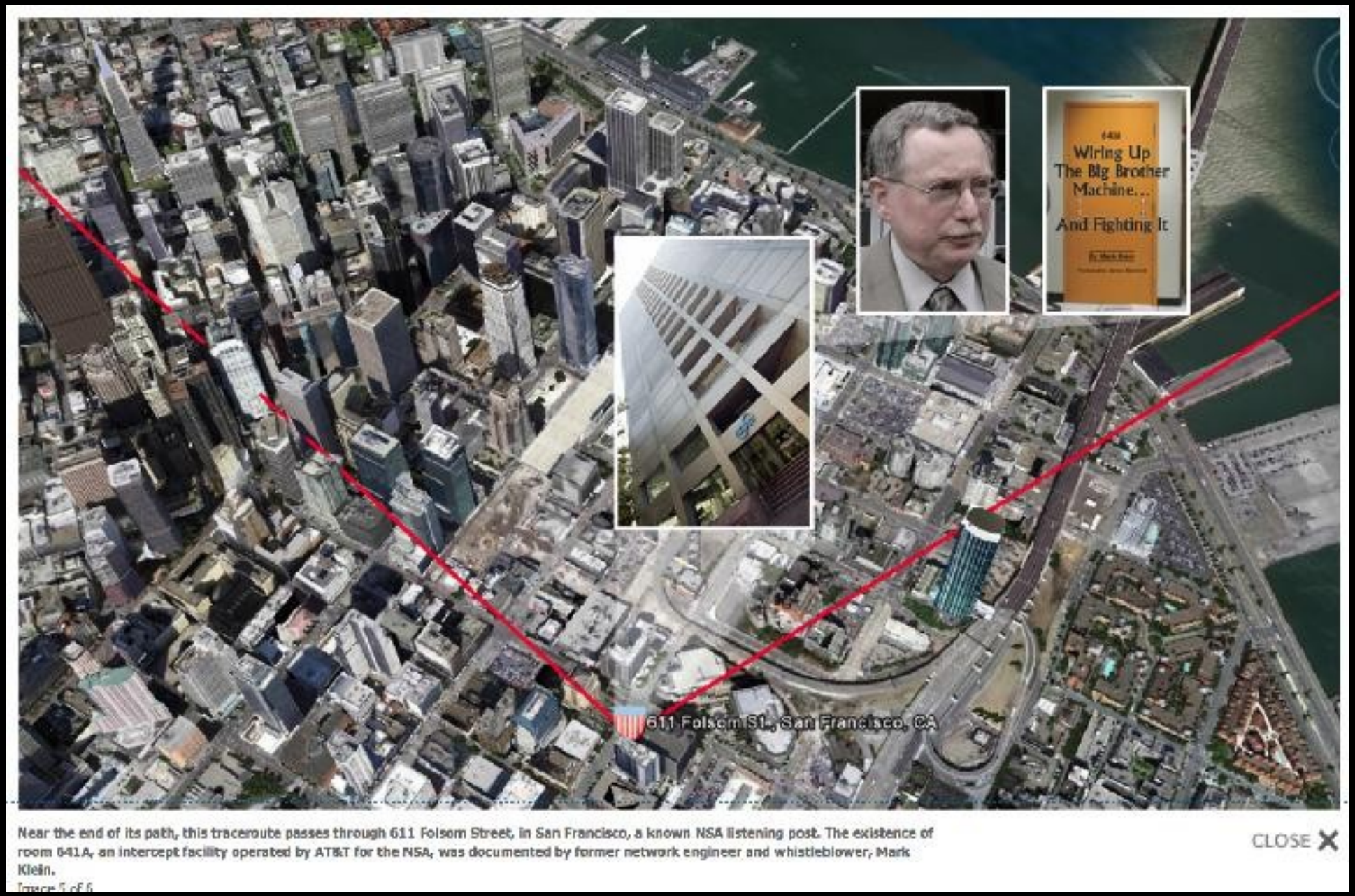


Crossing the Great Lakes, this traceroute passes through the Lakeside Technology Center at 350 E. Cermak Rd in Chicago, a 1.1 million square foot multi-tenant data center hub.

Image 3 of 6

CLOSE

San Francisco: 611 Folsom St



Near the end of its path, this traceroute passes through 611 Folsom Street, in San Francisco, a known NSA listening post. The existence of room 641A, an intercept facility operated by AT&T for the NSA, was documented by former network engineer and whistleblower, Mark Klein.

Image 5 of 6

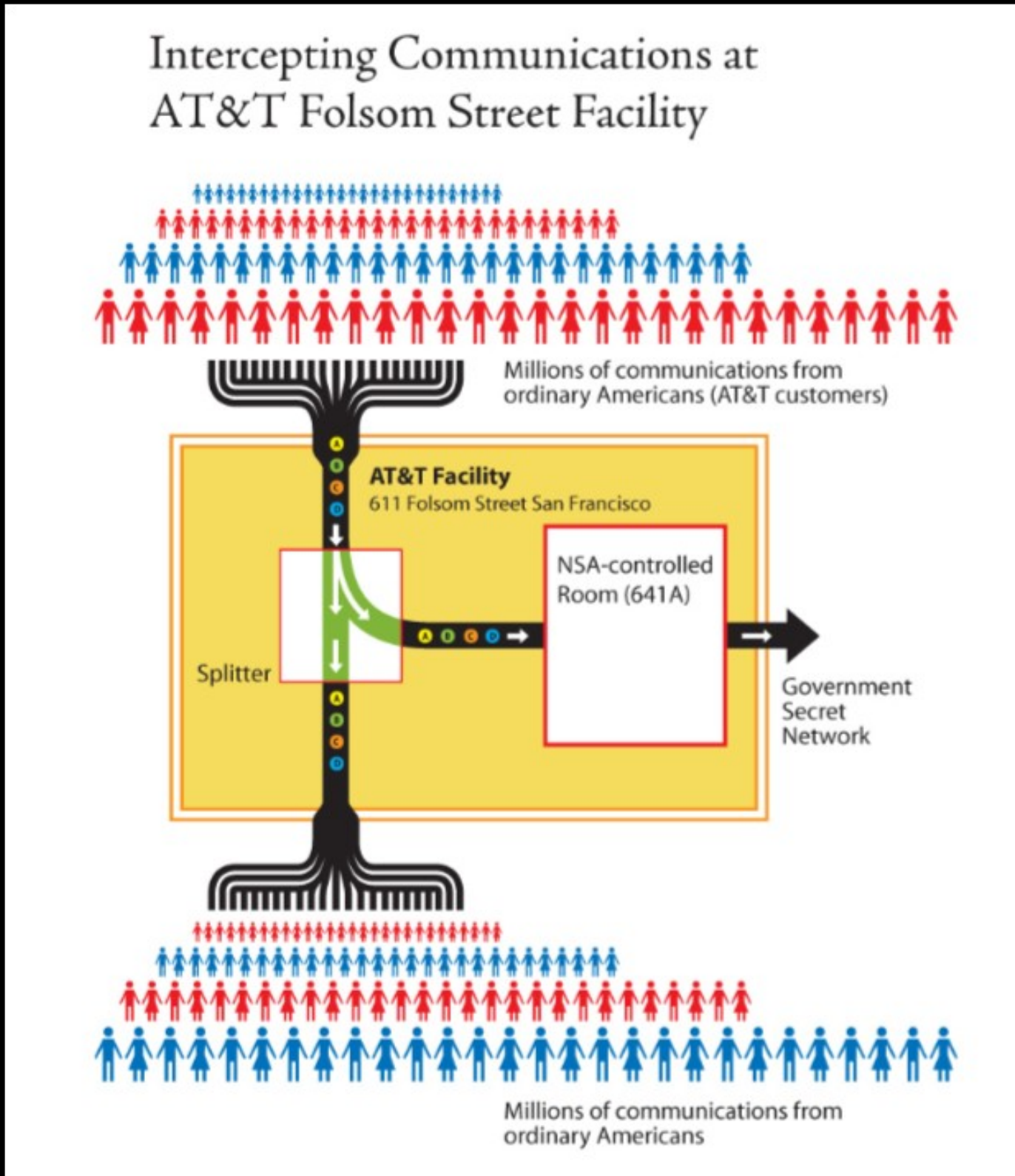
CLOSE ✕

Internet surveillance

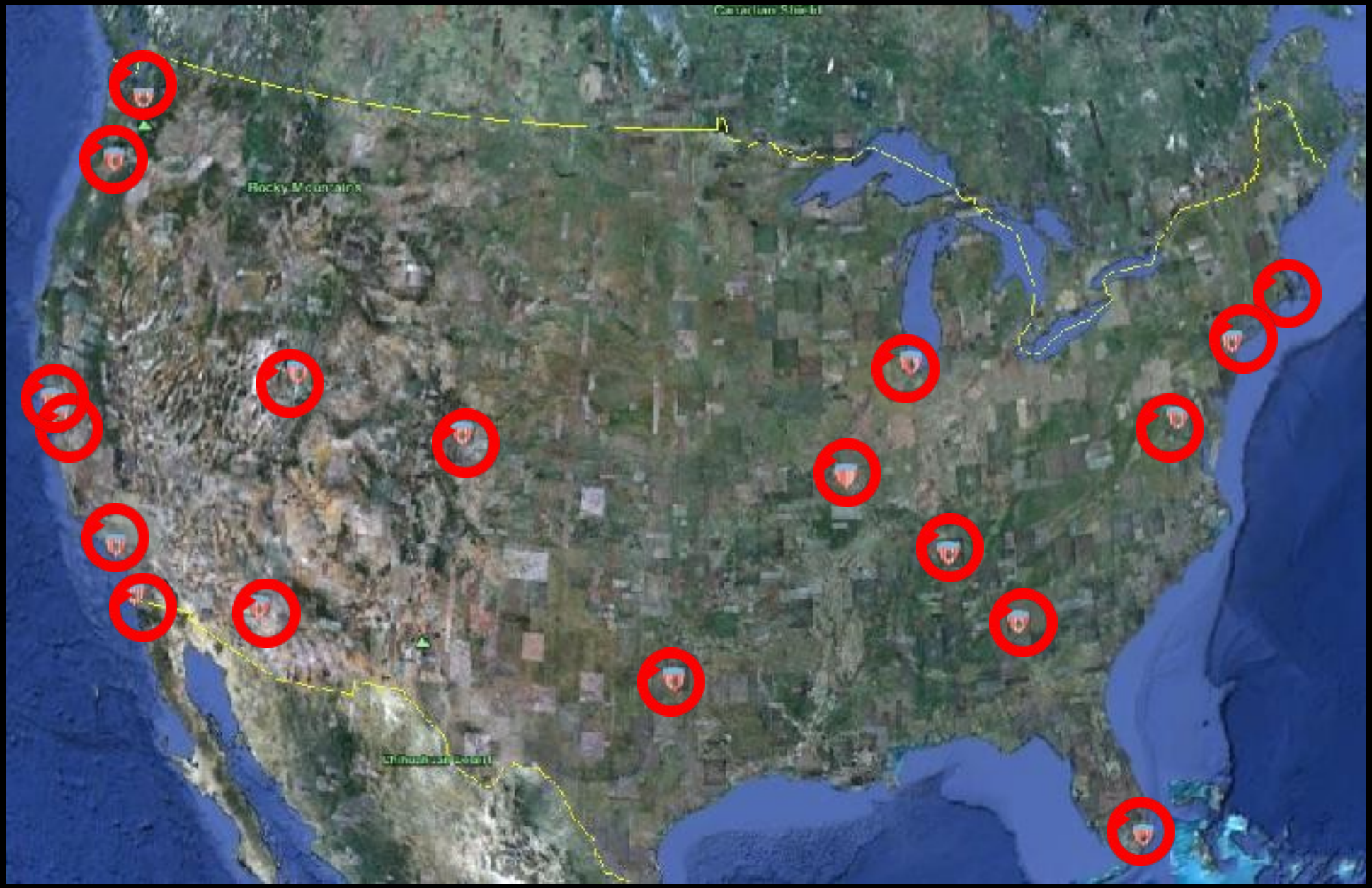
- USA PATRIOT Act
  - Expanded surveillance capabilities
    - Interception of messages
  - Extends to “protected computers” outside the US
  - Gag orders
- NSA Warrantless Wiretapping
  - Fibre-optic “splitters” at major internet gateways
    - San Francisco, Seattle, San Jose, Los Angeles, San Diego, Atlanta, + ~10 others (see Klein 2009; Bamford, 2008)
  - Traffic screened at carrier speed (10Gb/sec) and selectively stored by NSA (see Landau, 2011)

EFF's view:

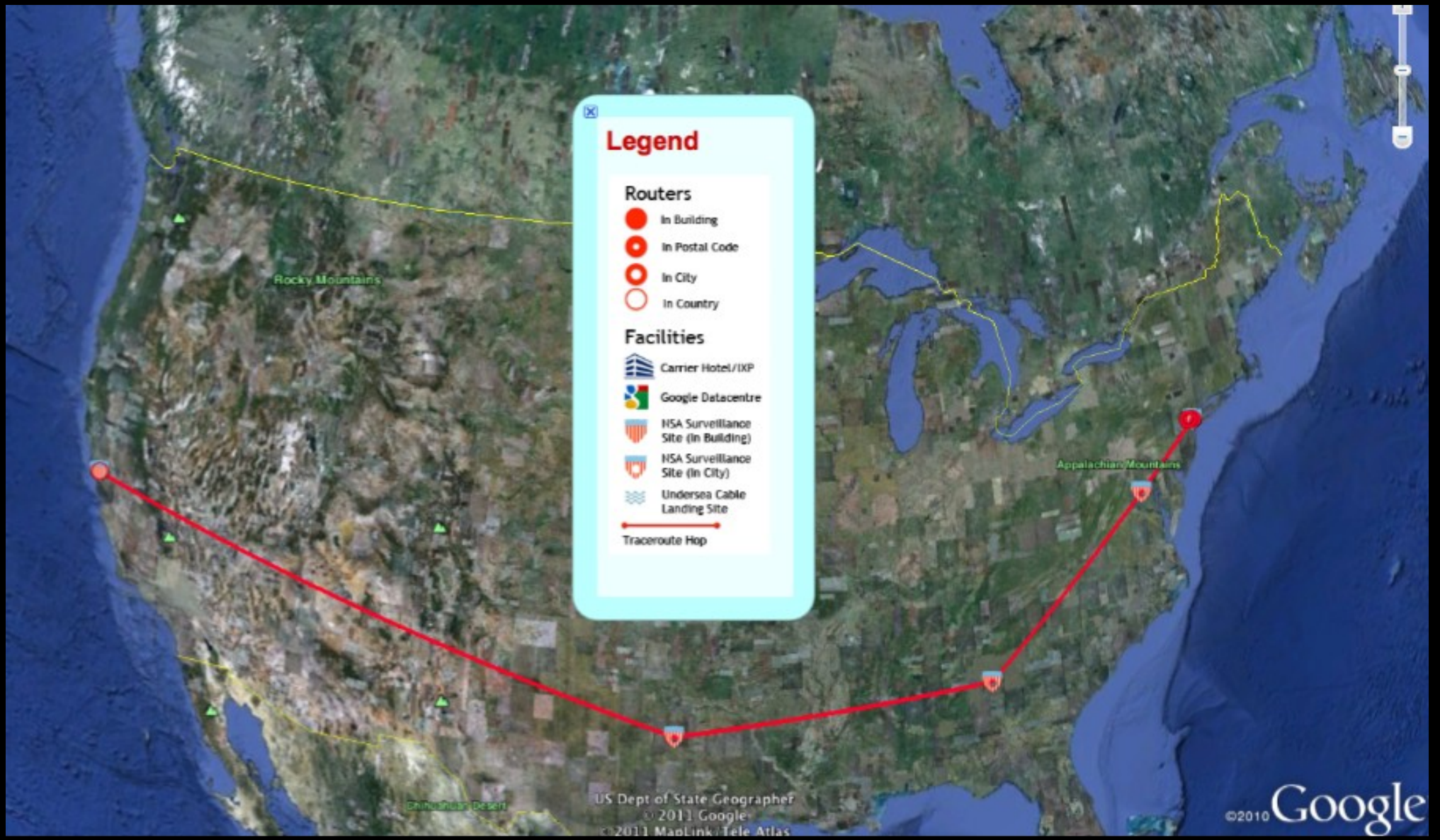
Source:
Electronic Frontier Foundation (EFF)



Suspected NSA surveillance sites



New York, NY > San Francisco, CA

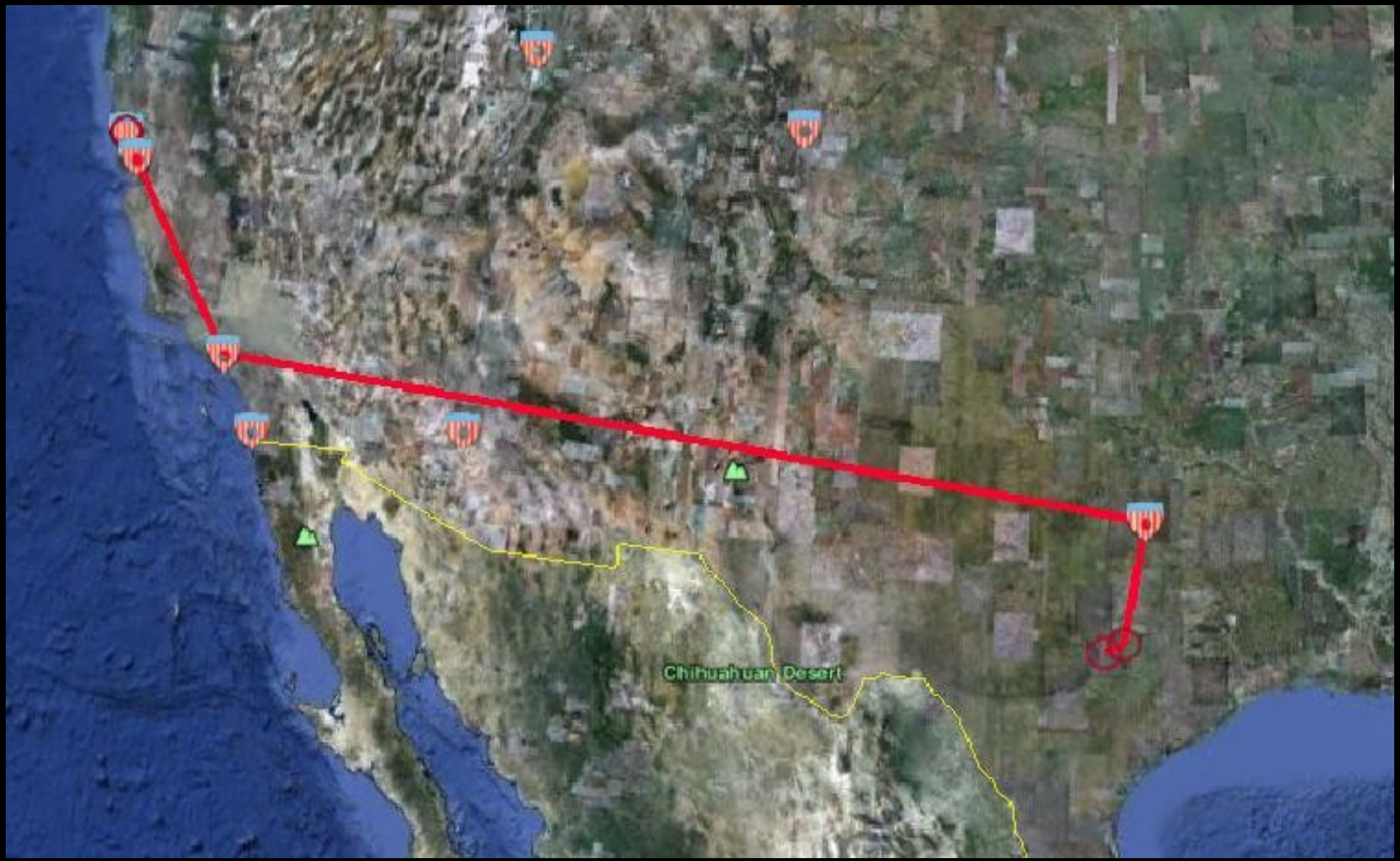


Can coast-to-cost US traffic avoid NSA cities?

So far as we've seen, no!

Traceroutes Generation and Visualization

Austin TX > San Francisco Law Library, SF CA (TR1751)



Austin TX > San Francisco Law Library, SF CA (TR1751)

Traceroute detail

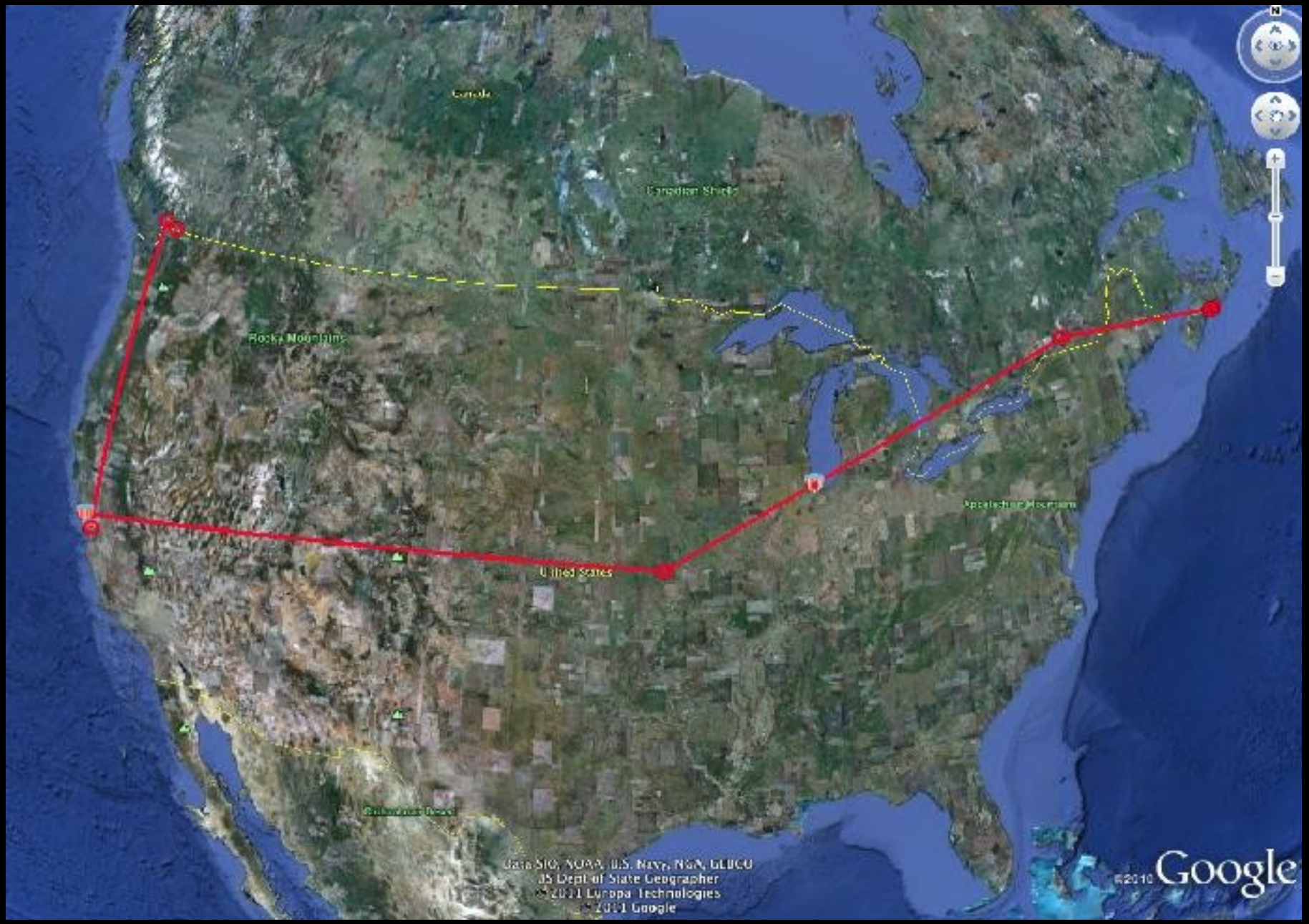
Traceroute id: **1751** Open in GoogleEarth
origin: **AustinTX** destination: **San Francisco CA** (sflawlib.ci.sf.ca.us [209.77.149.225])
submitter: AndrewC submitted: 2009-12-04 23:09

Hop	IP Address	Min. Latency	Carrier	Location	GeoPrecision	Hostname
1	12.231.120.0	0	AT&T WorldNet Services	Austin TX	Maxmind	12.231.120.0
2	12.89.72.5	0	AT&T WorldNet Services	Thrall TX	Maxmind	12.89.72.5
3	12.123.18.134	46	AT&T WorldNet Services	Dallas TX	city level	cr2.dlstx.ip.att.net
4	12.122.28.178	46	AT&T WorldNet Services	Los Angeles CA	city level	cr2.la2ca.ip.att.net
5	12.122.2.165	46	AT&T WorldNet Services	Los Angeles CA	city level	cr1.la2ca.ip.att.net
6	12.122.3.121	46	AT&T WorldNet Services	San Francisco CA	city level	cr1.sffca.ip.att.net
7	12.83.59.9	46	AT&T WorldNet Services	San Francisco CA	city level	12.83.59.9
8	151.164.38.26	46	AT&T Internet Services	San Francisco CA	city level	151.164.38.26
9	151.164.243.94	46	AT&T Internet Services	San Francisco CA	city level	ded1-g1-3-0.snfcca.sbcglobal.net
10	64.168.74.38	46	AT&T Internet Services	San Francisco CA	city level	VIP-CALNET-CCSF-Internet-City-1161485.cust-rtr.pacbell.net
11	208.121.241.249	47	CCSF	San Francisco CA	Maxmind	sf208-121-241-249.sfgov.org
12	209.77.149.225	47	CCSF	San Francisco CA	Maxmind	sflawlib.ci.sf.ca.us

Legend

- NSA: Known NSA listening facility in the city
- NSA: Suspected NSA listening facility in the city
- Hotel: Carrier hotel exchange point

Abbotsford BC > Halifax NS Telus > Cogent > DalhousieU (TR1486)



Abbotsford BC > Halifax NS Telus > Cogent > DalhousieU (TR1486)

Traceroute detail

Traceroute id: **1486**
origin: **V2T 5A5** destination: **Halifax NS** (www.dal.ca [129.173.1.241])
submitter: **Mark** submitted: **2009-12-01 19:43**

Open in GoogleEarth

Hop	IP Address		Min. Latency	Carrier	Location	GeoPrecision	Hostname
1	205.250.64.0		0	Telus	Abbotsford BC	Maxmind	d205-250-64-0.bchsia.telus.net
2	154.11.88.193		0	Telus	Vancouver BC	city level	VANCBC01GR01
3	154.11.10.74		31	Telus	San Jose CA	city level	154.11.10.74
4	154.11.2.54		31	Telus	San Jose CA	city level	154.11.2.54
5	66.28.4.49		31	Cogent	San Jose CA	city level	te3-2.mpd01.sjc04.atlas.cogentco.com
6	154.54.7.173		31	Cogent	San Francisco CA	city level	te8-2.ccr02.sfo01.atlas.cogentco.com
7	154.54.24.118		63	Cogent	Kansas City MO	city level	te9-2.ccr02.mci01.atlas.cogentco.com
8	154.54.7.166		79	Cogent	Chicago IL	city level	te8-2.mpd02.ord01.atlas.cogentco.com
9	66.28.4.58		93	Cogent	Montreal QC	city level	te7-7.mpd01.ymq02.atlas.cogentco.com
10	38.104.154.162		109	Cogent	Lawrencetown NS	city level	38.104.154.162
11	198.166.1.41		109	Dalhousie University	Halifax NS	Maxmind	GigaPOP-gw.acorn-ns.Ca
12	198.166.1.18		109	Dalhousie University	Halifax NS	Maxmind	dal-gw.Backbone.Dal.Ca
13	129.173.1.241		109	Dalhousie University	Halifax NS	Maxmind	kil-ws-2.UCIS.Dal.Ca

Legend

- NSA: Known NSA listening facility in the city
- NSA: Suspected NSA listening facility in the city
- Hotel: Carrier hotel exchange point

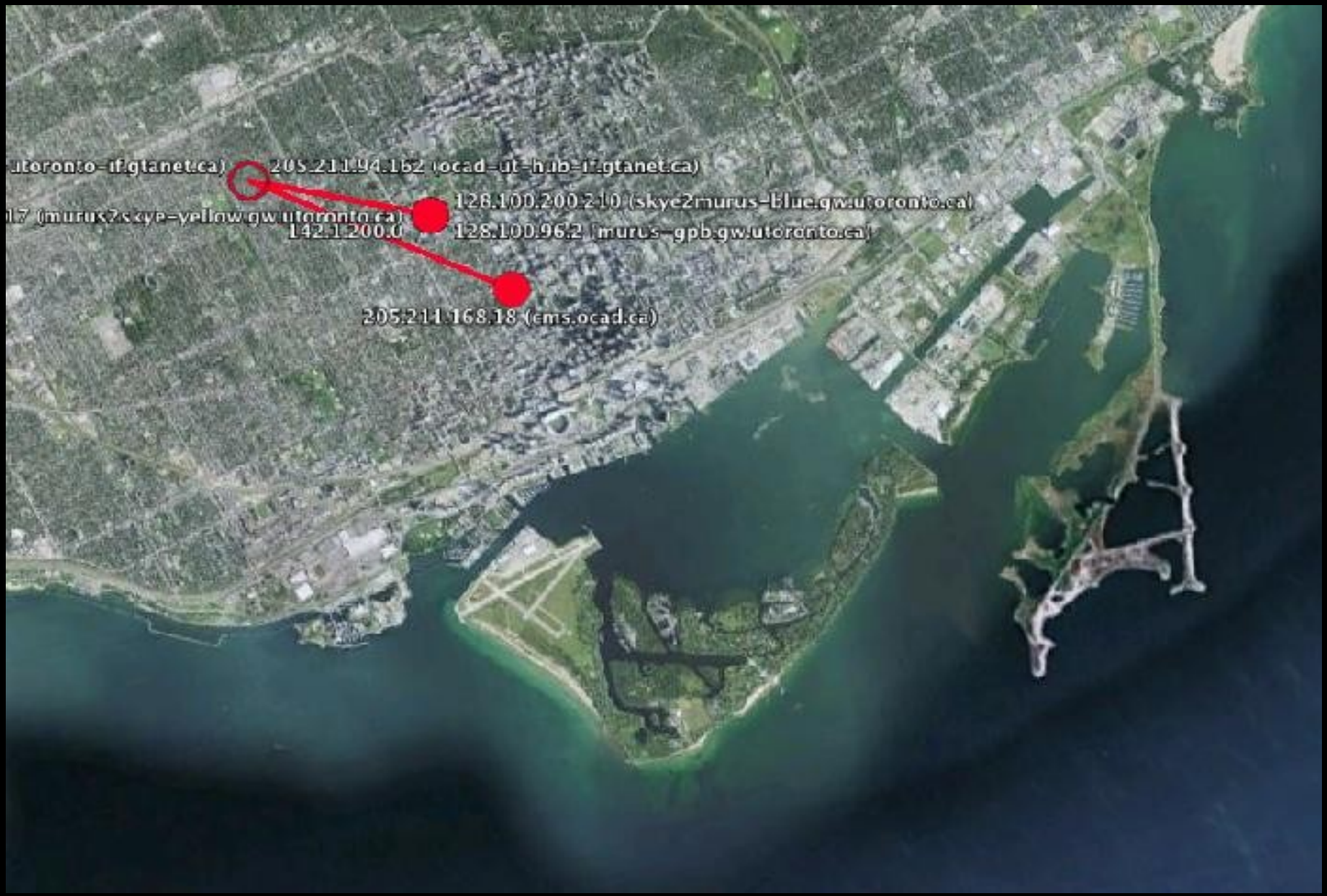
Network sovereignty –
A Canadian perspective

- Surveillance and privacy
  - Internet traffic via US routes or carriers brings exposure to USA PATRIOT Act and possibly NSA wiretapping
    - eg RefWorks case
- Cyber-infrastructure security
- Economic implications

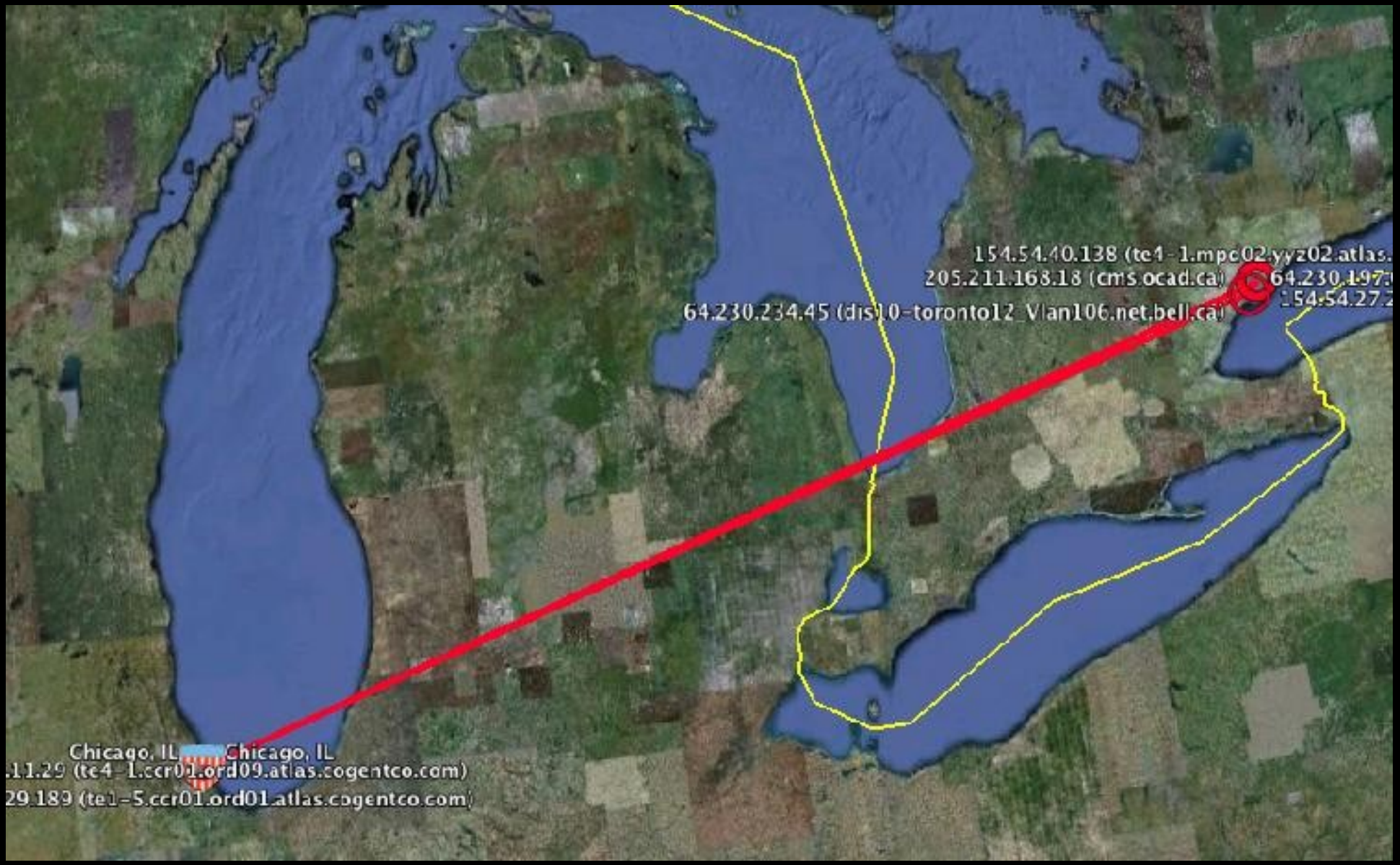
"Boomerang" routes

- Routes originate and terminate in Canada, but transit the US
- How common? About 40% of routes that originate and terminate in Canada go through the US
- Why?
  - Capacity/congestion. Cost. Carrier interconnection policies.
- Implications

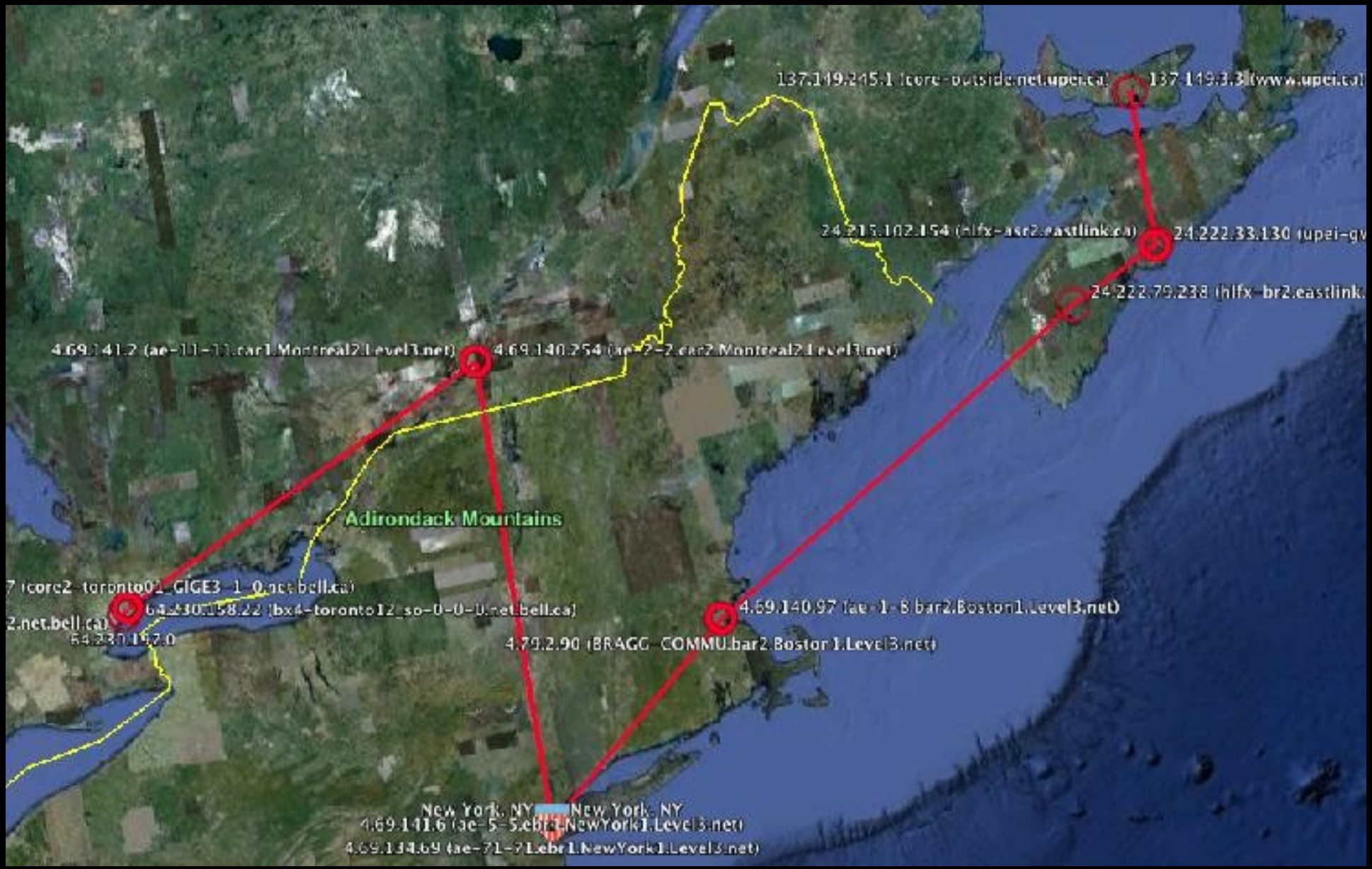
T.O. > T.O.(OCAD) UToronto > GTAnet (TR4158)



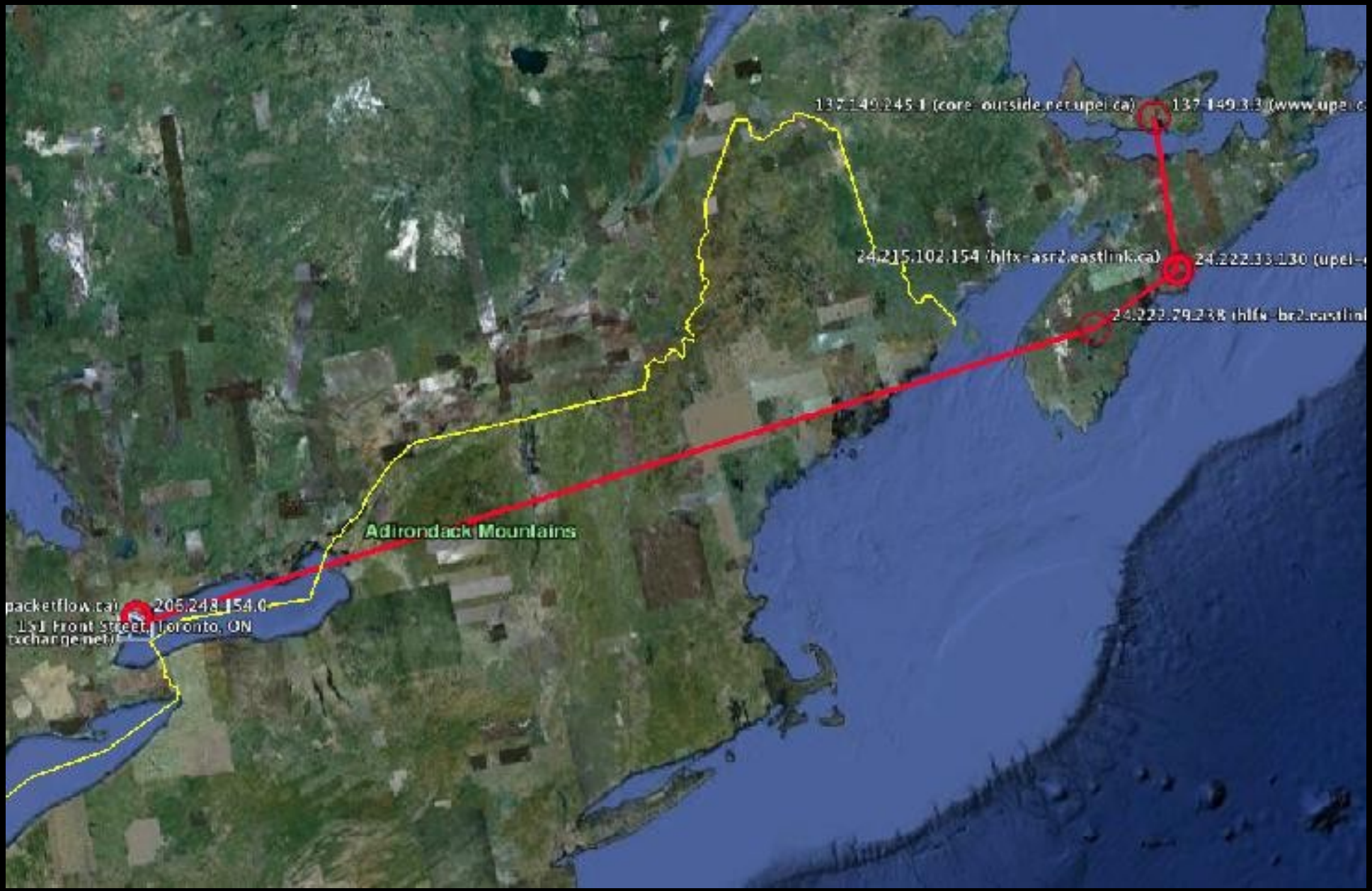
T.O. > T.O.(OCAD) Bell > Cogent > GTAnet (TR6828)



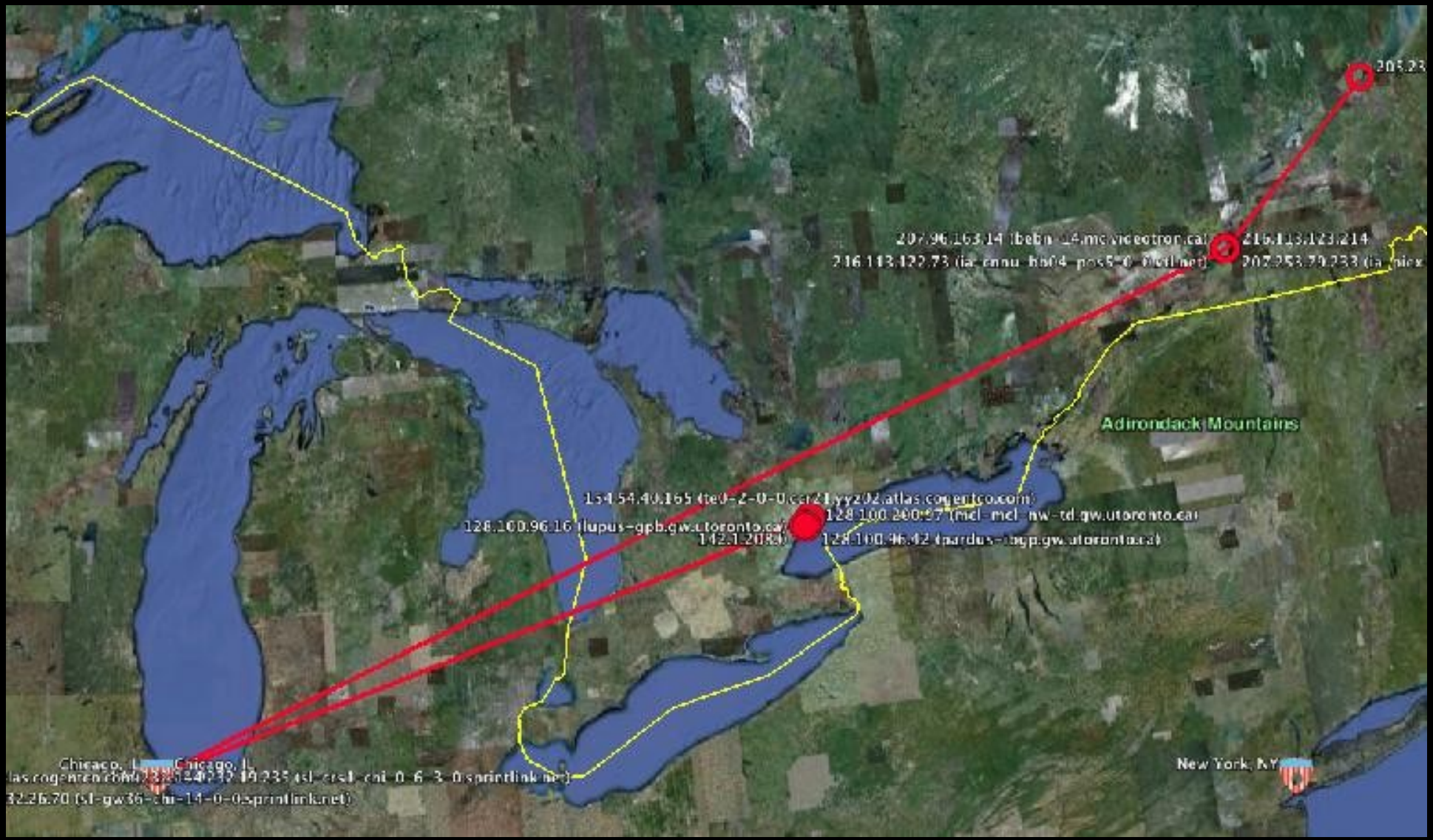
T.O. > PEI: Bell > Level3 > Eastlink (TR138)



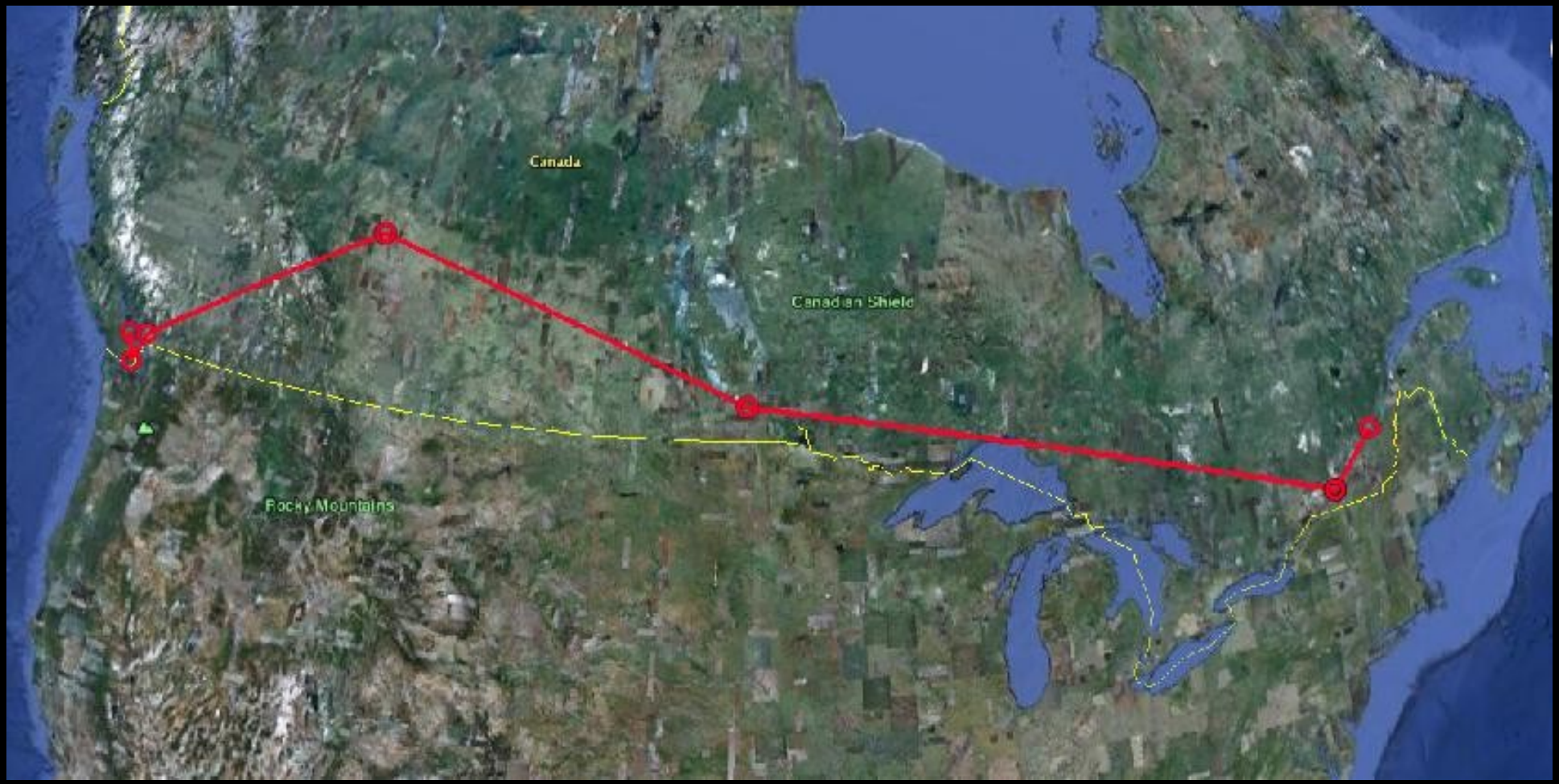
T.O. > PEI: Teksavvy > Eastlink (TR935)

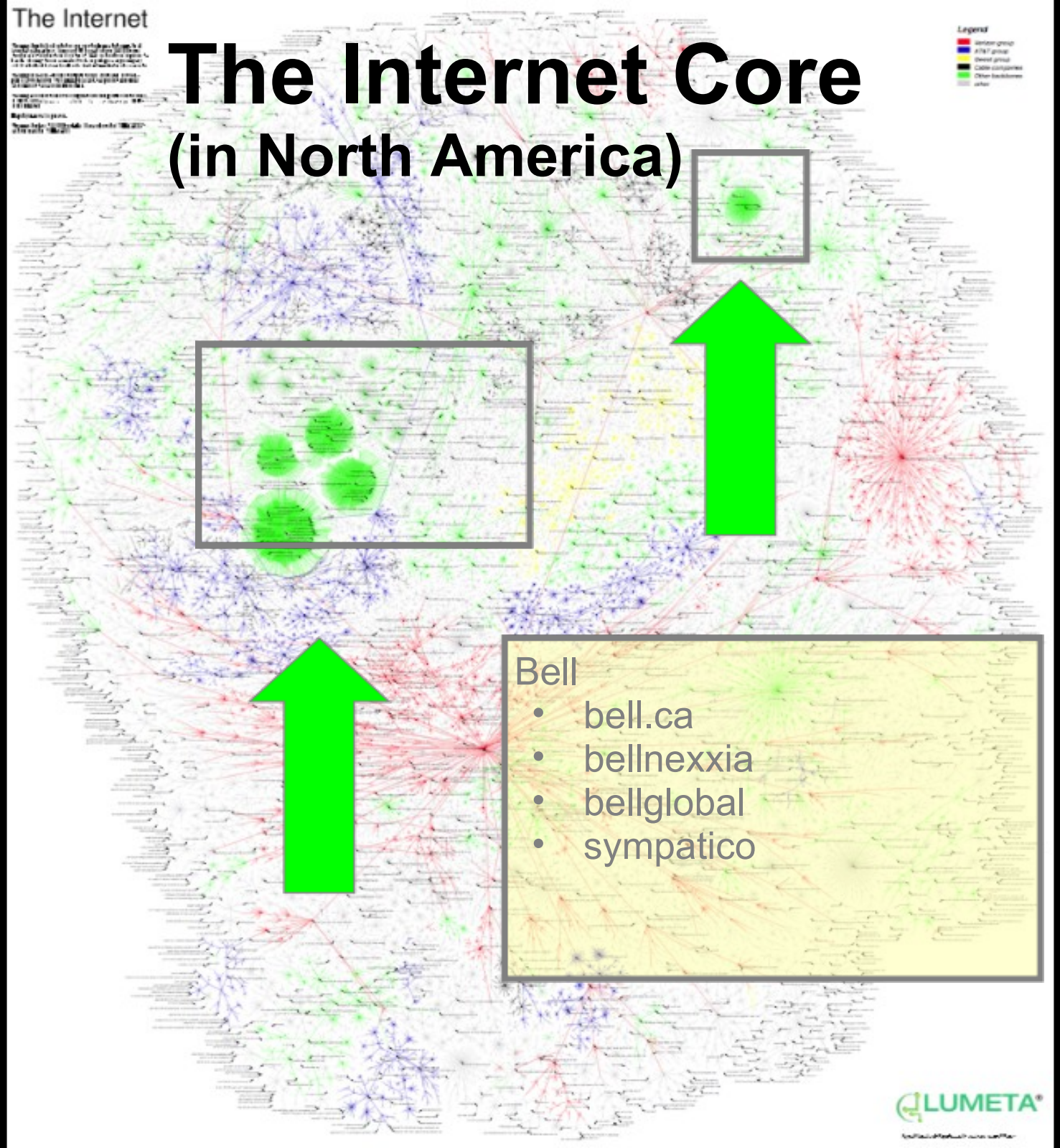


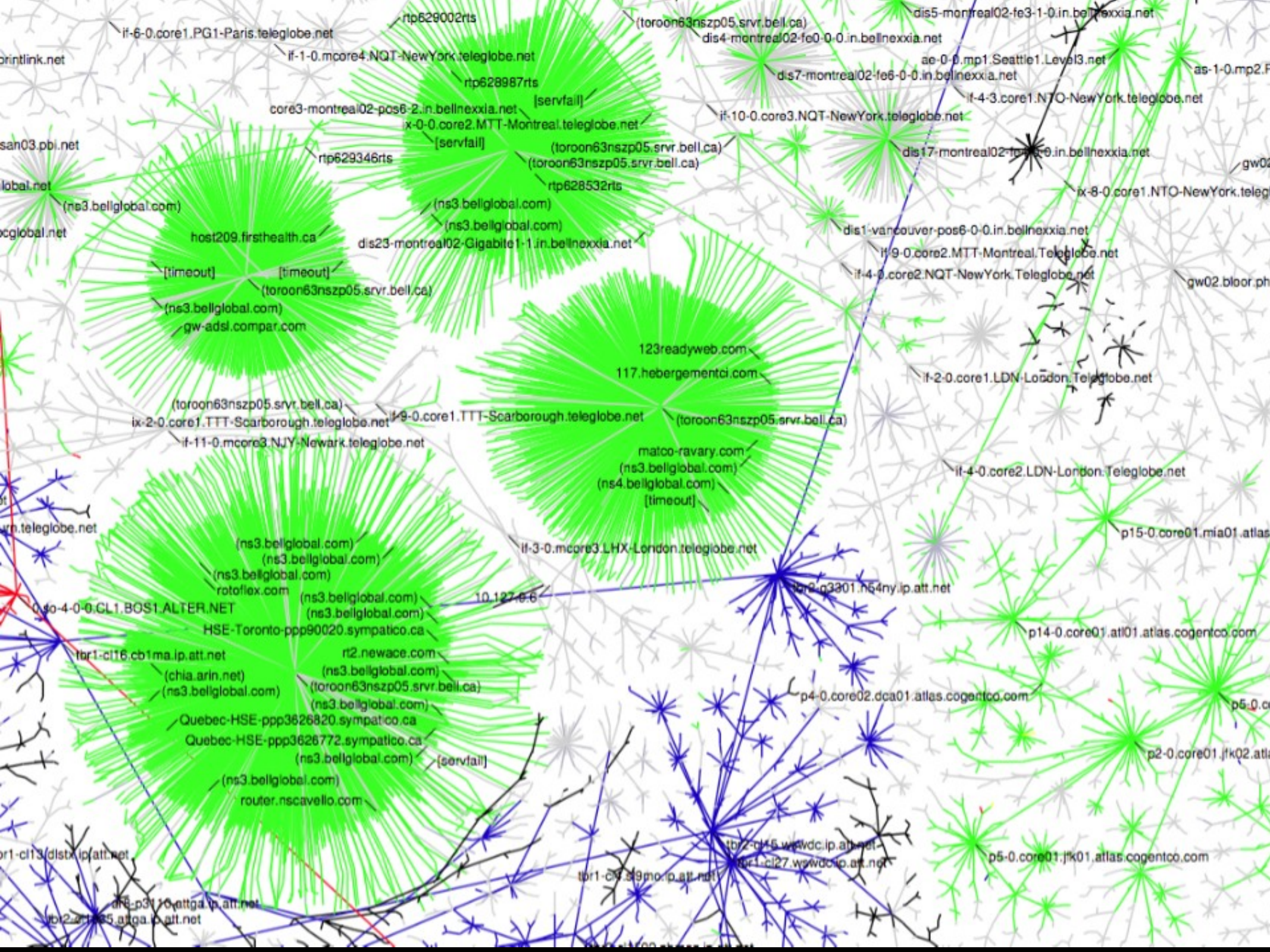
T.O> Quebec City: UToronto> Cogent>Sprint>Videotron (TR7518)

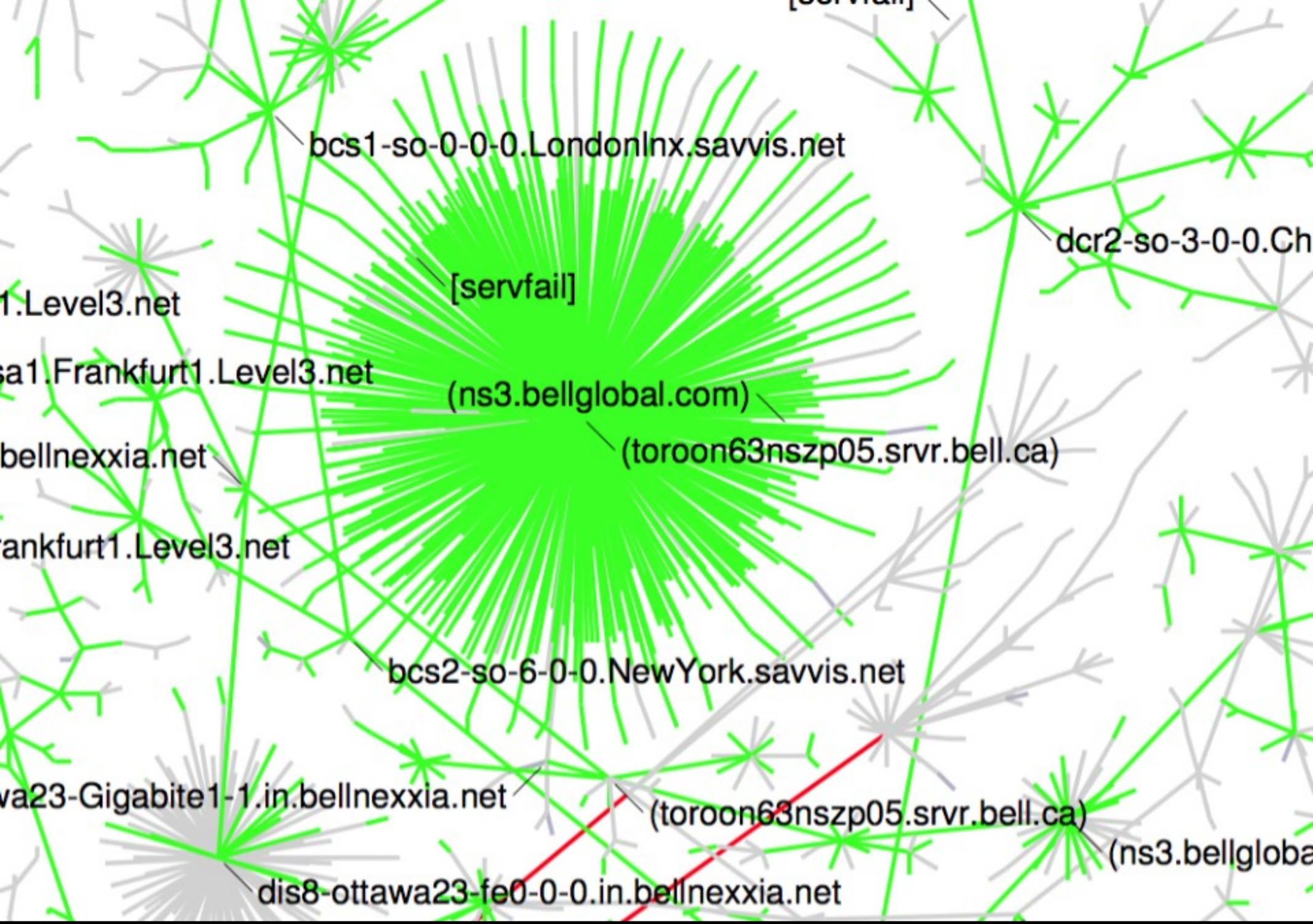


Nanaimo BC > Quebec City: Shaw > Videotron (TR1204)




The Internet
The Internet Core
(in North America)
Bell
• bell.ca
• bellnexxia
• bellglobal
• sympatico
LUMETA


rtp629002rts
(toroon63nszp05.srvr.bell.ca)
if-6-0.core1.PG1-Paris.teleglobe.net
dis5-montreal02-fe3-1-0.in.bellnexxia.net
dis4-montreal02-fe0-0-0.in.bellnexxia.net
if-1-0.mcore4.NQT-NewYork.teleglobe.net
ae-0-0.mp1.Seattle1.Level3.net
dis7-montreal02-fe6-0-0.in.bellnexxia.net
rtp628987rts
[servfail]
if-4-3.core1.NTO-NewYork.teleglobe.net
core3-montreal02-pos6-2.in.bellnexxia.net
if-10-0.core3.NQT-NewYork.teleglobe.net
ix-0-0.core2.MTT-Montreal.teleglobe.net
[servfail]
(toroon63nszp05.srvr.bell.ca)
rtp629346rts
(toroon63nszp05.srvr.bell.ca)
dis17-montreal02-fe3-0-0.in.bellnexxia.net
rtp628532rts
ix-8-0.core1.NTO-NewYork.teleg
(ns3.bellglobal.com)
(ns3.bellglobal.com)
(ns3.bellglobal.com)
dis1-vancouver-pos6-0-0.in.bellnexxia.net
host209.firsthealth.ca
dis23-montreal02-Gigabite1-1.in.bellnexxia.net
if-9-0.core2.MTT-Montreal.Teleglobe.net
[timeout]
[timeout]
if-4-0.core2.NQT-NewYork.Teleglobe.net
gw02.bloor.ph
(toroon63nszp05.srvr.bell.ca)
(ns3.bellglobal.com)
gw-adsl.compar.com
123readyweb.com
117.hebergementci.com
if-2-0.core1.LDN-London.Teleglobe.net
(toroon63nszp05.srvr.bell.ca)
if-9-0.core1.TTT-Scarborough.teleglobe.net
ix-2-0.core1.TTT-Scarborough.teleglobe.net
(toroon63nszp05.srvr.bell.ca)
if-11-0.mcore3.NJY-Newark.teleglobe.net
matco-ravary.com
(ns3.bellglobal.com)
if-4-0.core2.LDN-London.Teleglobe.net
(ns4.bellglobal.com)
[timeout]
p15-0.core01.mia01.atlas
if-3-0.mcore3.LHX-London.teleglobe.net
(ns3.bellglobal.com)
(ns3.bellglobal.com)
(ns3.bellglobal.com)
rotoflex.com
(ns3.bellglobal.com)
10.127.0.6
tbr2-g3301.n54ny.ip.att.net
0.so-4-0-0.CL1.BOS1.ALTER.NET
(ns3.bellglobal.com)
HSE-Toronto-ppp90020.sympatico.ca
p14-0.core01.atl01.atlas.cogentco.com
rt2.newace.com
tbr1-cl16.cb1ma.ip.att.net
(ns3.bellglobal.com)
(chia.arin.net)
(toroon63nszp05.srvr.bell.ca)
(ns3.bellglobal.com)
p4-0.core02.dca01.atlas.cogentco.com
(ns3.bellglobal.com)
Quebec-HSE-ppp3626820.sympatico.ca
Quebec-HSE-ppp3626772.sympatico.ca
p2-0.core01.jfk02.atl
(ns3.bellglobal.com)
[servfail]
(ns3.bellglobal.com)
router.nscavello.com
tbr2-cl15.wswdc.ip.att.net
tbr1-cl27.wswdc.ip.att.net
p5-0.core01.jfk01.atlas.cogentco.com
tbr1-cl13.dlstx.ip.att.net
tbr1-cl13.sl9mo.ip.att.net



http://blogs.cio.com/who_owns_the_internet_we_have_a_map_that_shows_you?

Policy Implications

Findings (Preliminary)

- Canadian boomerang routing is commonplace (1/3 IXmaps)
- Canadian boomerang routing is largely related to interconnection policies, not capacity/congestion
  - If originating or terminating carrier is a major carrier, even a ‘competitor’, routing generally stays in Canada
- Major Canadian carriers (Bell, Telus, Videotron …) avoid connecting with smaller Canadian carriers in Canada
  - Requires use of foreign carriers for non-local transfers
  - Exchanges often occur in US
  - Brings heightened interception and surveillance risks
- Caveats:
  - Haven’t investigated relative costs
  - Needs more systematic collection of traceroute data, across location, time and carrier.

'Lawful Access' legislation

C-50 (Improving Access to Investigative Tools for Serious Crimes Act)

- make it easier for the police to obtain judicial approval of multiple intercept and tracking warrants and production orders, to access and track e-communications.

C-51 (Investigative Powers for the 21st Century Act)

- give the police new powers to obtain court orders for remote live tracking, as well as suspicion-based orders requiring telecommunication service providers and other companies to preserve and turn over data of interest to the police.

C-52 (Investigating and Preventing Criminal Electronic Communications Act)

- require telecommunication service providers to build and maintain intercept capability into their networks for use by law enforcement, and gives the police warrantless power to access subscriber information.

Concerns

- Expands the scope and depth of surveillance
- Threatens fundamental rights and freedoms, most notably privacy
- Lack of justification
- Lack of public debate
- Lack of judicial oversight
- Lack of public accountability
- Lack of stringent conditions
- Builds surveillance capacity into the infrastructure

http://www.unlawfulaccess.net/

Implications

- Internet routing is a public interest concern
- Public education
  - Internet traffic visualization tools/routing options
- Promote greater operational transparency by carriers and service providers
- Investigate privacy risks and protections
- Investigate possible oligopolistic behaviour
- Promote traffic exchange within Canada
  - Challenge pending “lawful access” legislation
    - http://openmedia.ca/StopSpying

Implications

- Internet routing is a public interest concern
- Public education
  - Internet traffic visualization tools/routing options
- Need for greater operational transparency by carriers
- Investigate privacy risks and protections
- Investigate possible oligopolistic behaviour?
- Promote greater interconnection among Canadian carriers within Canada
- Resist pending “Lawful Access” legislation

Wrapup

See where your packets go!
(and contribute to the database)

Try it out and get more information at:
http://IXmaps.ca

Project team:

- Andrew Clement,[1] Steve Harvey, [3] Yannet Lathrop,[1] Colin McCann,[1] Nancy Paterson,[2] Gabby Resch[1] & Erik Stewart[3]

[1] Faculty of Information, Univ of Toronto
[2] OCAD University
[3] Independent

Funding:

- Social Sciences and Humanities Research Council (SSHRC)

References:

- Bamford, James (2008) *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*. Doubleday.
- Klein, Mark (2009) *Wiring Up The Big Brother Machine...And Fighting It.* Booksurge.
- Landau, Susan (2011) *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*, MIT Press.