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

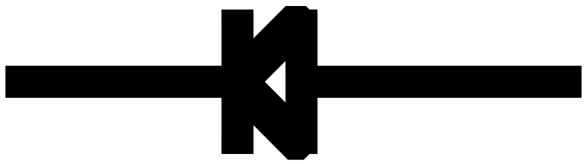
- Conferences
- BSTJ 1984: less is more

Bell Labs, late 1980s

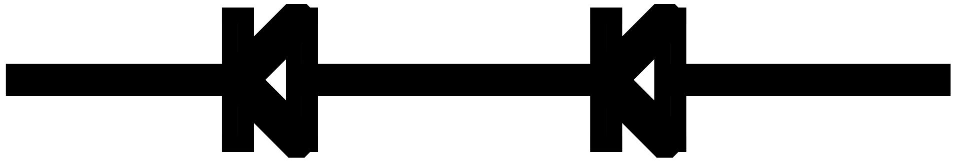
- Morris worm and the firewall
- Packet telescope
- read-only network link
- PC viruses: “falling tears”, etc.

ches Fri Apr 20 07:46:11 EDT 1990

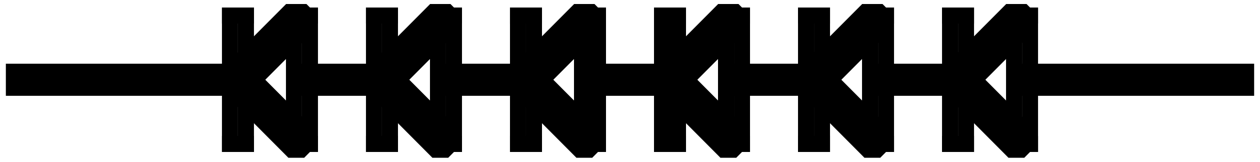
Original firewall



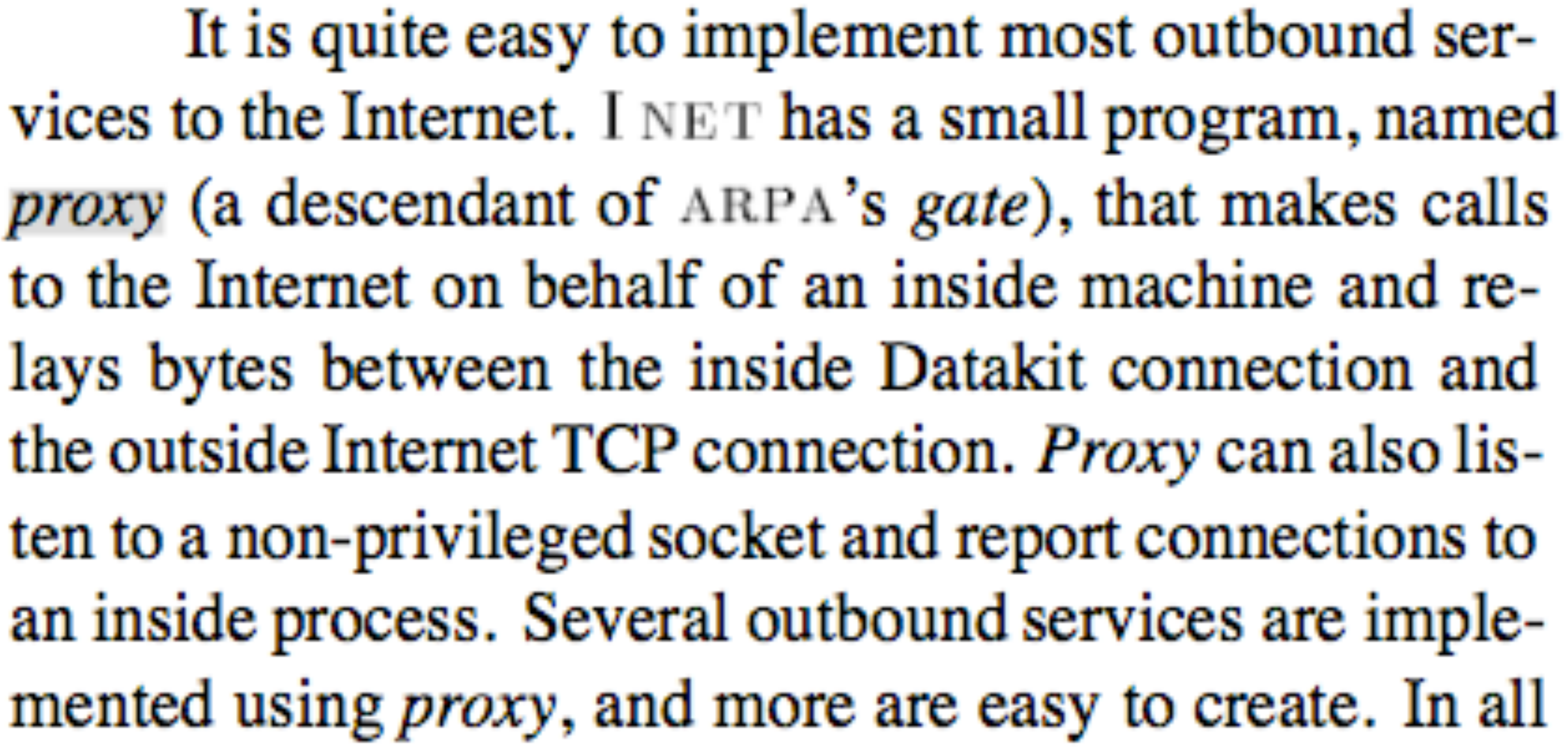
My (Safer!) Firewall



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
```

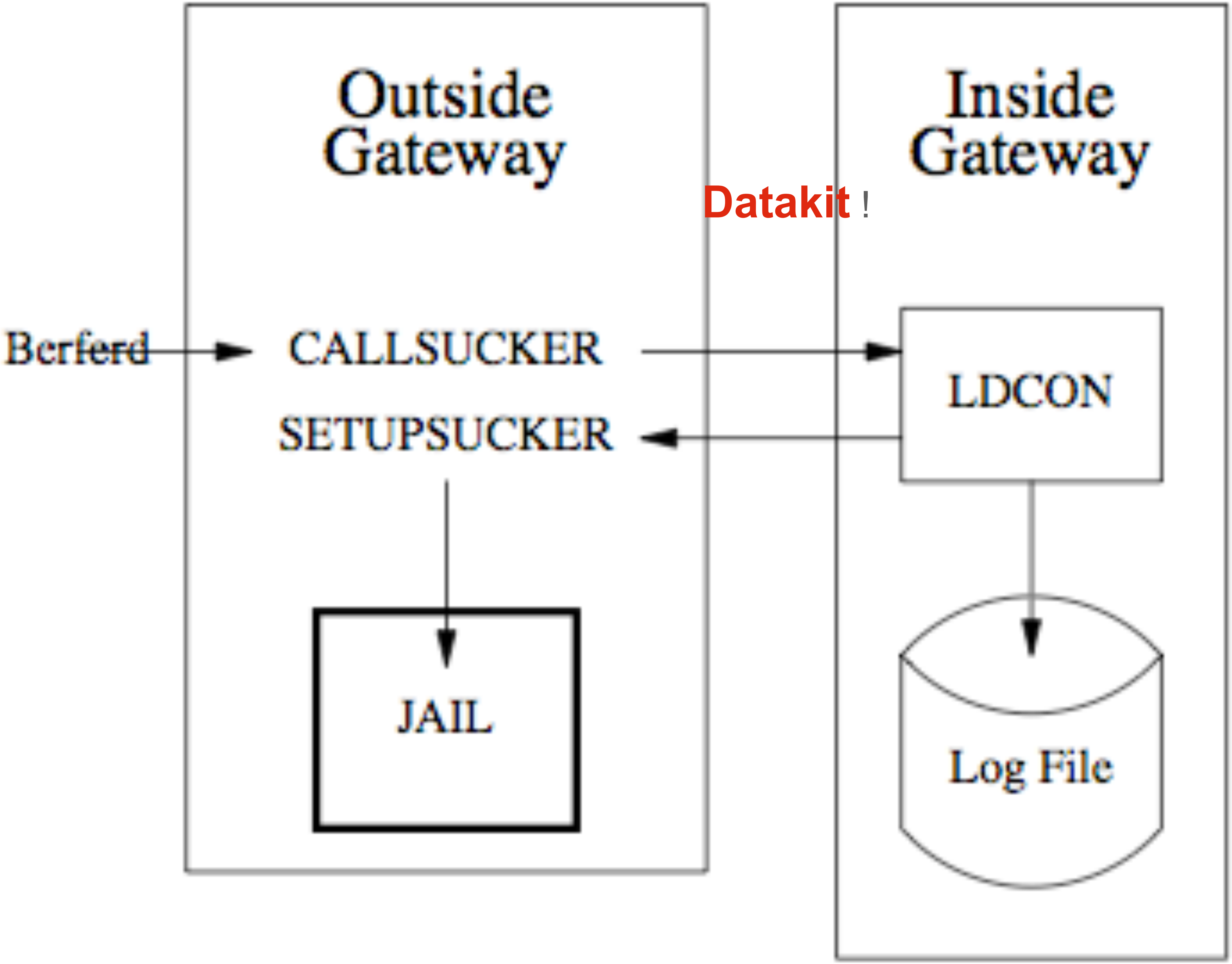
```
19:43:10 smtpd: <--- 220 inet.att.com SMTP
19:43:14 smtpd: -------> debug 19:43:14 smtpd: DEBUG attempt
19:43:14 smtpd: <--- 200 OK
19:43:25 smtpd: -------> mail from:</dev/null>
19:43:25 smtpd: <--- 503 Expecting HELO
19:43:34 smtpd: -------> helo
19:43:34 smtpd: HELO from
19:43:34 smtpd: <--- 250 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
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

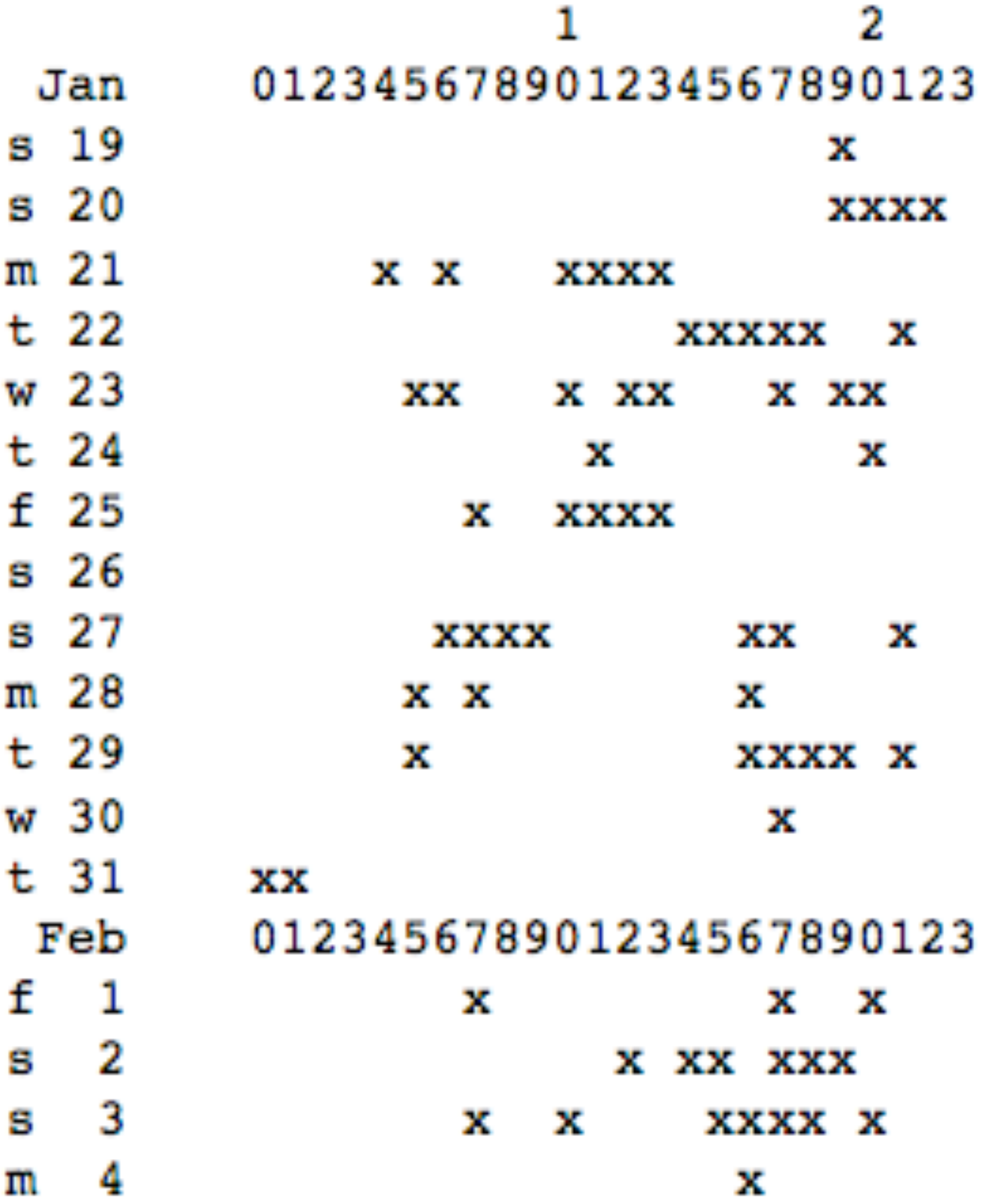
rm -rf /

```
rm -rf /&
finger attempt on berferd
/bin/rm -rf /&
/bin/rm -rf /&
/bin/rm -rf /&
Attempt to login with bfrd
 from embezzle.Stanford.EDU
```

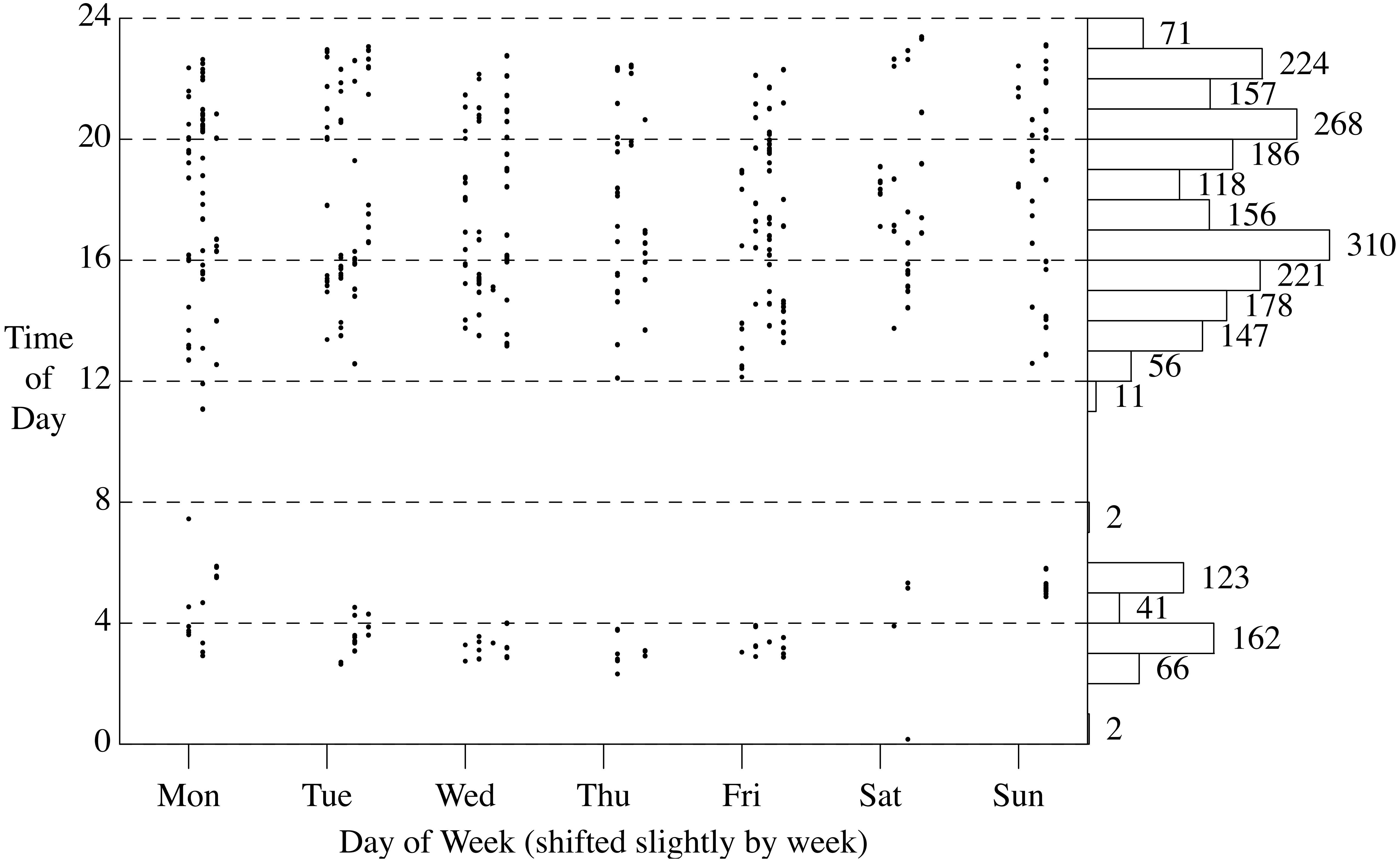


Datakit !

[illegible] or about [illegible]



```
                  1         2
 Jan    012345678901234567890123
s 19                       x
s 20                       xxxx
m 21        x x   xxxx
t 22                  xxxxx  x
w 23         xx   x xx   x xx
t 24               x        x
f 25           x  xxxx
s 26
s 27          xxxx      xx   x
m 28         x x        x
t 29         x          xxxx x
w 30                     x
t 31    xx
 Feb    012345678901234567890123
f  1           x         x  x
s  2                x xx xxx
s  3           x  x    xxxx x
m  4                    x
```



24
20
16
12
8
4
0
Time of Day
Mon
Tue
Wed
Thu
Fri
Sat
Sun
Day of Week (shifted slightly by week)
71
224
157
268
186
118
156
310
221
178
147
56
11
2
123
41
162
66
2

Internet Security, Second Edition

of *Firewalls and Internet Security* became the bible of Internet security
think about threats and solutions. This completely updated and expanded
security problems companies face in today's Internet, identifies the
ular security technologies, and illustrates the ins and outs of deploying
will learn how to plan and execute a security strategy that allows easy
while defeating even the wiliest of hackers.

rity, 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
tacks on hosts and networks and describes the tools and techniques used
such attacks. The focus then shifts to firewalls and virtual private
a step-by-step guide to firewall deployment. Readers are immersed in
ternet security through a critical examination of problems and practices
l as discussions on the deployment of a hacking-resistant host and on
IDSs. The authors scrutinize secure communications over insecure
their predictions about the future of firewalls and Internet security.

ide an introduction to cryptography and a list of resources (which will
Web site and updated there regularly) that readers can rely on for
ts in Internet security.

l-won knowledge of how to fight off hackers, readers of *Firewalls and*
dition, can make security [illegible] that will make the Internet [illegible] and

ef Scientist at Lumeta Corporation, which explores and maps clients'
finds perimeter leaks. Formerly he was a senior researcher at AT&T Bell
pioneering work in the areas of firewall design and implementation, PC
nications, and the Plan 9 operating system.

the creator of Netnews, is a Fellow at AT&T Labs Research. He is a
ademy of Engineering and a frequent participant in National Research
ently one of the Security Area directors of the Internet Engineering

bin.com) is an Associate Professor in the Computer Science Department
and serves as the Technical Director of the Information Security
Principal Researcher in the Secure Systems Research Department at
the author of *White-Hat Security Arsenal* (Addison-Wesley, 2001).

com

& Wiley Miller. Distributed by
ion. All rights reserved.

paper

7 85342 63466 2

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

Firewalls and Internet Security

Second Edition

Cheswick
Bellovin
Rubin

Addison
Wesley

Firewalls and Internet Security
Second Edition

Repelling the Wily Hacker

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

DANG... I KNEW WE SHOULD'VE STORMED THE CASTLE BEFORE IT GOT TRENDY...

ADDISON-WESLEY PROFESSIONAL COMPUTING SERIES

1996: Highlands Forum and DoS arrives

Highlands

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

DoS

- Panix 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

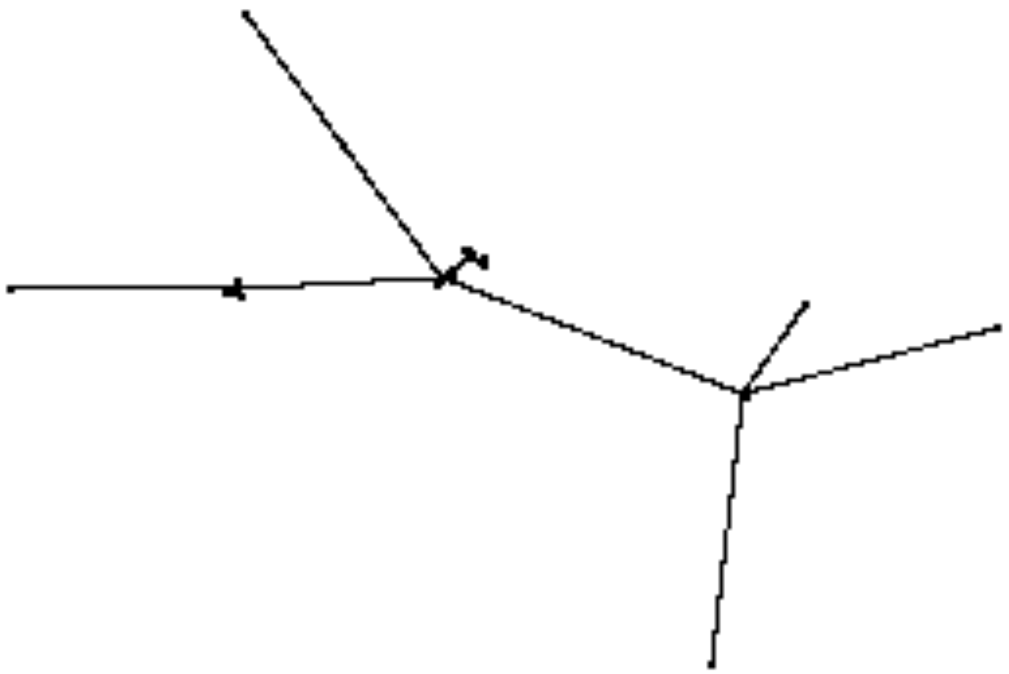
- traceroute + layout algorithm
- Hal Burch’s amazing programming

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

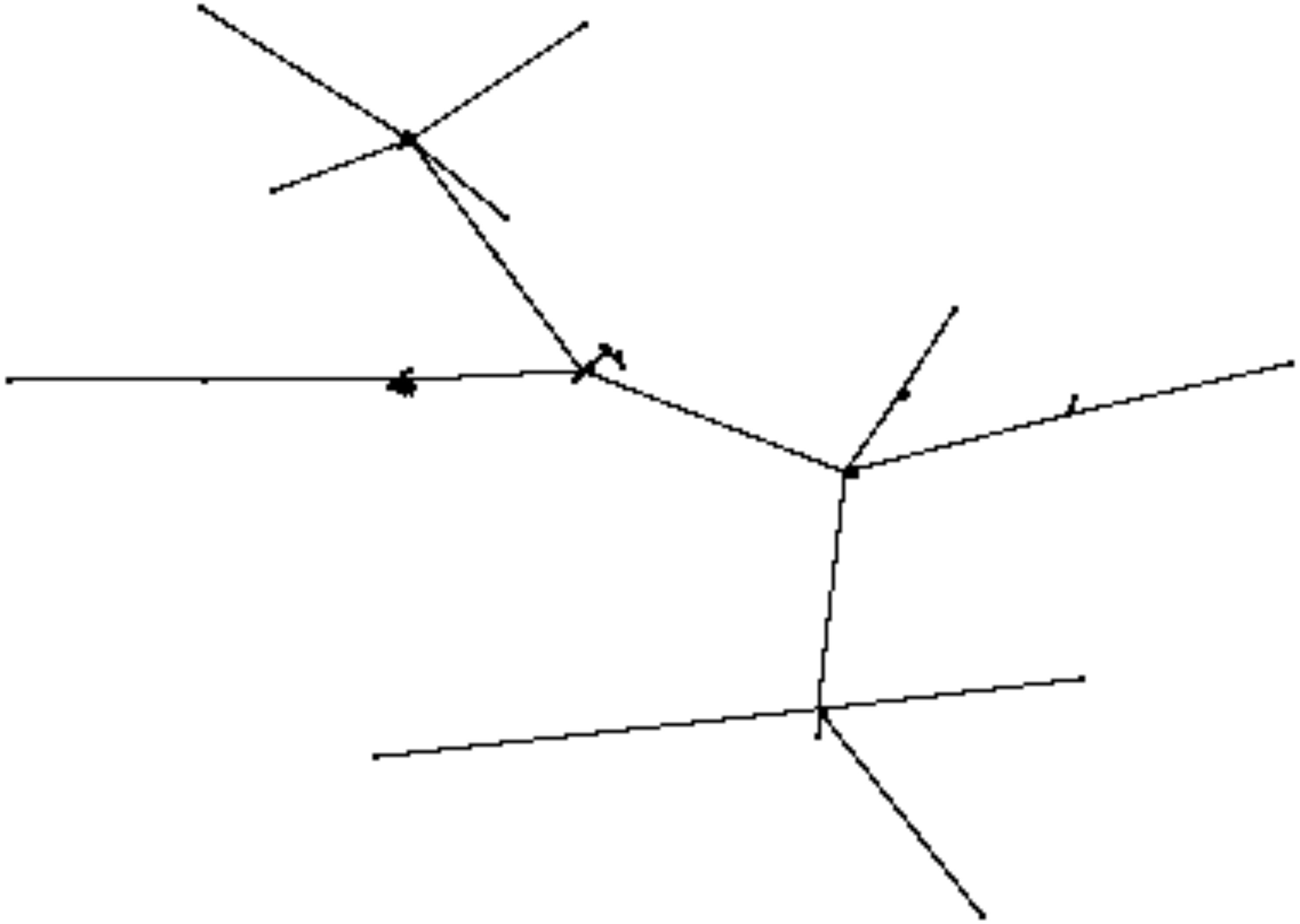
Visualization goals

- 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

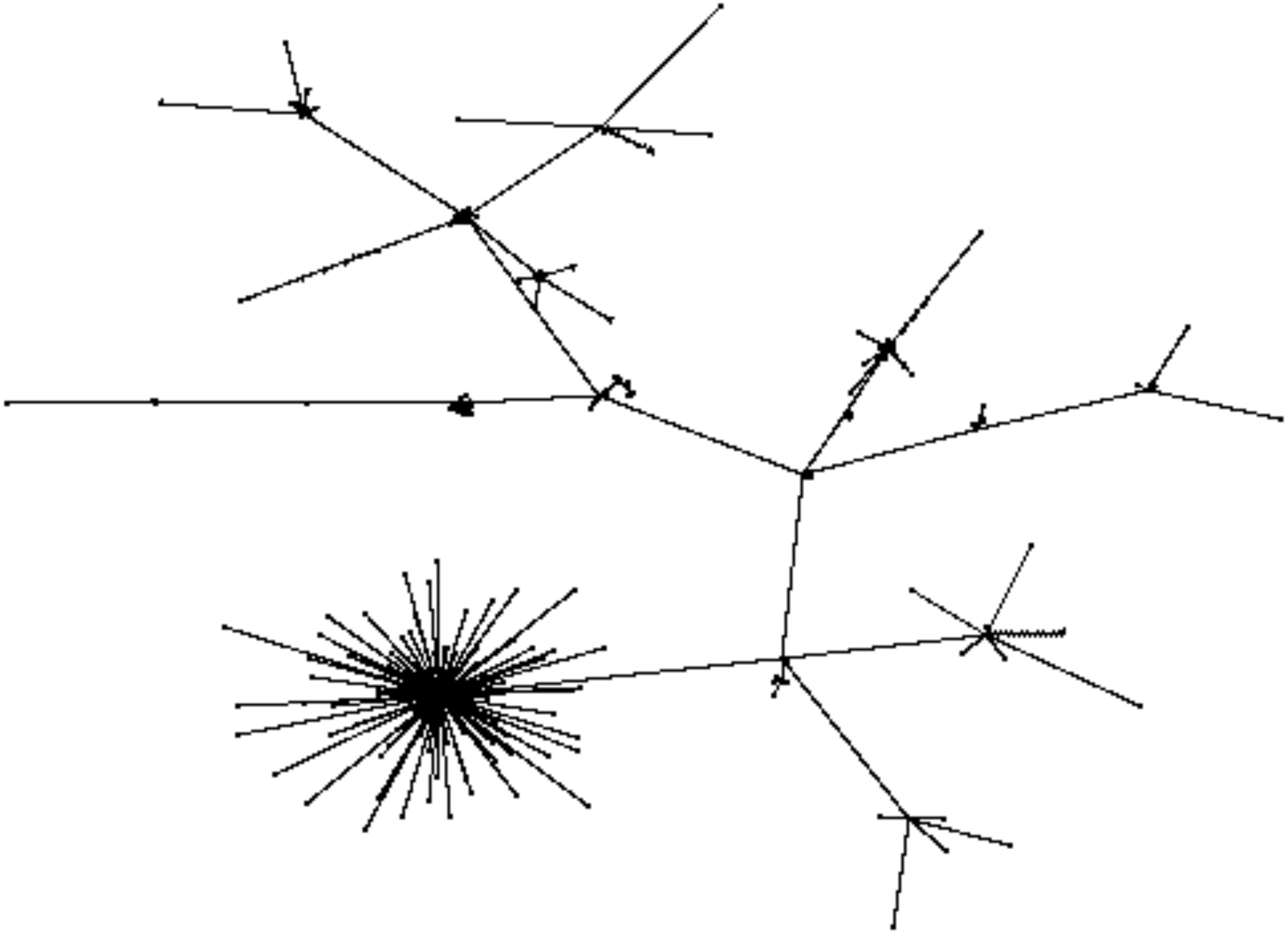
5 April 2014

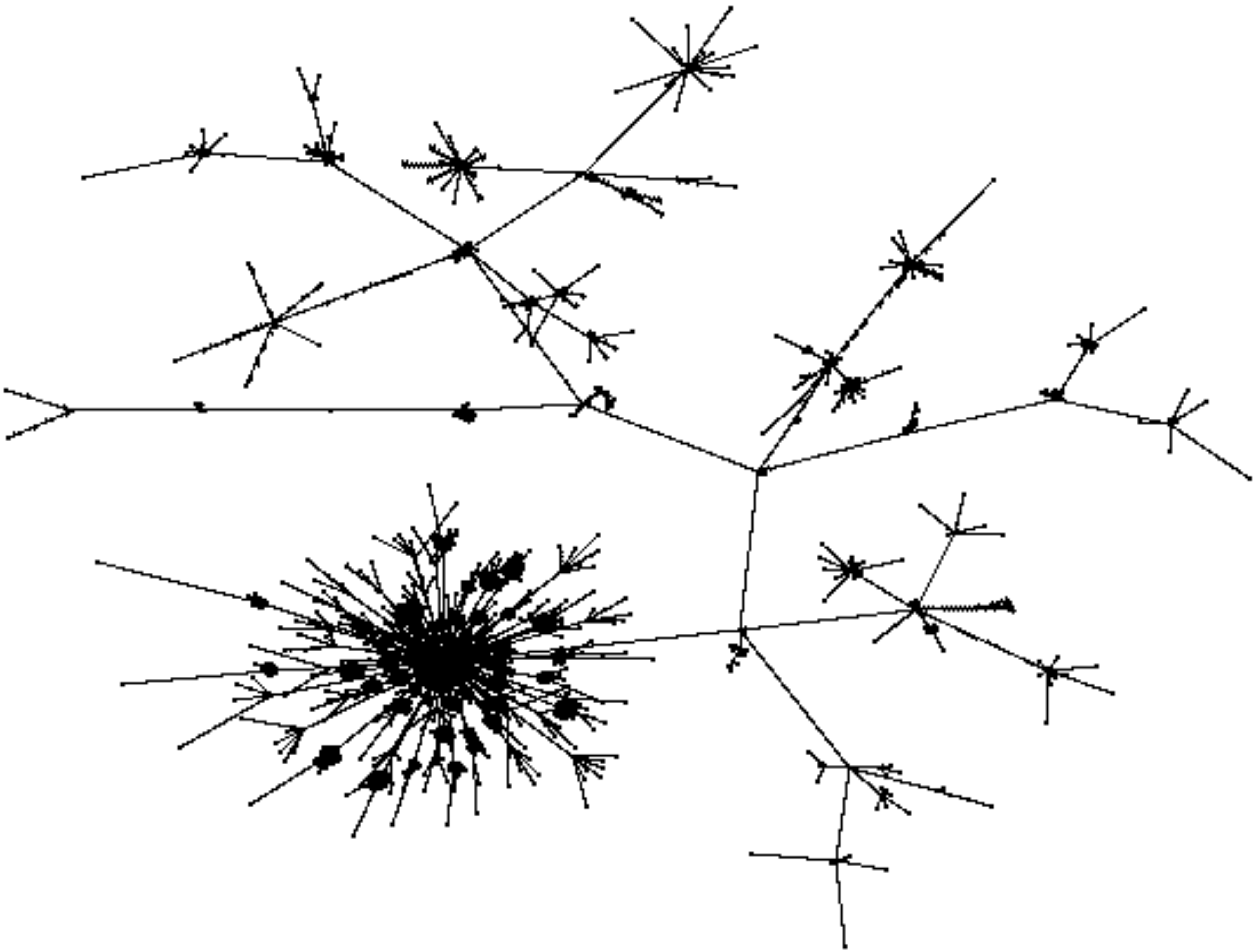


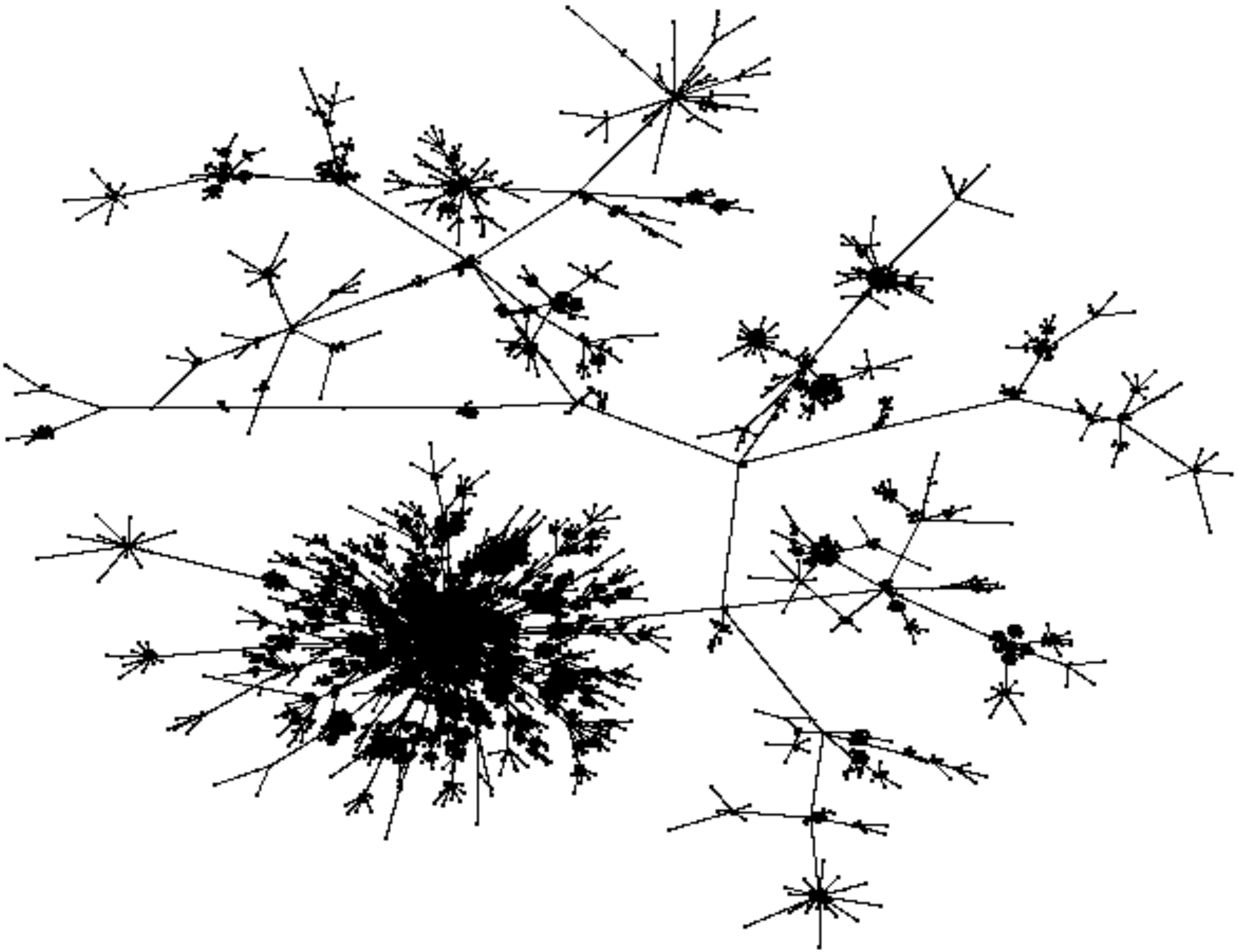
5 April 2014

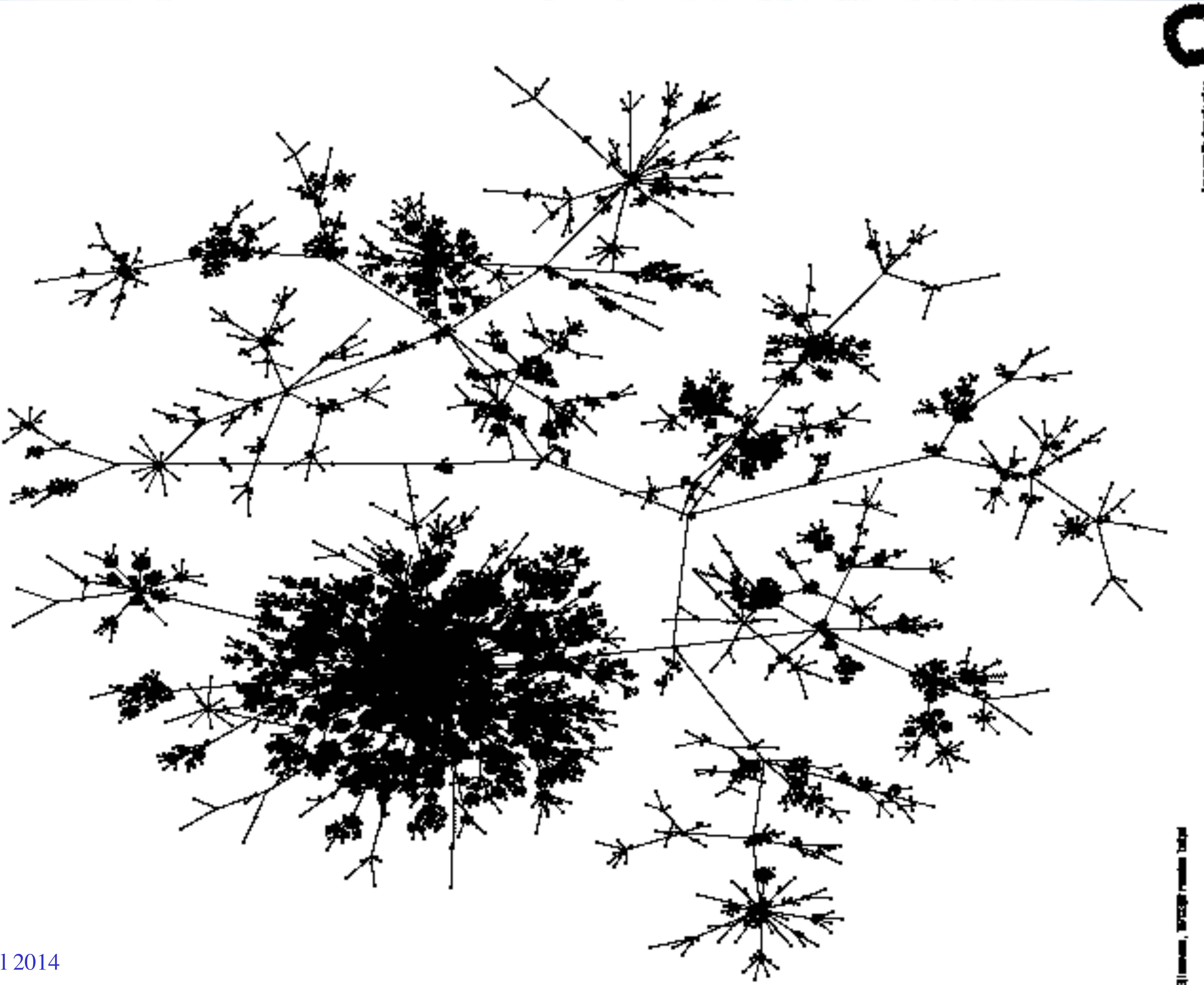


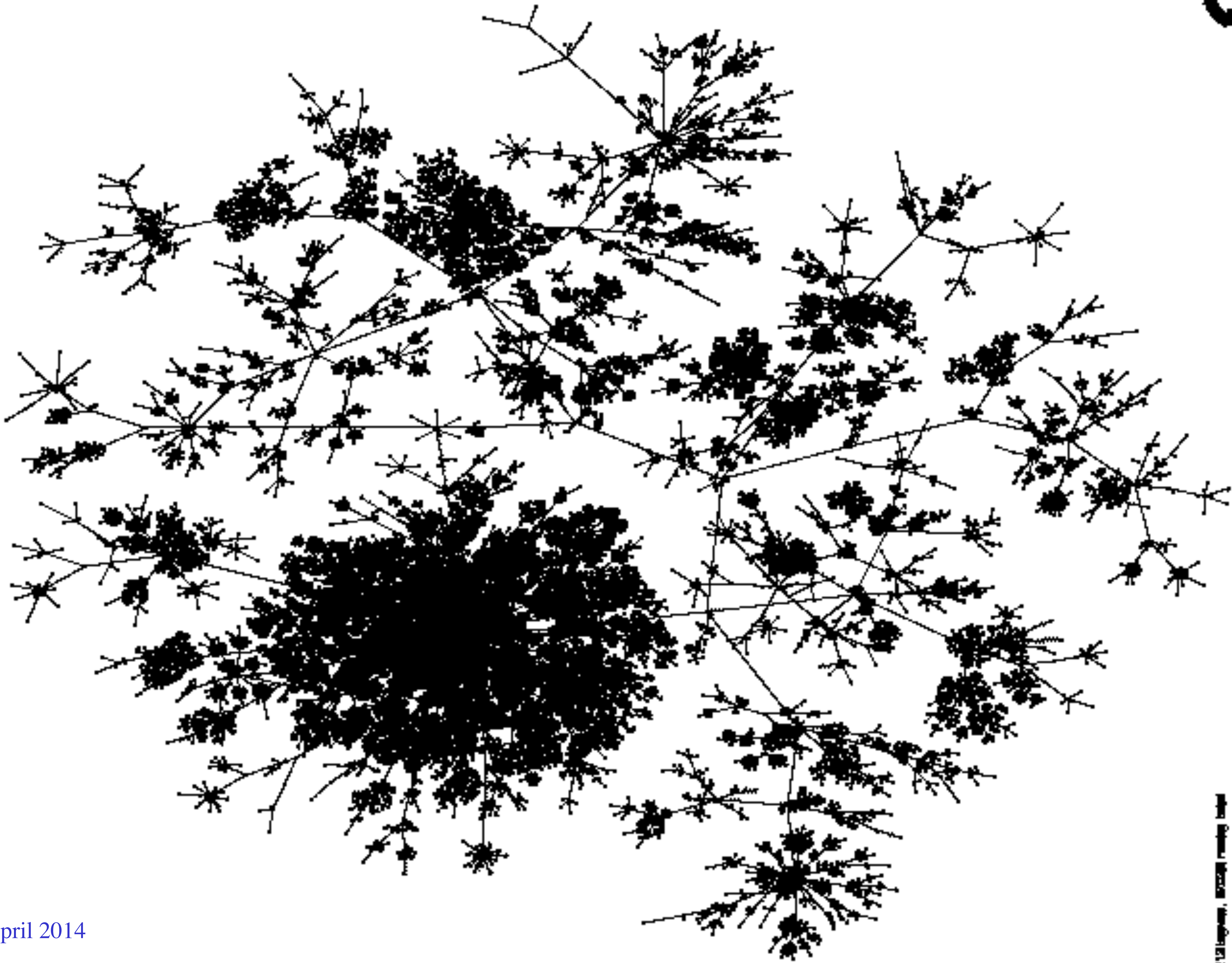
5 April 2014

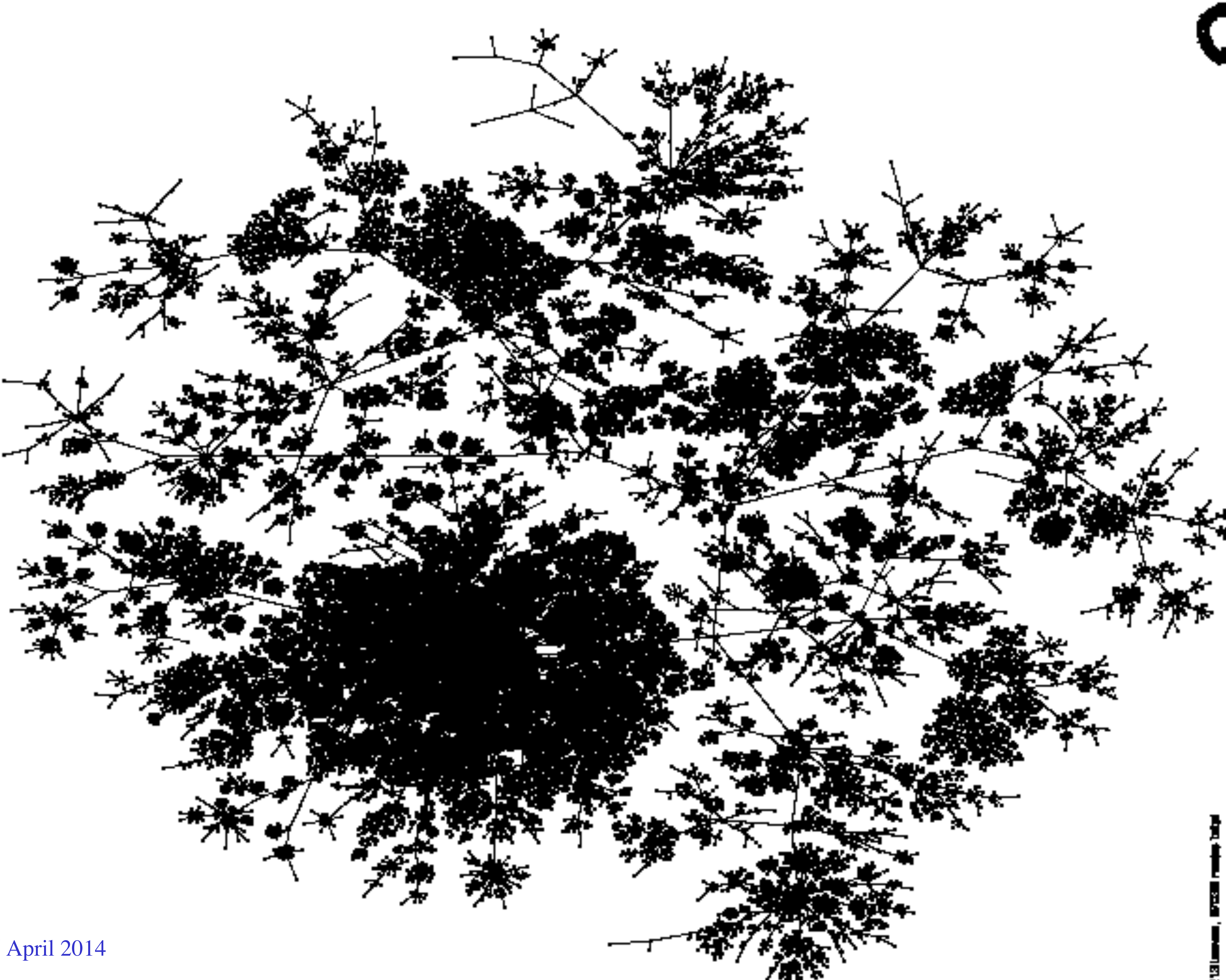




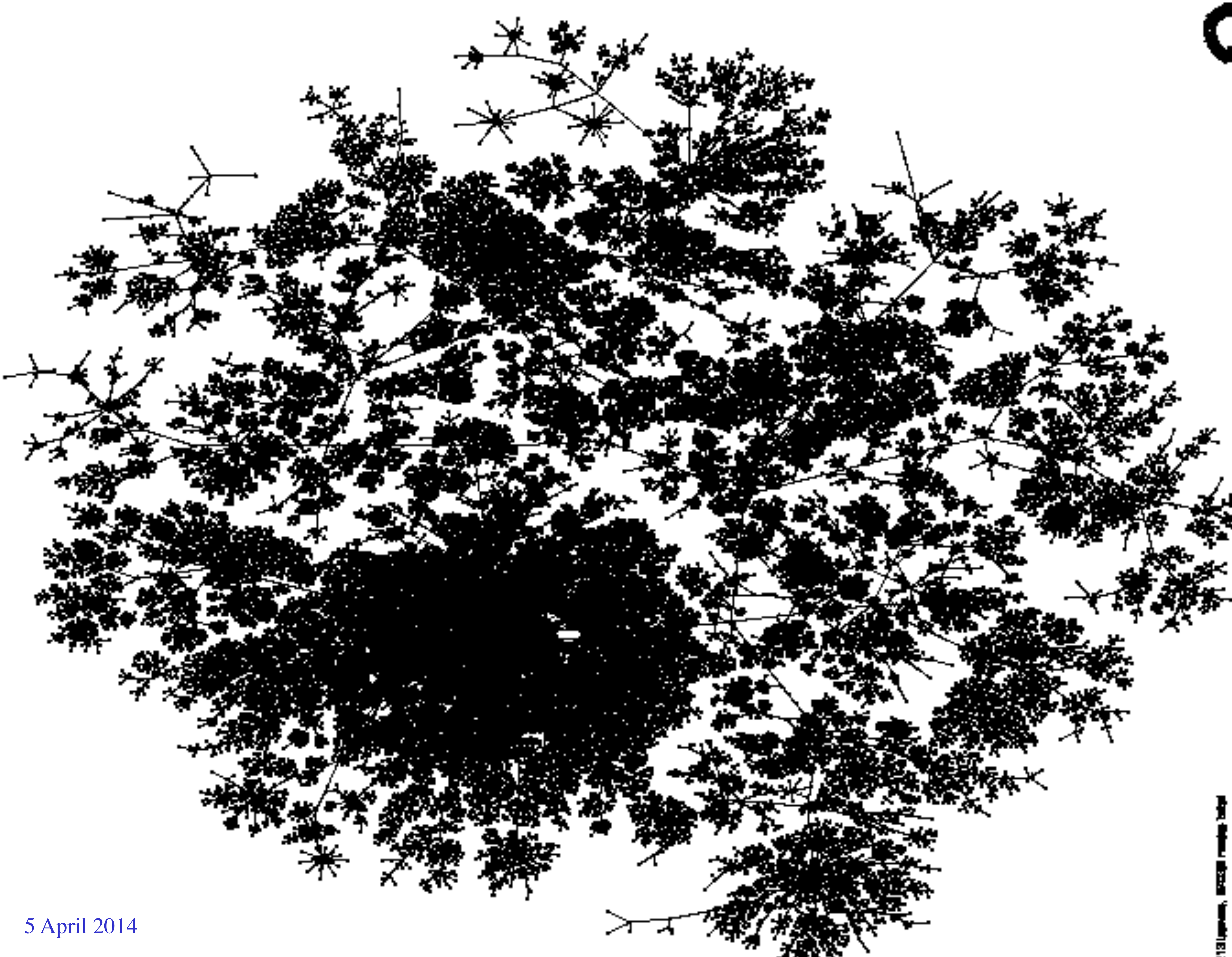






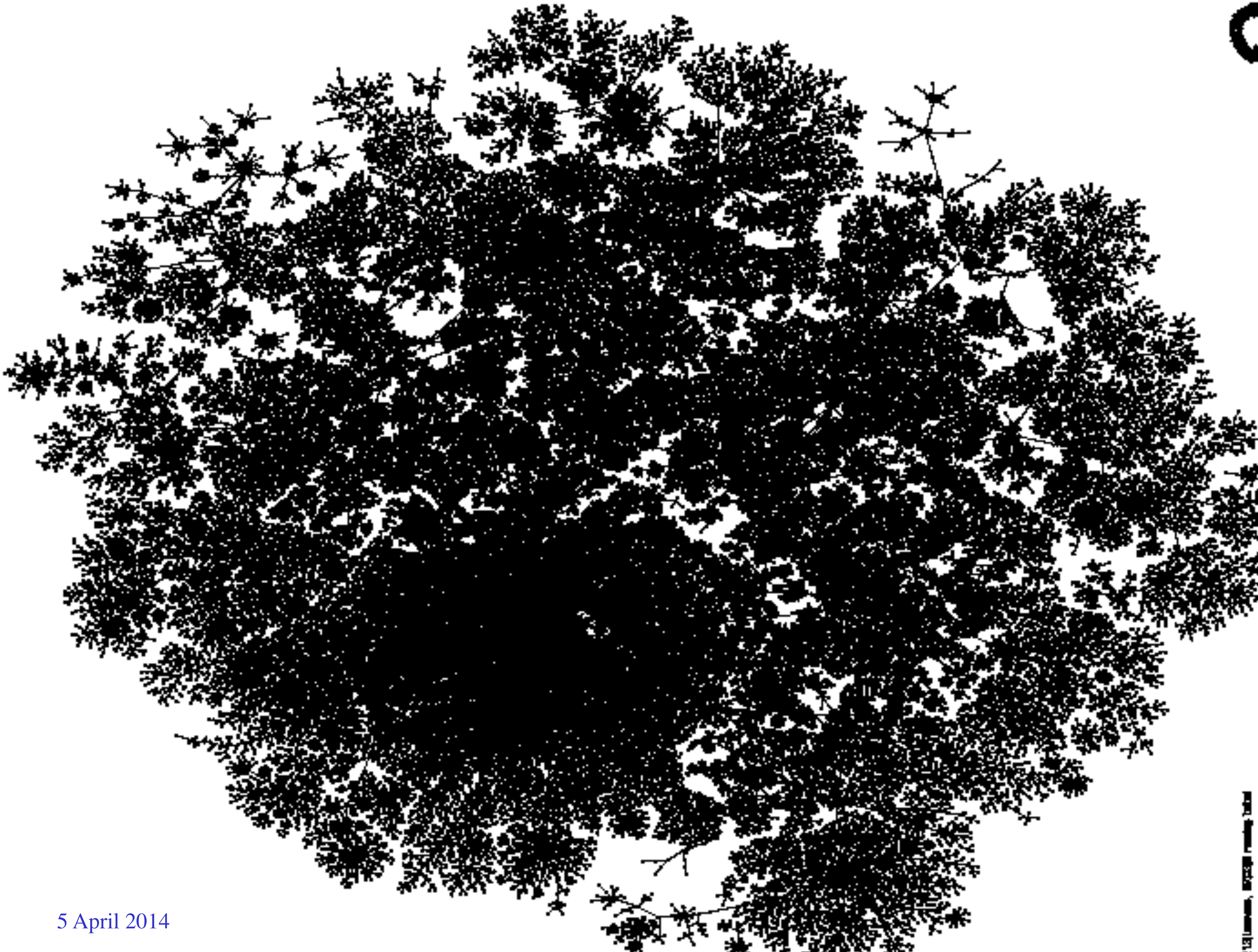


5 April 2014

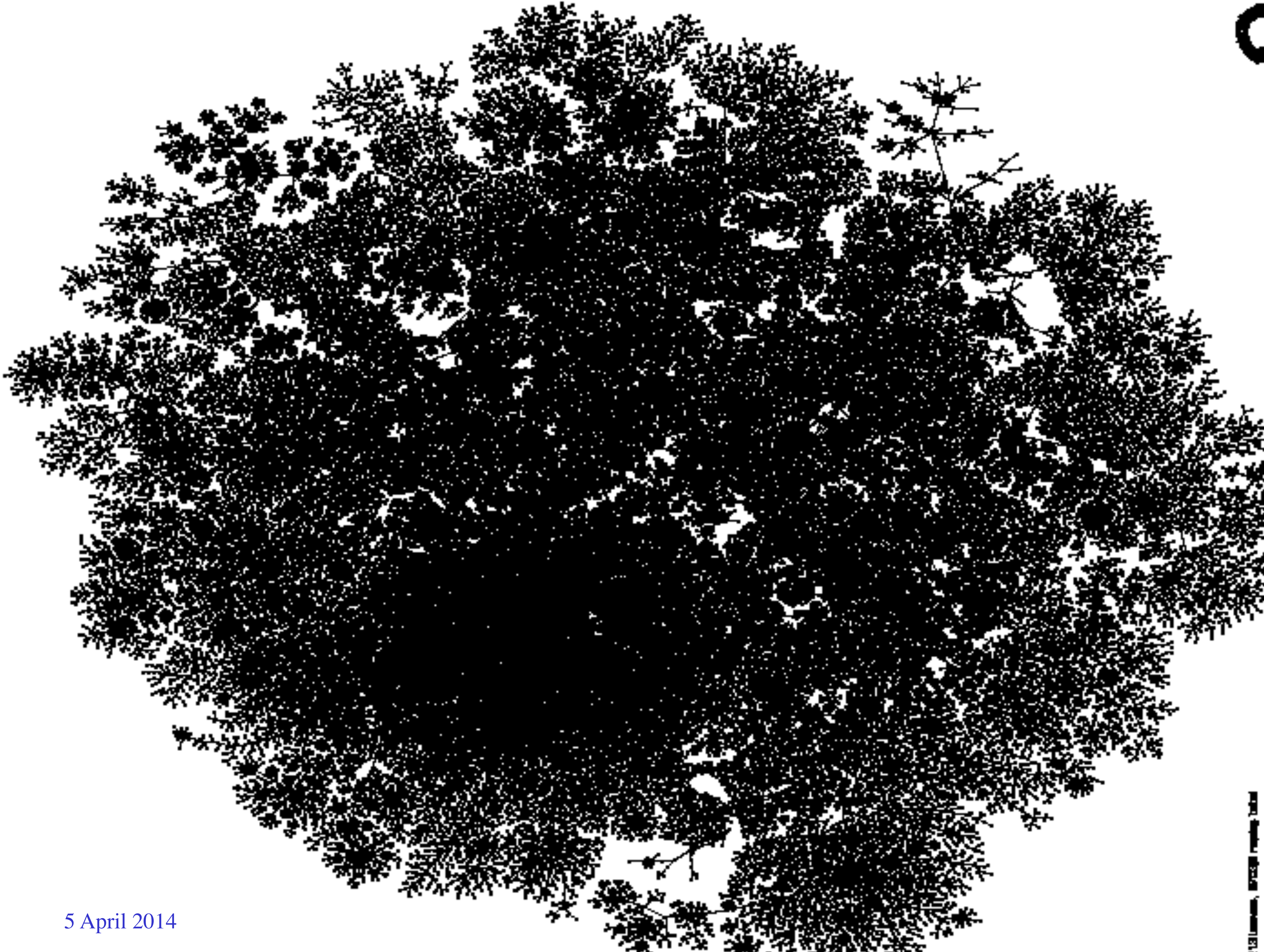


5 April 2014

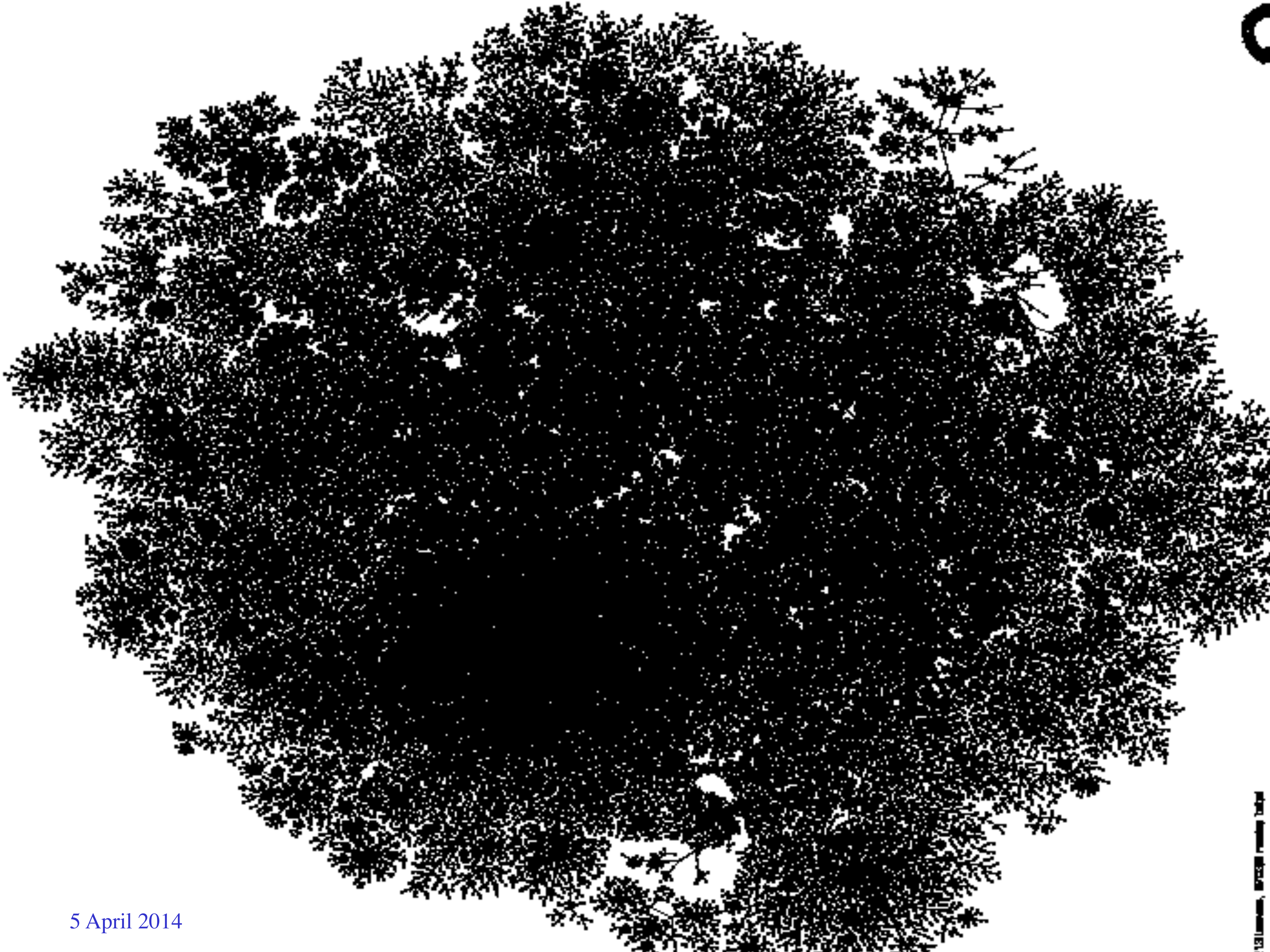
5 April 2014



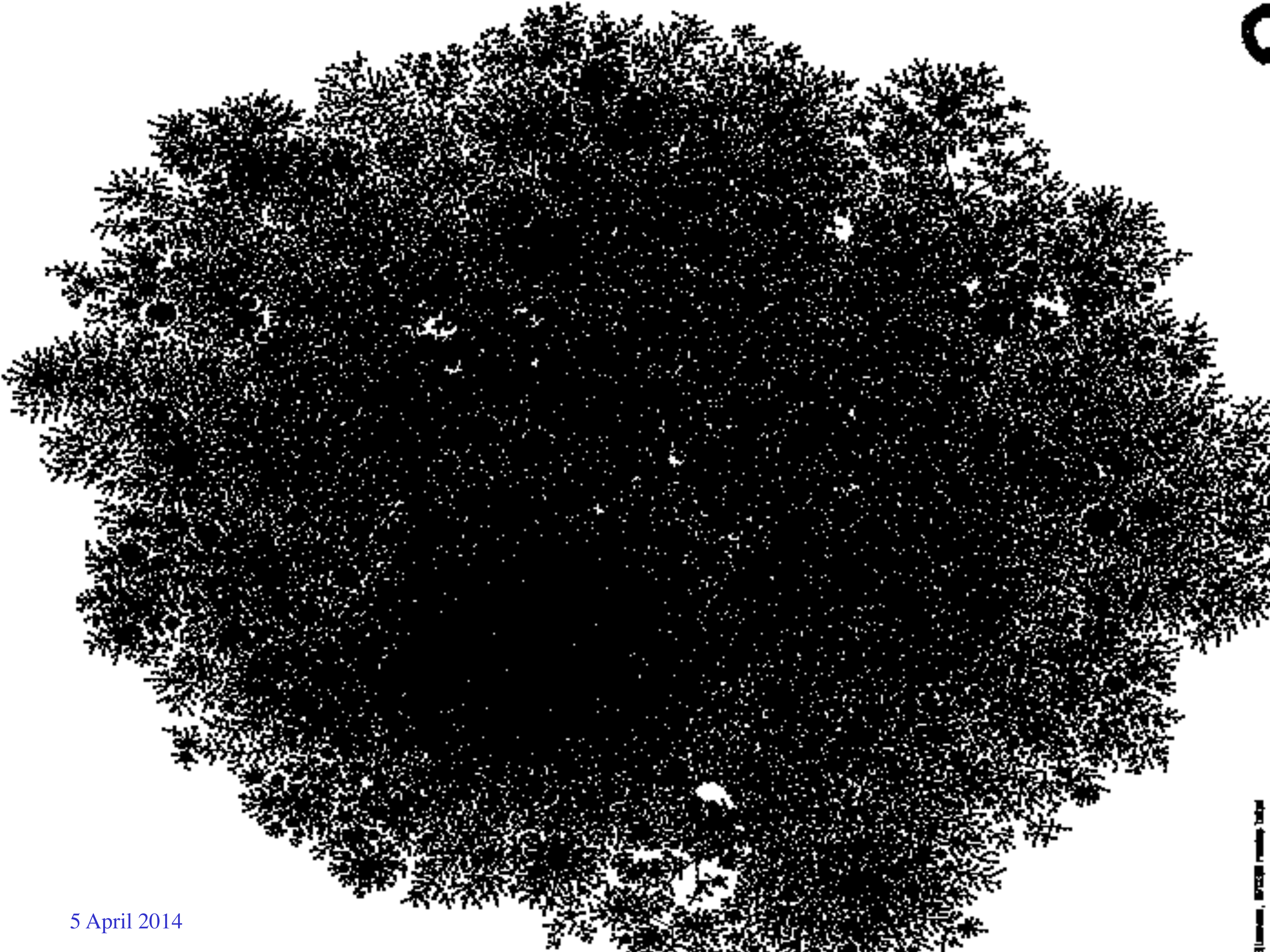
5 April 2014

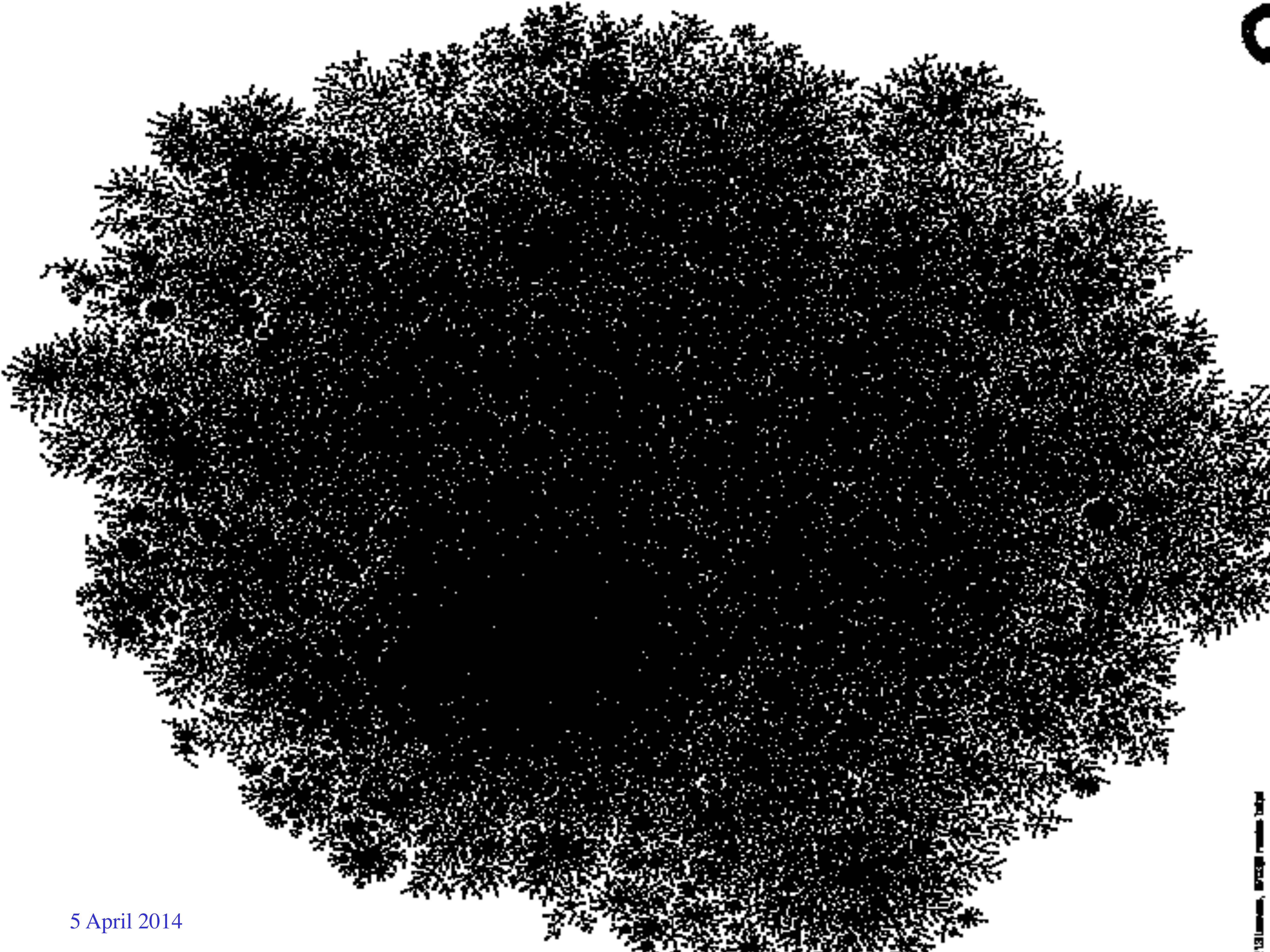


5 April 2014



5 April 2014

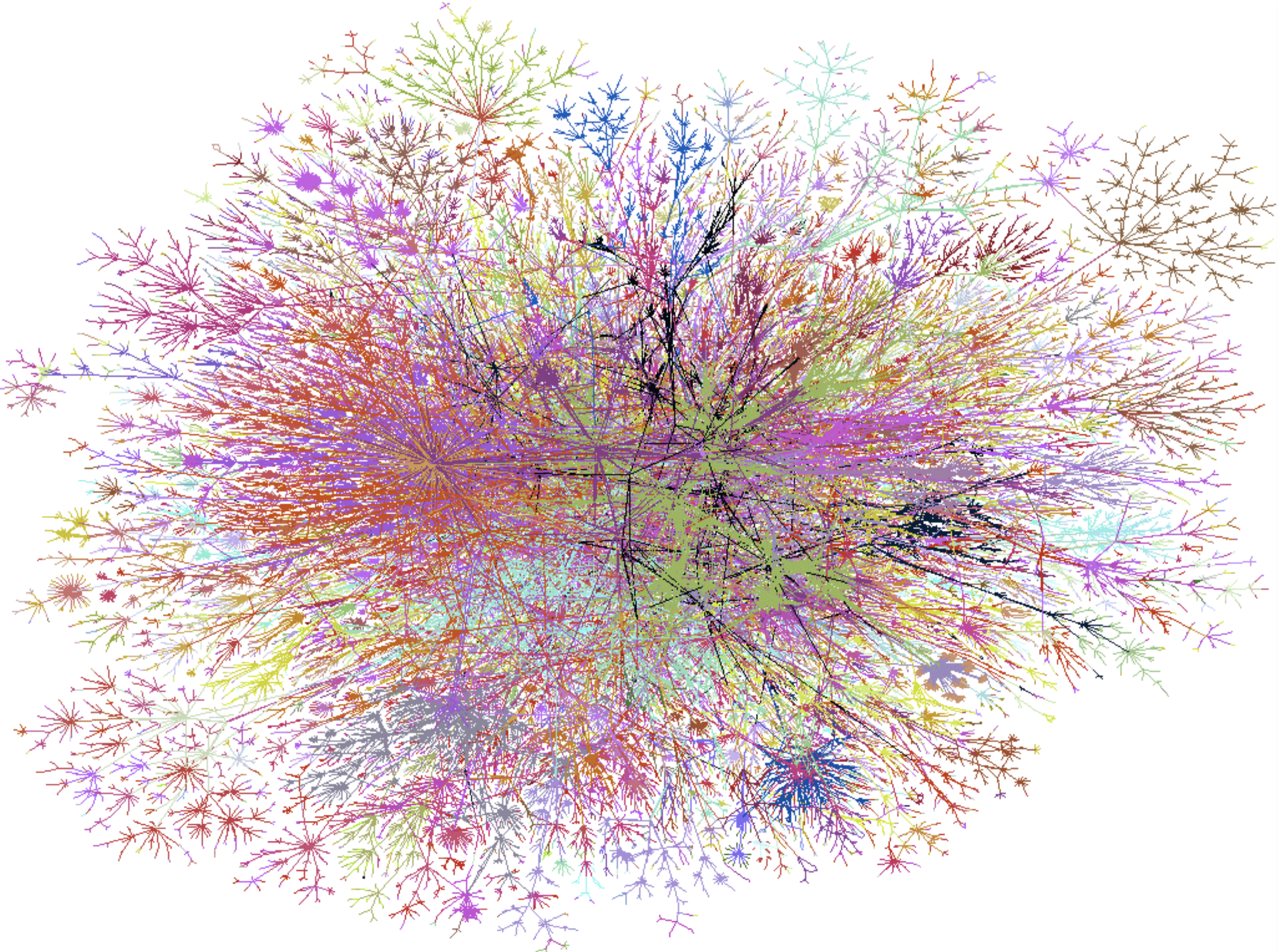




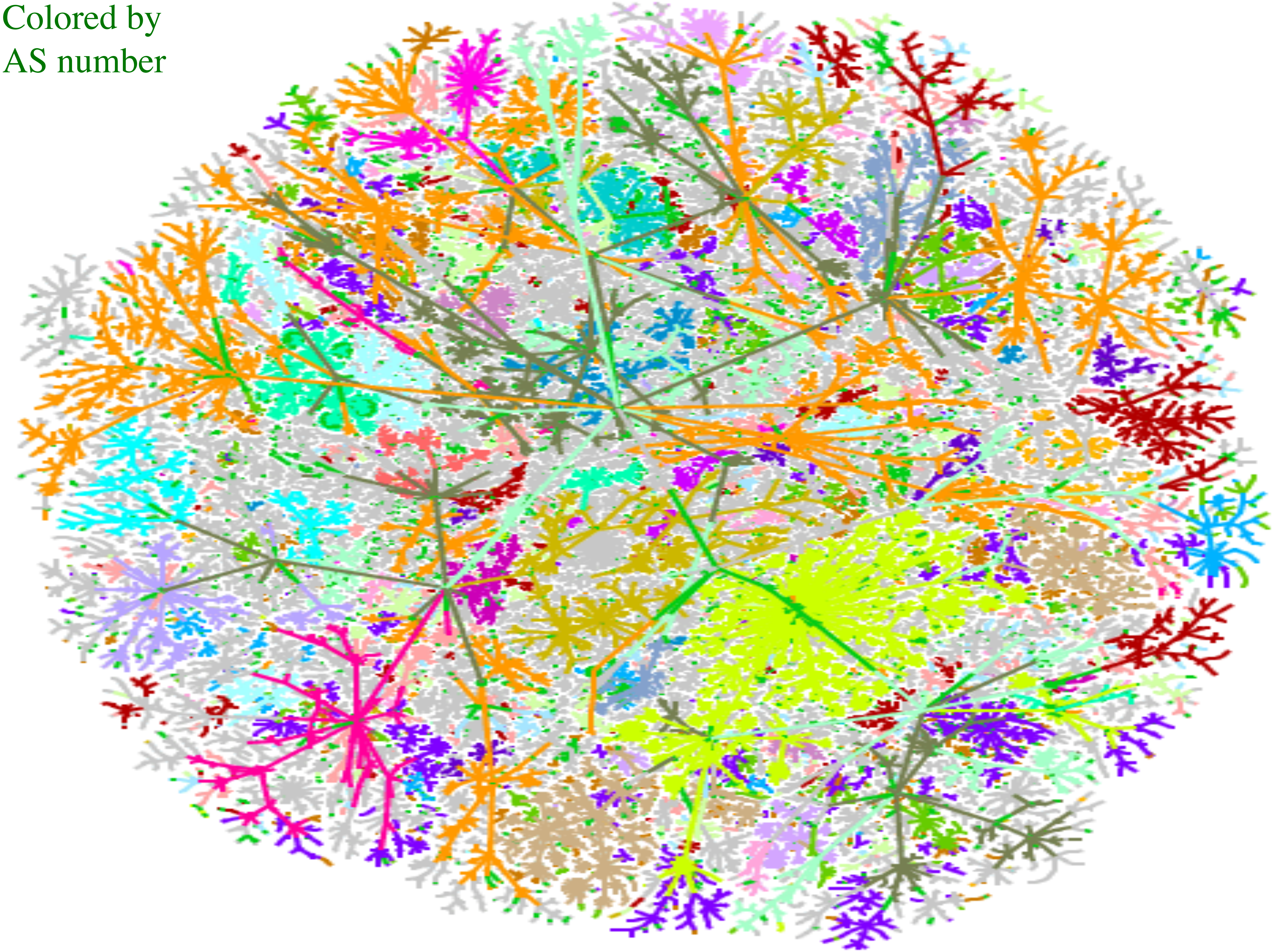
5 April 2014

Visualization of the layout algorithm

Laying out an intranet



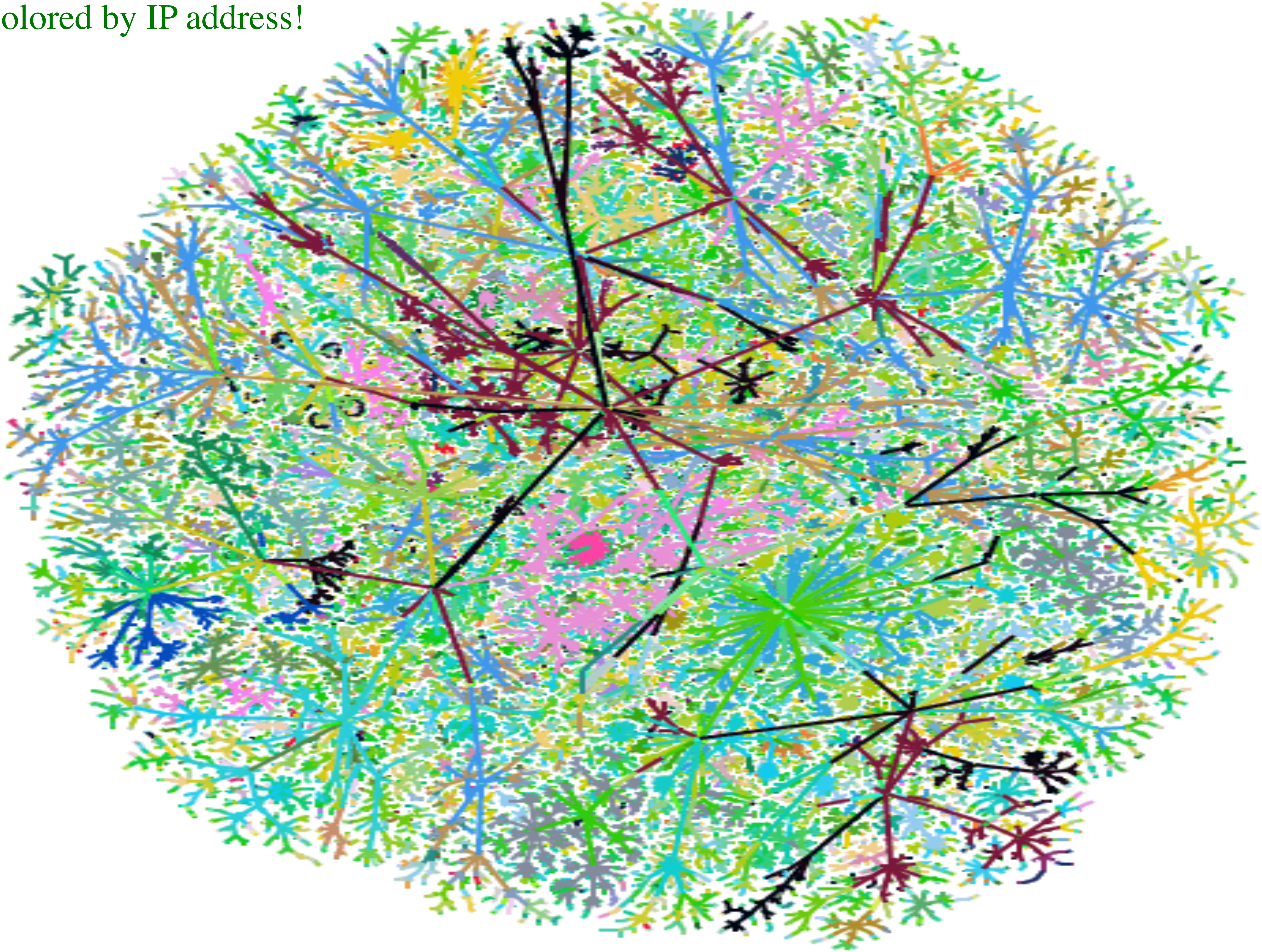
Colored by
AS number



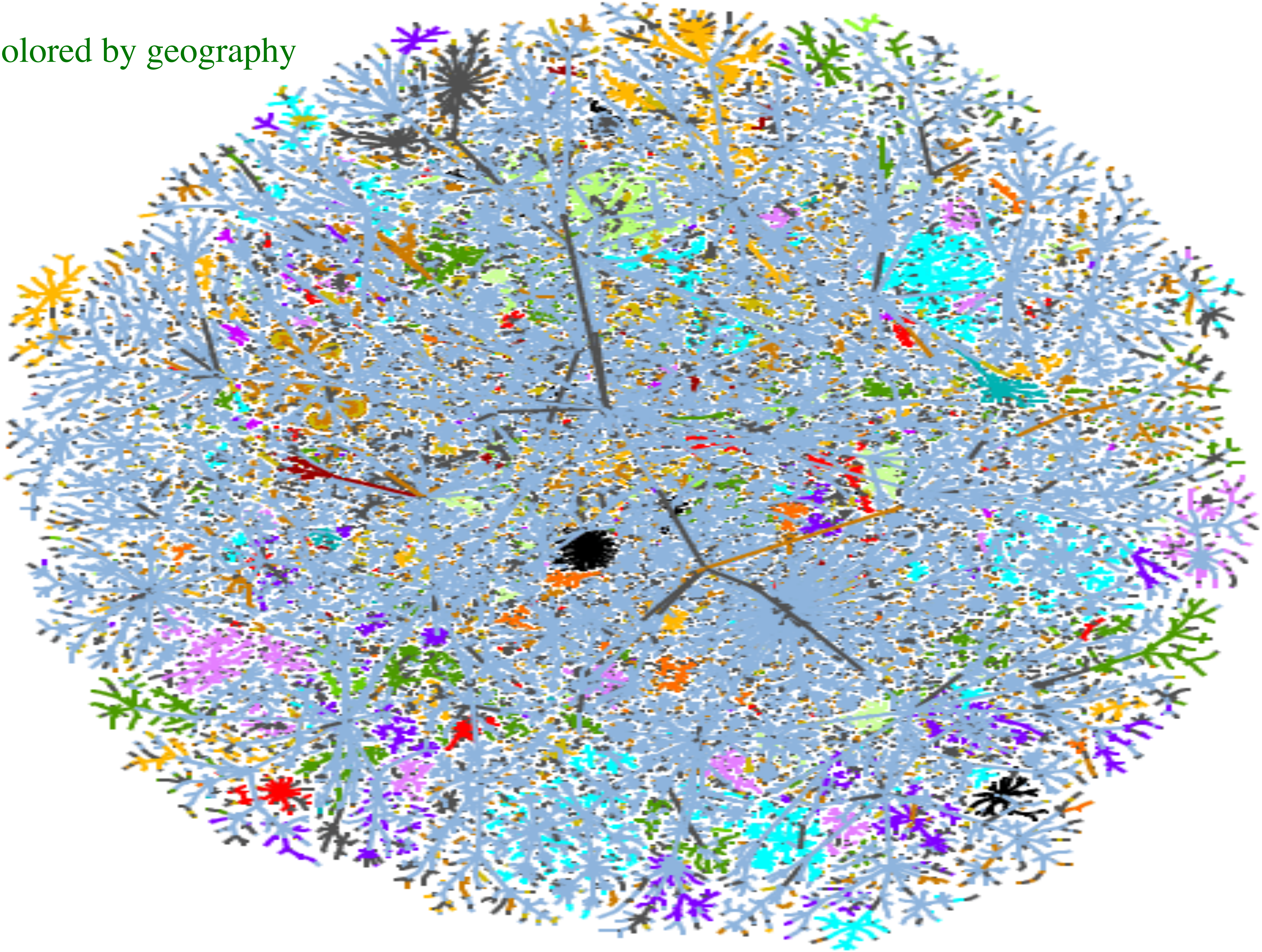
Map Coloring

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

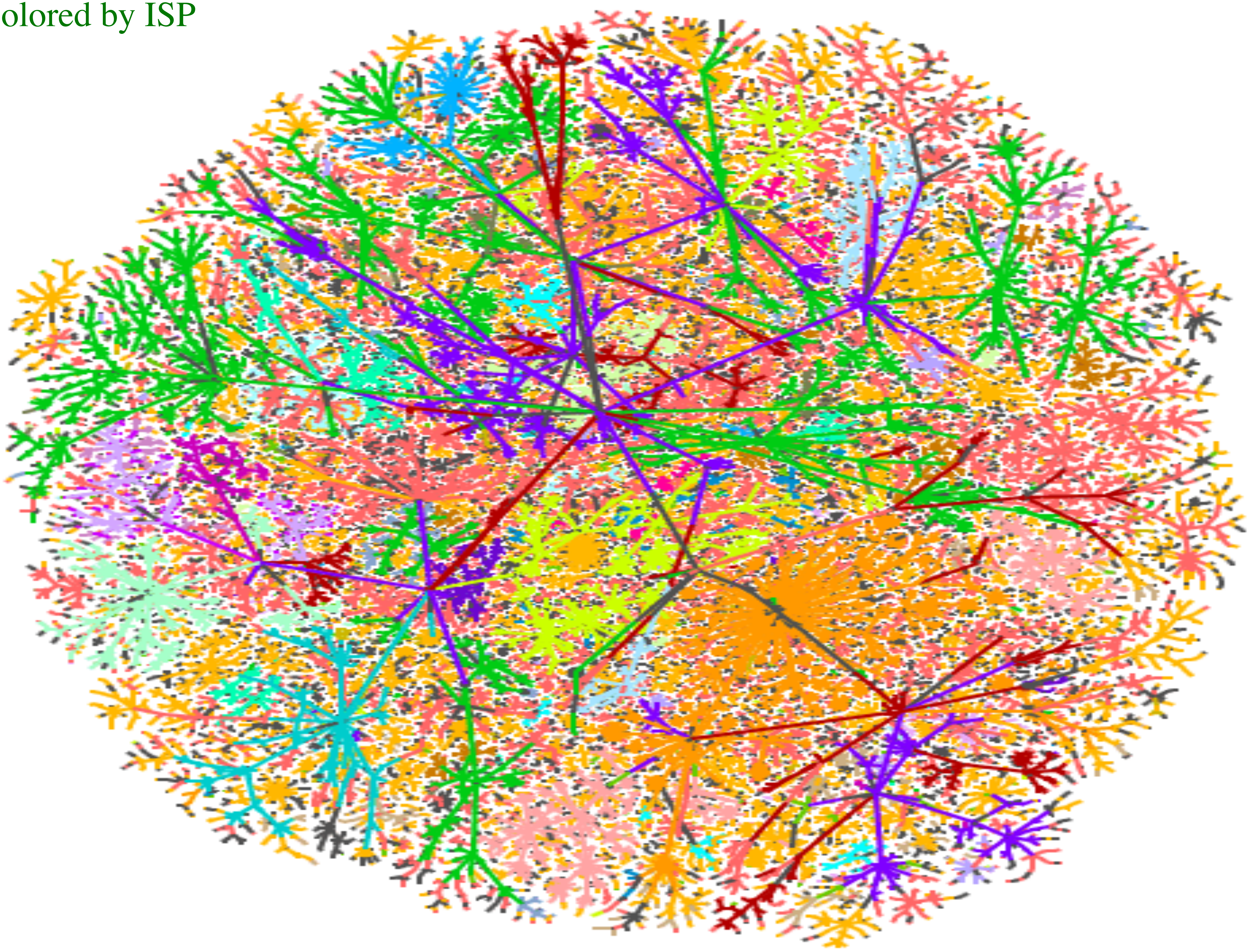
Colored by IP address!



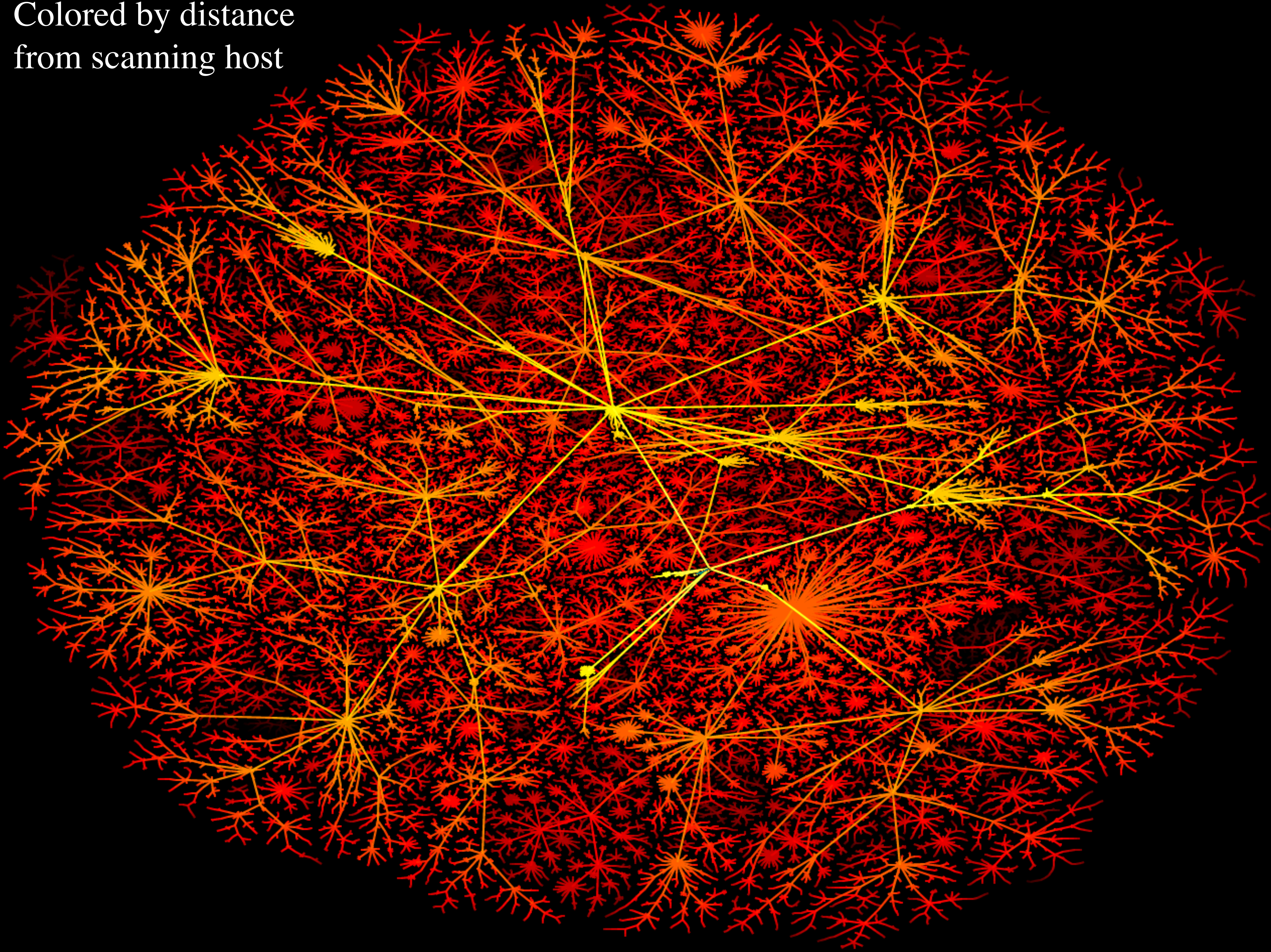
Colored by geography

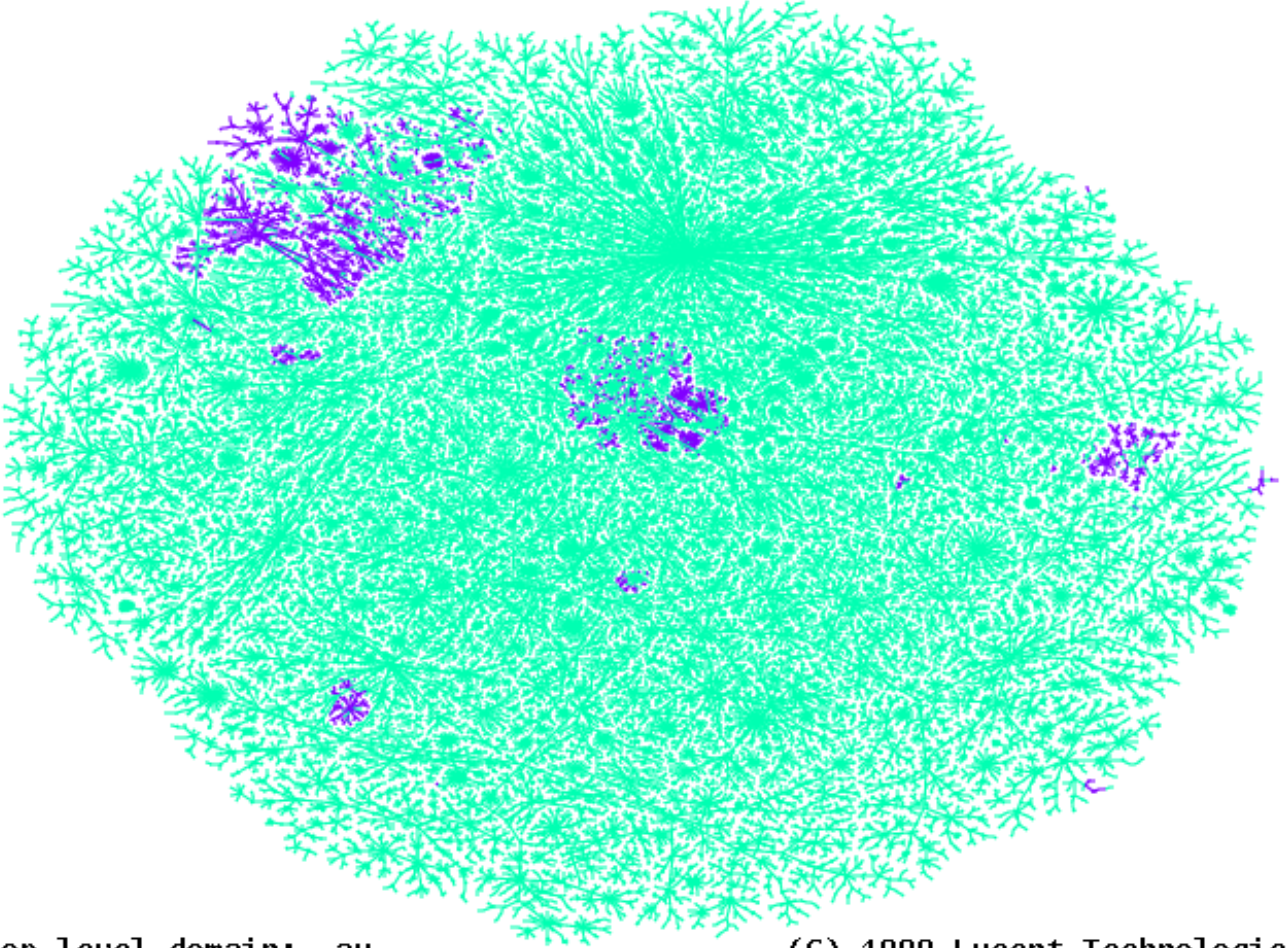


Colored by ISP

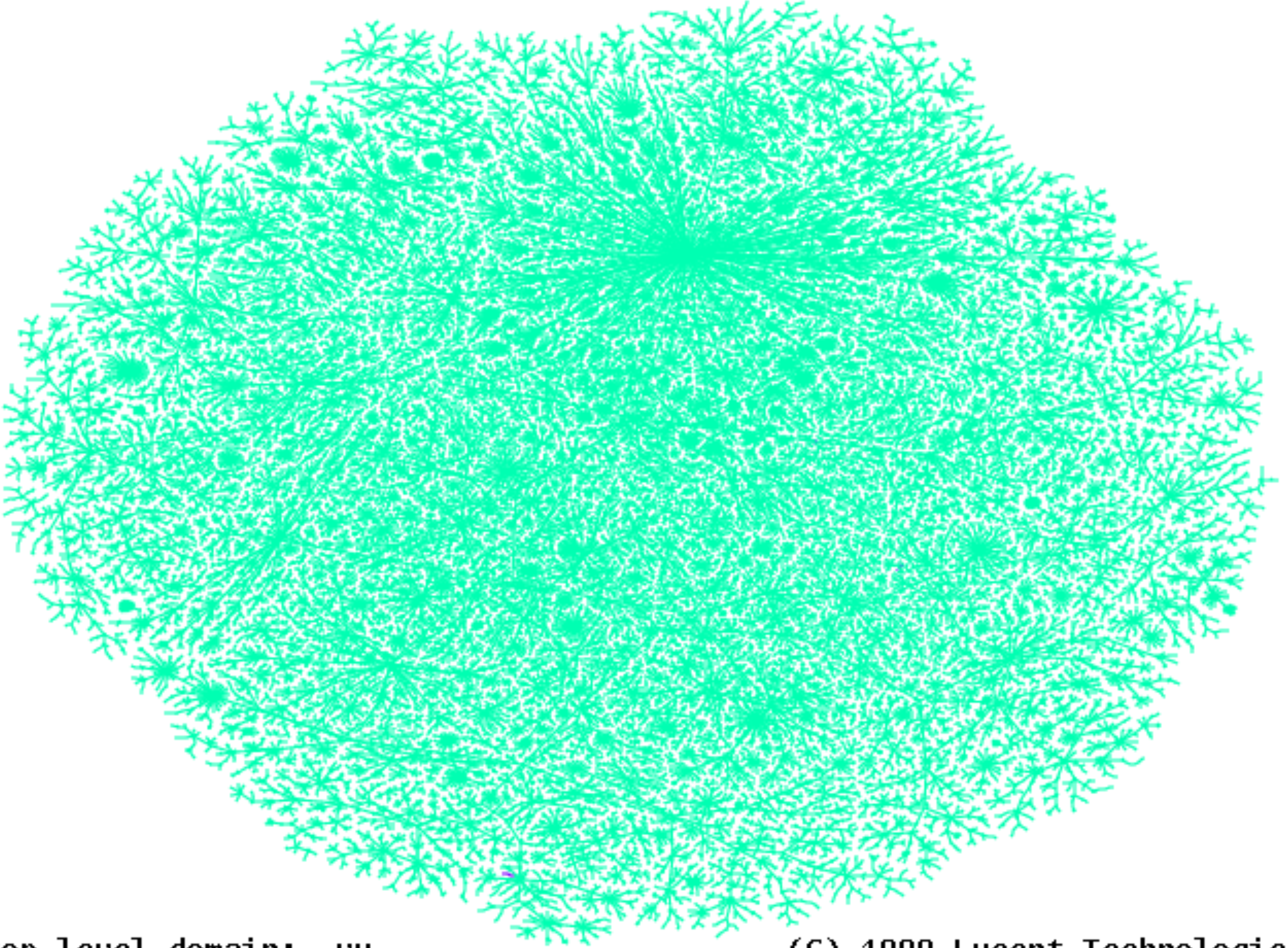


Colored by distance from scanning host





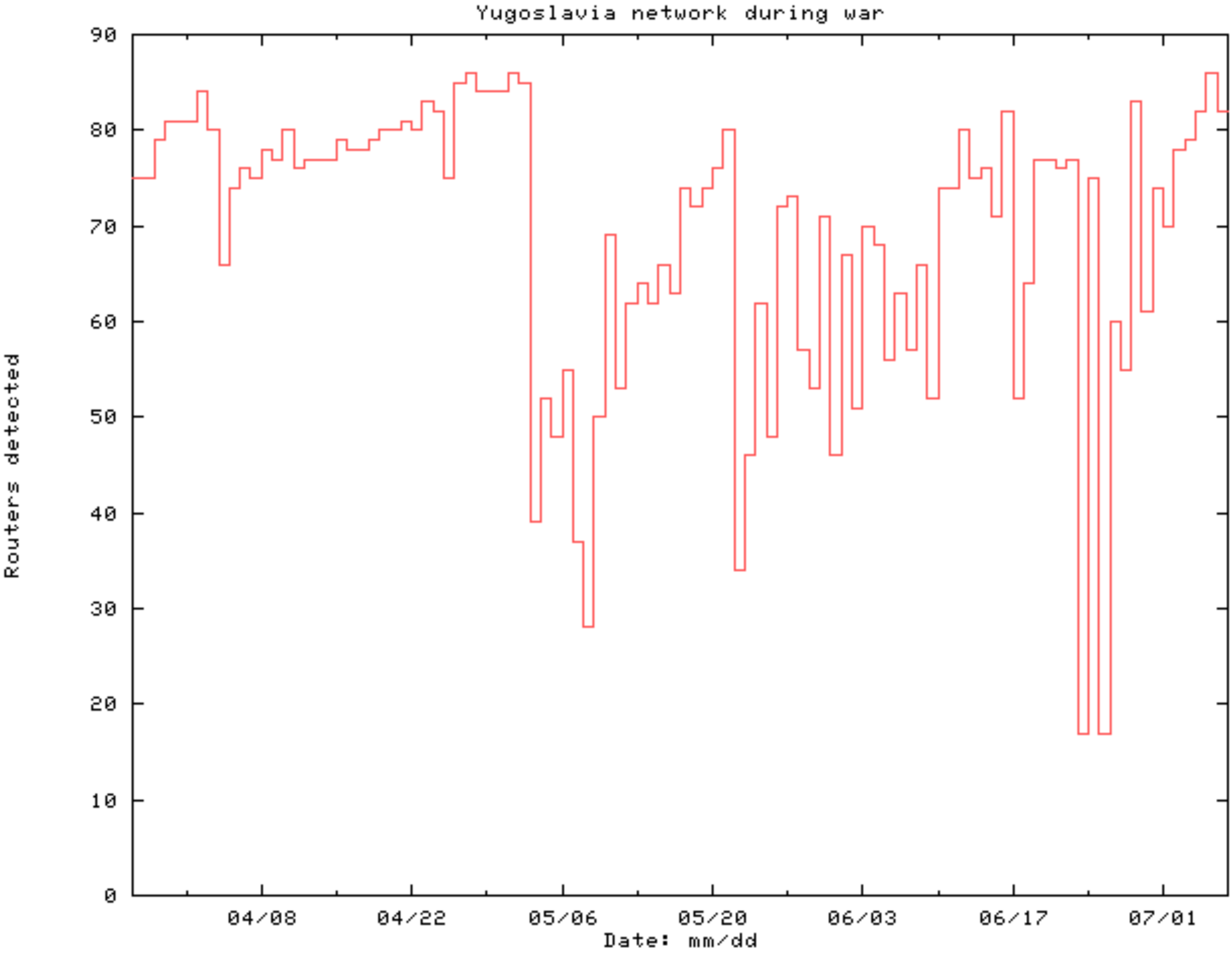
top level domain: .au

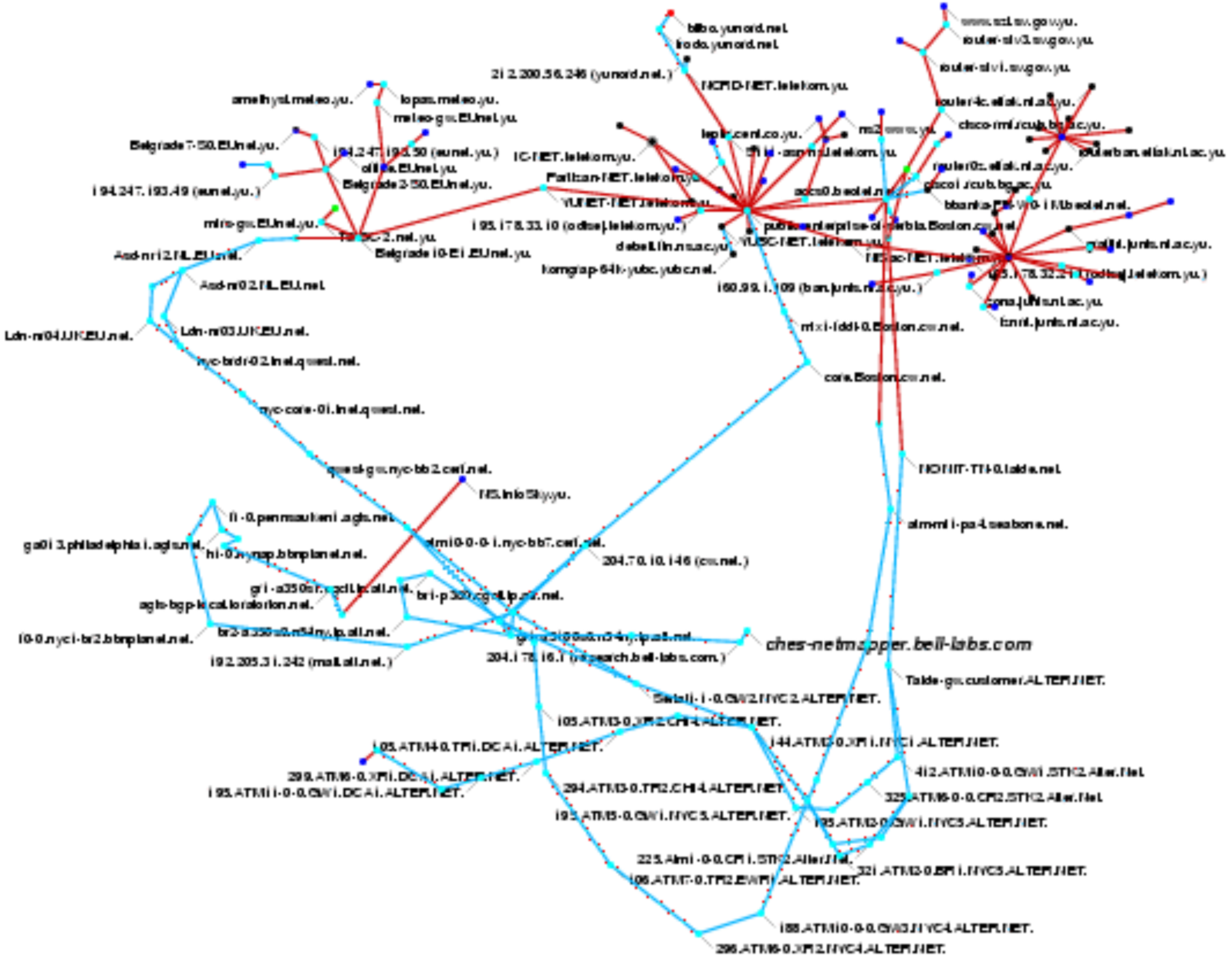


top level domain: .yu

Yugoslavia

An unclassified peek at a new battlefield

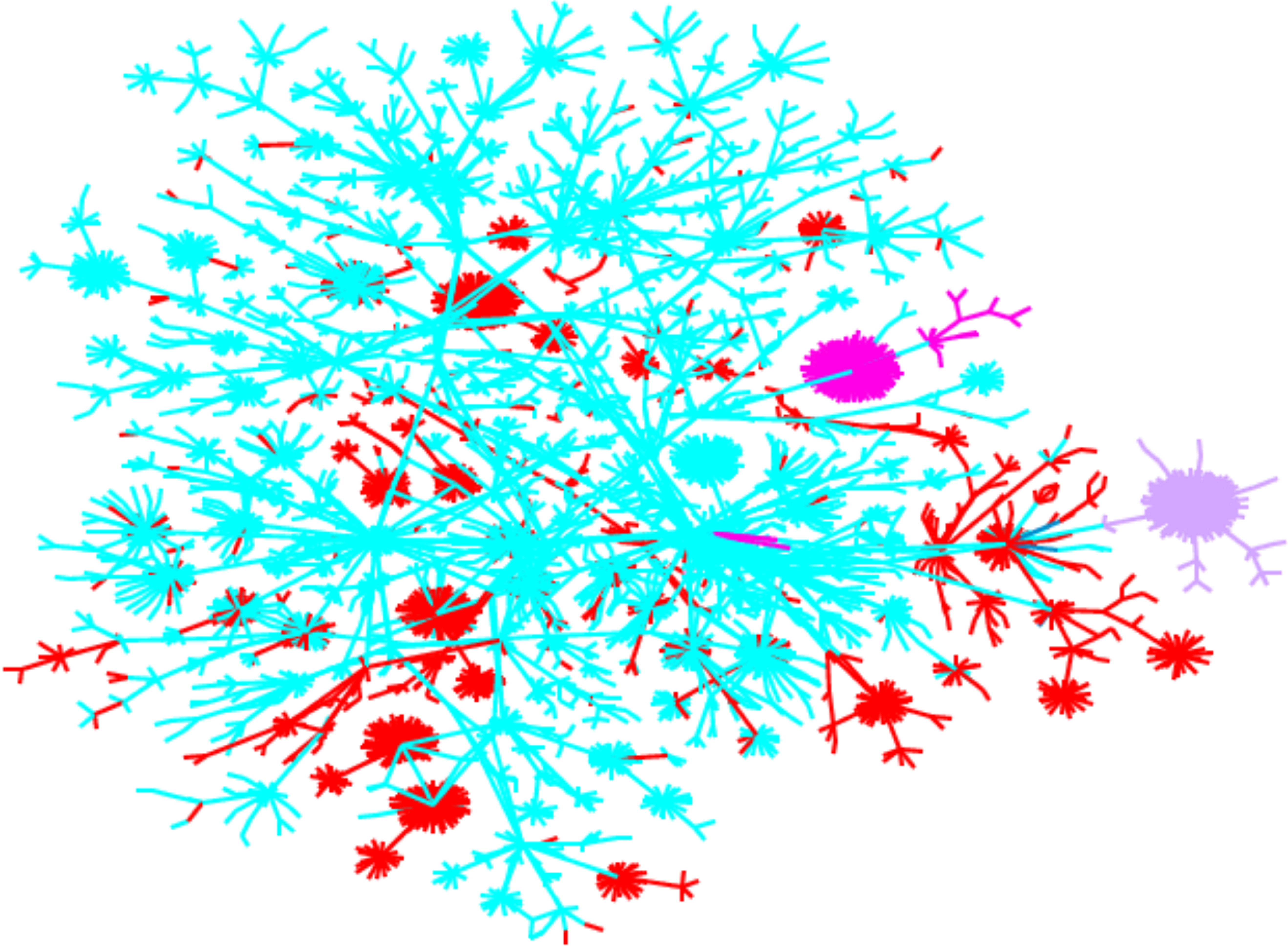

Yugoslavia network during war
Routers detected
0
10
20
30
40
50
60
70
80
90
04/08
04/22
05/06
05/20
06/03
06/17
07/01
Date: mm/dd


www.sci.sv.gov.yu.
bilbo.yunord.net.
router-siv3.sv.gov.yu.
frodo.yunord.net.
router-siv1.sv.gov.yu.
212.200.56.246 (yunord.net.)
NORD-NET.telekom.yu.
amethyst.meteo.yu.
topaz.meteo.yu.
router4c.elfak.ni.ac.yu.
meteo-gw.EUnet.yu.
cisco-rml.rcub.bg.ac.yu.
lepik.cent.co.yu.
ns2.www.yu.
Belgrade7-S0.EUnet.yu.
194.247.193.50 (eunet.yu.)
5111-asm1.telekom.yu.
routerban.elfak.ni.ac.yu.
IC-NET.telekom.yu.
office.EUnet.yu.
router0c.elfak.ni.ac.yu.
Partizan-NET.telekom.yu.
Belgrade2-S0.EUnet.yu.
cisco1.rcub.bg.ac.yu.
194.247.193.49 (eunet.yu.)
accs0.beotel.net.
YUNET-NET.telekom.yu.
bbanka-FE-W0-1M.beotel.net.
195.178.33.10 (odisej.telekom.yu.)
miro-gw.EUnet.yu.
public-enterprise-of-serbia.Boston.cw.net.
TelSC-2.net.yu.
YUBC-NET.telekom.yu.
debeli.fin.ns.ac.yu.
mail1.junis.ni.ac.yu.
Asd-nr12.NL.EU.net.
Belgrade10-E1.EUnet.yu.
NIS-ac-NET.telekom.yu.
komgrap-64k-yubc.yubc.net.
195.178.32.211 (odisej.telekom.yu.)
Asd-nr02.NL.EU.net
160.99.1.109 (ban.junis.ni.ac.yu.)
cone.junis.ni.ac.yu.
tcnrt.junis.ni.ac.yu.
mix1-fddi0.Boston.cw.net.
Ldn-nr03.UK.EU.net.
Ldn-nr04.UK.EU.net.
nyc-bdr-02.inet.qwest.net.
core.Boston.cw.net.
nyc-core-01.inet.qwest.net.
NONIT-TT-0.taide.net.
qwest-gw.nyc-bb2.cerf.net.
NS.InfoSky.yu.
f1-0.pennsauken1.agis.net.
atm-ml1-pa4.seabone.net.
ga013.philadelphia1.agis.net.
atm10-0-0-1.nyc-bb7.cerf.net.
hi-0.nynap.bbnplanet.net.
204.70.10.146 (cw.net.)
gr1-a3500s.cgcil.ip.att.net.
br1-p300.cgcil.ip.att.net.
agis-bgp-local.loralorion.net.
br2-a3500s0.n54ny.ip.att.net.
f0-0.nyc1-br2.bbnplanet.net.
gr1-a3500s0.n54ny.ip.att.net.
ches-netmapper.bell-labs.com
204.178.16.1 (research.bell-labs.com.)
192.205.31.242 (mail.att.net.)
Taide-gw.customer.ALTER.NET.
Serial1-1-0.GW2.NYC2.ALTER.NET.
105.ATM3-0.XR2.CHI4.ALTER.NET.
144.ATM3-0.XR1.NYC1.ALTER.NET.
105.ATM4-0.TR1.DCA1.ALTER.NET.
412.ATM10-0-0.GW1.STK2.Alter.Net
299.ATM6-0.XR1.DCA1.ALTER.NET.
294.ATM3-0.TR2.CHI4.ALTER.NET.
195.ATM11-0-0.GW1.DCA1.ALTER.NET.
325.ATM6-0-0.CR2.STK2.Alter.Net
195.ATM5-0.GW1.NYC5.ALTER.NET.
195.ATM2-0.GW1.NYC5.ALTER.NET.
225.Atm1-0-0.CR1.STK2.Alter.Net
321.ATM2-0.BR1.NYC5.ALTER.NET.
106.ATM7-0.TR2.EWR1.ALTER.NET.
188.ATM10-0-0.GW3.NYC4.ALTER.NET.
296.ATM6-0.XR2.NYC4.ALTER.NET.

03/26/1999

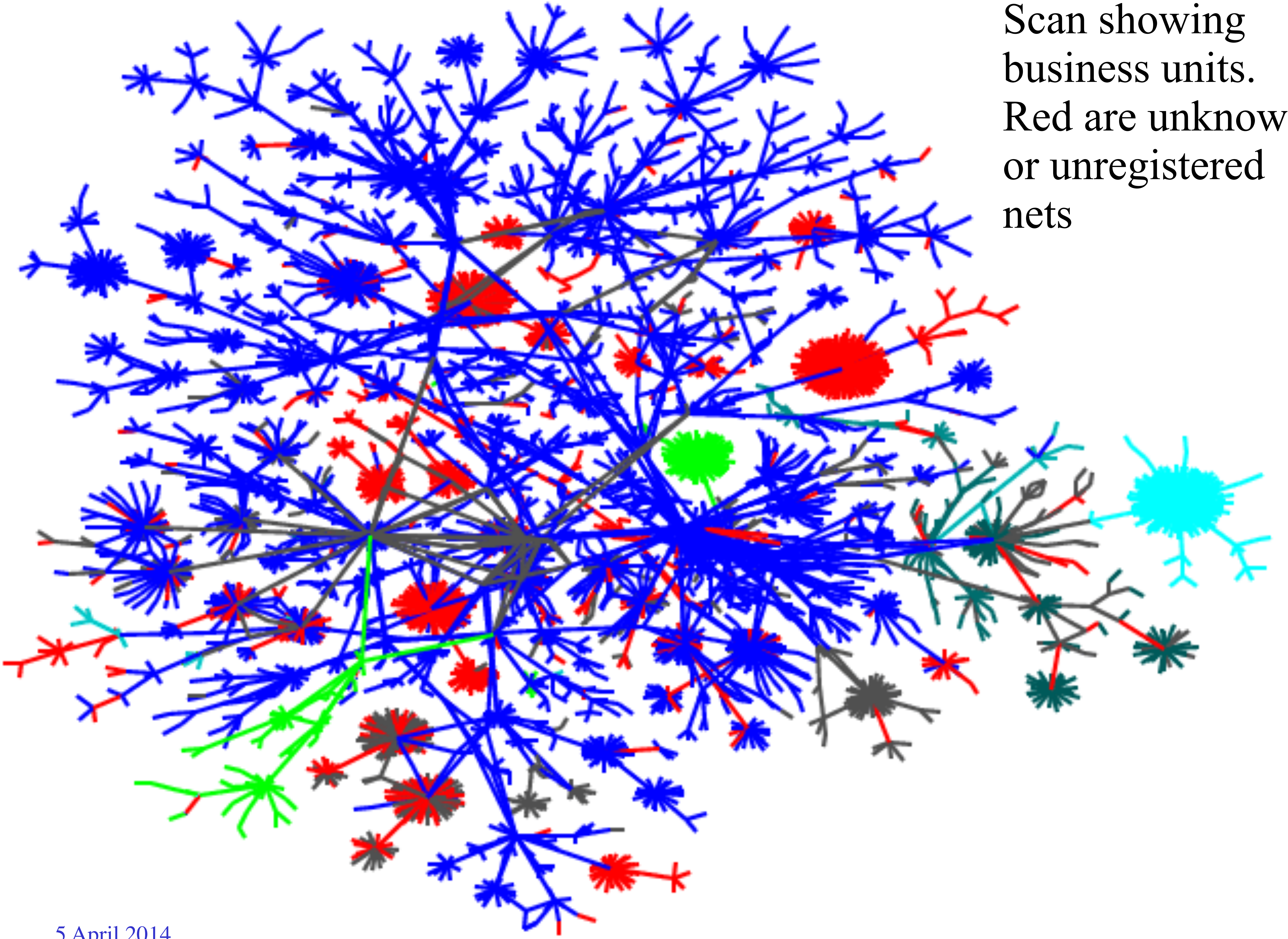
Lumeta: mapping intranets for fun and profit

Founded October 2000

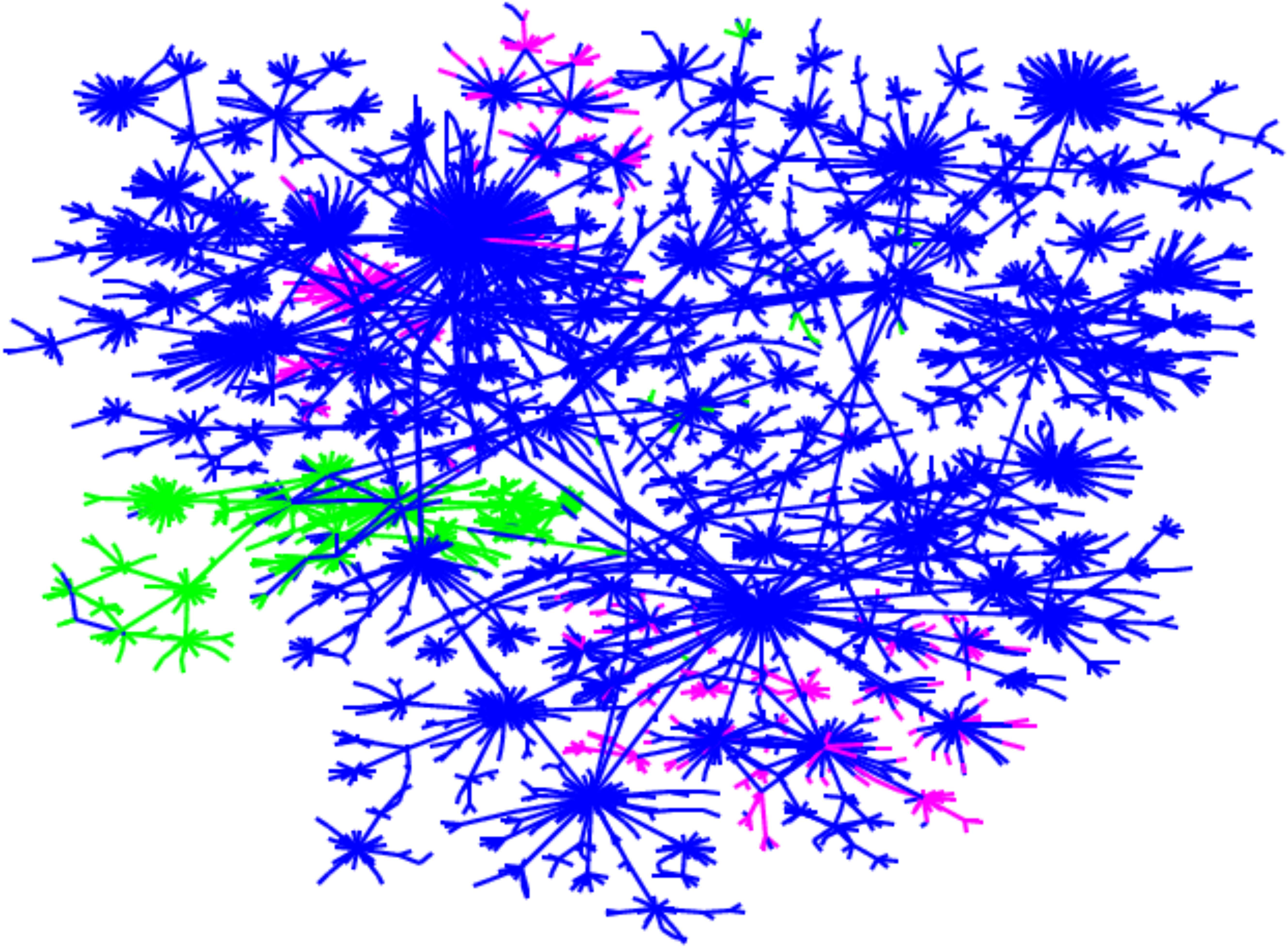


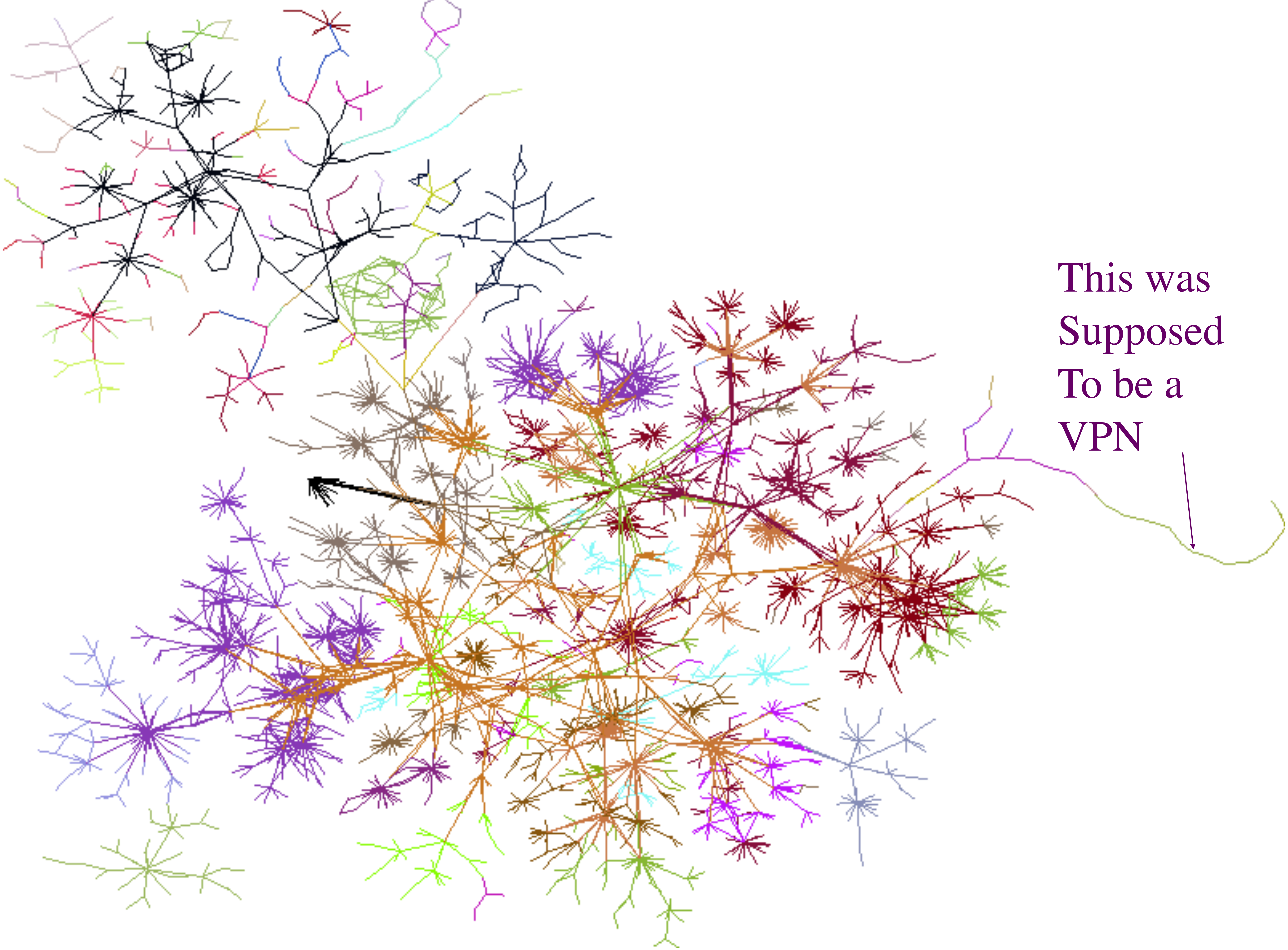
Lucent’s intranet

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

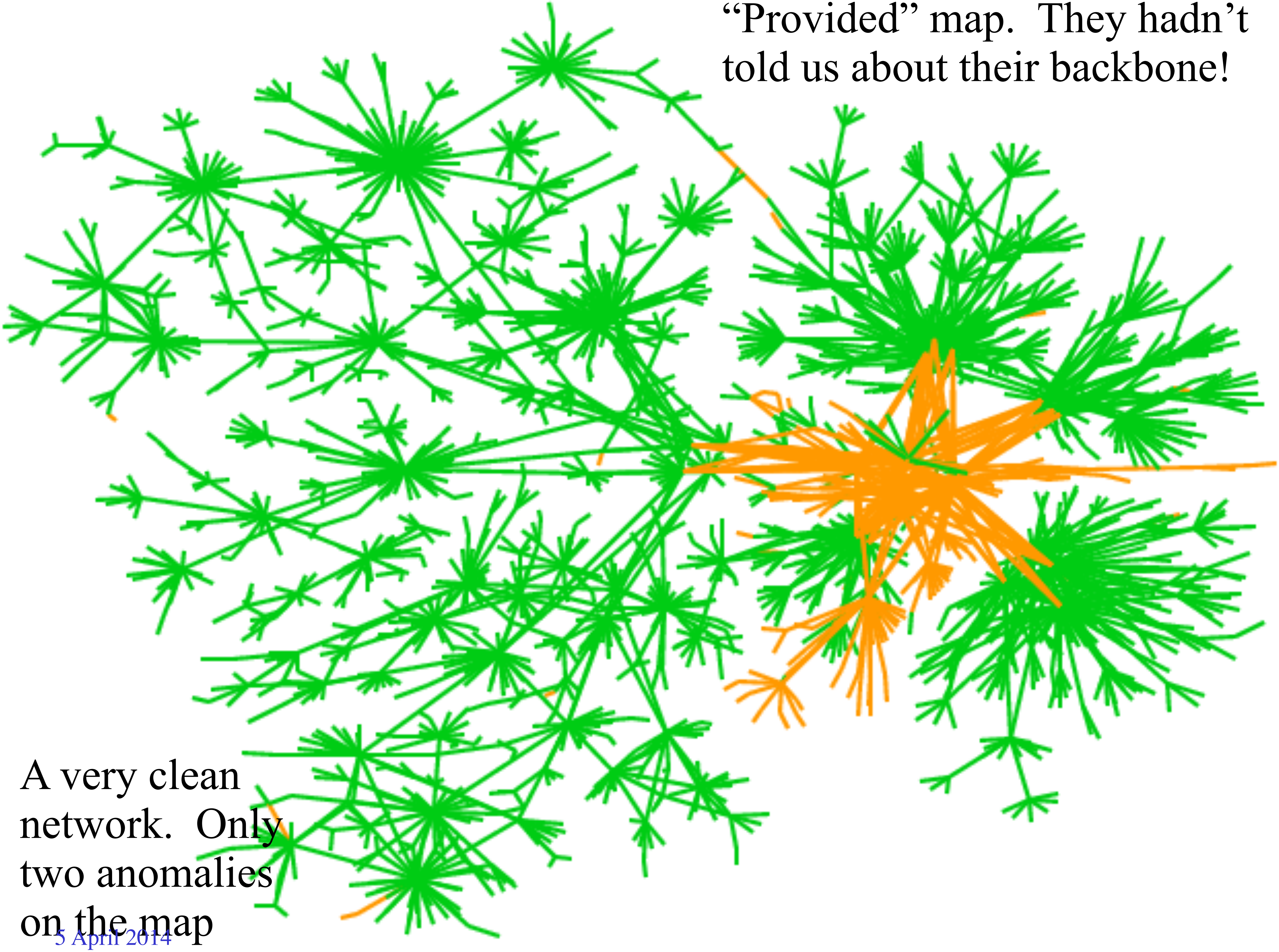


Scan showing business units. Red are unknown or unregistered nets



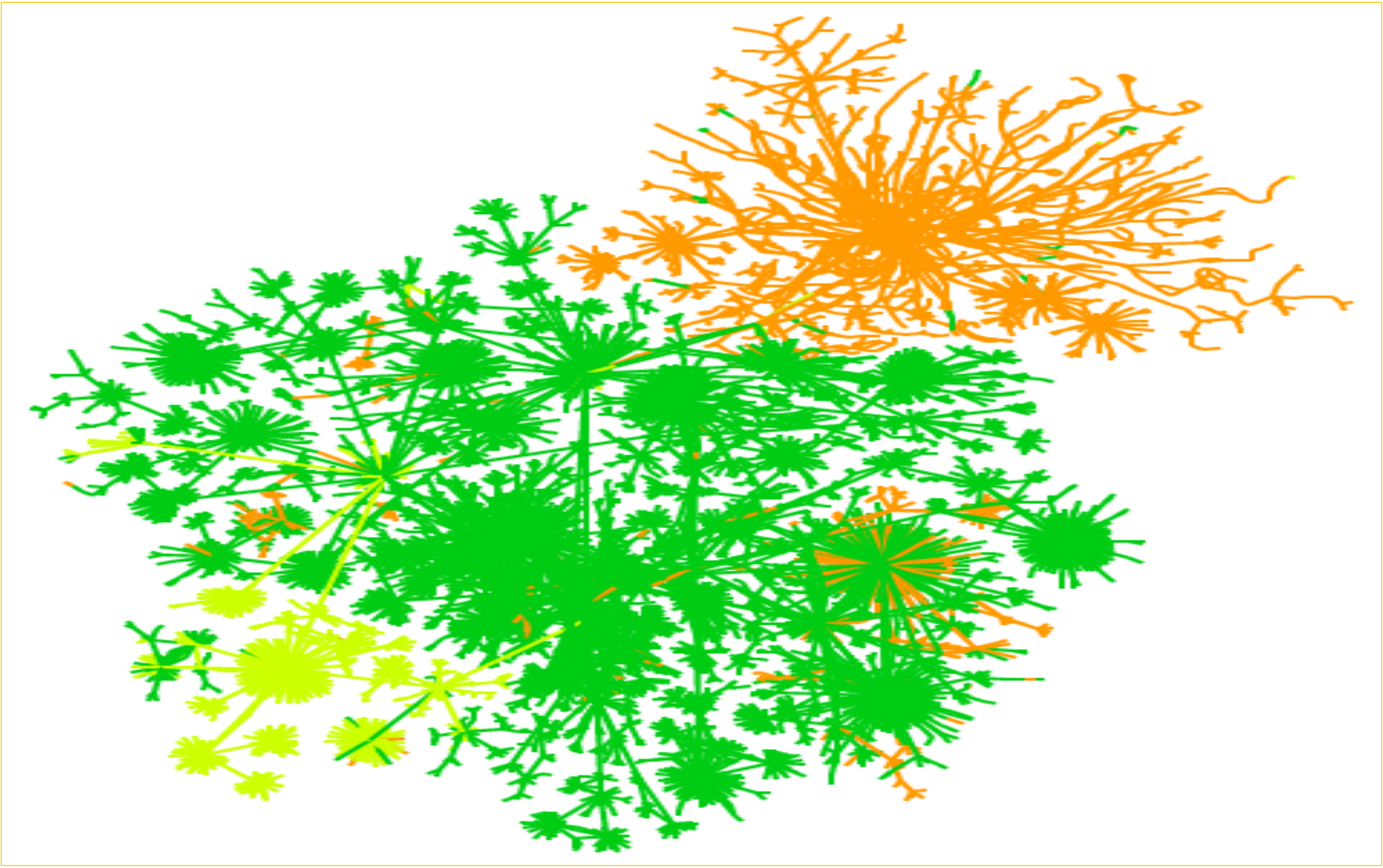


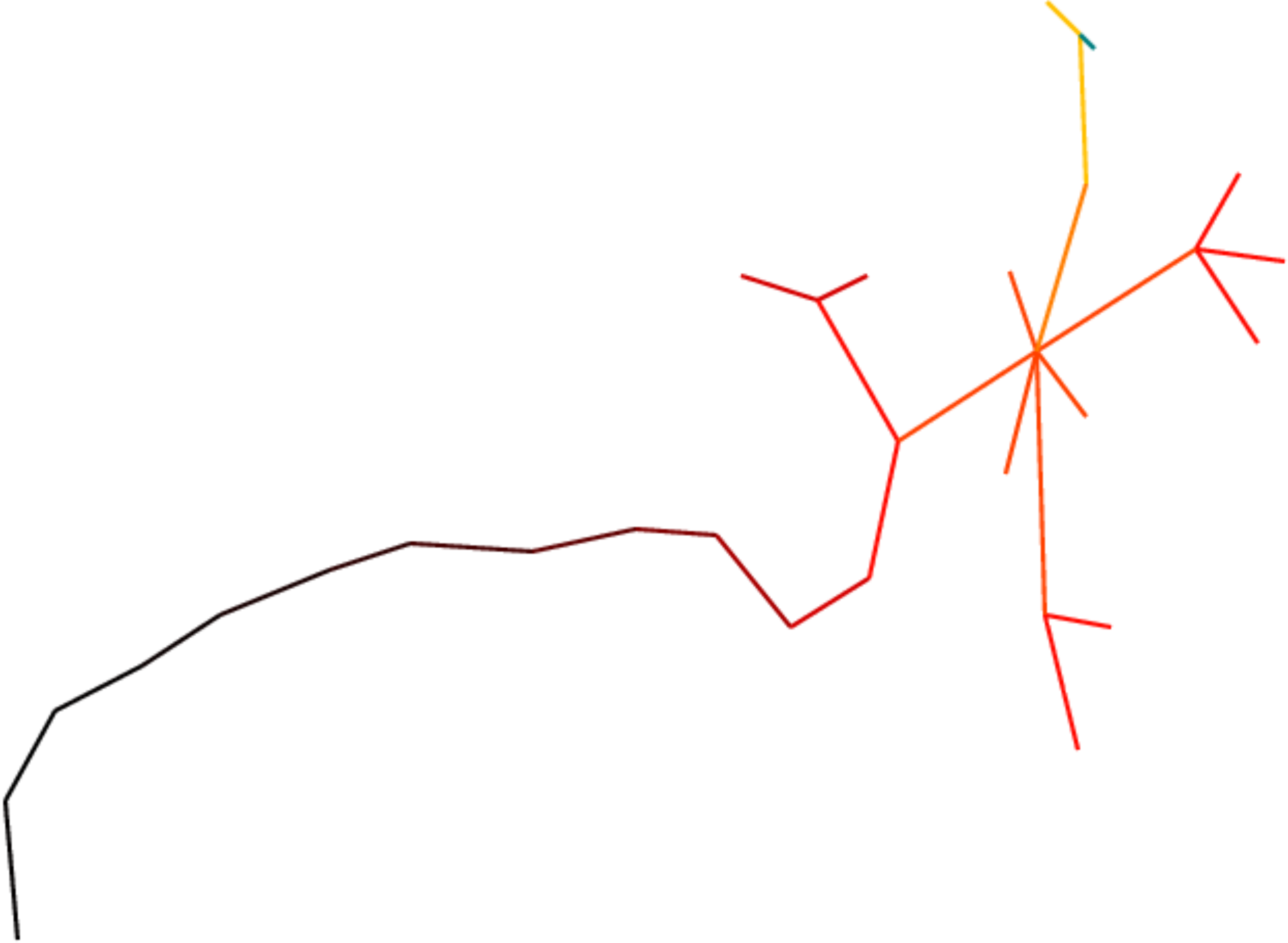
This was Supposed To be a VPN

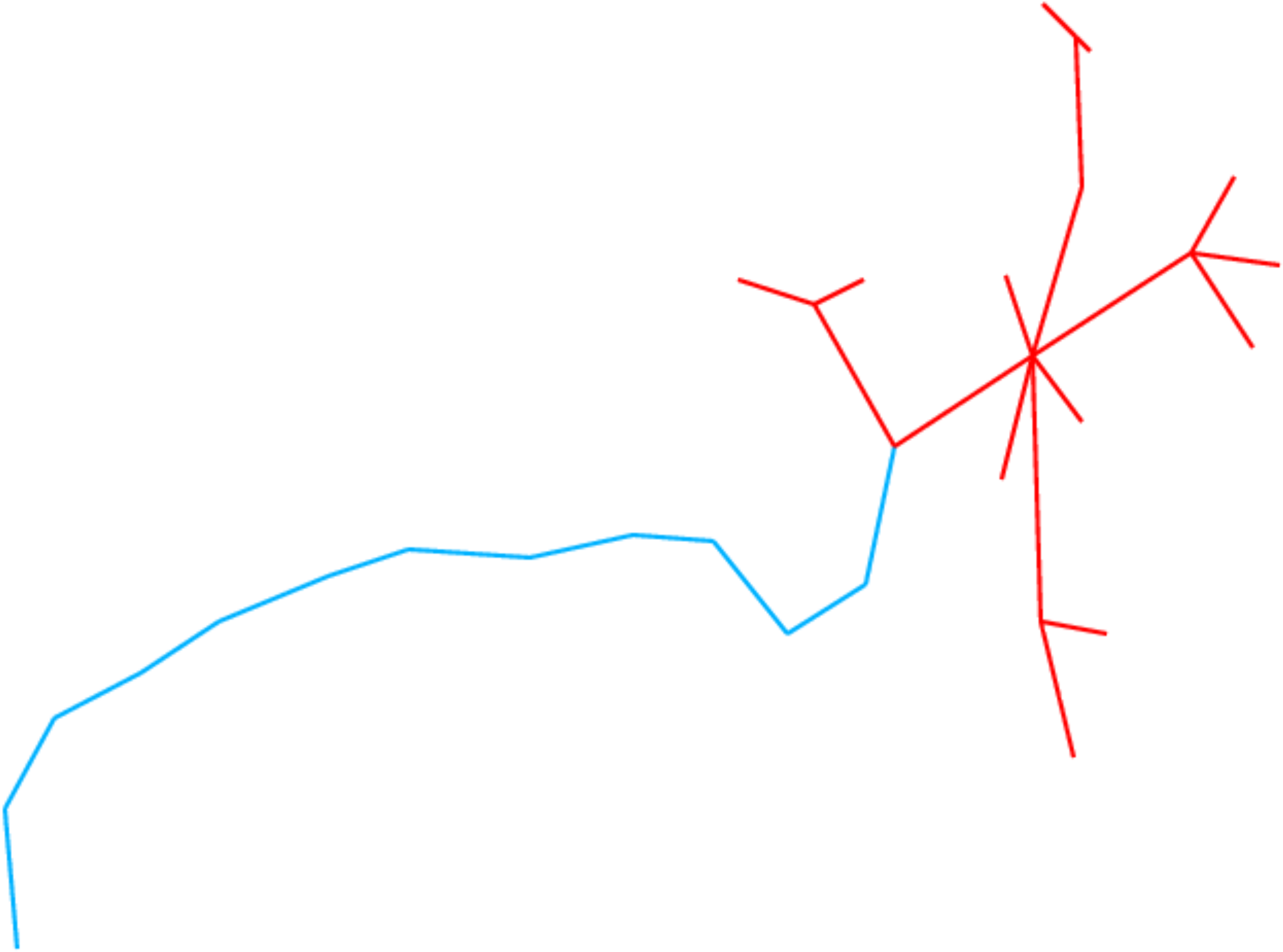


“Provided” map. They hadn’t told us about their backbone!

A very clean network. Only two anomalies on the map

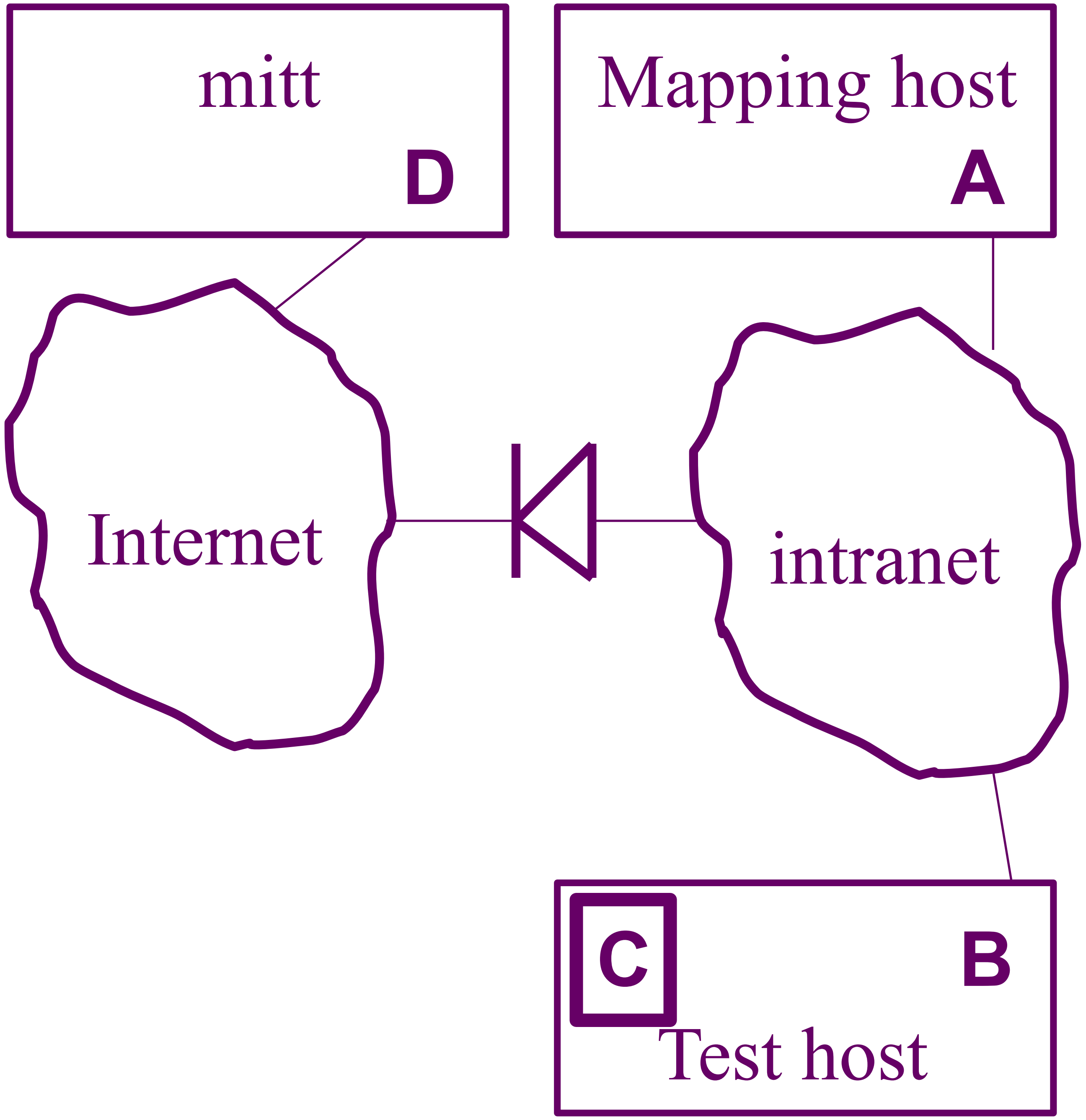






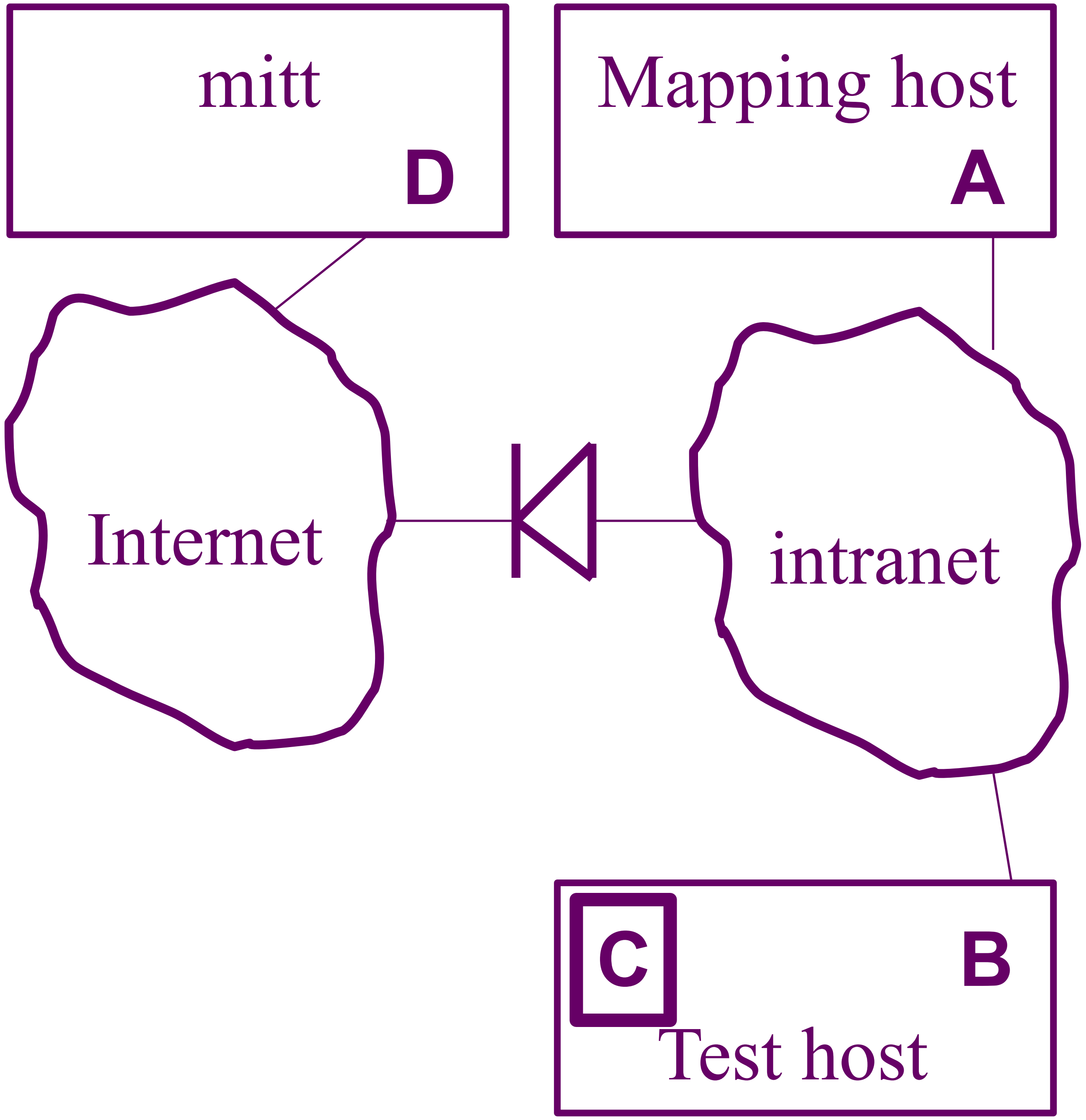
Also, “leak detection”

Leak Detection Layout



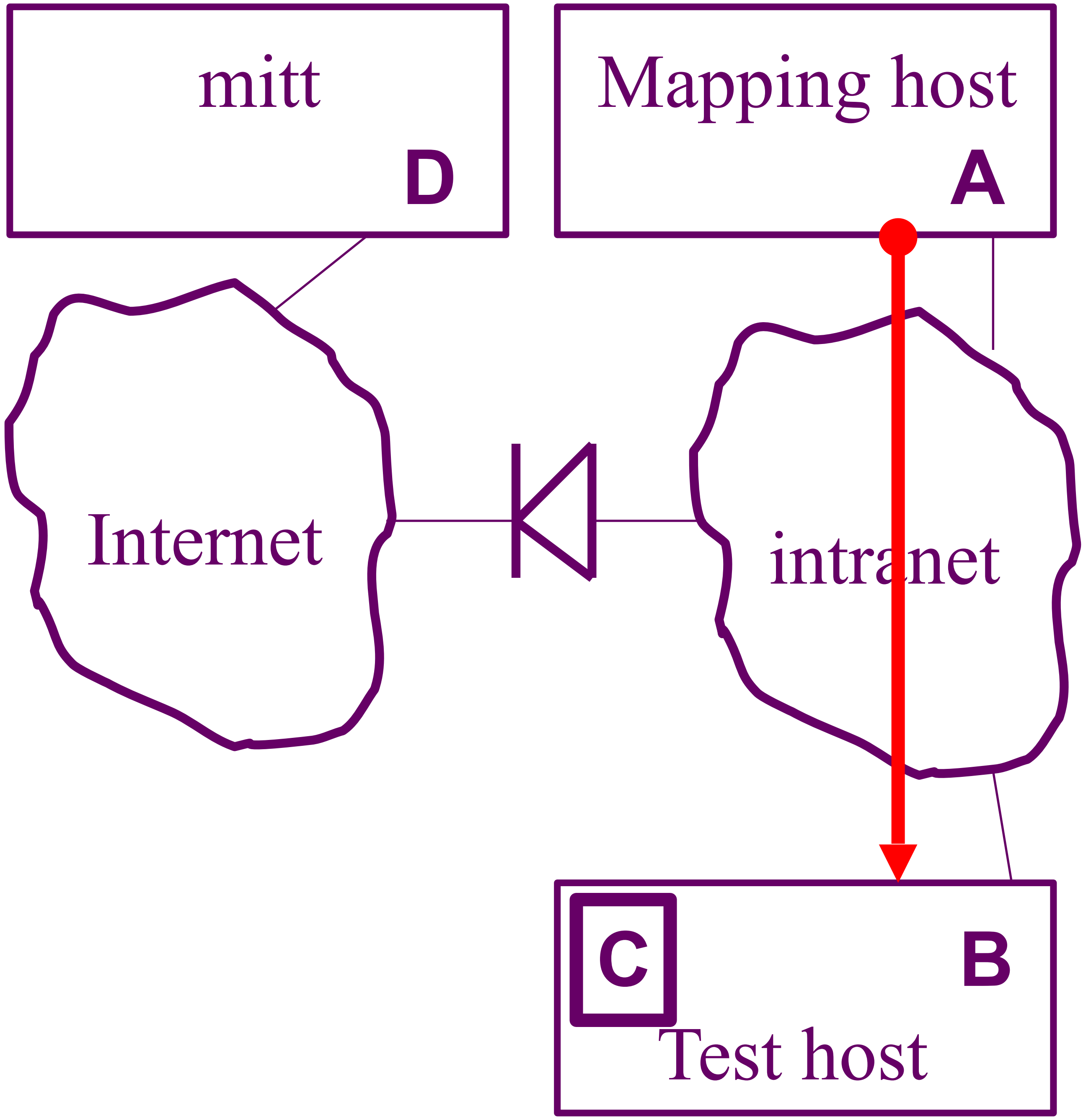
- Mapping host with address A is connected to the intranet
- Mitt with address D has Internet access
- Mapping host and mitt are currently the same host, with two interfaces

Leak Detection



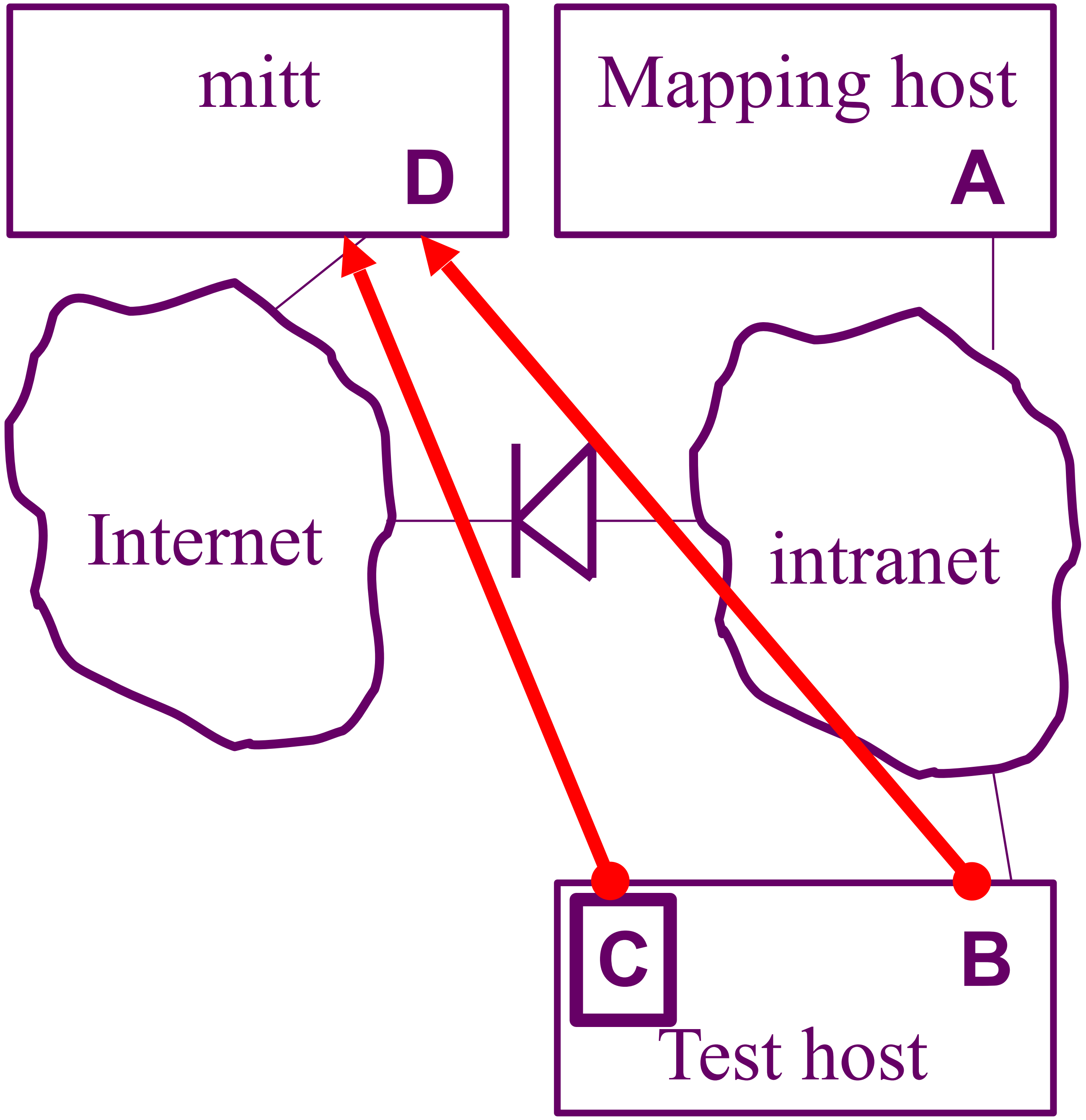
- Test host has known address B on the intranet
- It was found via census
- We are testing for unauthorized access to the Internet, possibly through a different address, C

Leak Detection



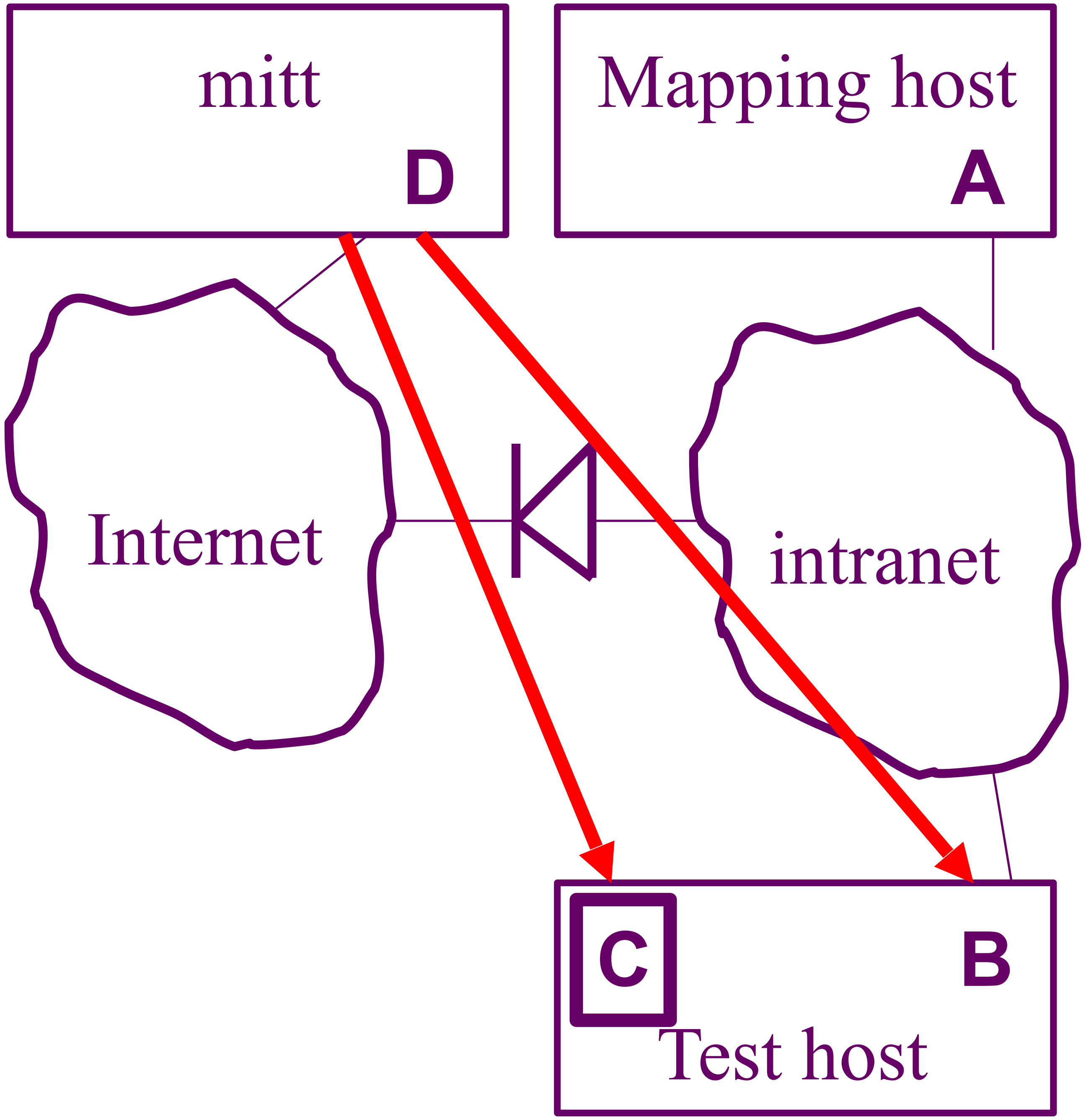
- A sends packet to B, with spoofed return address of D
- If B can, it will reply to D with a response, possibly through a different interface

Leak Detection



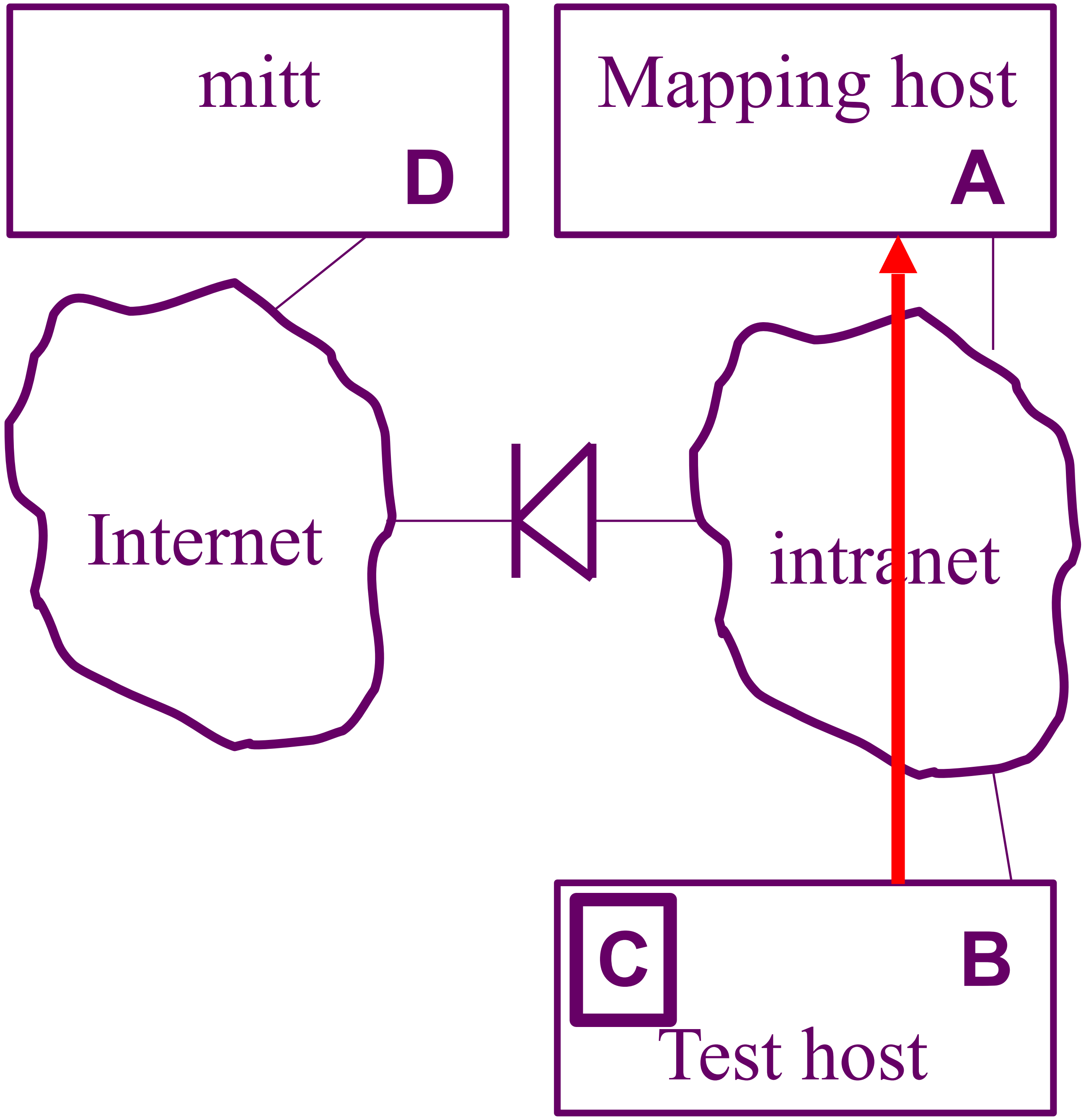
- Packet must be crafted so the response won't be permitted through the firewall
- A variety of packet types and responses are used
- Either inside or outside address may be discovered
- Packet is labeled so we know where it came from

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

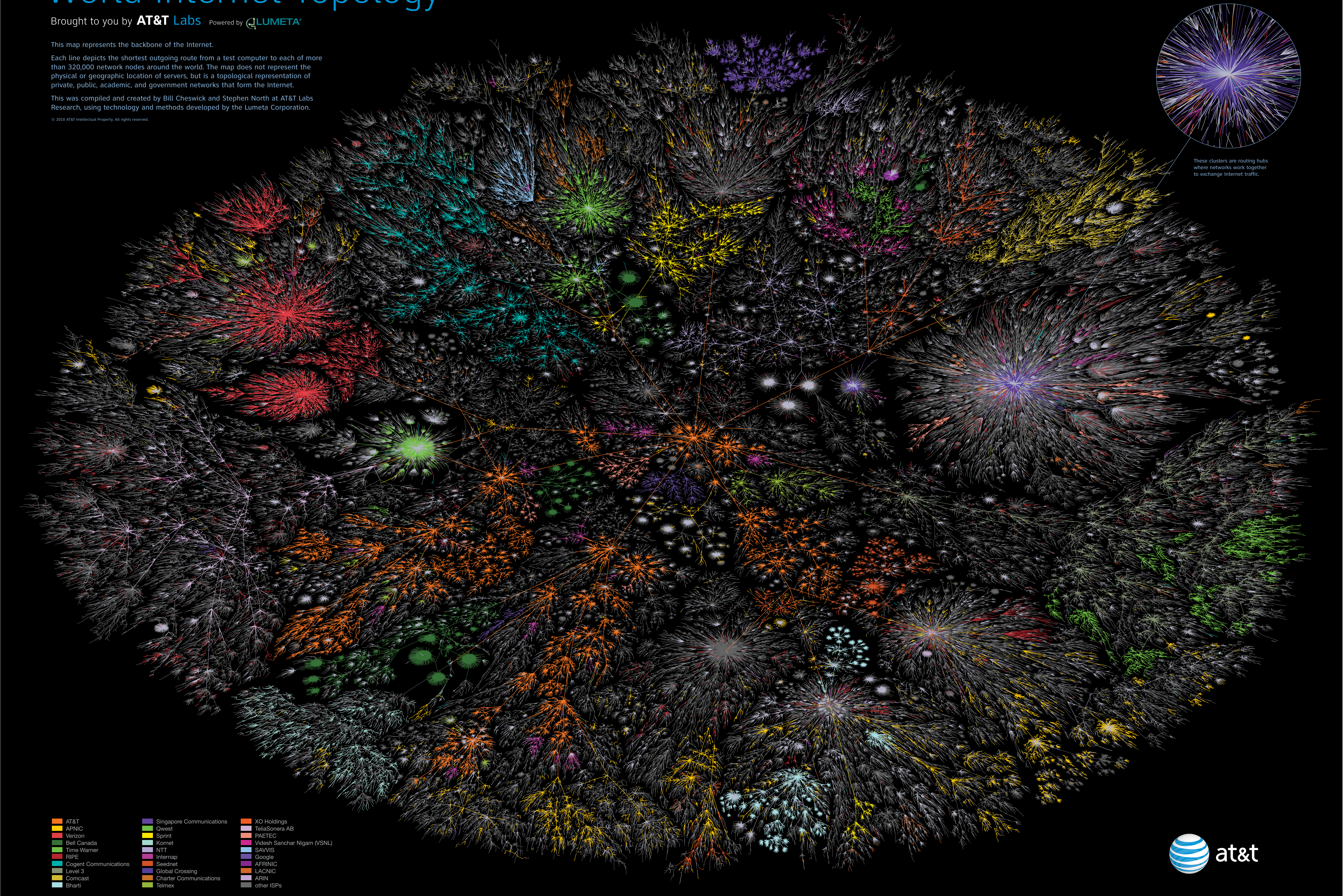
World Internet Topology

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.



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

More work on visualizations:

I AM THE
CONTENT
INDUSTRY

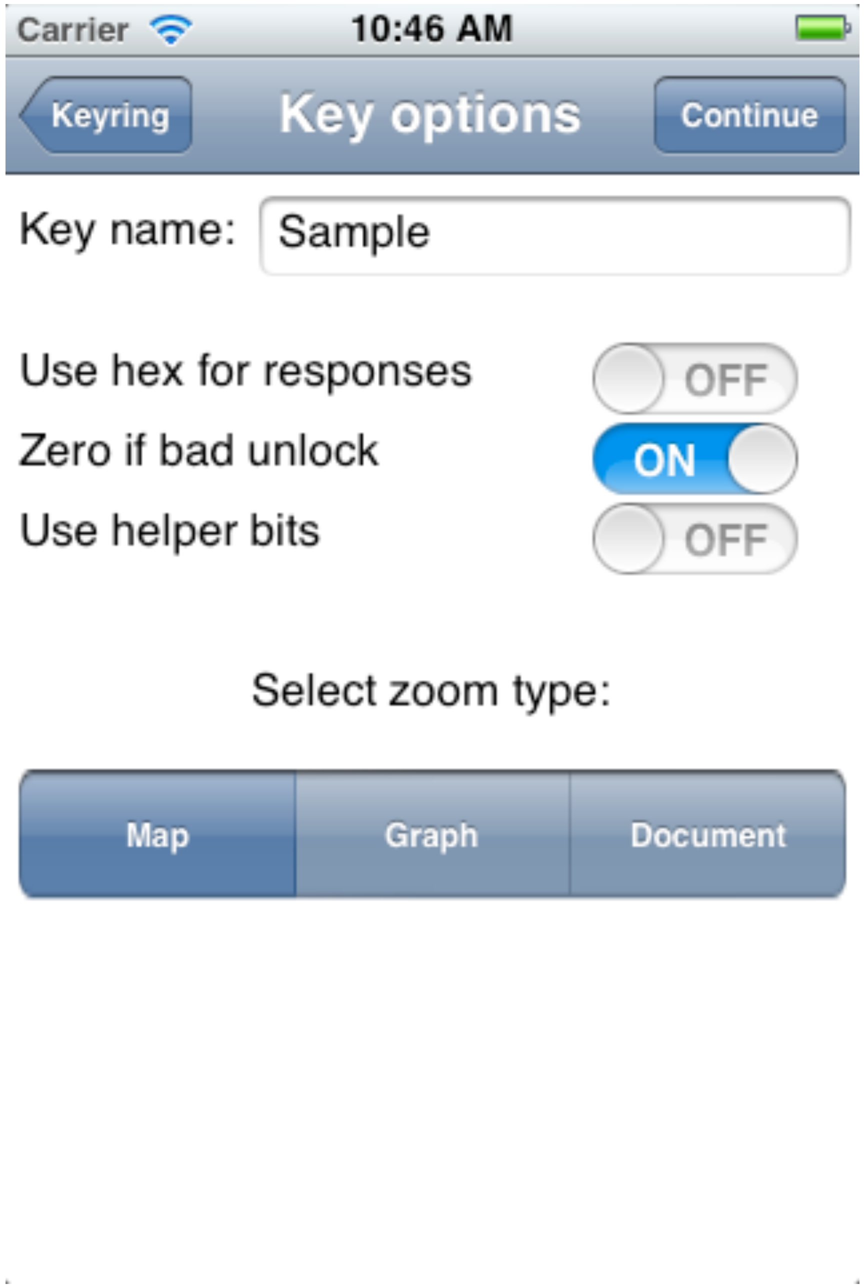
Shannon Labs

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

Current work

- Zoom authentication
- Strong authentication: the long passphrase experiment
    - app “105”, to appear shortly in iTunes.

(Zoomauth demo)



Key name: Sample

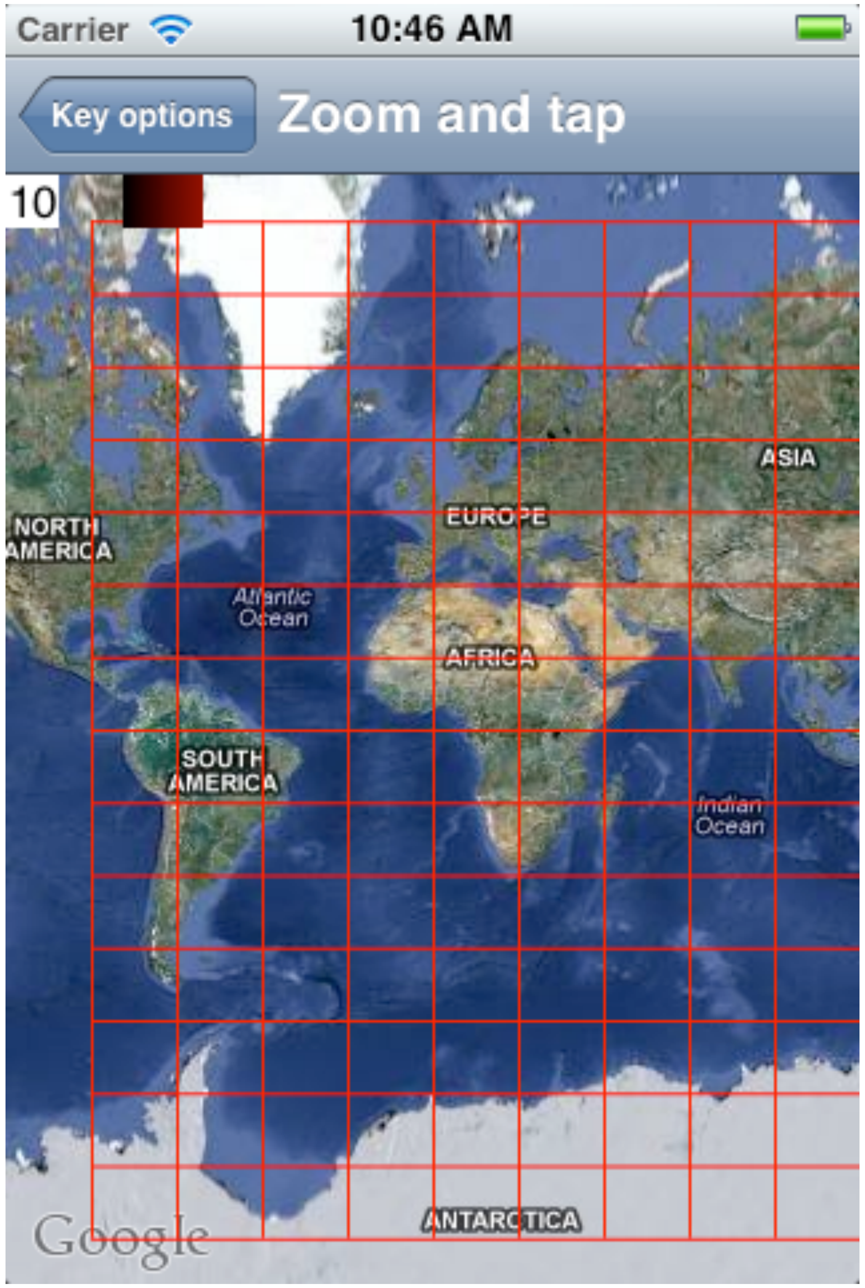
Use hex for responses: OFF

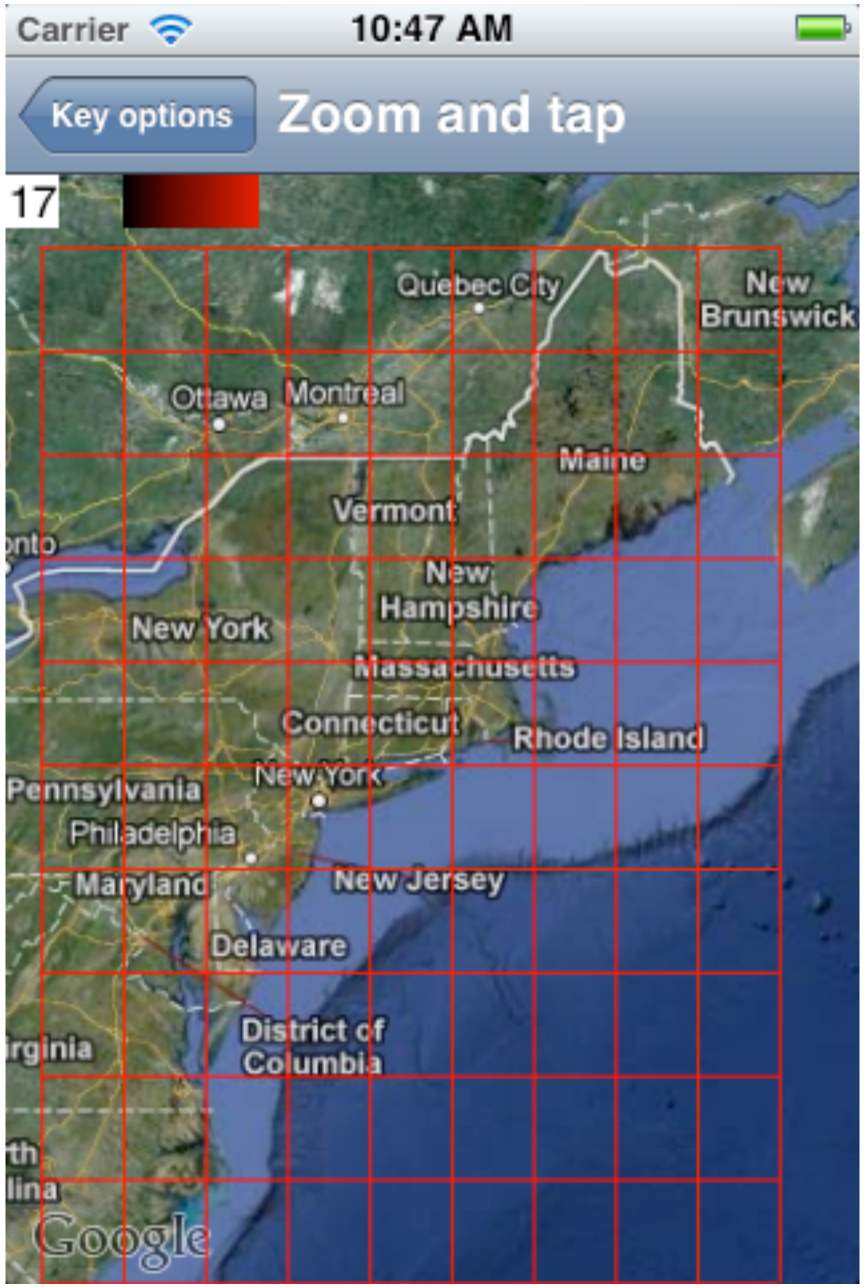
Zero if bad unlock: ON

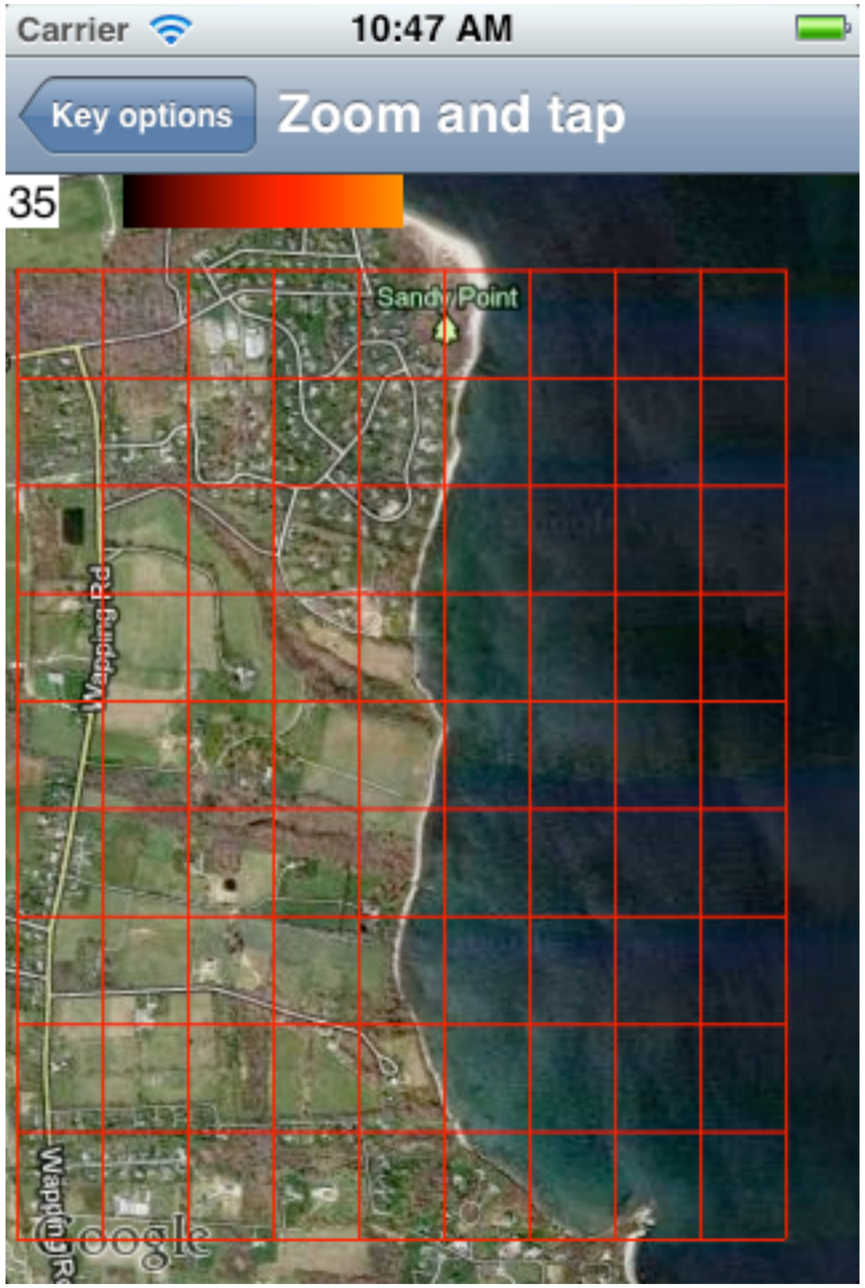
Use helper bits: OFF

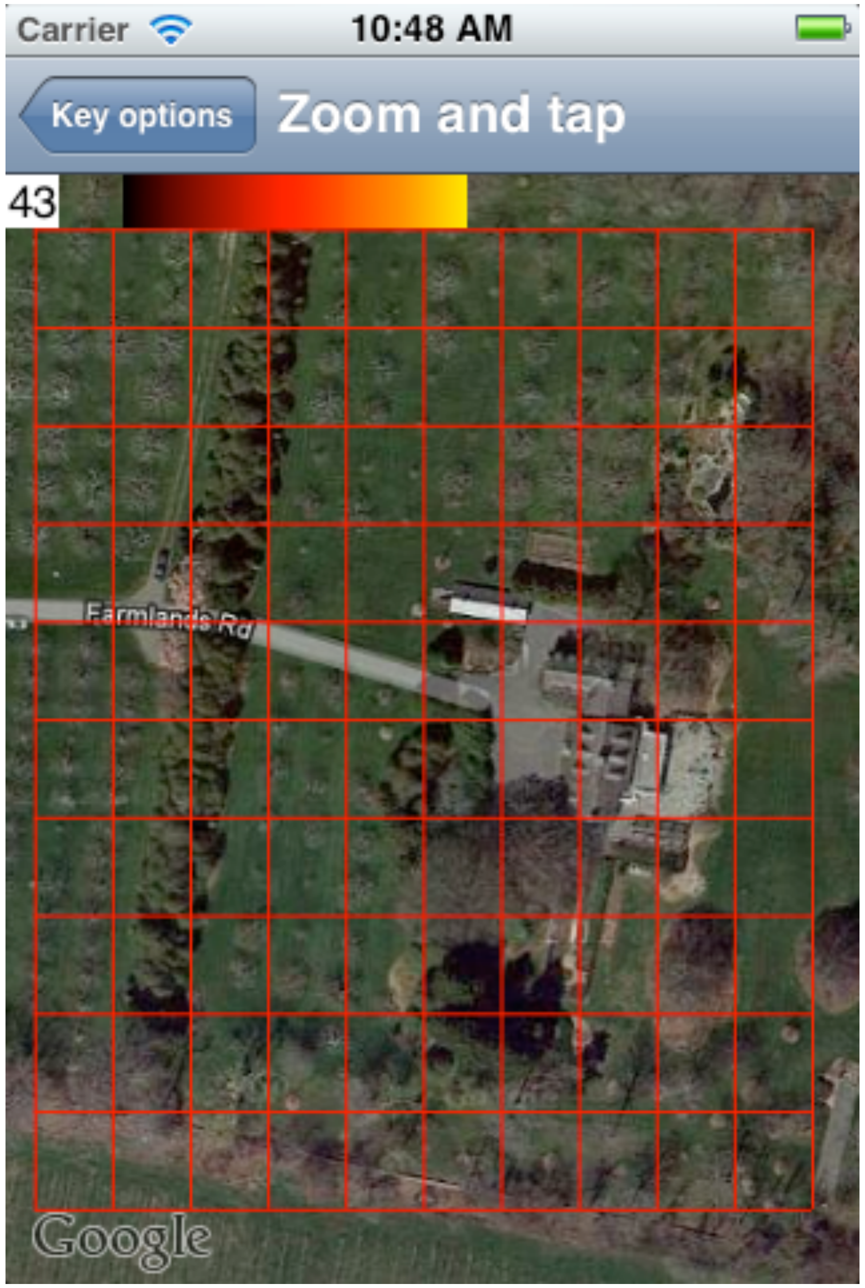
Select zoom type:

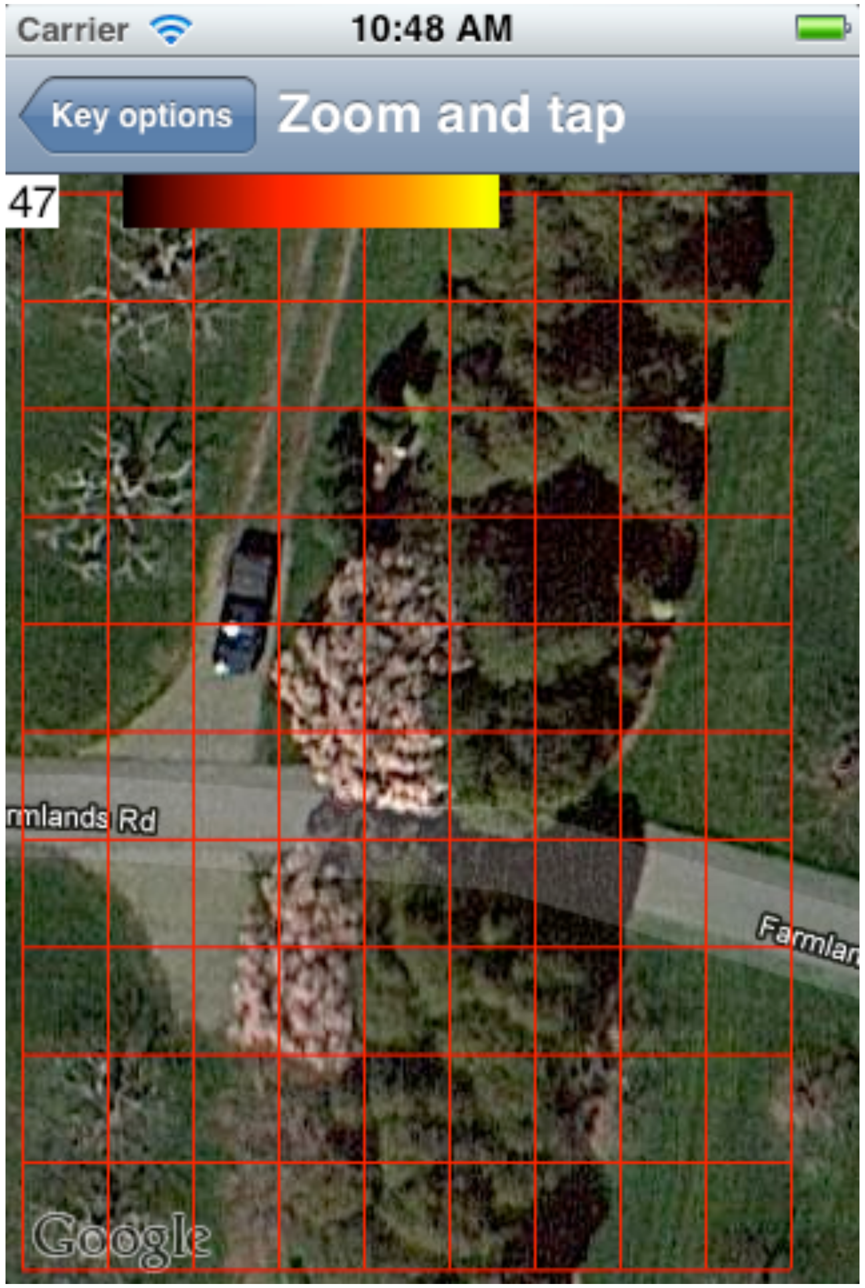
Select zoom type: [✓ Map] Graph Document

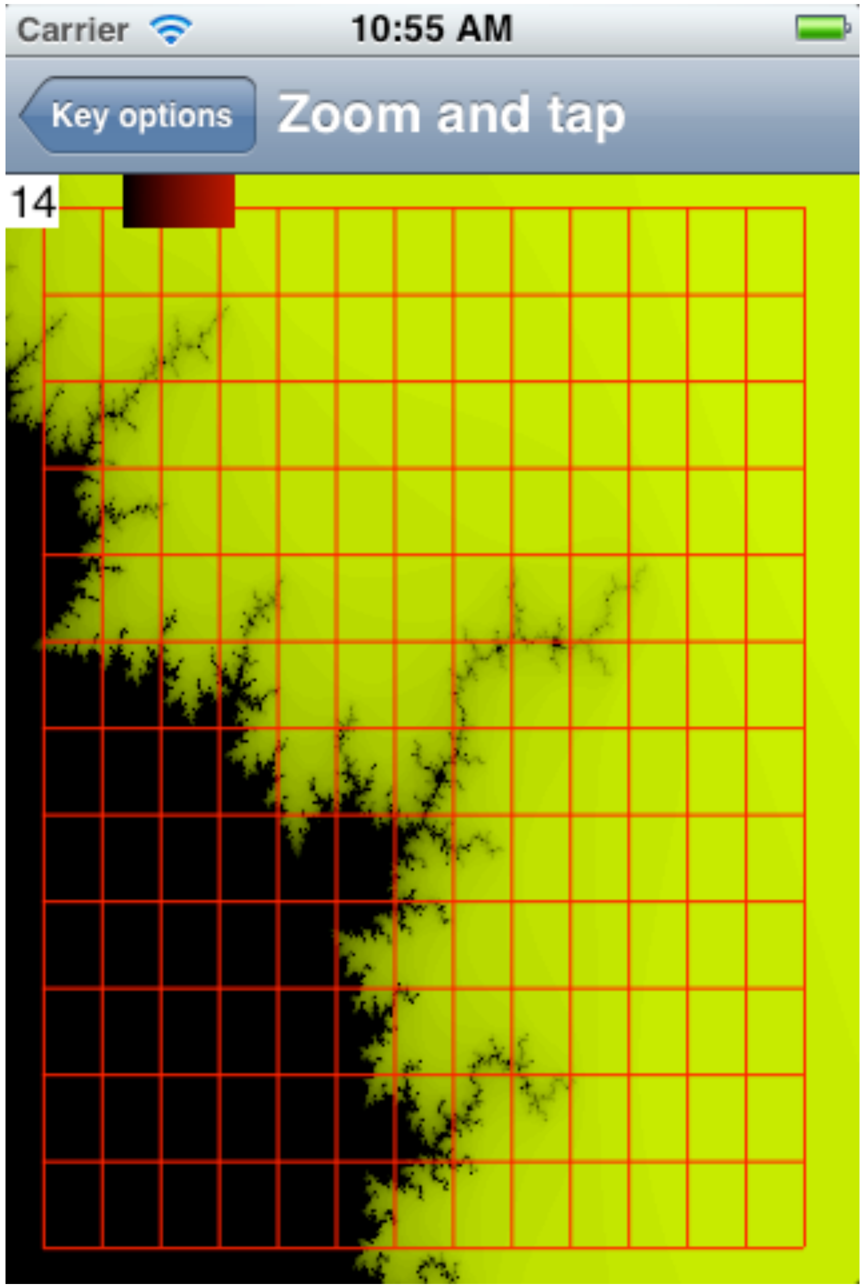




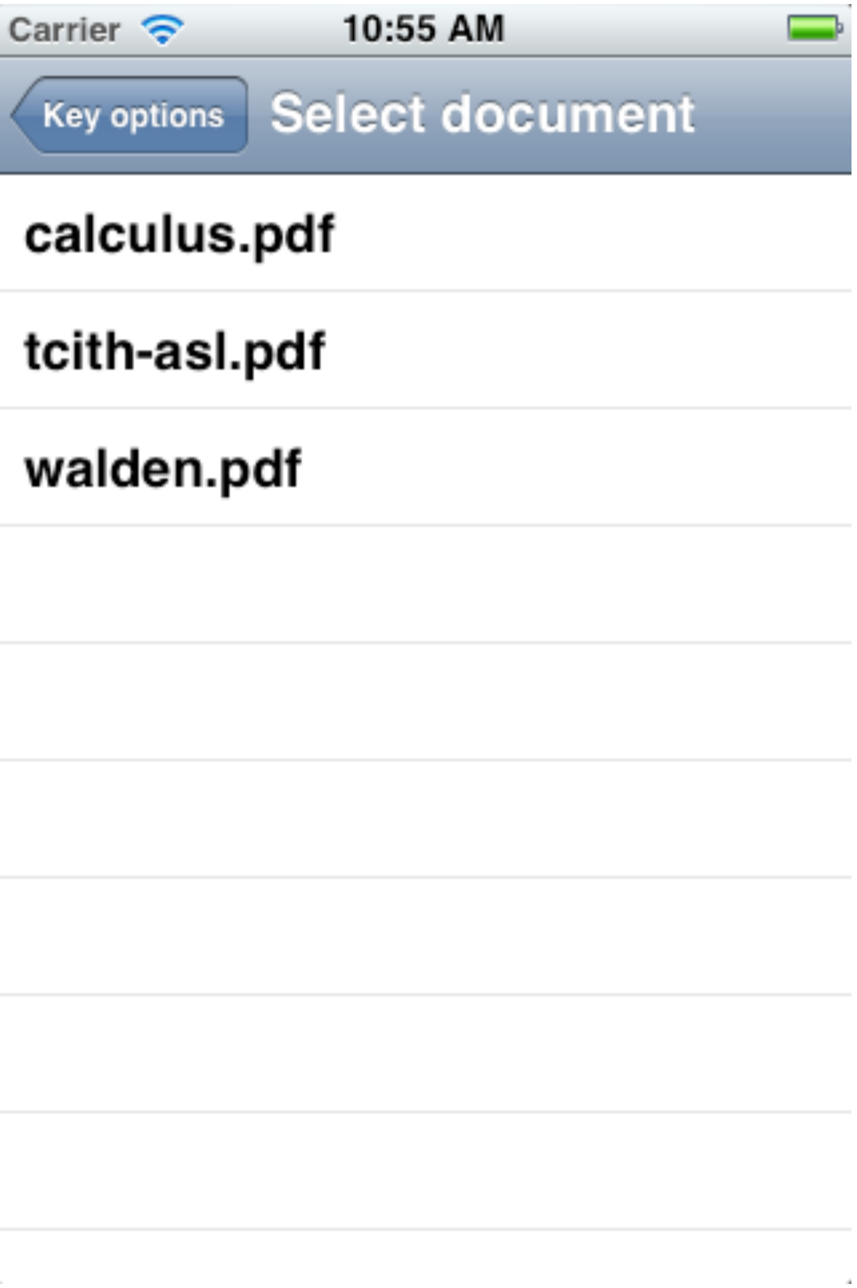

Carrier
10:47 AM
Key options
Zoom and tap
35
Sandy Point
Wapping Rd
Wapping Rd
Google

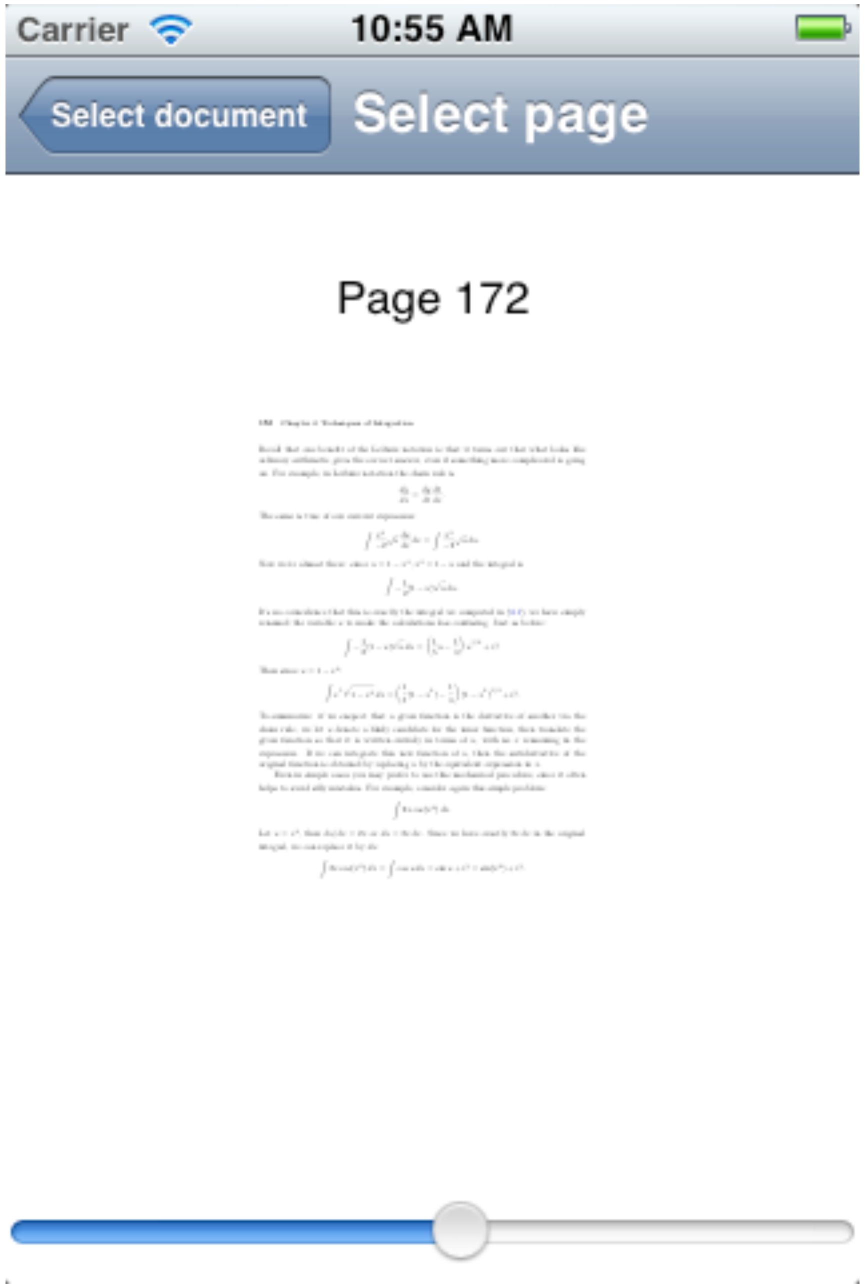

Carrier
10:48 AM
Key options
Zoom and tap
43
Farmlands Rd
Google

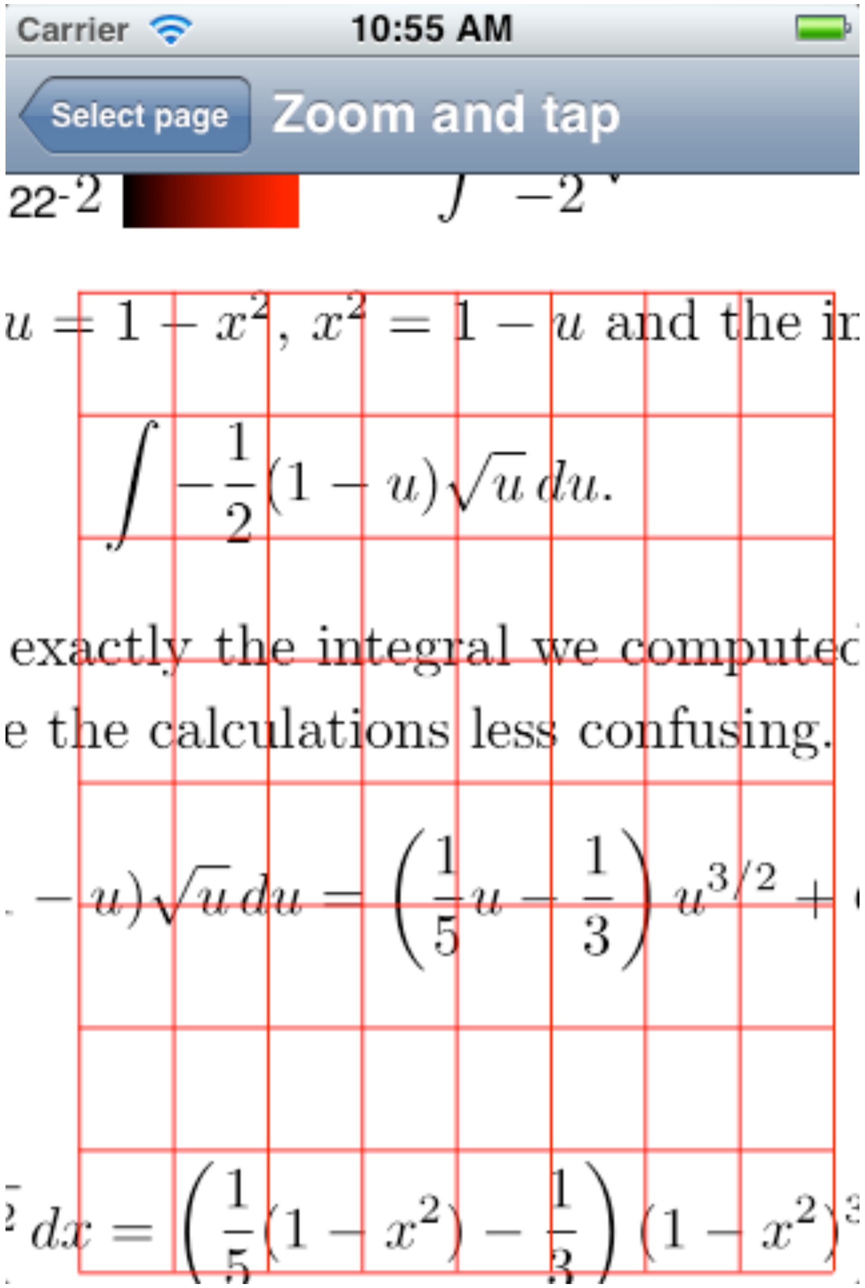

Carrier
10:48 AM
Key options
Zoom and tap
47
rmlands Rd
Farmlan
Google

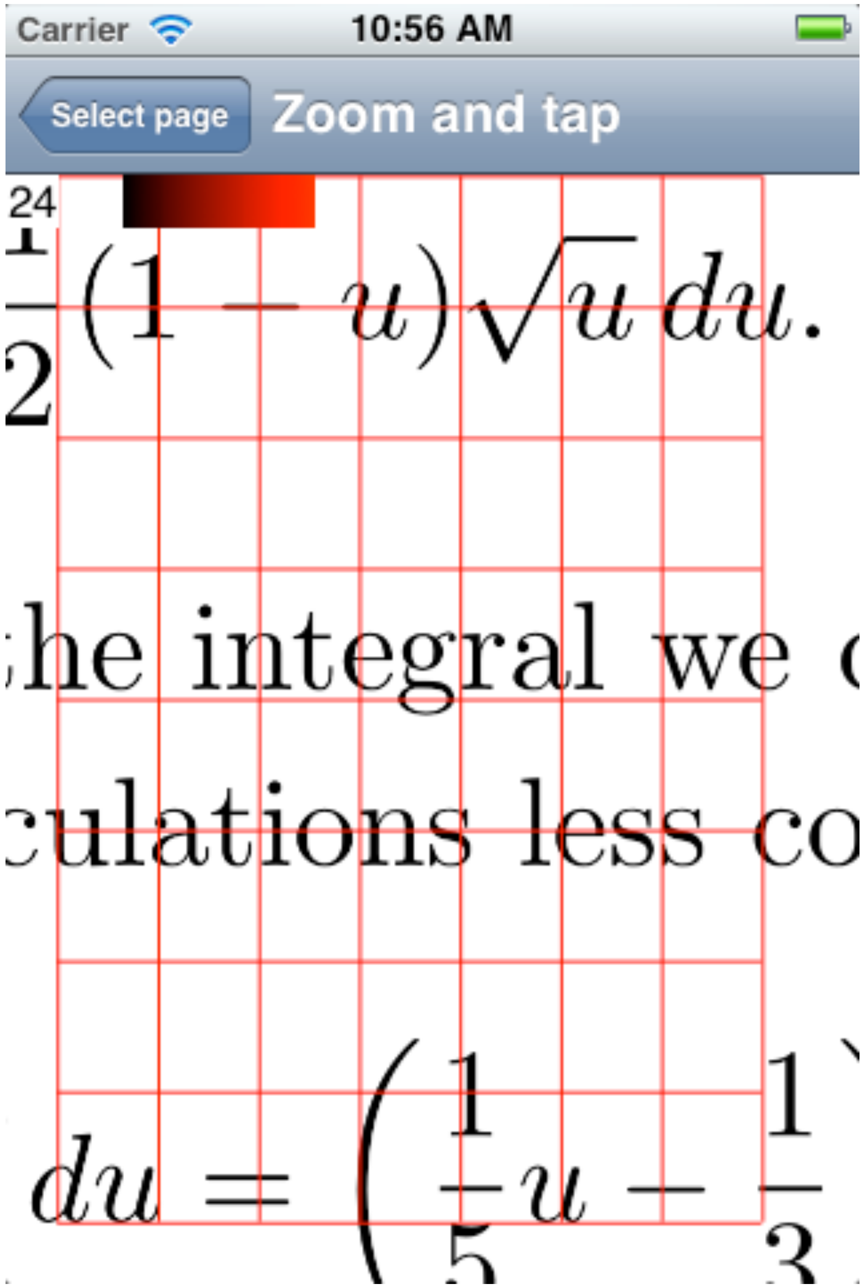


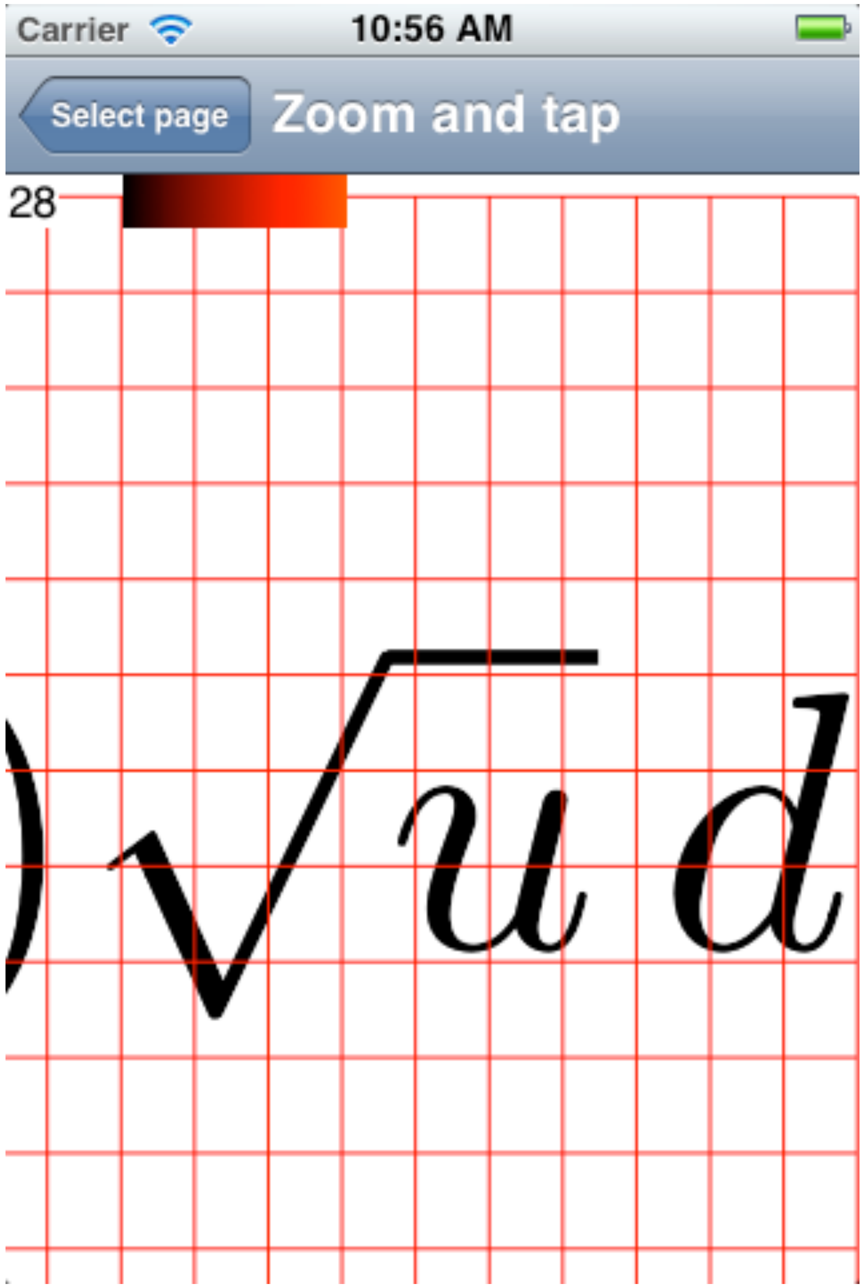
Carrier
10:55 AM
Key options
Zoom and tap
14


Carrier
10:55 AM
Key options
Select document
calculus.pdf
tcith-asl.pdf
walden.pdf


Carrier
10:55 AM
Select document
Select page
Page 172


Carrier
10:55 AM
Select page
Zoom and tap
22-2
$u = 1 - x^2$, $x^2 = 1 - u$ and the in
$\int -\frac{1}{2}(1-u)\sqrt{u}\,du.$
exactly the integral we computed
e the calculations less confusing.
$-u)\sqrt{u}\,du = \left(\frac{1}{5}u - \frac{1}{3}\right)u^{3/2} +$
$dx = \left(\frac{1}{5}(1-x^2) - \frac{1}{3}\right)(1-x^2)$


Carrier
10:56 AM
Select page
Zoom and tap
24
$\frac{1}{2}(1-u)\sqrt{u}\,du.$
he integral we
culations less co
$du = \Big(\frac{1}{5}u - \frac{1}{3}$


Carrier
10:56 AM
Select page
Zoom and tap
28
$)\sqrt{u}\,d$

A Very Short Course on Work Factor

2^{10} = 1024 of the most common British words

the of and a in to it is to was for that you he with on by at are not this but had they his from she that which or we an were as do been their has would there what will all if can said who one so up as them some when could him into its then two out time my about did your now me no other only just more these also people know any first see very new may well should like than how get way one our made got after think between many years er those go being down yeah three good back make such on there through year over must still even take too more here own come last does oh say no work where erm us government same man might day yes however put world over another in want as life most against again never under old much something why each while house part number out off different went really thought came used children always four where without give few within about system local place great during although small before look next when case end things social most find group quite mean five party every company women says important took much men information per both national often seen given school fact money told away high point night state business second need taken done right having thing looked area perhaps head water right family long hand like already possible nothing yet large left side asked set whether days mm home called development week such use country power later almost young council himself of far both use room together tell little political before able become six general service eyes members since times problem anything market towards court public others face full doing war car felt police keep held problems road probably help interest available law best form looking early making today mother saw knew education work actually policy ever so at office am research feel big body door let name person services months report question using health turned million main though words enough child less book period until several sure father for level control known society major seemed around began itself themselves minister economic wanted upon areas after therefore woman city community only including centre gave job among position effect likely real clear staff black kind read provide particular became line moment international action special difficult certain particularly either open management taking across idea whole age process act around evidence view better off mind sense rather seems believe morning third else half white death sometimes thus brought getting church ten shall try behind heard table change support back sort whose industry ago free care so order century range gone yesterday training working ask street home word groups history central all study usually remember trade hundred programme food committee air hours experience rate hands indeed sir language land result course someone everything certainly based team section leave trying coming similar once minutes authority human changes little cases common role true necessary nature class reason long saying town show subject voice companies since because simply especially department single short personal as pay value member started run patients paper private seven eight systems herself practice wife price type seem figure former rather lost right need matter decision bank countries until makes union terms financial needed south university club president friend parents quality building north stage meeting foreign soon strong situation comes late bed recent date low concerned girl hard according as twenty higher tax used production various understand led bring schools ground conditions secretary weeks clearly bad art start up include poor hospital friends decided shown music month tried game anyone wrong ways chapter followed cost play present love issue at goes described more award king royal results workers expected amount students despite knowledge moved news light approach lord cut basis hair required further paid series better before field allowed easy kept questions natural live future rest project greater feet meet simple died for happened added manager computer security near met evening means round carried hear heart forward sent above attention story structure move agreed nine letter individual force studies movement account per call board success following considered current everyone fire agreement please boy capital stood analysis whatever population modern theory books stop in legal material son received model chance environment finally performance sea rights growth authorities provided nice whom produced relationship talk turn built final east talking fine worked west parties size record red close property myself example space giving normal nor reached buy serious quickly along plan behaviour recently term previous couple included pounds anyway cup treatment energy total thank director prime levels significant issues sat income top choice away costs design pressure scheme change a list suddenly continue technology hall takes ones details happy consider won defence following parts loss industrial activities throughout spent outside teachers generally opened floor round activity hope points association nearly allow rates sun army sorry wall hotel forces contract dead stay reported as hour difference meant summer county specific numbers wide appropriate husband top played relations figures chairman set lower product colour ideas look arms obviously unless produce changed season developed unit appear investment test basic write village reasons military original successful garden effects each aware yourself exactly help suppose showed style employment passed appeared page hold suggested continued offered products popular science window expect beyond resources rules professional announced economy picture okay needs doctor maybe events a direct gives advice running circumstances sales risk interests dark event thousand involved written park returned ensure fish wish opportunity commission oil sound ready lines shop looks immediately worth in college press fell blood goods playing carry less film prices useful conference operation follows extent designed application station television access response degree majority effective established wrote region green ah western traditional easily cold shows offer though statement published forms down accept miles independent election support importance lady site jobs needs plans earth earlier title parliament standards leaving interesting houses planning considerable girls involved increase species stopped concern public means caused raised through glass physical thought eye left heavy walked daughter existing competition speak responsible up river follow

Pick one at random, entropy = 10 bits ($2^{10} = 1024$)

the of and a in to it is to was for that you he with on by at are not this but had they his from she that which or we an were as do been their has would there what will all if can said who one so up as them some when could him into its then two out time my about did your now me no other only just more these also people know any first see very new may well should like than how get way one our made got after think between many years er those go being down yeah three good back make such on there through year over must still even take too more here own come last does oh say no work where erm us government same man might day yes however put world over another in want as life most against again never under old much something why each while house part number out off different went really thought came used children always four where without give few within about system local place great during although small before look next when case end things social most find group quite mean five party every company women says important took much men information per both national often seen given school fact money told away high point night state business second need taken done right having thing looked area perhaps head water right family long hand like already possible nothing yet large left side asked set whether days mm home called development week such use country power later almost young council himself of far both use room together tell little political before able become six general service eyes members since times problem anything market towards court public others face full doing war car felt police keep held problems road probably help interest available law best form looking early making today mother saw knew education work actually policy ever so at office am research feel big body door let name person services months report question using health turned million main though words enough child less book period until several sure father for level control known society major seemed around began itself themselves minister economic wanted upon areas after therefore woman city community only including centre gave job among position effect likely real clear staff black kind read provide particular became line moment international action special difficult certain particularly either open management taking across idea whole age process act around evidence view better off mind sense rather seems believe morning third else half white death sometimes thus brought getting church ten shall try behind heard table change support back sort whose industry ago free care so order century range gone yesterday training working ask street home word groups history central all study usually remember trade hundred programme food committee air hours experience rate hands indeed sir language land result course someone everything certainly based team section leave trying coming similar once minutes authority human changes little cases common role true necessary nature class reason long saying town show subject voice companies since because simply especially department single short personal as pay value member started run patients paper private seven eight systems herself practice wife price type seem figure former rather lost right need matter decision bank countries until makes union terms financial needed south university club president friend parents quality building north stage meeting foreign soon strong situation comes late bed recent date low concerned girl hard according as twenty higher tax used production various understand led bring schools ground conditions secretary weeks clearly bad art start up include poor hospital friends decided shown music month tried game anyone wrong ways chapter followed cost play present love issue at goes described more award king royal results workers expected amount students despite knowledge moved news light approach lord cut basis hair required further paid series better before field allowed easy kept questions natural live future rest project greater feet meet simple died for happened added manager computer security near met evening means round carried hear heart forward sent above attention story structure move agreed nine letter individual force studies movement account per call board success following considered current everyone fire agreement please boy capital stood analysis whatever population modern theory books stop in legal material son received model chance environment finally performance sea rights growth authorities provided nice whom produced relationship talk turn built final east talking fine worked west parties size record red close property myself example space giving normal nor reached buy serious quickly along plan behaviour recently term previous couple included pounds anyway cup treatment energy total thank director prime levels significant issues sat income top choice away costs design pressure scheme change a list suddenly continue technology hall takes ones details happy consider won defence following parts loss industrial activities throughout spent outside teachers generally opened floor round activity hope points association nearly allow rates sun army sorry wall hotel forces contract dead stay reported as hour difference meant summer county specific numbers wide appropriate husband top played relations figures chairman set lower product colour ideas look arms obviously unless produce changed season developed unit appear investment test basic write village reasons military original successful garden effects each aware yourself exactly help suppose showed style employment passed appeared page hold suggested continued offered products popular science window expect beyond resources rules professional announced economy picture okay needs doctor maybe events a direct gives advice running circumstances sales risk interests dark event thousand involved written park returned ensure fish wish opportunity commission oil sound ready lines shop looks immediately worth in college press fell blood goods playing carry less film prices useful conference operation follows extent designed application station television access response degree majority effective established wrote region green ah western traditional easily cold shows offer though statement published forms down accept miles independent election support importance lady site jobs needs plans earth earlier title parliament standards leaving interesting houses planning considerable girls involved increase species stopped concern public means caused raised through glass physical thought eye left heavy walked daughter existing competition speak responsible up river follow

Two random choices = 20 bits

the of and a in to it is to was for that you he with on by at are not this but had they his from she that which or we an were as do been their has would there what
will all if can said who one so up as them some when could him into its then two out time my about did your now me no other only just more these also people
know any first see very new may well should like than how get way one our made got after think between many years er those go being down yeah three good
back make such on there through year over must still even take too more here own come last does oh say no work where erm us government same man might
day yes however put world over another in want as life most against again never under old much something why each while house part number out off different
went really thought came used children always four where without give few within about system local place great during although small before look next when
case end things social most find group quite mean five party every company women says important took much men information per both national often seen
given school fact money told away high point night state business second need taken done right having thing looked area perhaps head water right family long
hand like already possible nothing yet large left side asked set whether days mm home called development week such use country power later almost young
council himself of far both use room together tell little political before able become six general service eyes members since times problem anything market
towards court public others face full doing war car felt police keep held problems road probably help interest available law best form looking early making today
mother saw knew education work actually policy ever so at office am research feel big body door let name person services months report question using health
turned million main though words enough child less book period until several sure father for level control known society major seemed around began itself
themselves minister economic wanted upon areas after therefore woman city community only including centre gave job among position effect likely real clear
staff black kind read provide particular became line moment international action special difficult certain particularly either open management taking across idea
whole age process act around evidence view better off mind sense rather seems believe morning third else half white death sometimes thus brought getting
church ten shall try behind heard table change support back sort whose industry ago free care so order century range gone yesterday training working ask street
home word groups history central all study usually remember trade hundred programme food committee air hours experience rate hands indeed sir language
land result course someone everything certainly based team section leave trying coming similar once minutes authority human changes little cases common role
true necessary nature class reason long saying town show subject voice companies since because simply especially department single short personal as pay value
member started run patients paper private seven eight systems herself practice wife price type seem figure former rather lost right need matter decision bank
countries until makes union terms financial needed south university club president friend parents quality building north stage meeting foreign soon strong
situation comes late bed recent date low concerned girl hard according as twenty higher tax used production various understand led bring schools ground
conditions secretary weeks clearly bad art start up include poor hospital friends decided shown music month tried game anyone wrong ways chapter followed
cost play present love issue at goes described more award king royal results workers expected amount students despite knowledge moved news light approach
lord cut basis hair required further paid series better before field allowed easy kept questions natural live future rest project greater feet meet simple died for
happened added manager computer security near met evening means round carried hear heart forward sent above attention story structure move agreed nine
letter individual force studies movement account per call board success following considered current everyone fire agreement please boy capital stood analysis
whatever population modern theory books stop in legal material son received model chance environment finally performance sea rights growth authorities
provided nice whom produced relationship talk turn built final east talking fine worked west parties size record red close property myself example space giving
normal nor reached buy serious quickly along plan behaviour recently term previous couple included pounds anyway cup treatment energy total thank director
prime levels significant issues sat income top choice away costs design pressure scheme change a list suddenly continue technology hall takes ones details happy
consider won defence following parts loss industrial activities throughout spent outside teachers generally opened floor round activity hope points association
nearly allow rates sun army sorry wall hotel forces contract dead stay reported as hour difference meant summer county specific numbers wide appropriate
husband top played relations figures chairman set lower product colour ideas look arms obviously unless produce changed season developed unit appear
investment test basic write village reasons military original successful garden effects each aware yourself exactly help suppose showed style employment passed
appeared page hold suggested continued offered products popular science window expect beyond resources rules professional announced economy picture okay
needs doctor maybe events a direct gives advice running circumstances sales risk interests dark event thousand involved written park returned ensure fish wish
opportunity commission oil sound ready lines shop looks immediately worth in college press fell blood goods playing carry less film prices useful conference
operation follows extent designed application station television access response degree majority effective established wrote region green ah western traditional
easily cold shows offer though statement published forms down accept miles independent election support importance lady site jobs needs plans earth earlier
title parliament standards leaving interesting houses planning considerable girls involved increase species stopped concern public means caused raised through
glass physical thought eye left heavy walked daughter existing competition speak responsible up river follow

20 bits = 2^{20} = 1,048,576

- “example early”
- to guess our two words, requires:
  - 1,048,576/2 guess, on average
- 6 random words would be 2^{60}
  - 1.15 x 10^{18}
- 8 random words gives you Avogadro’s number, a mole of work to do!

Good stuff!

- The list of words isn’t secret
- so spelling checker is okay!
    - so is error correction! In a password!
- easy words to type
- on an iPhone, pick words where the “tappos” give the word you wanted

Required entropy, according to Florêncio and Herley

- Facebook, Twitter, etc. are a minimum of ~20 bits
- Banks are in the 30s
- Government in the mid 40s and up

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

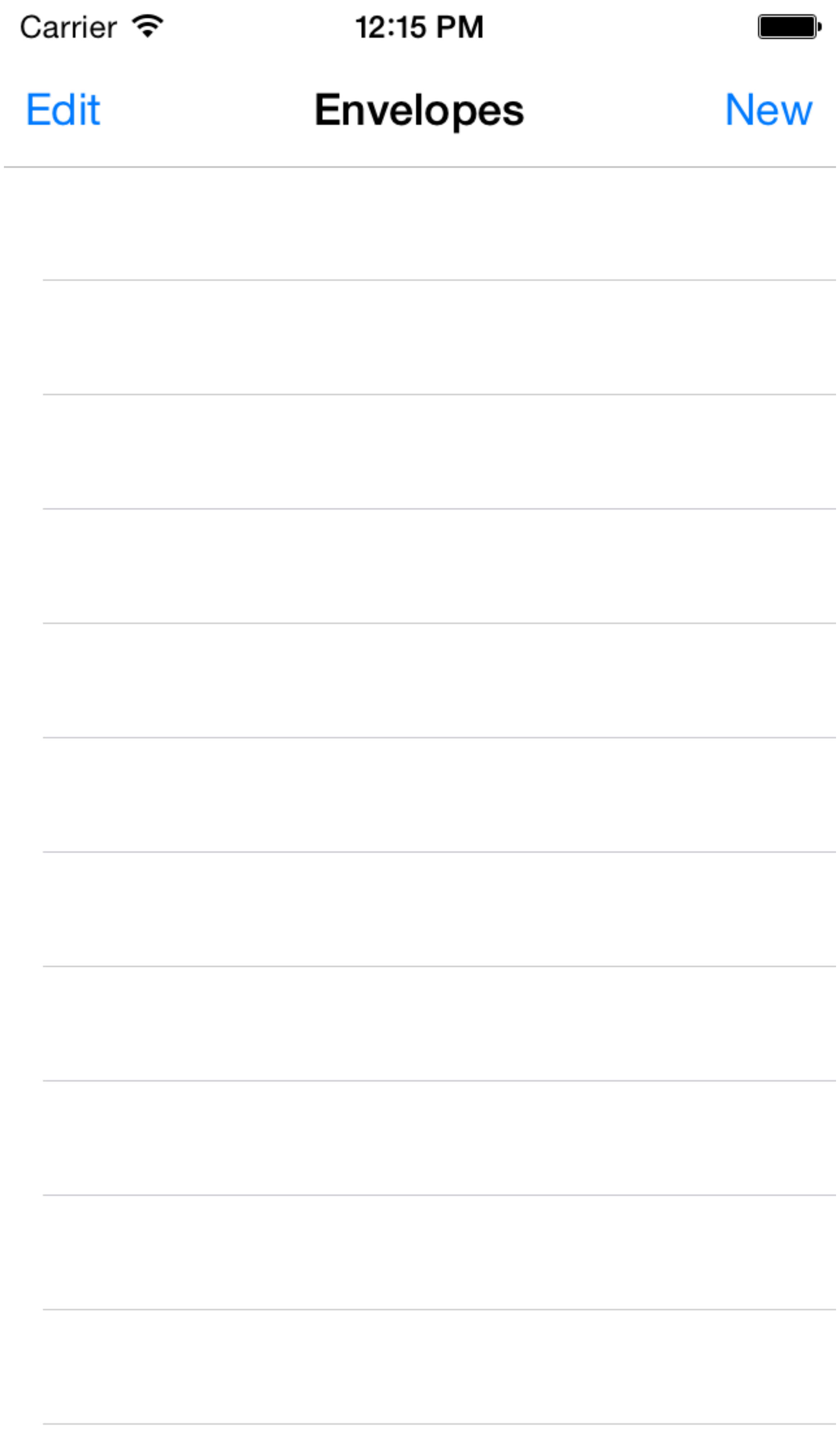
www.cheswick.com/ches/insults.html
(42 bits)

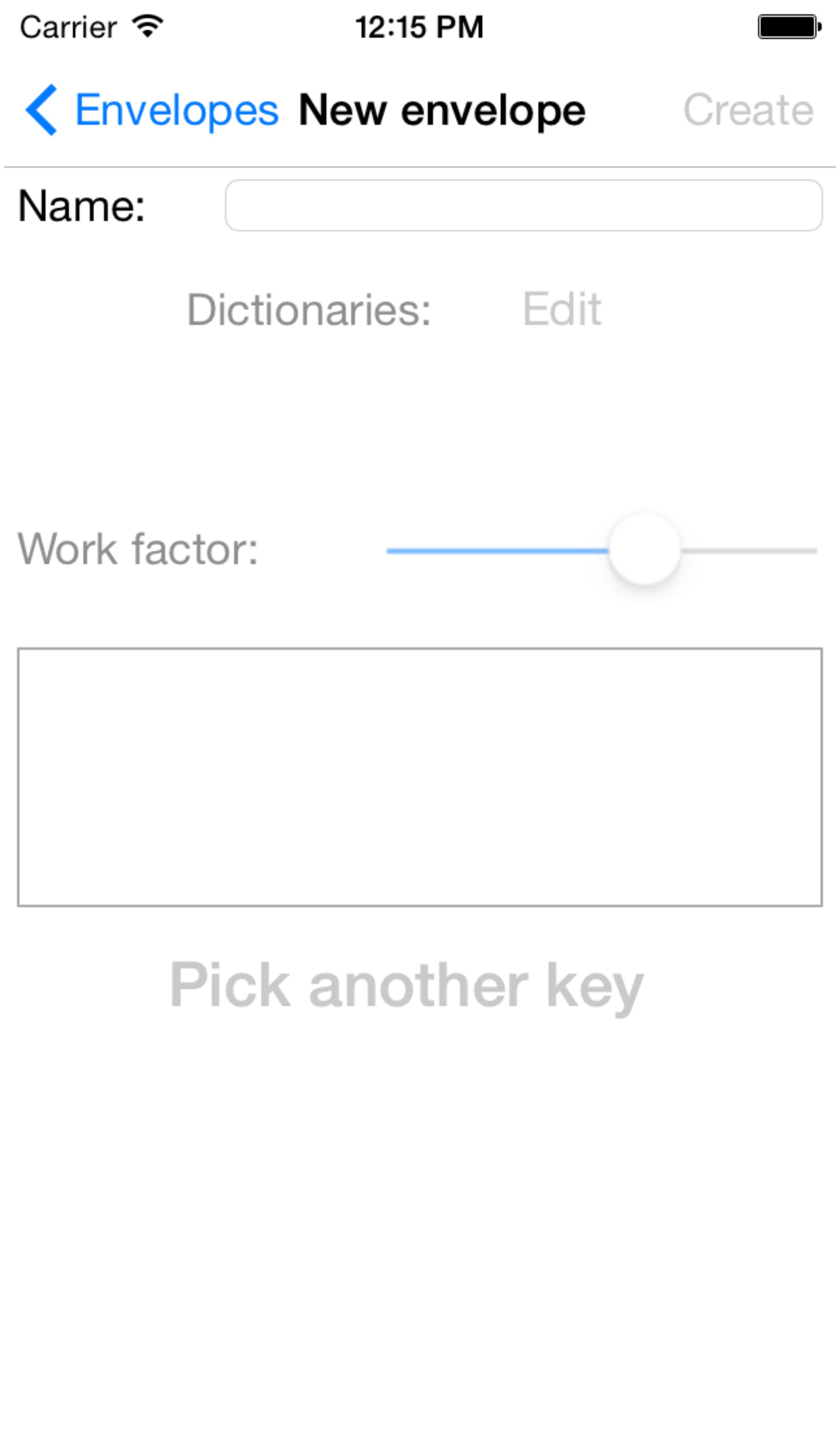
```
You grim-faced pipe of pleuritic snipe sweat
You dire chiffonier of foul miniature poodle squirt
You teratic theca of pathogenic moth dingleberry
You worrying pan broiler of bilious puff adder slobber
You vile wok of tumorigenic aphid leftovers
You baneful reliquary of pneumonic miller stumps
You 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
```

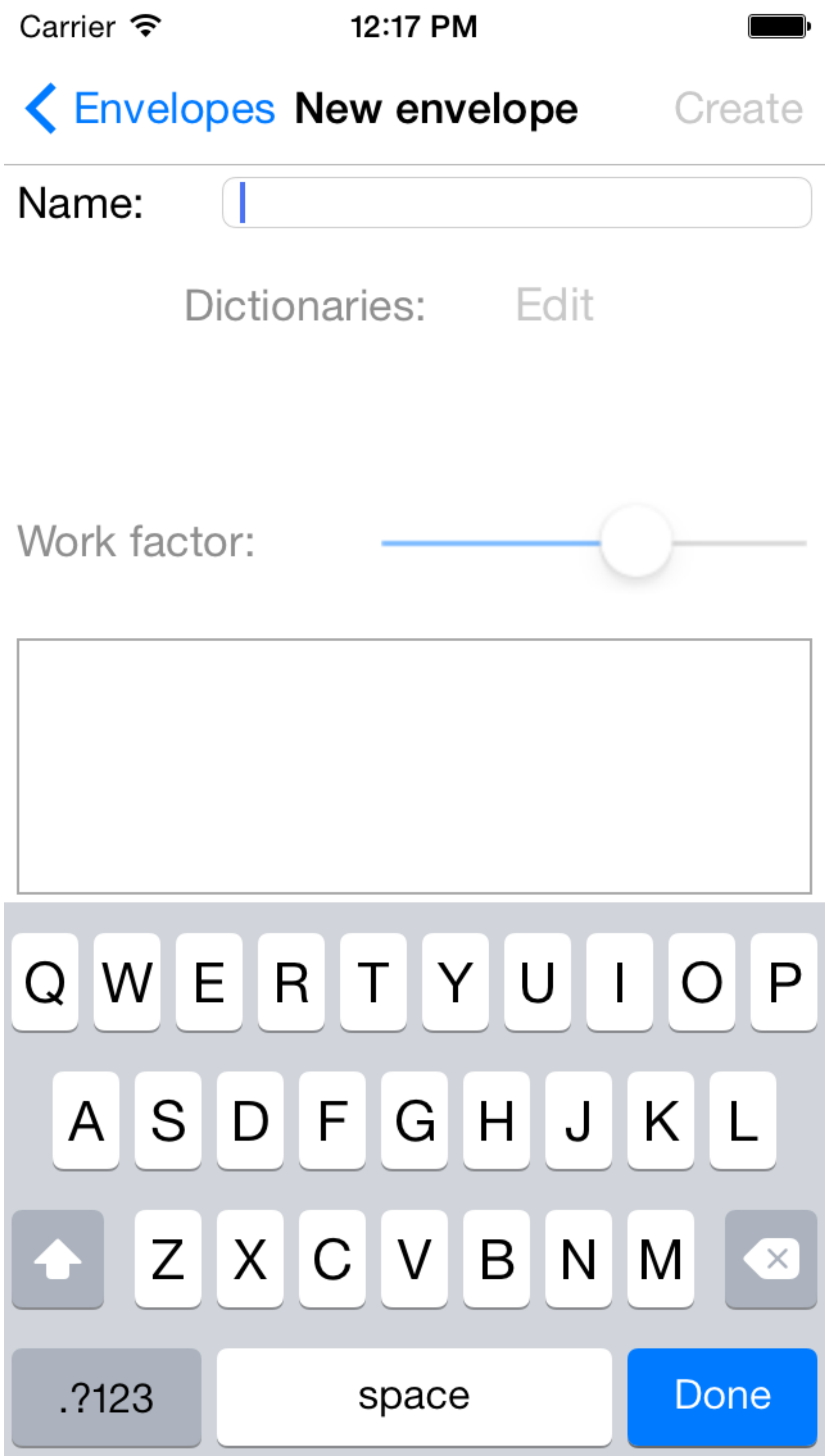
If you really need “high entropy” passwords

- 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?

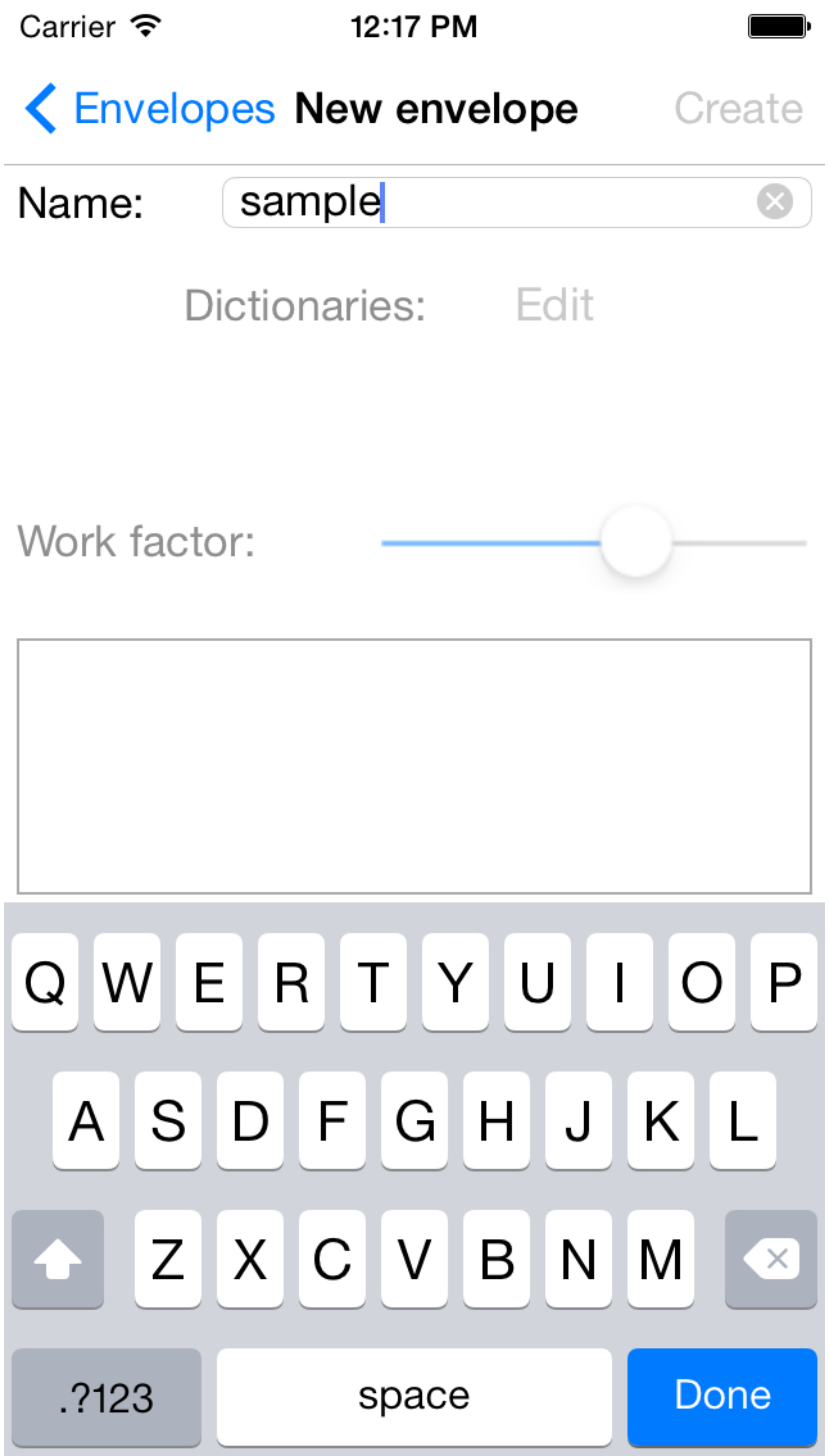
(105 demo)


Carrier
12:15 PM
Edit
Envelopes
New

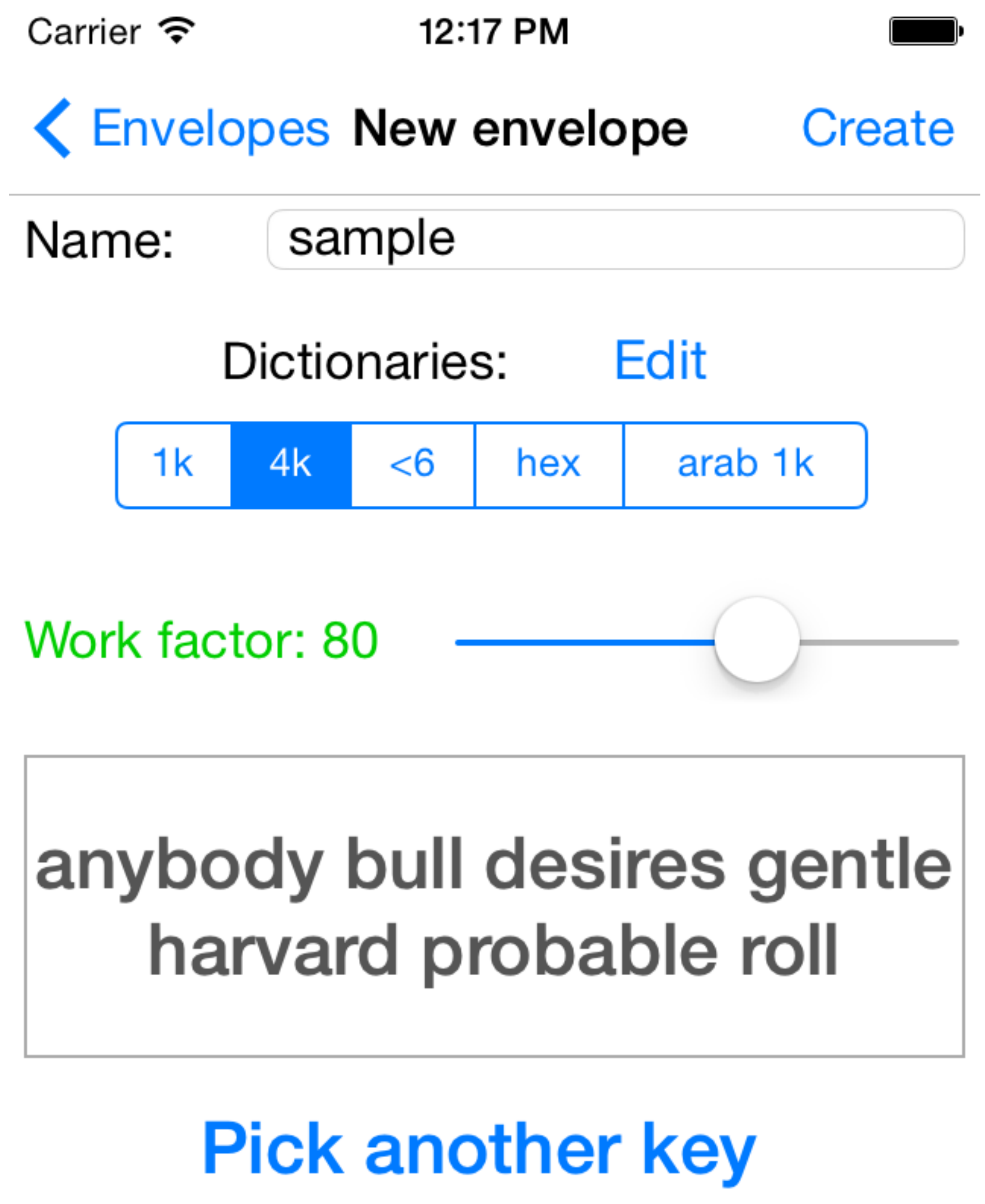

Carrier
12:15 PM
Envelopes
New envelope
Create
Name:
Dictionaries:
Edit
Work factor:
Pick another key



Name:



Name: sample

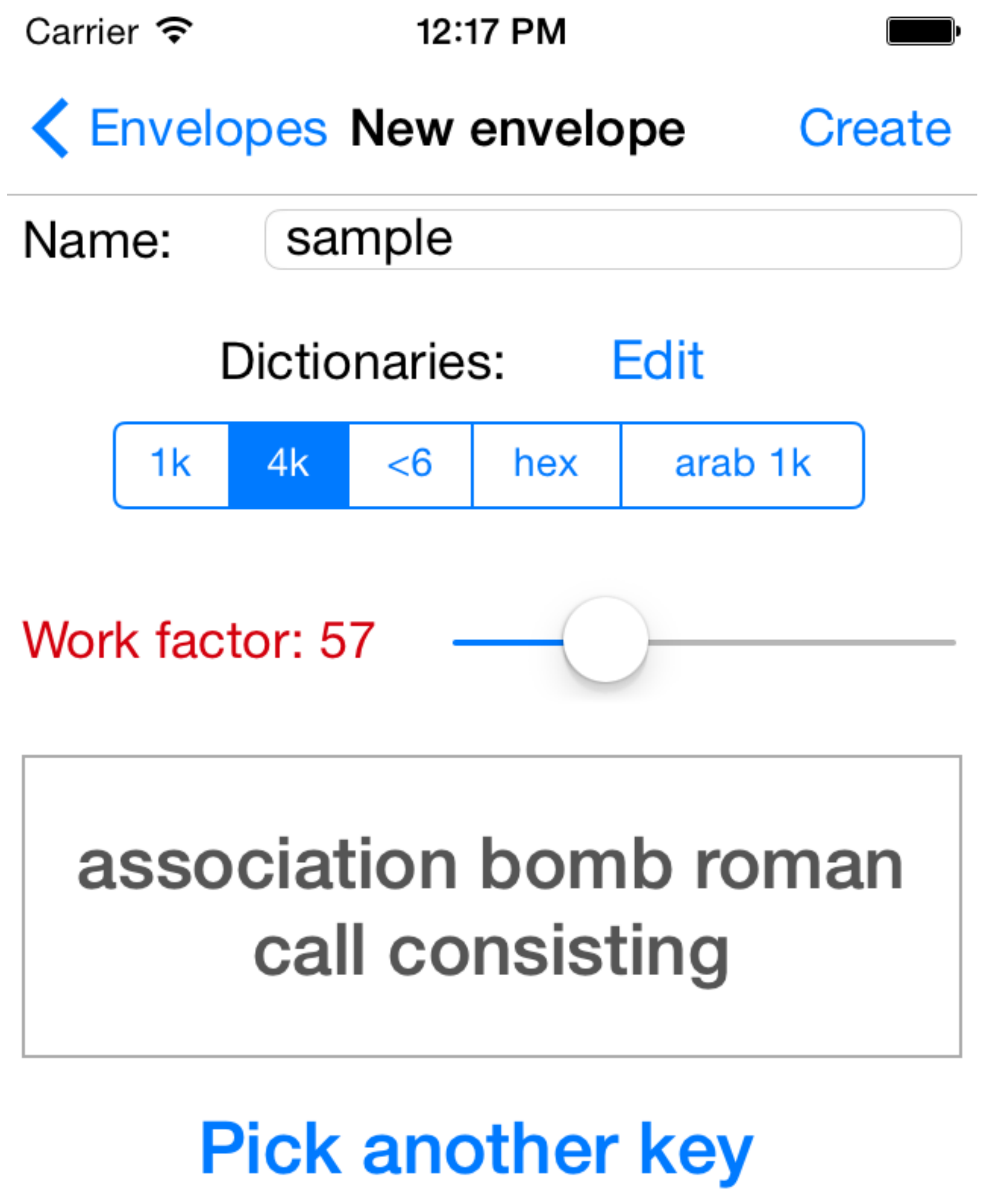


Name: sample

Dictionaries: 4k

Work factor: 80

anybody bull desires gentle harvard probable roll

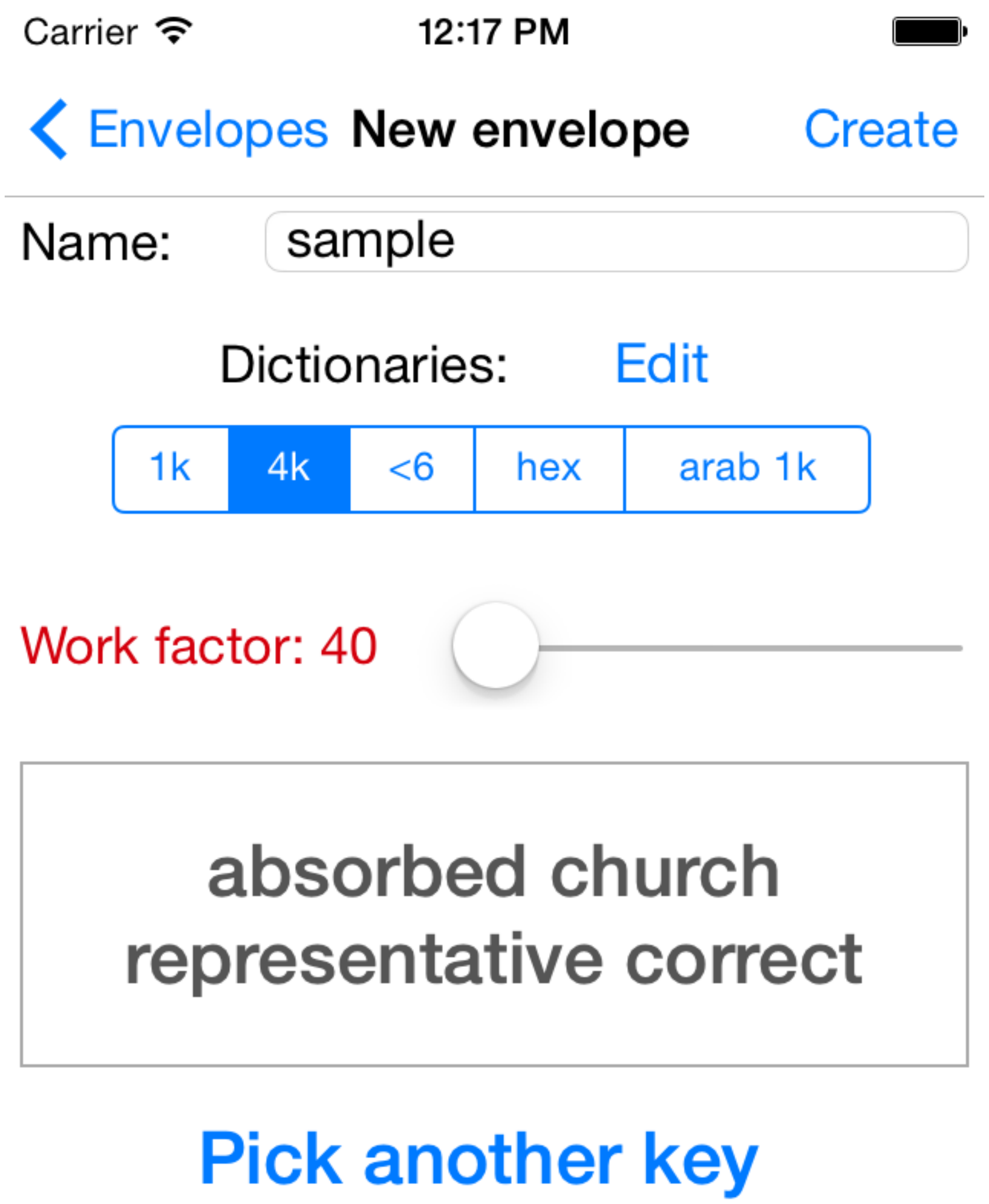


Name: sample

Dictionaries: 4k

Work factor: 57

association bomb roman call consisting

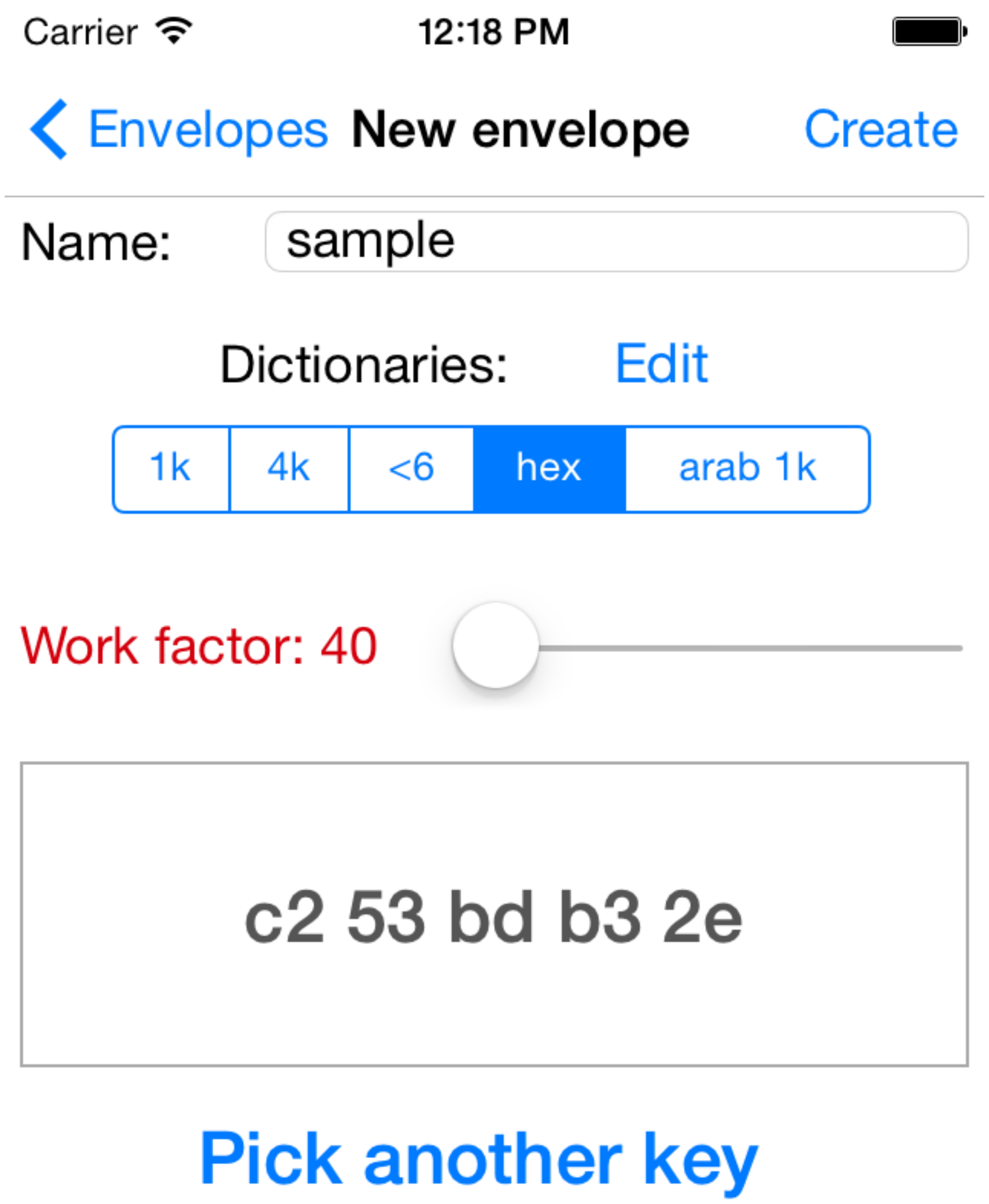


Name: sample

Dictionaries: 1k [✓ 4k] <6 hex arab 1k

Work factor: 40

absorbed church representative correct

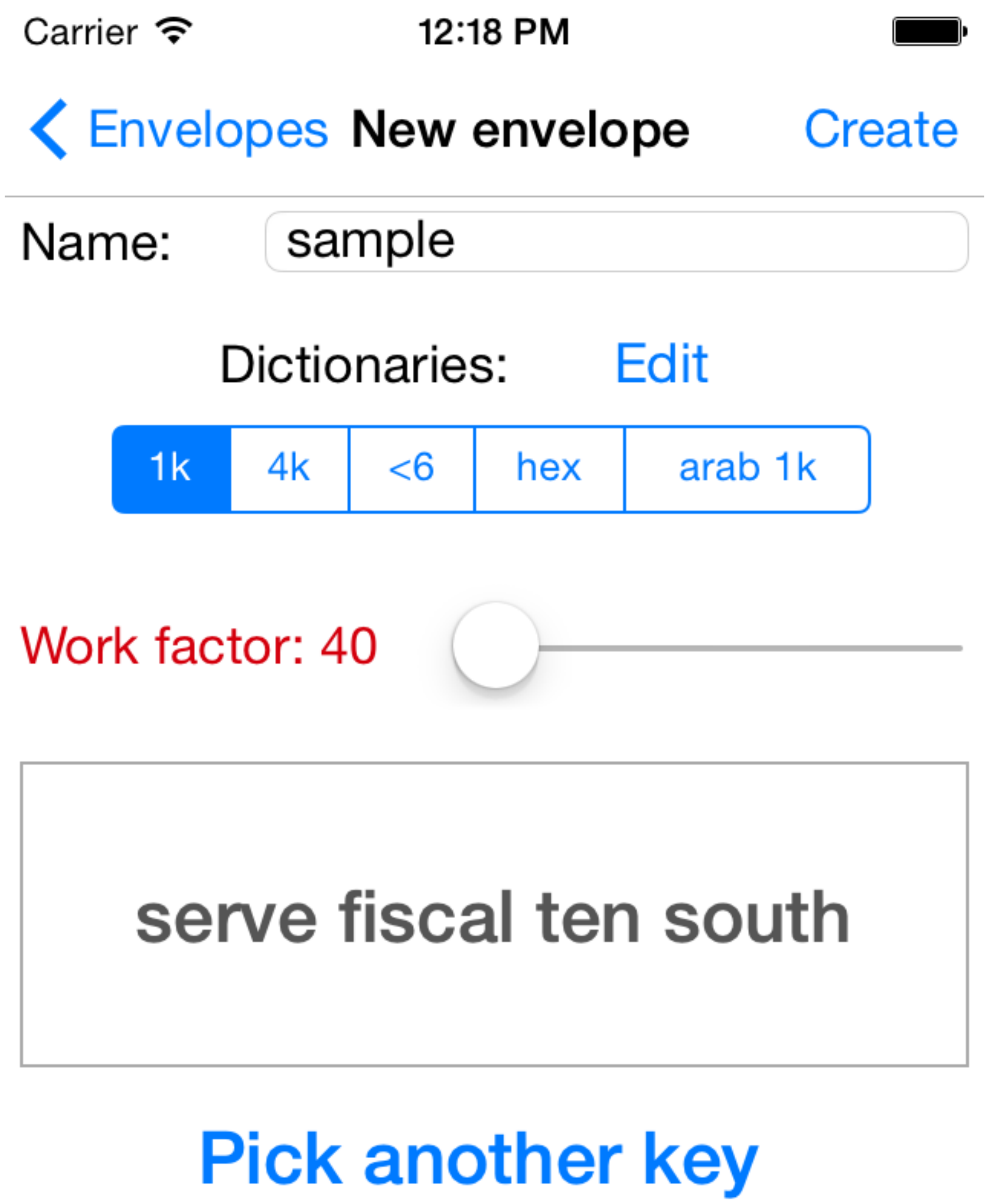


Name: sample

Dictionaries: 1k 4k <6 [✓ hex] arab 1k

Work factor: 40

c2 53 bd b3 2e



Carrier 12:18 PM

Envelopes New envelope Create

Name: sample

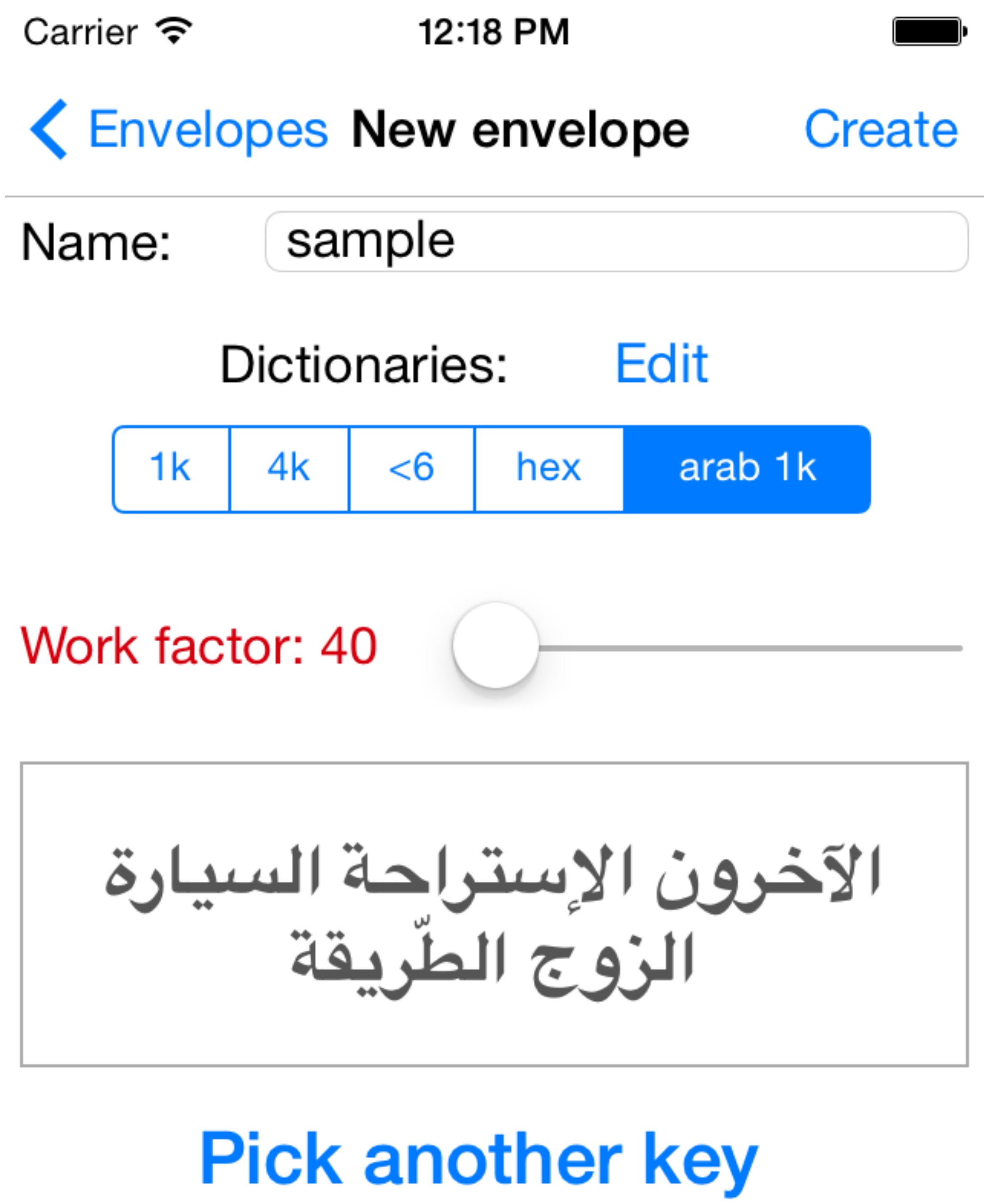
Dictionaries: Edit

[✓ 1k] | 4k | <6 | hex | arab 1k

Work factor: 40

serve fiscal ten south

Pick another key



Carrier 12:18 PM

Envelopes New envelope Create

Name: sample

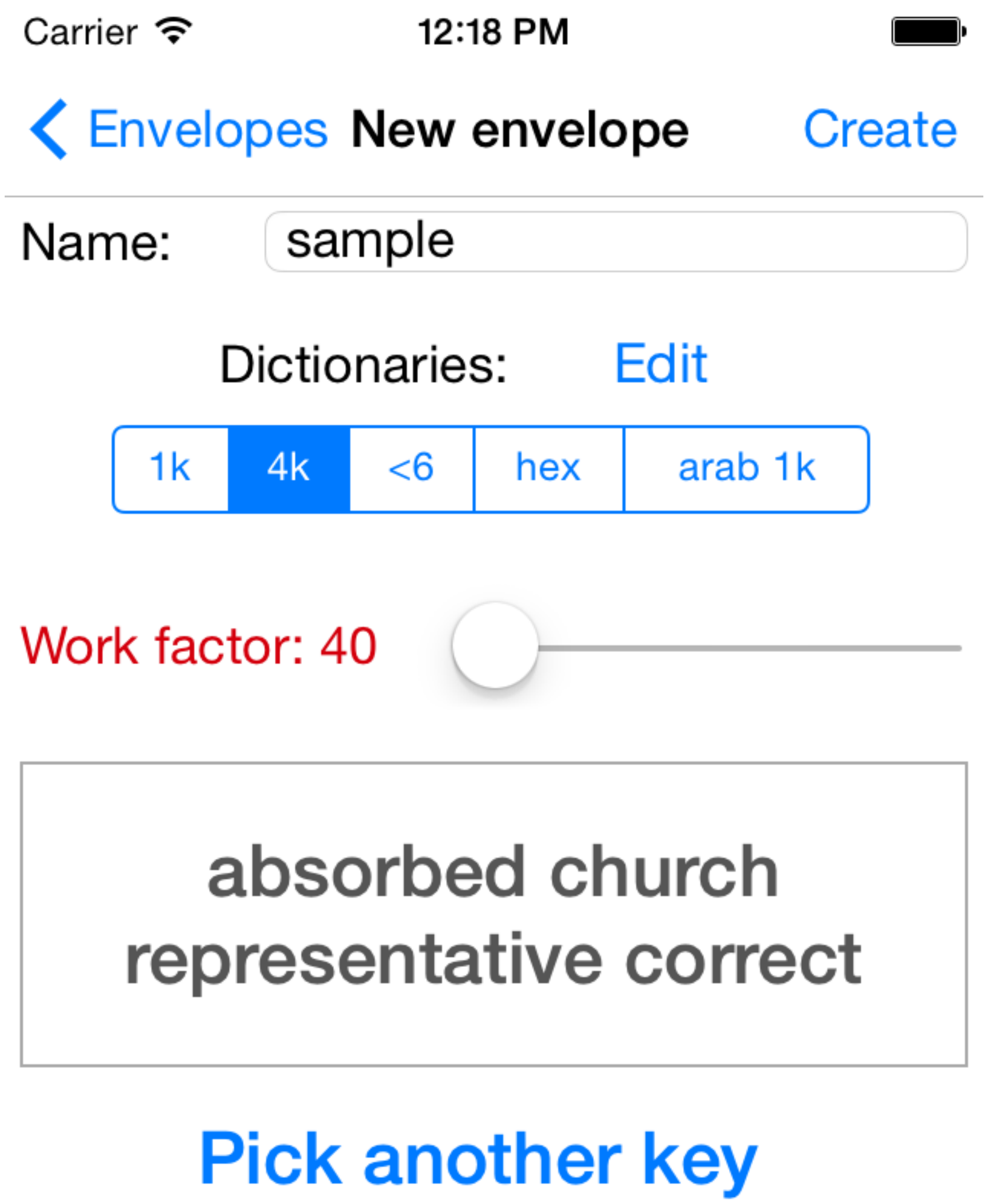
Dictionaries: Edit

1k | 4k | <6 | hex | [✓ arab 1k]

Work factor: 40

الآخرون الإستراحة السيارة
الزوج الطّريقة

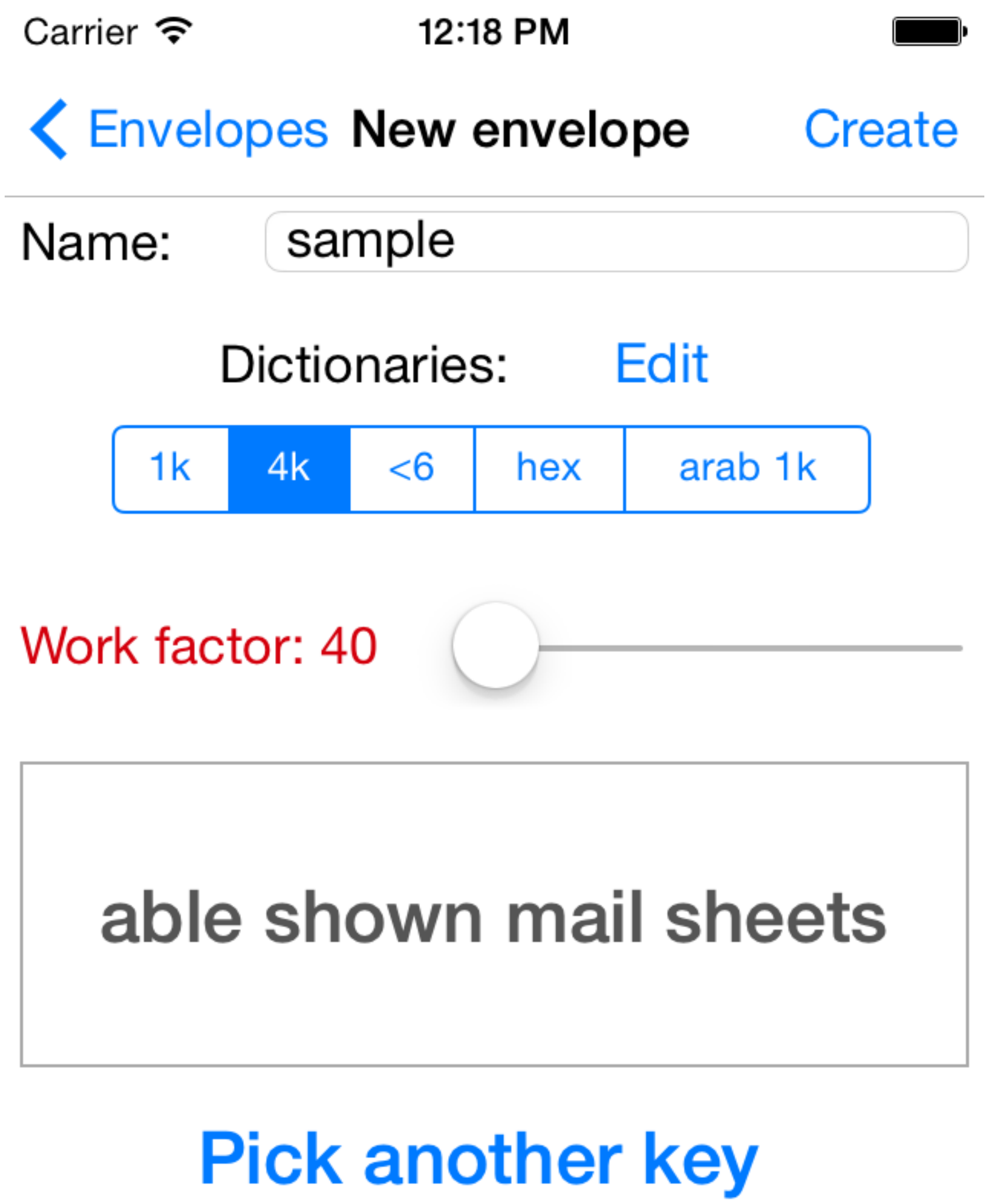
Pick another key



Name: sample

Work factor: 40

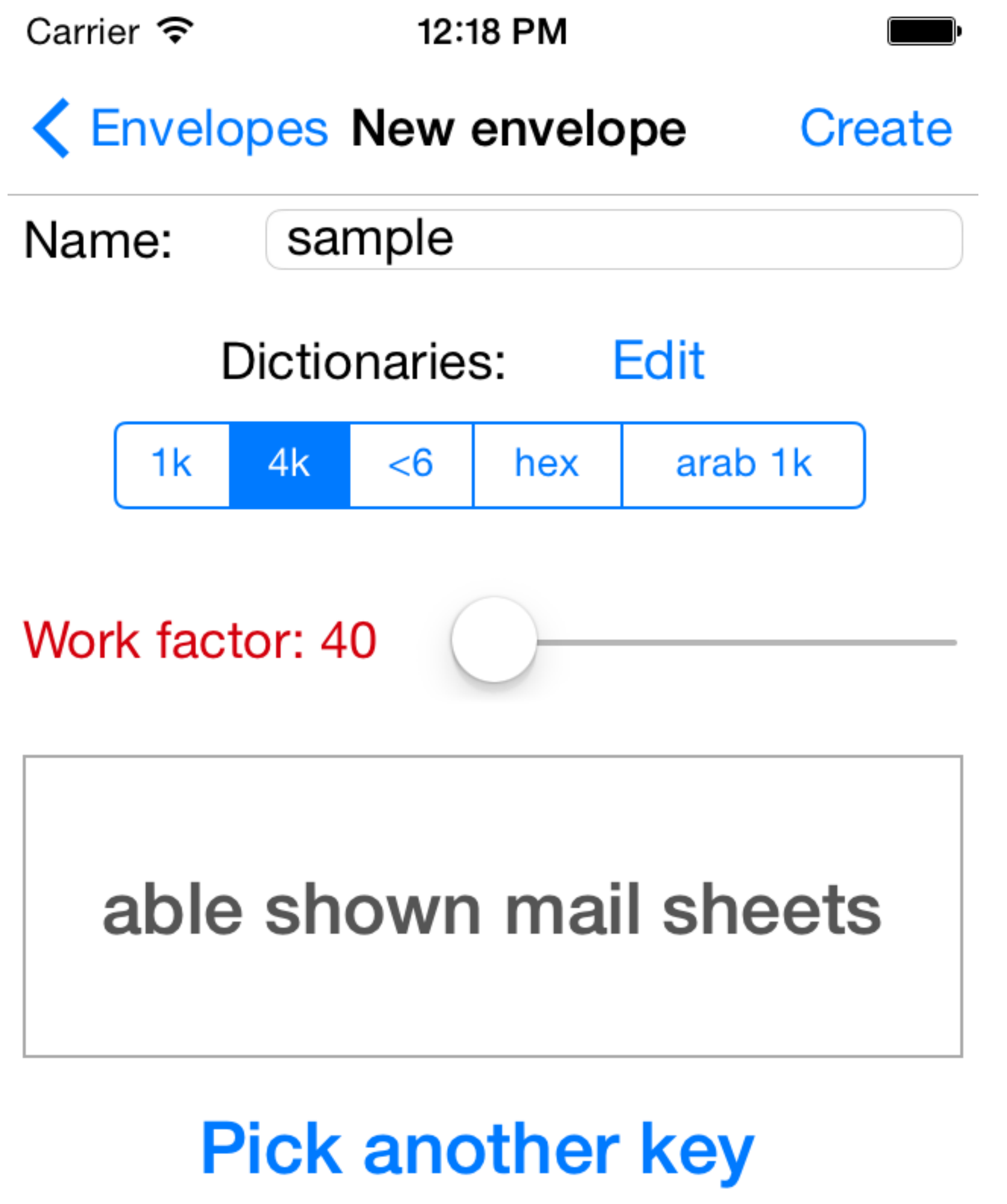
absorbed church representative correct



Name: sample

Work factor: 40

able shown mail sheets

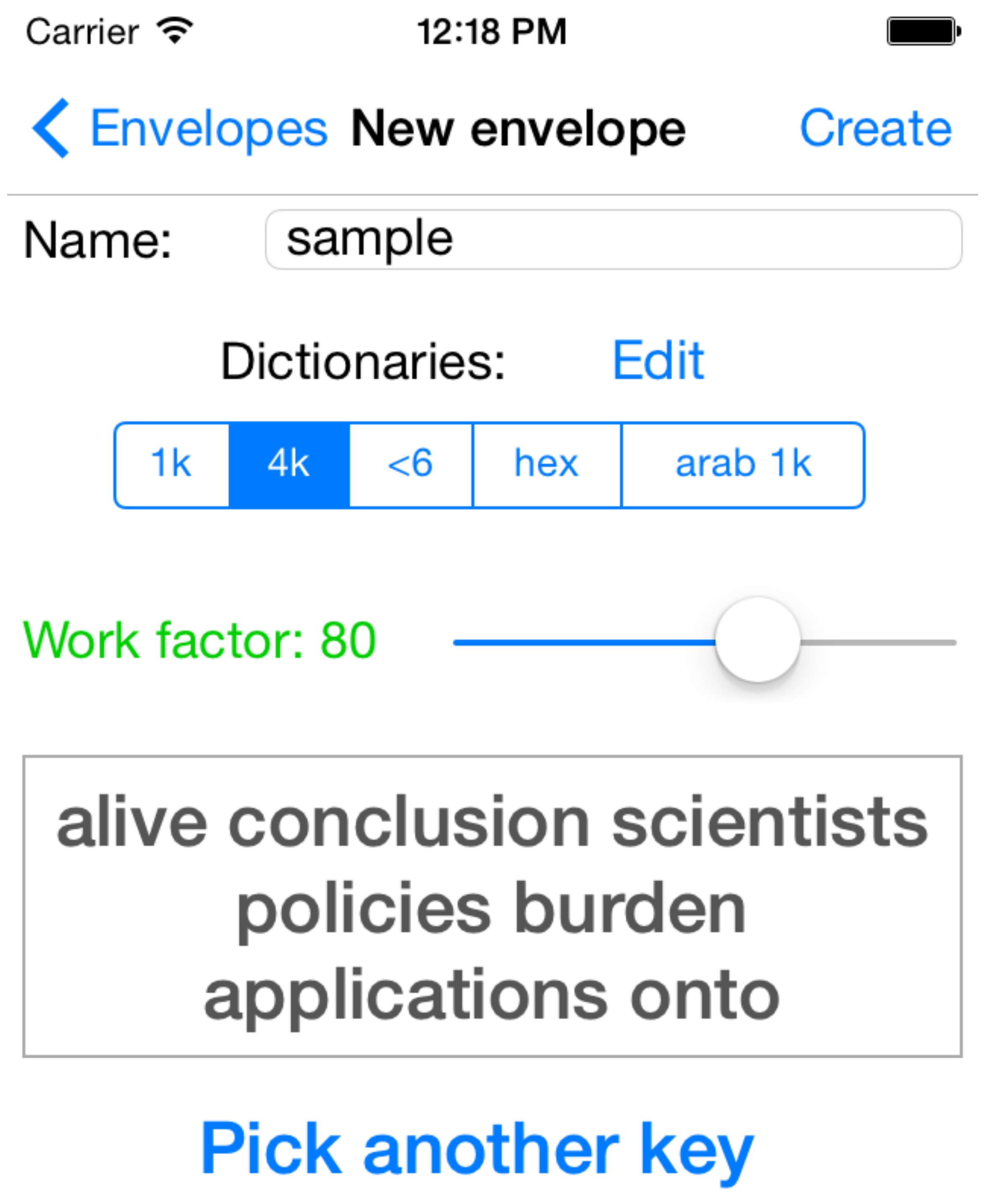


Name: sample

Dictionaries:

Work factor: 40

able shown mail sheets

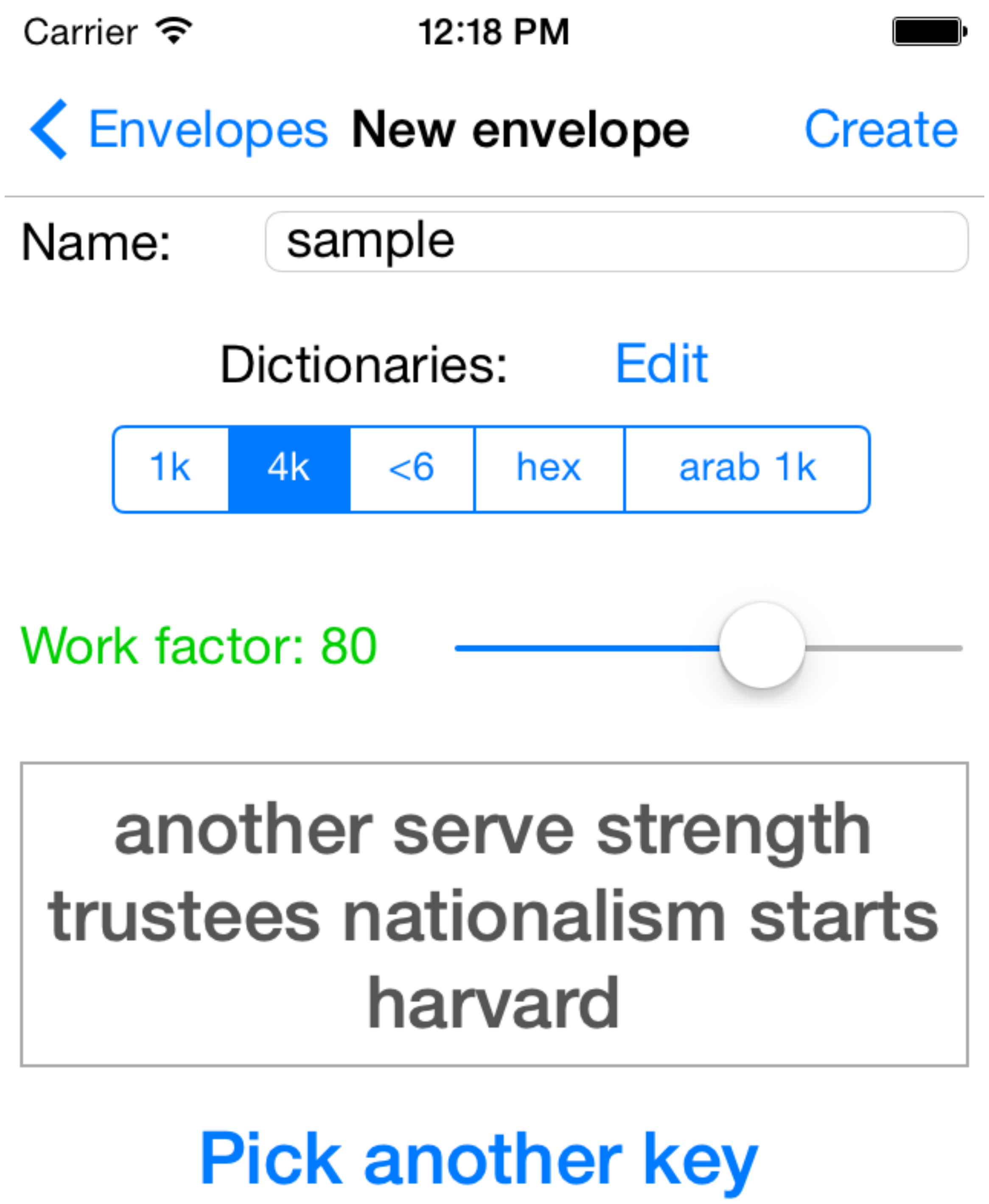


Name: sample

Dictionaries:

Work factor: 80

alive conclusion scientists policies burden applications onto



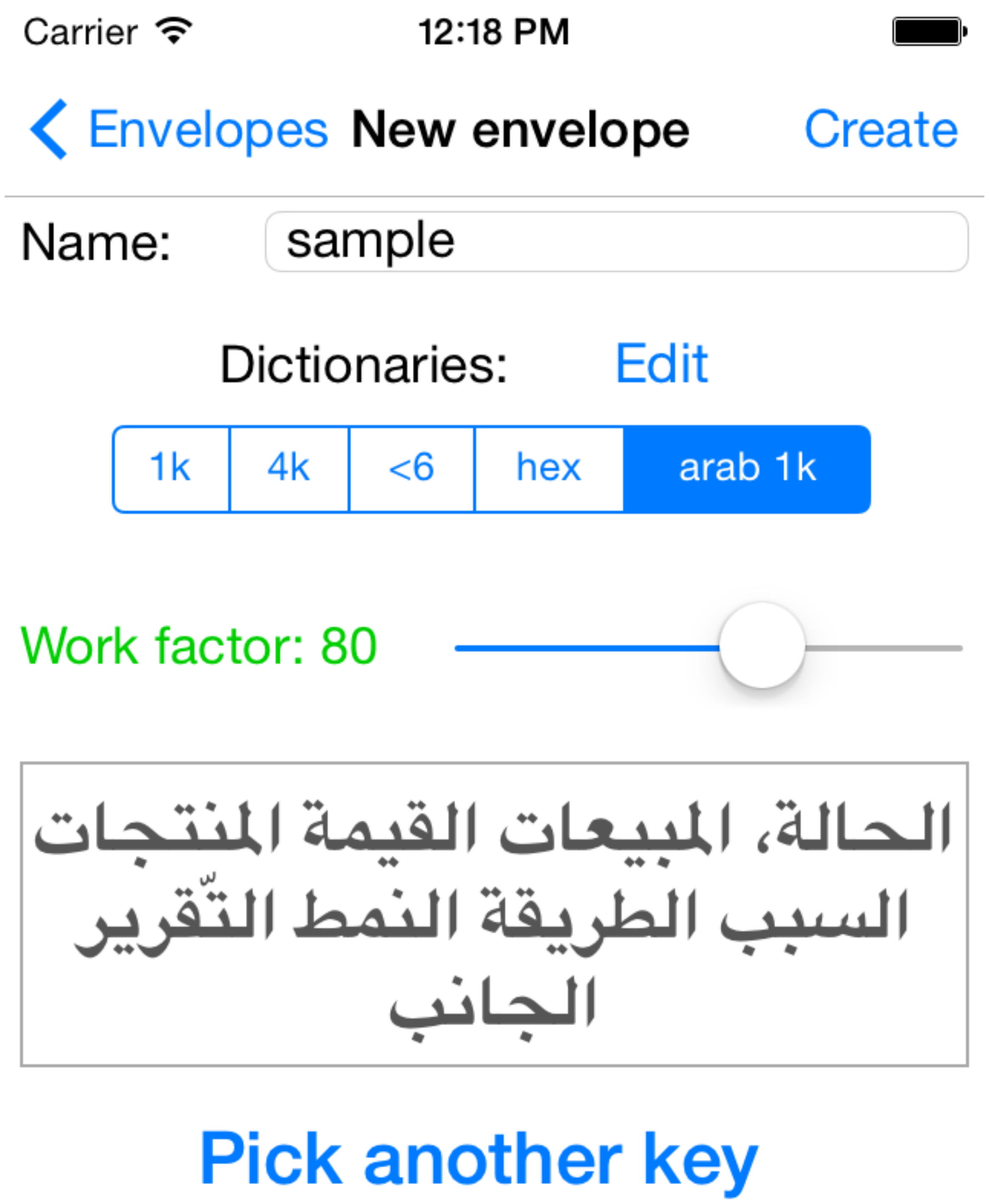
New envelope

Name: sample

Dictionaries: 1k [✓ 4k] <6 hex arab 1k

Work factor: 80

another serve strength trustees nationalism starts harvard



New envelope

Name: sample

Dictionaries: 1k 4k <6 hex [✓ arab 1k]

Work factor: 80

الحالة، المبيعات القيمة المنتجات
السبب الطريقة النمط التّقرير
الجانب

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

For me, what’s next?

- 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