

# Fun With Research

**Bill Cheswick**  
**ches@cheswick.com**

# Outline

- **A short bio with some observations that I hope will be helpful**
- **A brief look at some opportunities you might want to think about**
- **What is research like?**
- **Some current research on passwords**

**WDY WTB WYGU?**

**WKO SDY LTD?**

**Bio**



# Key: right place at the right time

- **Don't be the smartest person in the room, at least not all the time.**
- **Go to conferences. Hang out with the leaders, and the keynote speakers.**
- **This can be gamed, with a little luck**
  - **look for exponential growth**
  - **(this is true with stock picking, too.)**
- **The result can be fame and fortune, while you are having fun and changing the world**
- **You might create a new job!**

# Waves of the future

- **Genetics**
- **Diseases**
- **Plant research**
- **Advanced and cheap engineering**
- **Big Data**

# Genetics

- **gene sequencing is getting cheaper at near exponential rates**
- **we are only starting to understand what it all means**
- **combine with micro fluidics, electronic circuits**

# Human diseases

- **We know we can cure a number of diseases**
  - malaria
  - dracunculosis (Guinea worm, almost done)
  - measles
  - schistosomiasis
  - anything that requires humans in the reproductive cycle
- **Aging is a disease**

# Plant research

- **not quite as busy a field**
- **extremely important**

# Advanced engineering on the cheap

- **the world needs an \$8 kitchen stove that lasts a long time and doesn't dump smoke in the house**
- **a \$300 paper house that lasts a year in all sorts of weather (it has been done)**
- **aim high: most poor Africans would love to own a used Toyota**
- **it is hard to make big advances in materials science, but they are valuable**
  - **batteries**

# Big data

- **“disk” storage space is getting exponentially cheaper**
- **cameras, microphones, GPS are everywhere**
- **all this calls for vast processing and analysis**
  - **system and data administration**
  - **statistics**
- **this is a lucrative and dangerous technology**
  - **want to help us get it right?**

# Problems to solve

- **we can greatly improve teaching**
- **this grade system was designed to create good factory workers**
- **some learning styles fare much better than others**
- **insidious problem: addictive computer games**
- **Build first world solutions**



# What's possible

- **Diamond window glass**
  - It's just carbon!
- **Energy from the sun**
  - sunlight has enough energy to split water
- **Gasoline is not evil**
  - it can be a renewable resource!
- **Human body parts**
  - raw materials are cheap, we just need some smarts

# What's possible (cont)

- **Let's get good at nuclear power**
- **energy can get much cheaper**
- **there is a lot of water in the world**
- **we know how to make people rich**
- **we know how to cut family sizes**

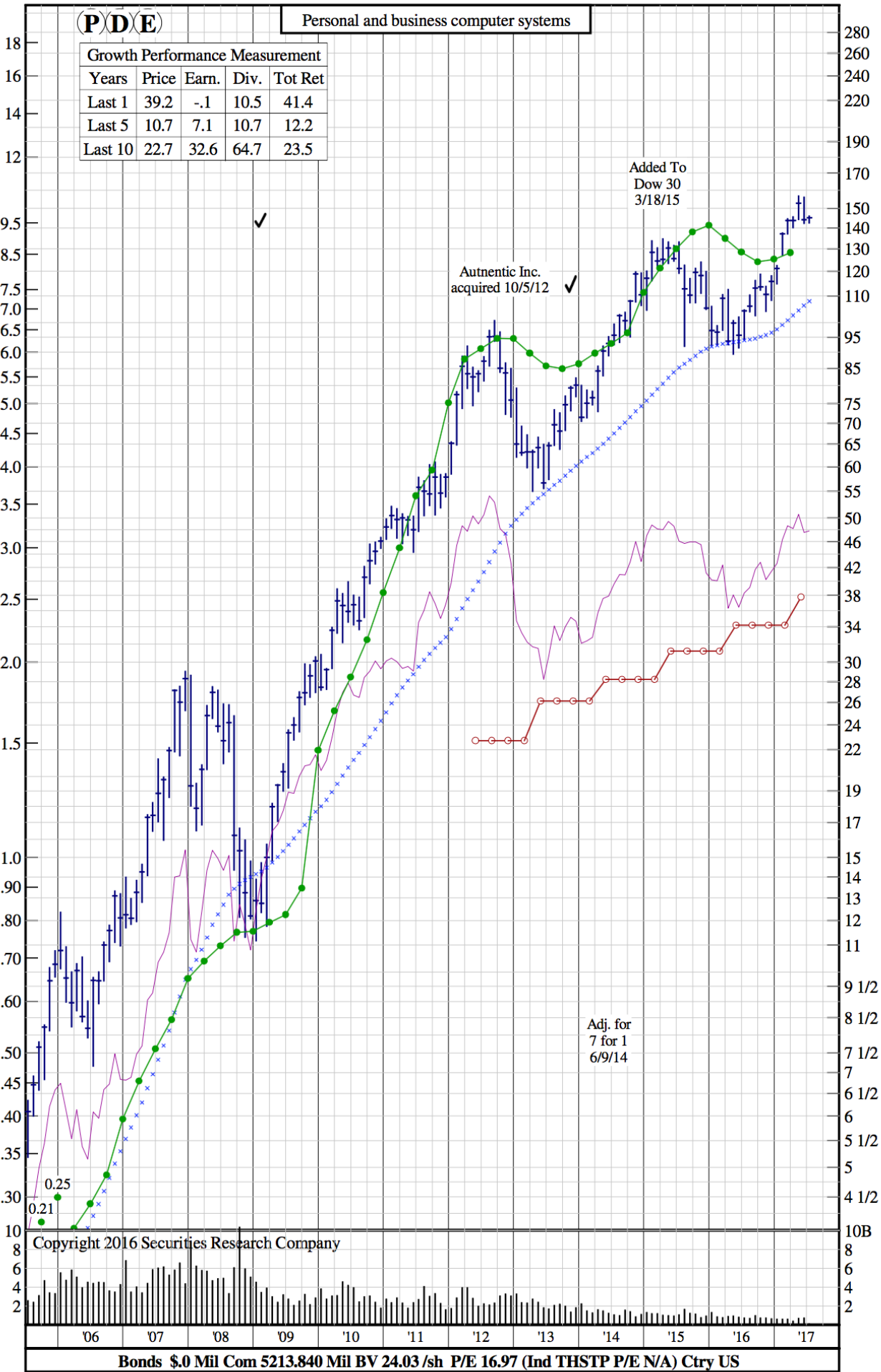
# Advice from your future self

- **Take good care of your teeth. You are going to be old for a long time**
- **Start saving soon for old age: don't expect the government to help you out**
  - **learn how to invest long term**
- **avoid fruit juices and sugared sodas (and maybe any sodas)**

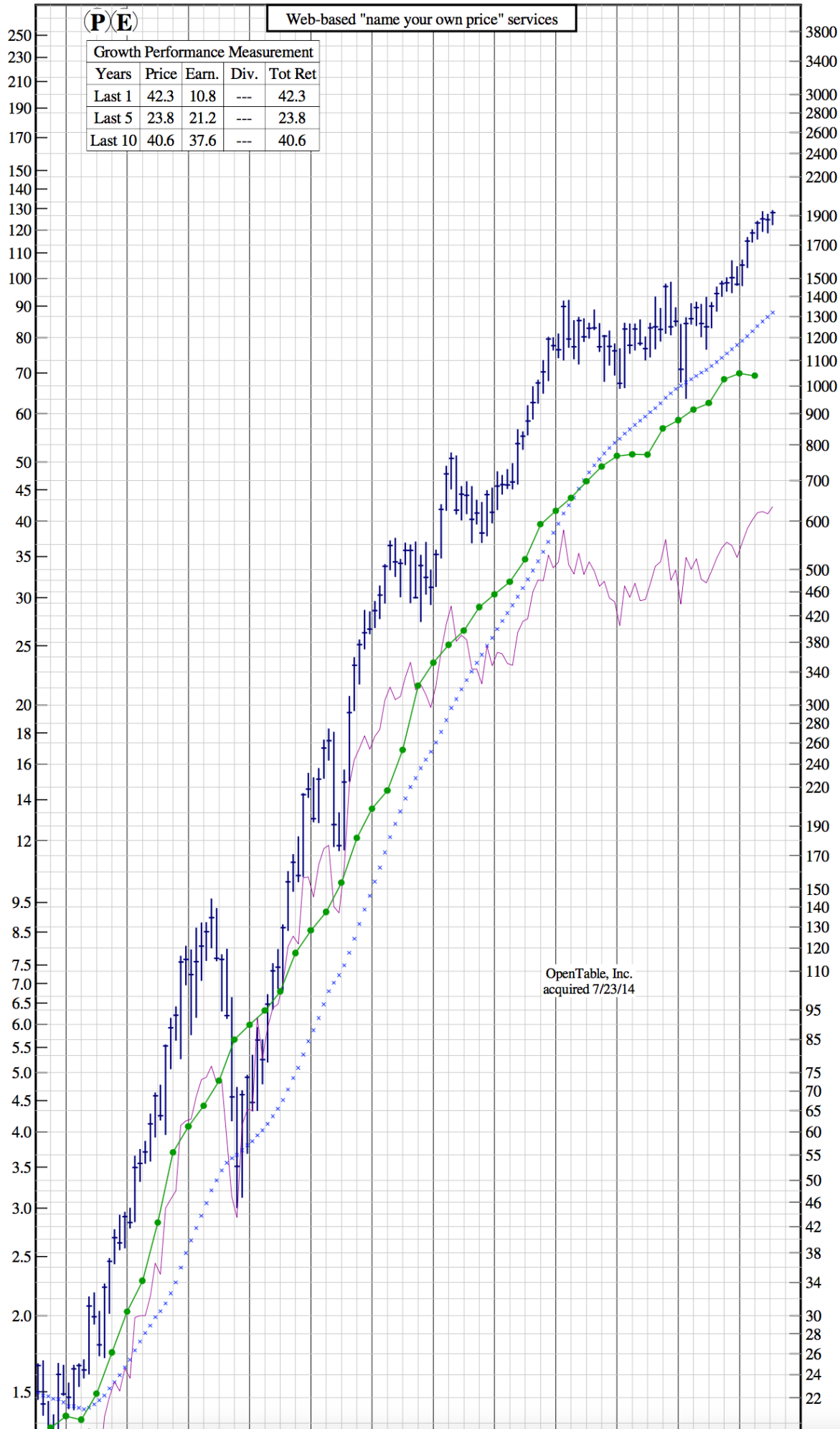
# Money

- **Pick growing businesses, industries, research areas**
- **Money doesn't have to be a goal, but life is better if it isn't a problem**
- **Start saving immediately: 10+10**
  - **do not expect the government to be there for you in old age**
  - **that means at least \$1million (present value) in the bank when you are 65!**

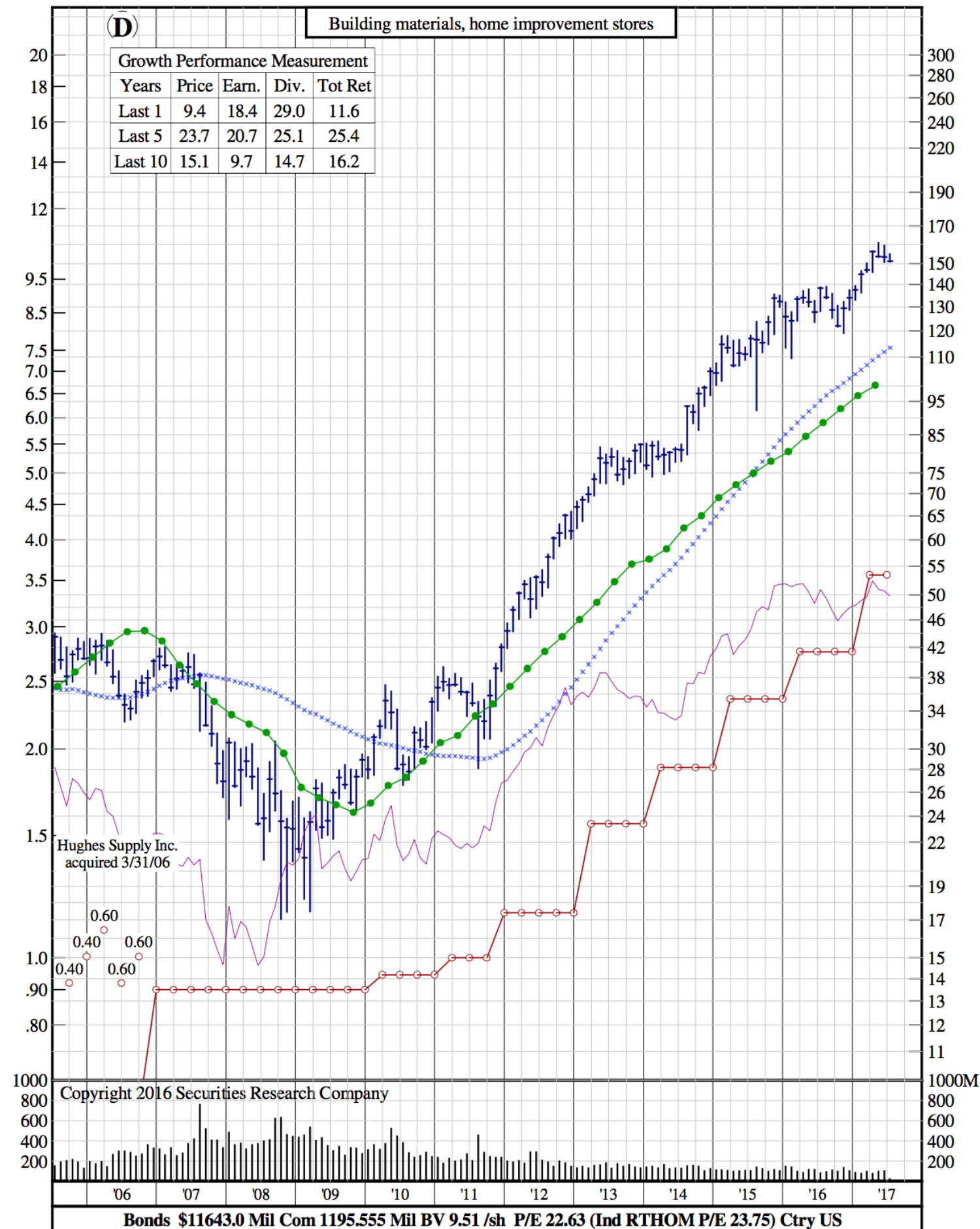
APPLE INC (AAPL)



PRICELINE GRP INC (PCLN)



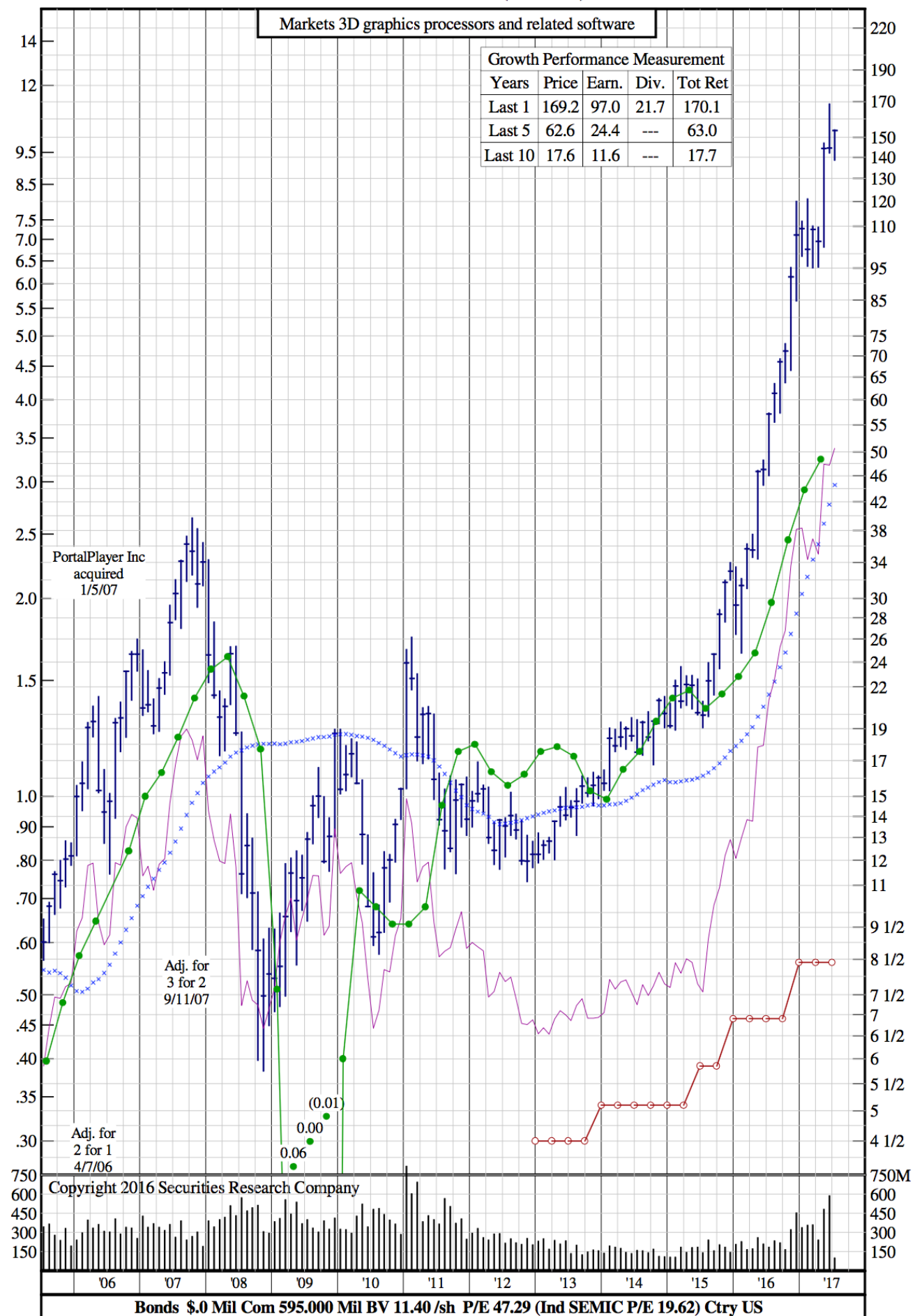
# HOME DEPOT INC (HD)



# NVIDIA CORP (NVDA)

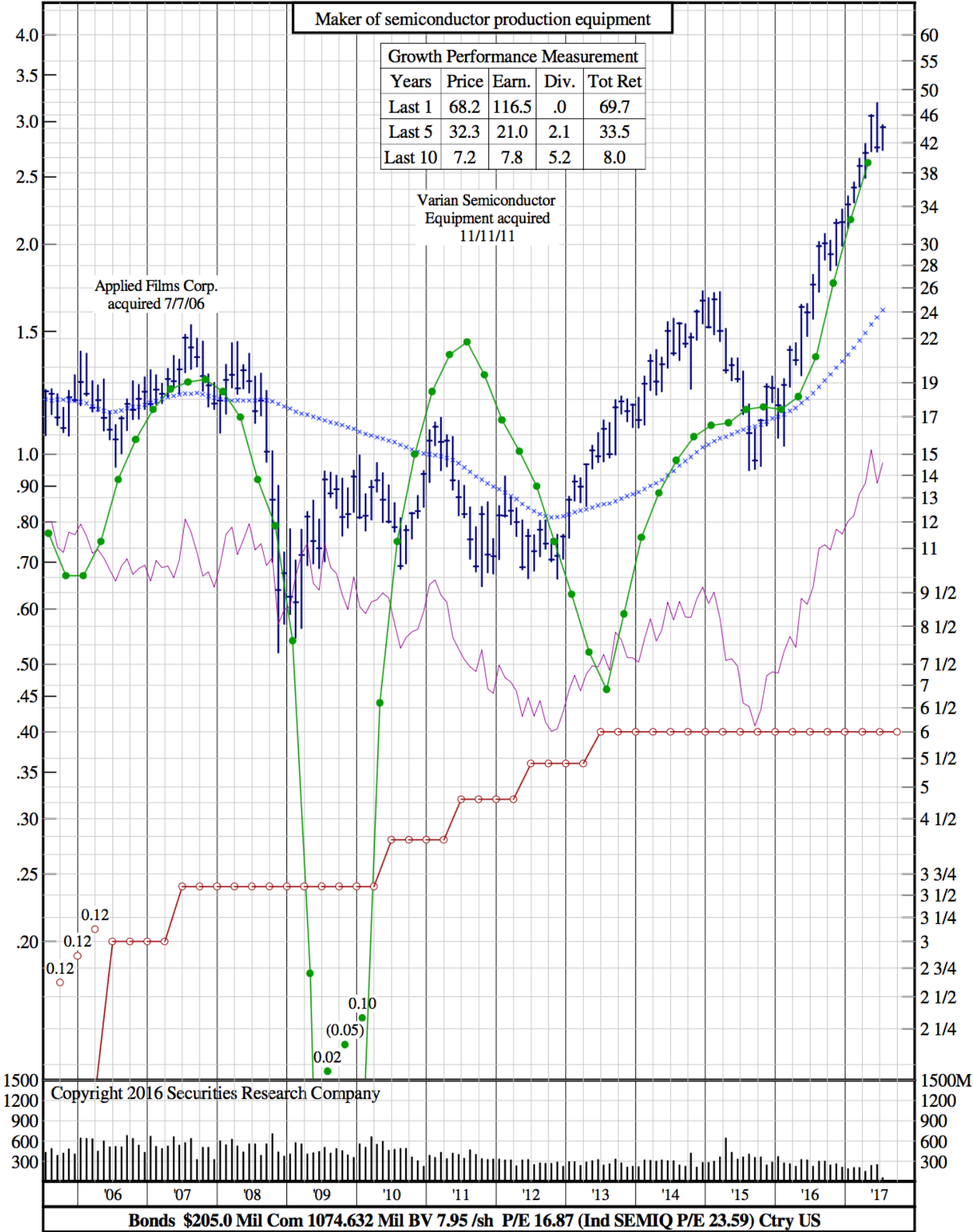
Markets 3D graphics processors and related software

Growth Performance Measurement				
Years	Price	Earn.	Div.	Tot Ret
Last 1	169.2	97.0	21.7	170.1
Last 5	62.6	24.4	---	63.0
Last 10	17.6	11.6	---	17.7

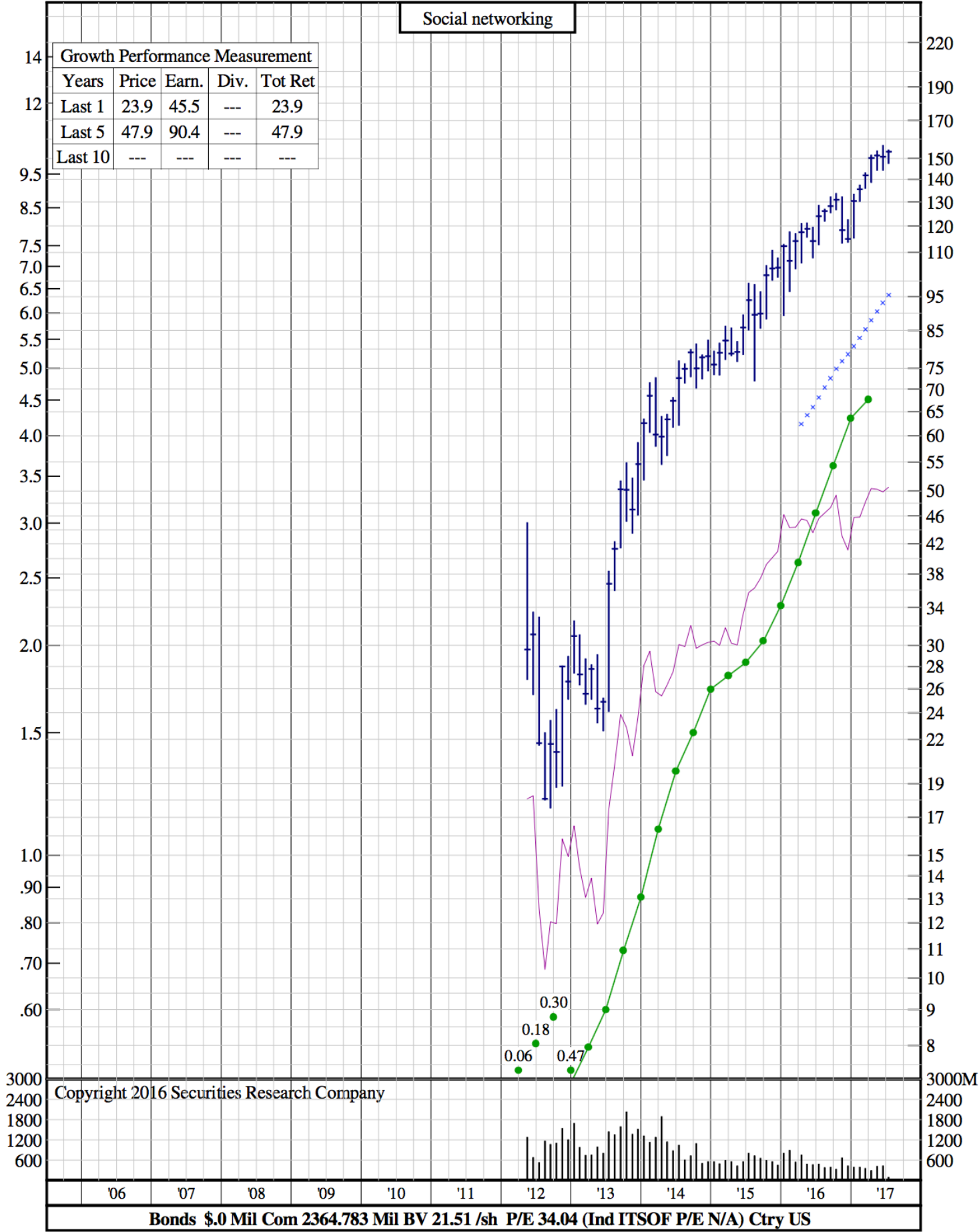




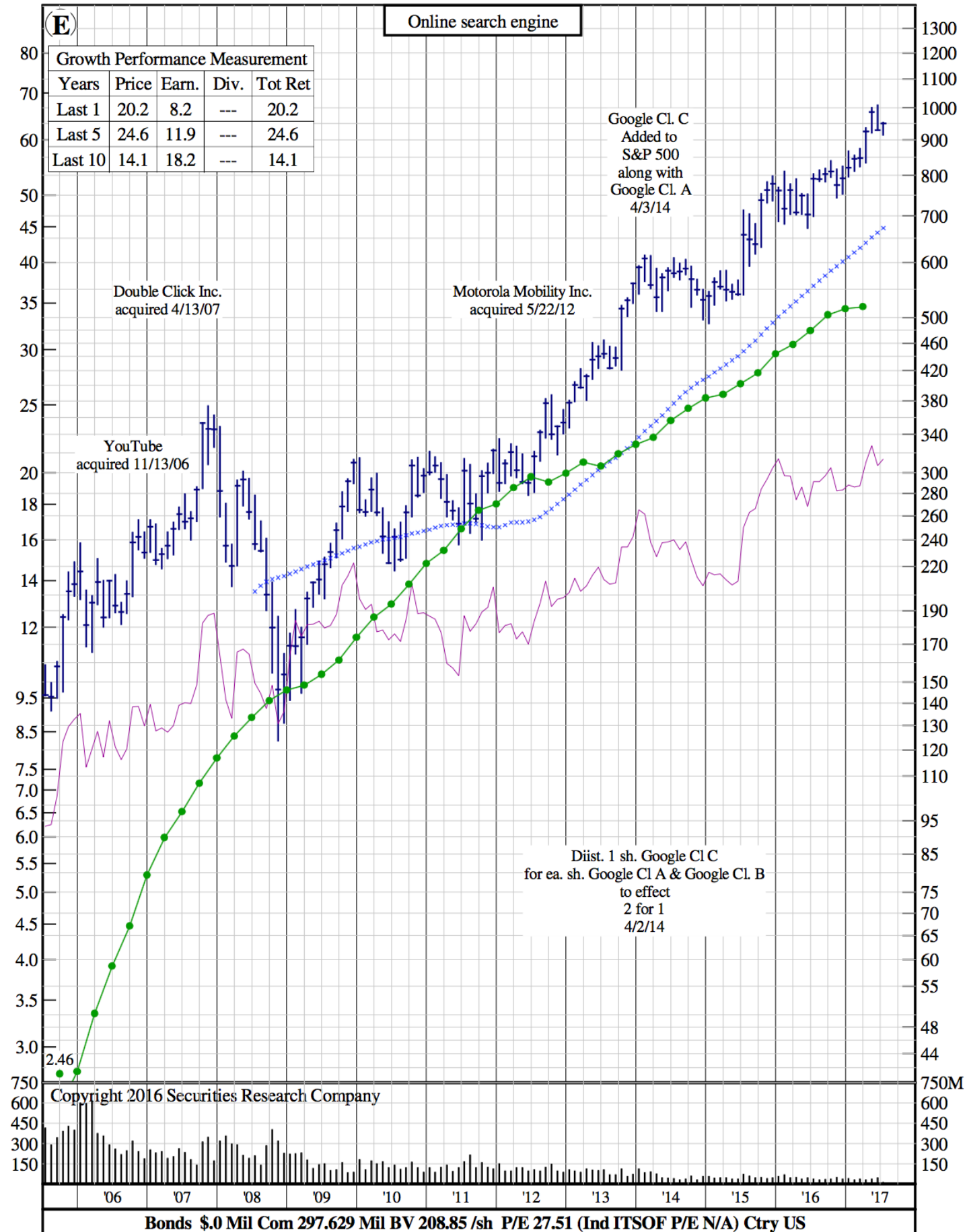
APPLIED MATERIALS INC (AMAT)



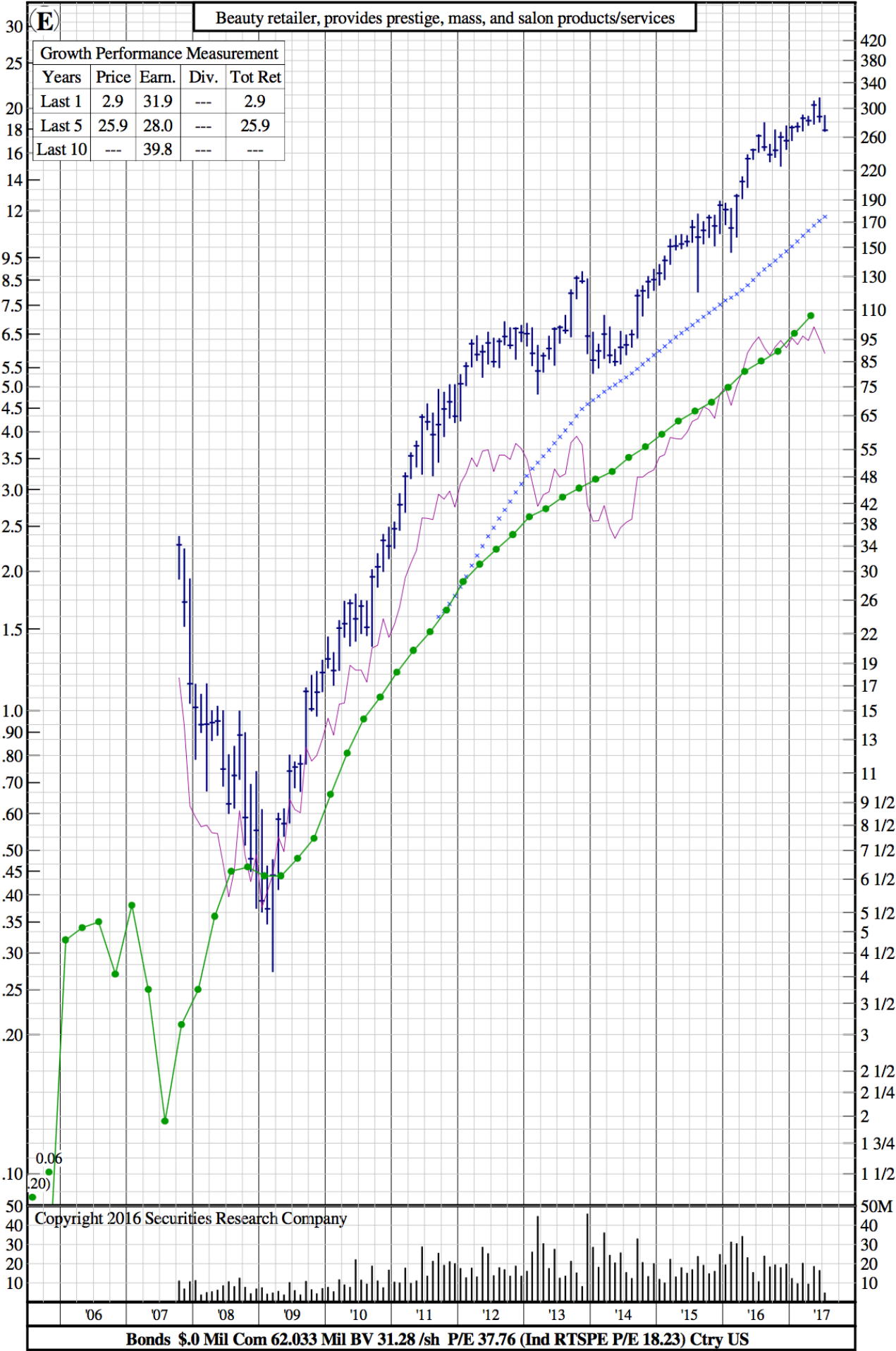
FACEBOOK INC (FB)



# ALPHABET INC (GOOGL)



ULTA BEAUTY INC (ULTA)



# Research

- **government**
  - **probably under major funding squeeze over your lifetimes (not a good sign).**
- **academic**
  - **teach, publish, or perish. Get your PhD, write grant proposals, and do awesome stuff.**
- **corporate**
  - **alas, a fading opportunity. I apologize: it was a magnificent ride**

# Rethinking Passwords

# Intel's rules

- The password must be **at least 8 characters long**.
- The password **must** contain at least:
  - **one** alpha character [a-zA-Z];
  - **one** numeric character [0-9];
  - **one** special character from this set:  
` ! @ \$ % ^ & \* ( ) - \_ = + [ ] ; : ' " , < . > / ?
- The password **must not**:
  - **contain spaces**;
  - **begin with an exclamation [!] or a question mark [?]**;
  - **contain your login ID**.
- The first 3 characters cannot be the same.
- The sequence of the first 3 characters cannot be in your login ID.
- The first 8 characters cannot be the same as in your previous password.
- Passwords are treated as **case sensitive**.

# Golden Rule Health

PASSWORD RULES (Please note the password is case sensitive)

Must contain at least 8 characters.

Must include a number and a letter.

No more than two consecutive characters may be the same.

Passwords must be changed at least every 180 days.

No password may be re-used for a period of 1 year.

3 invalid attempts to login will result in a 30 minute lockout.



# Wachovia (now Wells Fargo)

Passwords must be 7-20 characters

Must include at least one letter and one number, with no spaces

Semi-colons cannot be part of a Password

Passwords are case sensitive

Do not use your User ID as your Password

# Dartmouth

- It should be **eight characters long** using only numbers and **upper- and lower-case letters**. **Note:** Passwords longer than eight characters will not work to authenticate you with some applications used at Dartmouth, such as Kerberos and Oracle Calendar.
- There can be **no more than four characters in sequence** (e.g., **12345** or **abcde** are not allowed).
- It must contain at least **five different characters** (e.g., **2a3a2a3a** only contains three different characters so is not allowed).
- It **cannot be a word found in the dictionary, including foreign languages** (e.g., **password**).
- It cannot be a **reversal of a word found in the dictionary** (e.g., **drowssap**).
- It cannot be a **word found in the dictionary, plus one additional character** either before or after the word (e.g., **xalgebra** or **algebrax**).
- It cannot be a word found in the dictionary with numbers substituted for look-alike letters (e.g., **passw0rd** or **pa55word**).
- It cannot be a word found in the dictionary minus any punctuation, symbols, or numbers (e.g., **oclock** or **soninlaw**).

	length	case sens.	A-Z	a-z	0-9	sym	OK	not OK
Intel	>=8	Yes	R	R	R	ok		<u>          </u>
Golden Rule	>=8							
Wachovia	7-20	Yes	ok	R		no		
Dartmouth	8		ok	ok	ok	no		
AT&T Uvers	6-24	Yes	R		R	no	<u>          </u>	
AT&T GNO	5-8	No						
OAG	7-50	Yes	R		R			<u>          </u> ‘ “
War-craft	8-16		R		R			-! " # \$
DHS	8-15		R		R			<u>          </u>
Calnet	9-255		3	3	3	3	<u>          </u>	
UAL	6-24	No						
Lehigh	>=7		2	2	2	2		

# These “eye-of-newt” rules are not user-friendly

- **hard to remember**
- **hard to type**
- **doesn't increase the search space (password strength) that much**
- **Enforcing these rules excludes genuinely strong and easier pass phrases**

Fillet of a fenny snake,  
In the cauldron boil and bake;  
Eye of newt and toe of frog,  
Wool of bat and tongue of dog,  
Adder's fork and blind-worm's sting,  
Lizard's leg and howlet's wing,  
For a charm of powerful trouble,  
Like a hell-broth boil and bubble.

-- Macbeth, Act 1, Scene 1

**Use A Different Password on each  
System**

# **Change Your Password Frequently**

**Don't Reuse Passwords**



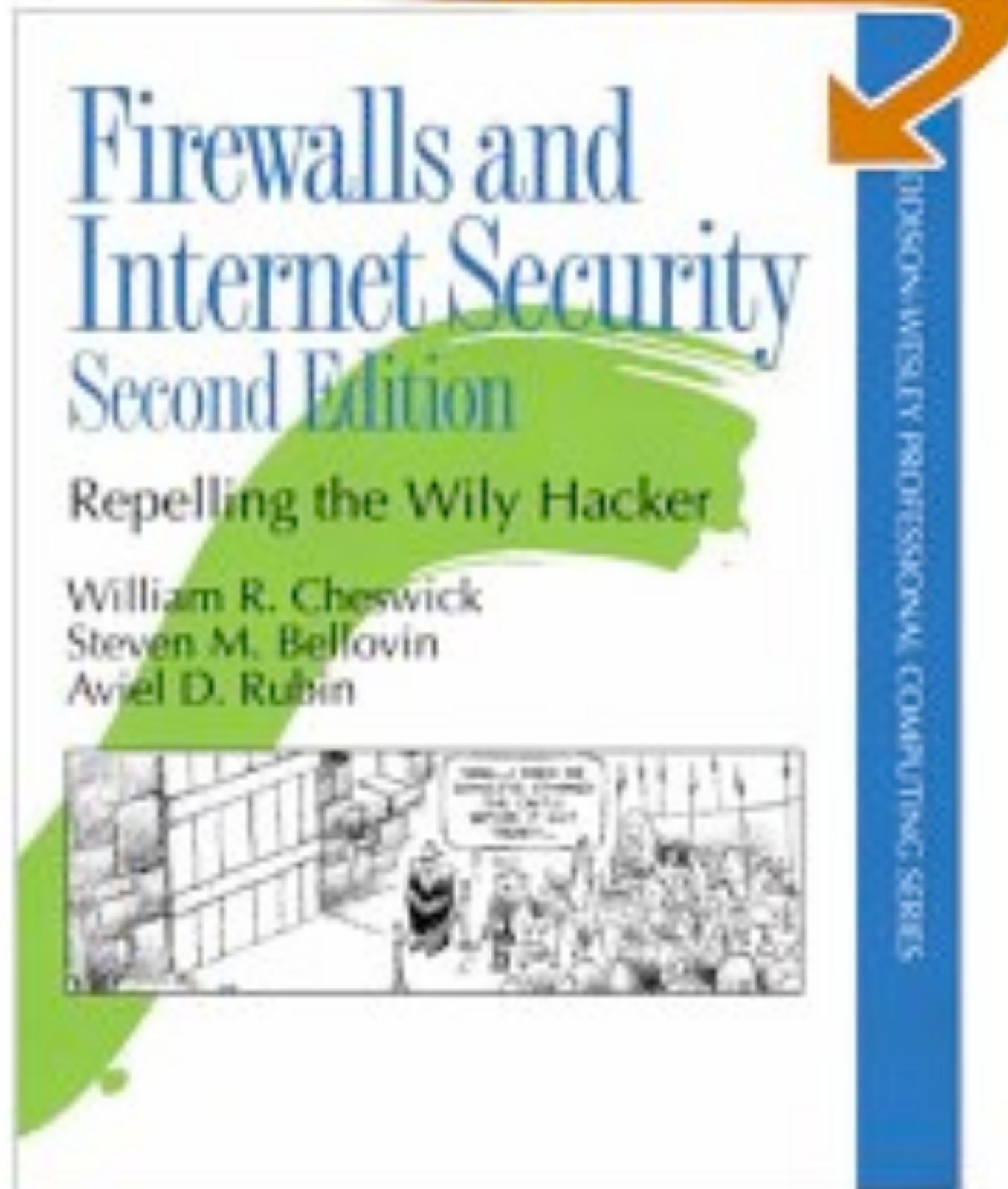
**Don't Write Your Password Down**

**This is a usability nightmare!**

**Who's responsible for this?**

Well, I am, a Little

SEARCH INSIDE!™



**What are these rules for?**

# Dictionary Attacks

# Dictionary Attacks

- **Have a computer try as many password guesses as possible**
- **The required effort is called the “work factor”, and the resistance to attack is often (incorrectly) called the “entropy” of the password.**
- **These attacks can be directed at online authentication services, or against stolen hashed password files.**

[mail.coastal.cheswick.com](mailto:mail.coastal.cheswick.com) login failures:

Sep 21 03:11:03 mail sshd[90325]: Invalid user cgi from 219.139.108.134  
Sep 21 03:11:15 mail sshd[90335]: Invalid user oracle from 219.139.108.134  
Sep 21 03:11:18 mail sshd[90337]: Invalid user tomcat from 219.139.108.134  
Sep 21 03:11:47 mail sshd[90361]: Invalid user nagios from 219.139.108.134  
Sep 21 04:50:29 mail sshd[54849]: Invalid user devtest from 58.213.48.82  
Sep 21 04:50:33 mail sshd[54851]: Invalid user dede from 58.213.48.82  
Sep 21 04:51:49 mail sshd[54895]: Invalid user anja from 58.213.48.82  
Sep 21 04:51:55 mail sshd[54897]: Invalid user anja from 58.213.48.82  
Sep 21 04:51:59 mail sshd[54899]: Invalid user platinum from 58.213.48.82  
Sep 21 04:52:03 mail sshd[54901]: Invalid user plcmspip from 58.213.48.82  
Sep 21 04:52:06 mail sshd[54903]: Invalid user teamcity from 58.213.48.82  
Sep 21 04:52:13 mail sshd[54905]: Invalid user teamspeak from 58.213.48.82  
Sep 21 04:59:33 mail sshd[55143]: Invalid user addr from 58.213.48.82  
Sep 21 04:59:37 mail sshd[55145]: Invalid user adempiere from 58.213.48.82  
Sep 21 04:59:40 mail sshd[55147]: Invalid user admin2 from 58.213.48.82  
Sep 21 04:59:43 mail sshd[55149]: Invalid user admin from 58.213.48.82  
Sep 21 04:59:57 mail sshd[55157]: Invalid user admin from 58.213.48.82  
Sep 21 05:00:02 mail sshd[55159]: Invalid user admin from 58.213.48.82  
Sep 21 05:00:05 mail sshd[55177]: Invalid user adminftp from 58.213.48.82  
Sep 21 05:00:08 mail sshd[55179]: Invalid user adminhelp from 58.213.48.82  
Sep 21 05:00:12 mail sshd[55181]: Invalid user admin from 58.213.48.82  
Sep 21 05:00:15 mail sshd[55183]: Invalid user admin from 58.213.48.82





# ***Where Do Security Policies Come From?***

**Dini Florêncio and Cormac Herley**

**SOUPS 2010**

**Those that accept advertising, purchase  
sponsored links, or user has a choice have  
weakest password requirements**

**Strongest passwords: .gov, then .edu**

# These rules come from the Deep Past in computing and security

- **Time sharing terminals in public places**
- **Attacks on the login interfaces on network services**
- **Network eavesdropping was often trivial**
- **The stakes were usually much lower**
- **Institutionalized passwords on, say, telephone switches**
- **Changing passwords: lost military crypto gear**

# CSC-STD-002-85: DOD Password Management Guideline

- **The “green book”.**
- **A variety of mostly-excellent security suggestions**

Scheme	Cracked in		Change time	
8 character, full alphanumeric	6.72	mins.	0.40	ms.
8 character, EoN	9.25	days	31.19	ms.
11 character, EoN	20,390	years	7.4	days
13 character, full alphanumeric	906,123	years	331	days
12 character, Eye-of-newt	1,896,229	years	692	days

# The Dictionary Attack Arms Race

- **Moore's Law: 12 doublings since 1990**
  - **Look for outdated assumptions!**
- **And multi-core CPUs are perfect for password cracking**
- **Can a human choose and remember a password that a computer can't guess when limited only by computer speed and time available?**
- **Guessing rates can be  $8 \times 10^9$  guesses per second per CPU!**

# 100 Most Influential People in IT

## eWeek, 2008-04-04

### **96. Dave Winer**

**Software developer and entrepreneur**

Winer is the developer of RSS.

### **97. Thornton May**

**Florida Community College, IT Leadership Academy**

May is a noted technology futurist.

### **98. William**

**Cheswick**

**Lead member of technical staff, AT&T Labs**

Cheswick continues to innovate in the area of communications research.

### **99. Chris Anderson**

**Author**

Anderson, editor in chief of Wired, proffered the notion of the niche in his book, "The Long Tail: Why the Future of Business Is Selling Less of More."

### **100. Ben Bernanke**

**Chairman, Federal Reserve Board**

No one will have a bigger impact on the fate of the nation's banks and financial services companies, interest rates, or access to credit.



# A note on Grandma



# What are the most common current threats

- **Keystroke loggers**
- **Phishing attacks**
- **Password database compromise**



# None of these are grandma's fault!

- ***Users are Not the Enemy*, A. Adams and M.A. Sasse, *Commun. ACM*, 42(12), 1999.**

***It is simply poor engineering to  
expect people to select and  
remember passwords that are  
resistant to dictionary attacks***

# Results

- **People violate many of these rules routinely, for usability reasons**
- **Stringent rules increase use of fall-back systems, which are usually less secure, or more expensive**
- **The rules don't make most things more secure in the face of most current threats**

# **Some Password Ideas**

**From academia, and me**

**For a complete survey, see**

- <http://people.scs.carleton.ca/~paulv/papers/gpsurvey-27sept2010.pdf>



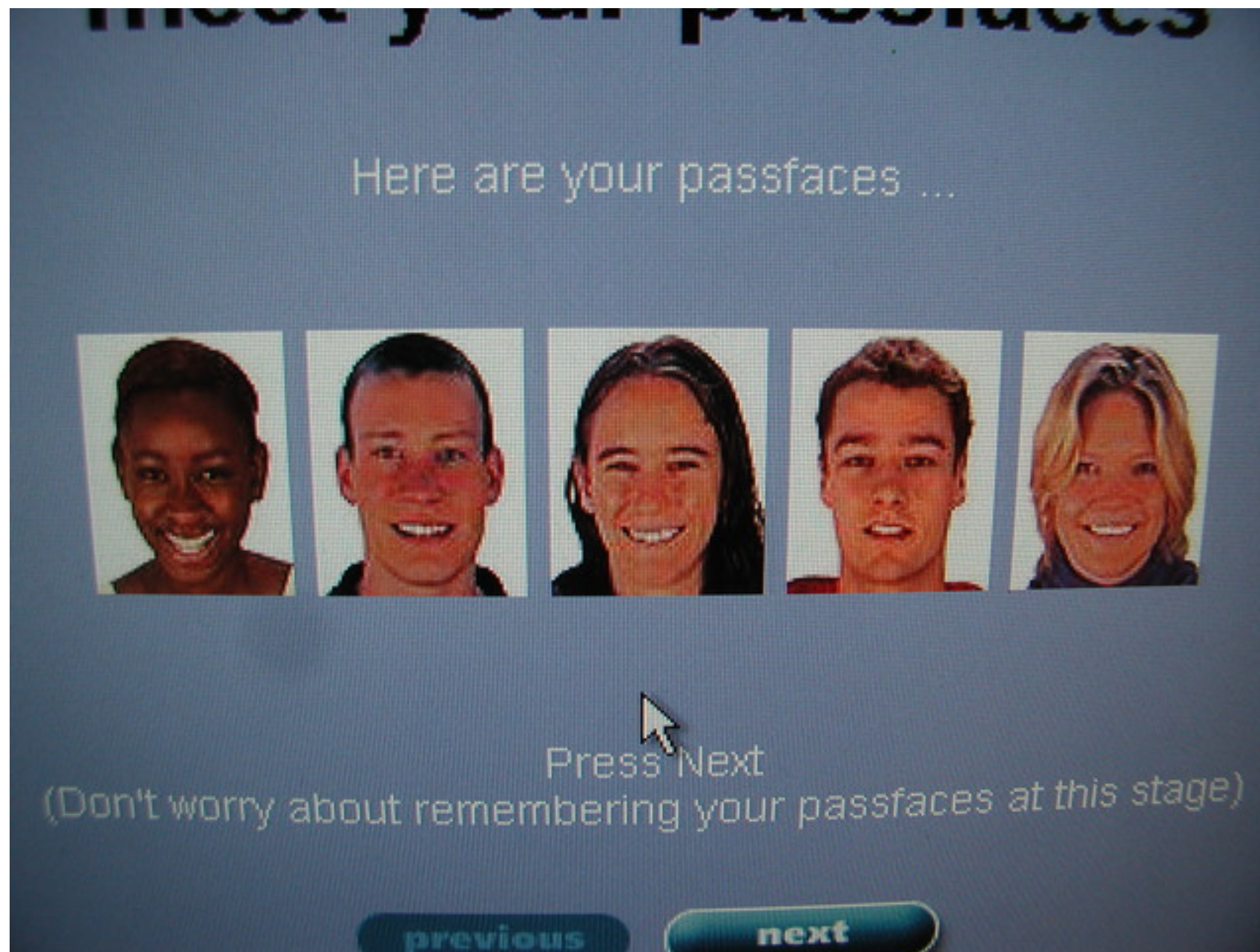
from *Dirik, Memon, Birget*; SOUPS 2007

# Passfaces



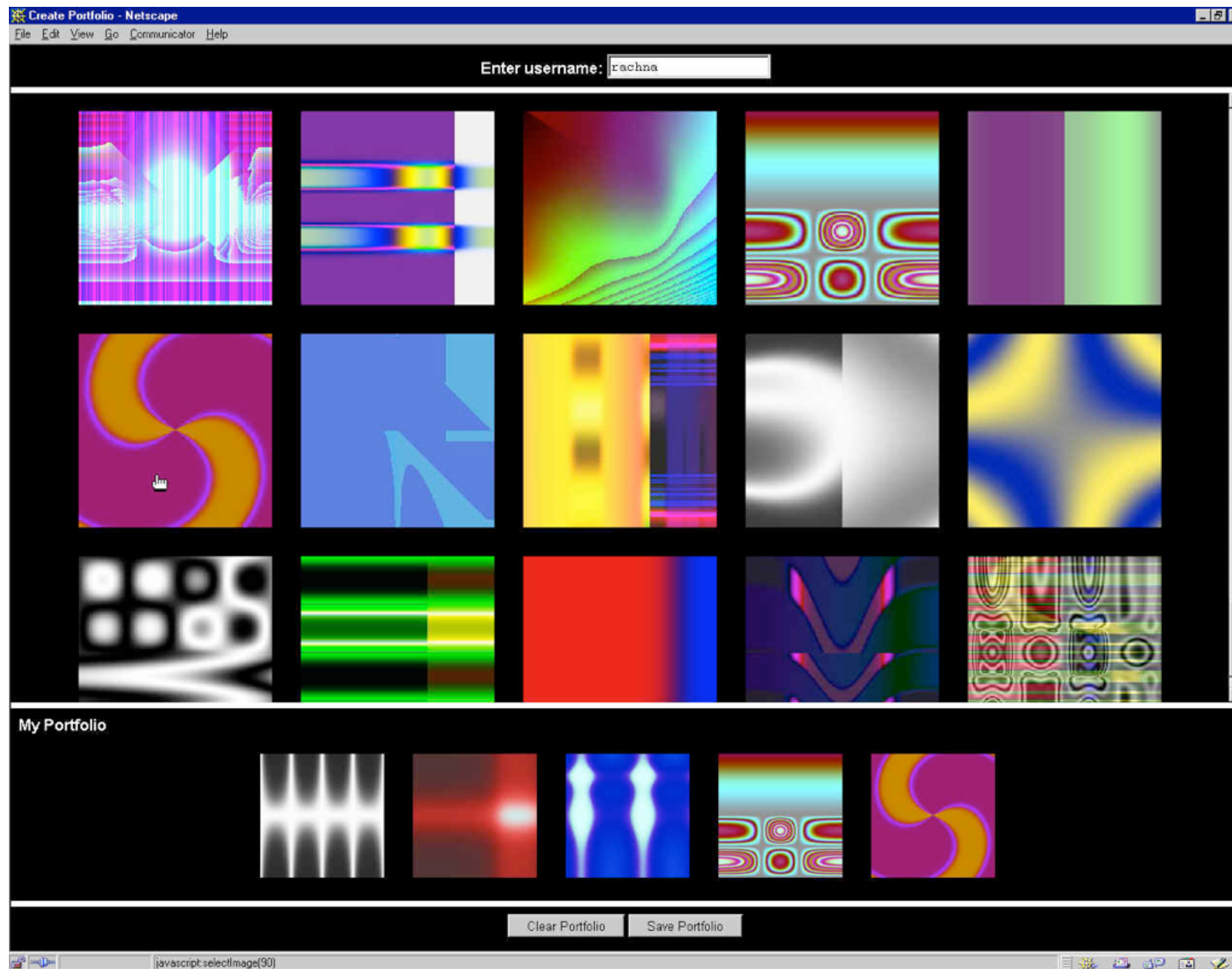


# My passfaces

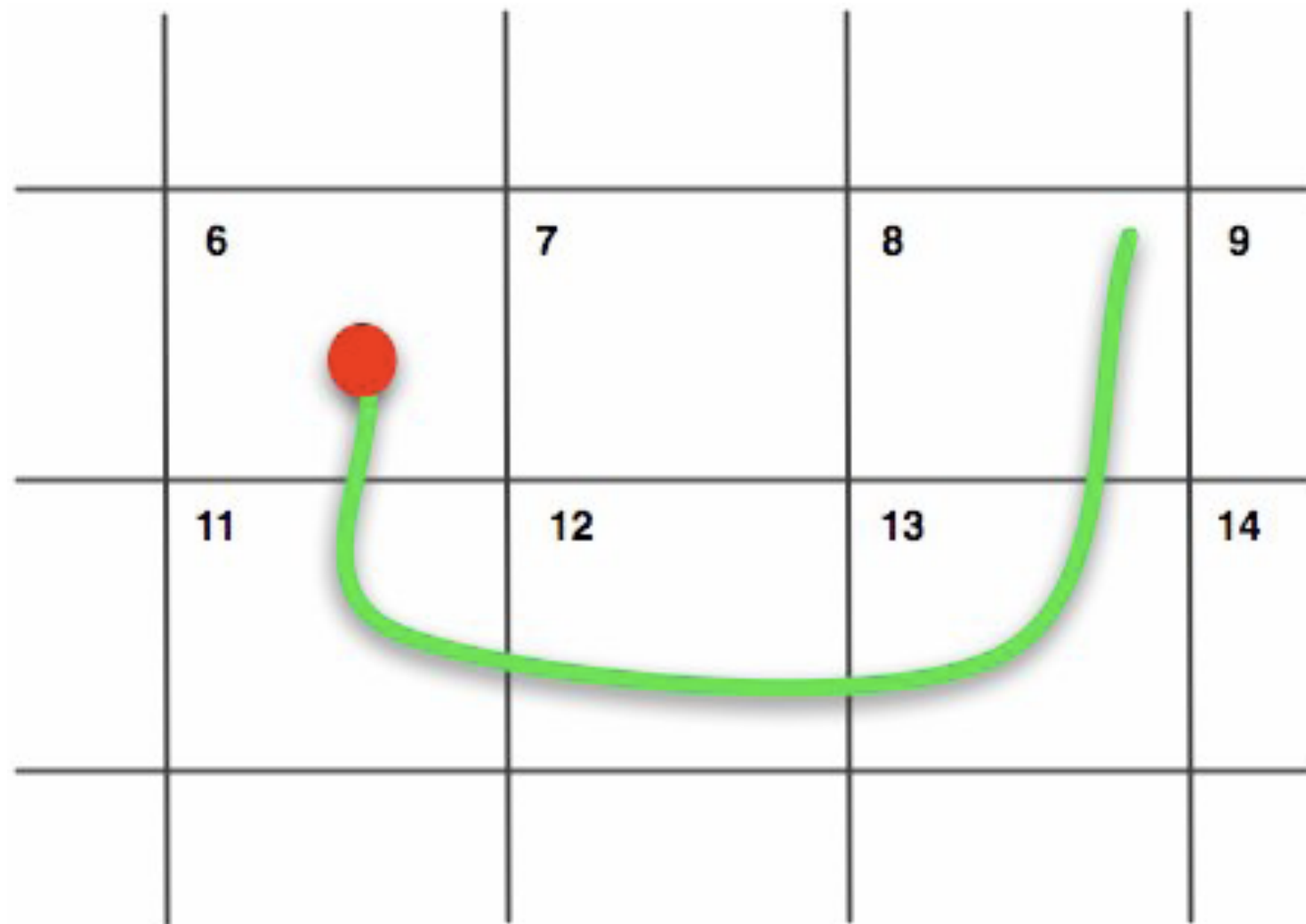




# Deja Vu (Recognition-based)



# Draw a Secret



Lin, Dunphy, *et al.* SOUPS 2007

# Use Your Illusion (SOUPS 2008)



# **A Very Short Course on Entropy**

# $2^{10} = 1024$ 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, our two words

- “example early”



# Good stuff!

- **The list of words isn't secret**
- **so spelling checker is okay!**
- **easy words to type**
- **on an iPhone, pick words where the "tappos" give the word you wanted**

# Some Whacko Ideas from ches

## **Passmaps**

**(Zoomauth demo)**

Carrier 10:46 AM

Keyring Key options Continue

Key name: Sample

Use hex for responses OFF

Zero if bad unlock ON

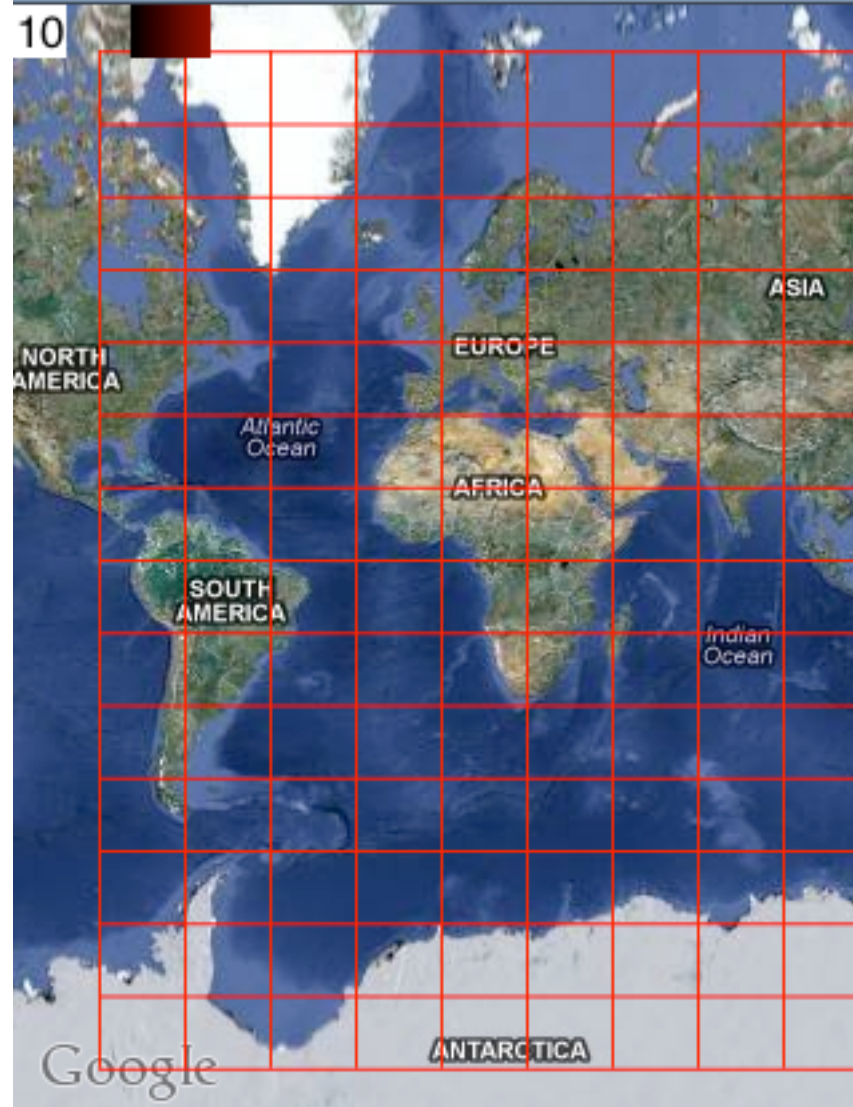
Use helper bits OFF

Select zoom type:

Map Graph Document

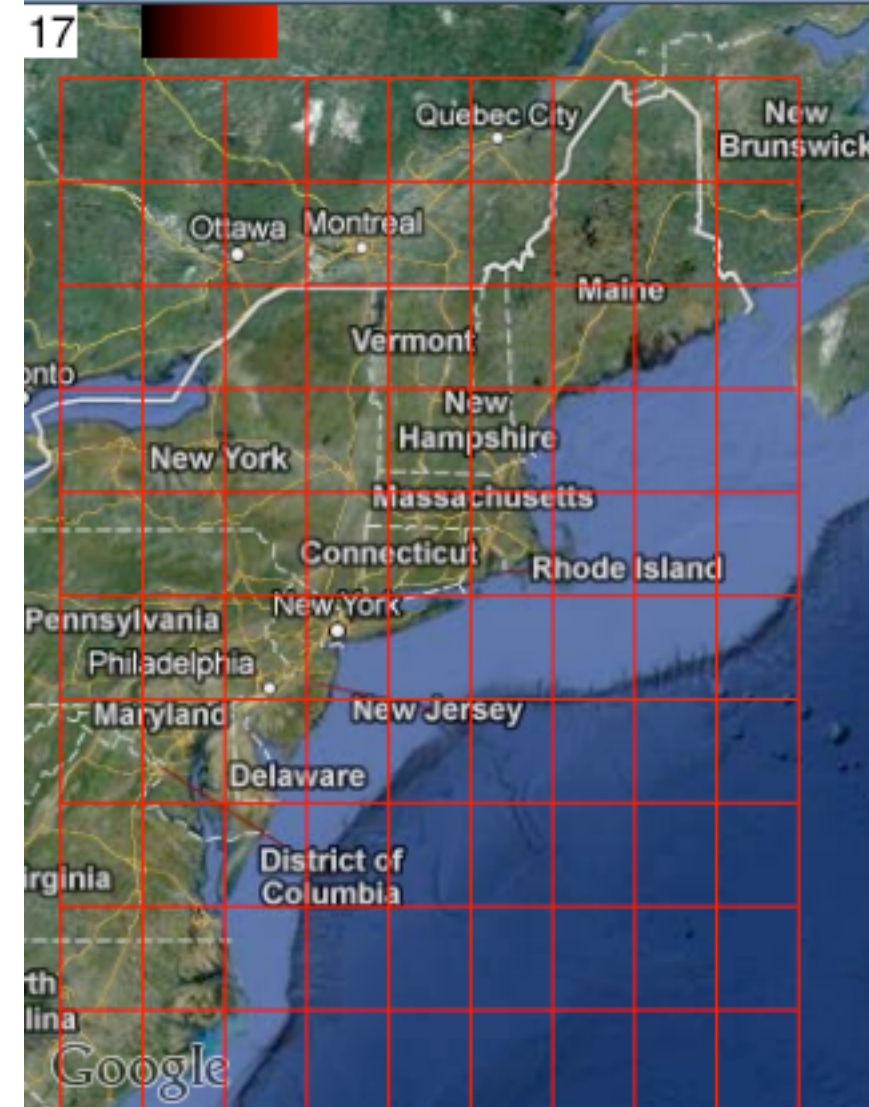
Carrier 10:46 AM

Key options Zoom and tap

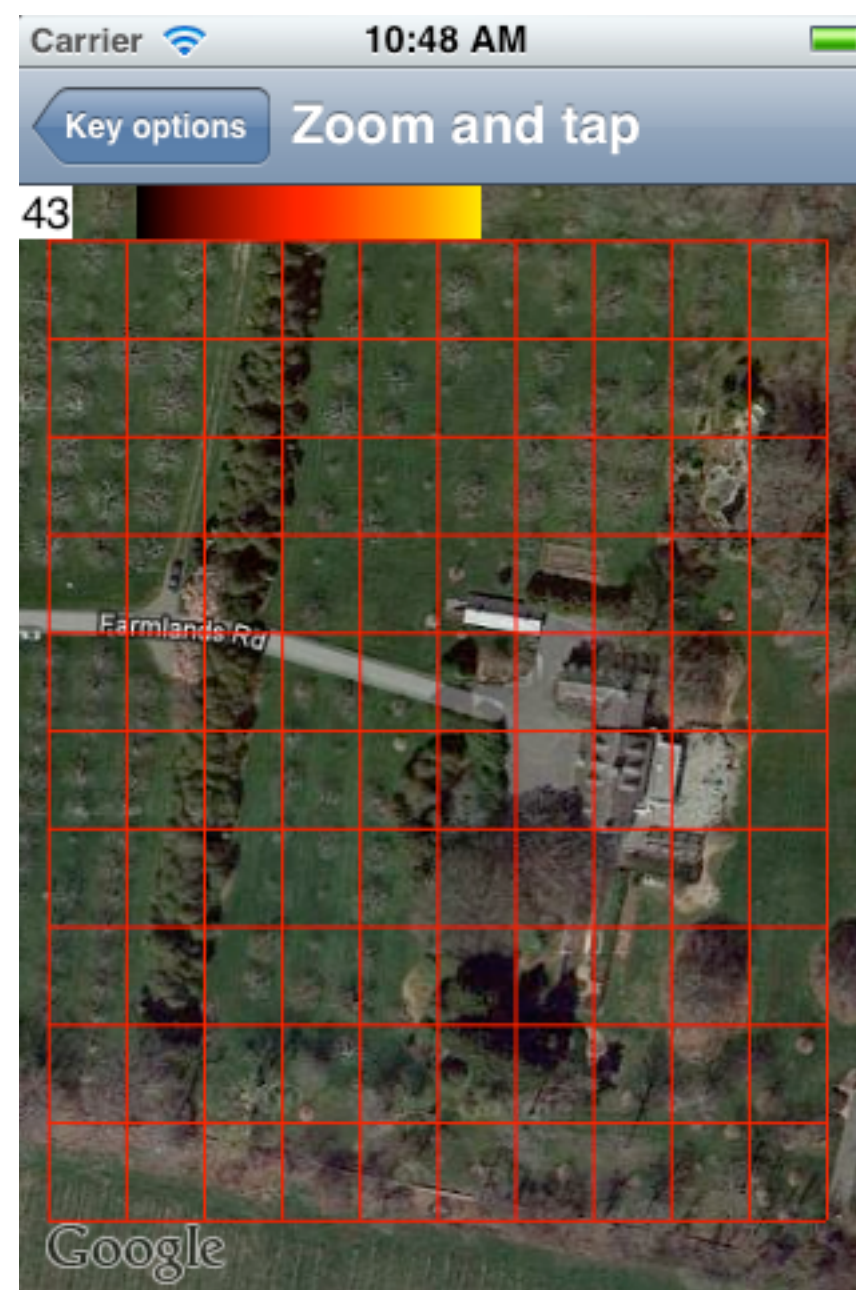
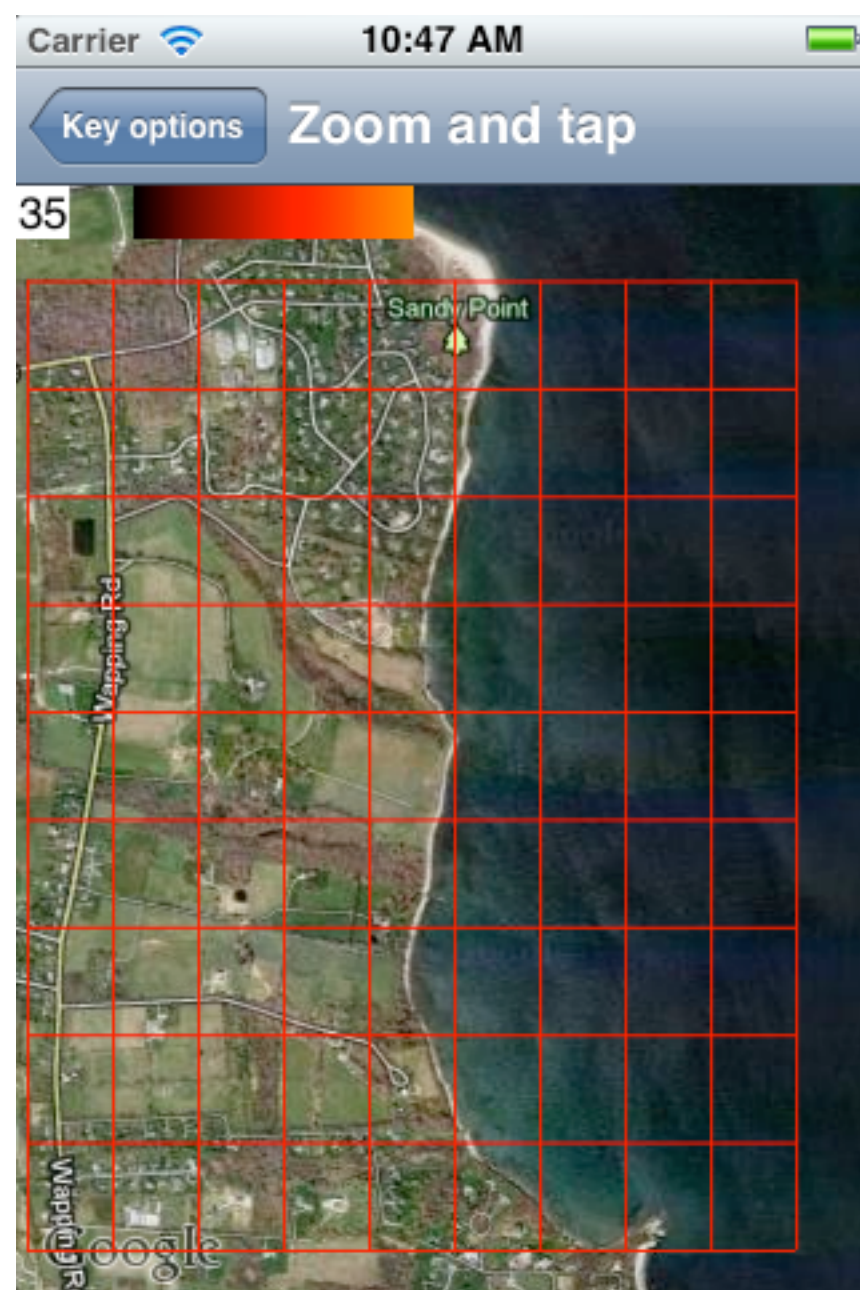


Carrier 10:47 AM

Key options Zoom and tap



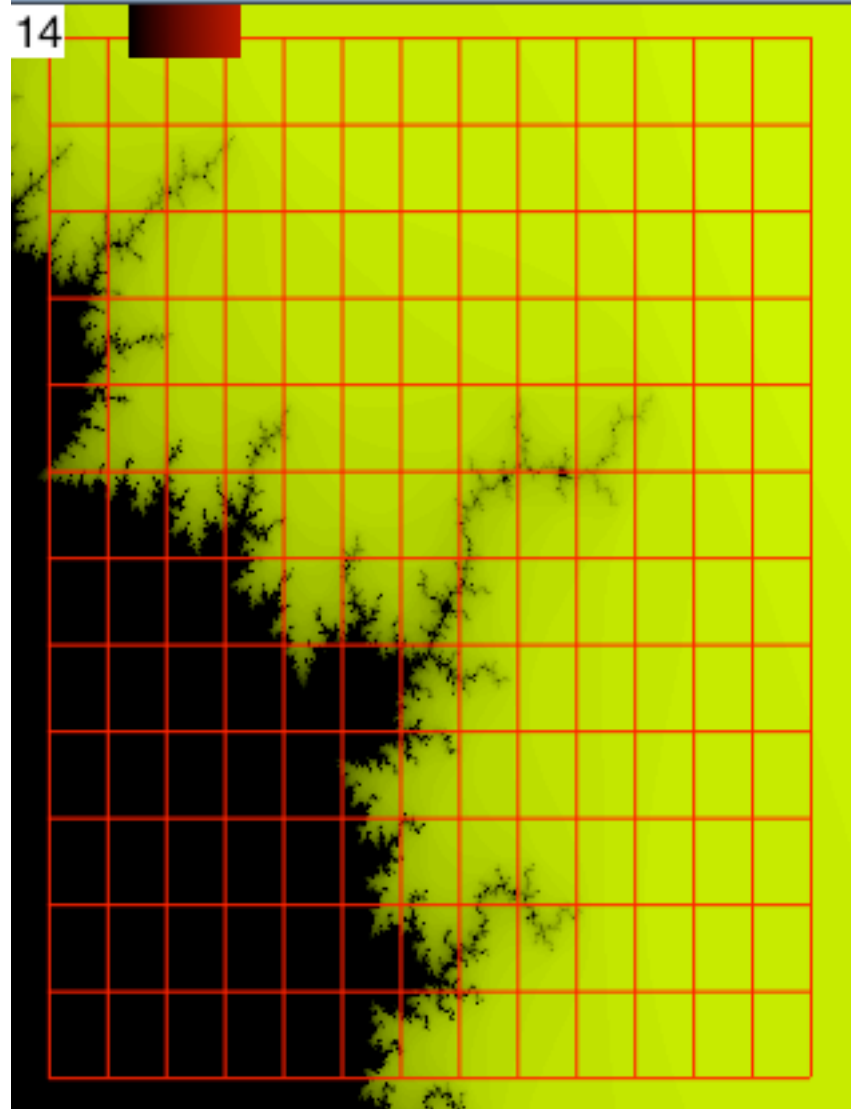




Key options

Zoom and tap

14





calculus.pdf

tcith-asl.pdf

walden.pdf



Page 172

188 Chapter 4 Techniques of Integration

Based on our knowledge of the definite integral, we know that the definite integral of a function  $f$  over the interval  $[a, b]$  is the area under the curve  $y = f(x)$  from  $x = a$  to  $x = b$ . For example, we know that the definite integral of the function  $f(x) = 2x$  over the interval  $[0, 1]$  is the area under the curve  $y = 2x$  from  $x = 0$  to  $x = 1$ . This area is the area of a triangle with base 1 and height 2, so it is 1. We can also compute this area using the definite integral:

$$\int_0^1 2x \, dx = \left[ x^2 \right]_0^1 = 1^2 - 0^2 = 1.$$

Now we know that the definite integral of  $f(x) = 2x$  over the interval  $[0, 1]$  is 1. We can also compute this area using the definite integral:

$$\int_0^1 2x \, dx = \left[ x^2 \right]_0^1 = 1^2 - 0^2 = 1.$$

It is important to note that the definite integral of a function  $f$  over the interval  $[a, b]$  is the area under the curve  $y = f(x)$  from  $x = a$  to  $x = b$ . This area is the area of a region in the plane. For example, the area of a triangle with base 1 and height 2 is 1. We can also compute this area using the definite integral:

$$\int_0^1 2x \, dx = \left[ x^2 \right]_0^1 = 1^2 - 0^2 = 1.$$

Now we know that the definite integral of  $f(x) = 2x$  over the interval  $[0, 1]$  is 1. We can also compute this area using the definite integral:

$$\int_0^1 2x \, dx = \left[ x^2 \right]_0^1 = 1^2 - 0^2 = 1.$$

It is important to note that the definite integral of a function  $f$  over the interval  $[a, b]$  is the area under the curve  $y = f(x)$  from  $x = a$  to  $x = b$ . This area is the area of a region in the plane. For example, the area of a triangle with base 1 and height 2 is 1. We can also compute this area using the definite integral:

$$\int_0^1 2x \, dx = \left[ x^2 \right]_0^1 = 1^2 - 0^2 = 1.$$

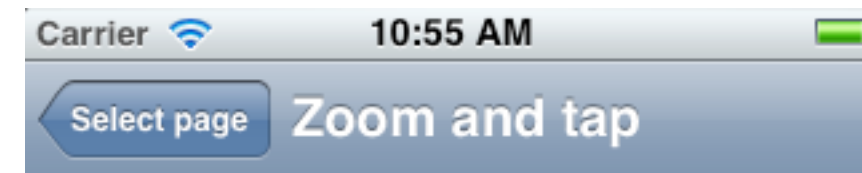
Now we know that the definite integral of  $f(x) = 2x$  over the interval  $[0, 1]$  is 1. We can also compute this area using the definite integral:

$$\int_0^1 2x \, dx = \left[ x^2 \right]_0^1 = 1^2 - 0^2 = 1.$$

It is important to note that the definite integral of a function  $f$  over the interval  $[a, b]$  is the area under the curve  $y = f(x)$  from  $x = a$  to  $x = b$ . This area is the area of a region in the plane. For example, the area of a triangle with base 1 and height 2 is 1. We can also compute this area using the definite integral:

$$\int_0^1 2x \, dx = \left[ x^2 \right]_0^1 = 1^2 - 0^2 = 1.$$

Now we know that the definite integral of  $f(x) = 2x$  over the interval  $[0, 1]$  is 1. We can also compute this area using the definite integral:

$$\int_0^1 2x \, dx = \left[ x^2 \right]_0^1 = 1^2 - 0^2 = 1.$$


22-2   $\int -2x$

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

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

exactly the integral we computed  
e the calculations less confusing.

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

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



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

the integral we (

culations less co

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

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



# Better Solutions

## **#1: Getting out of the game**

# SecureNet Key SNK-004



# A login from my distant past

**RISC/os (inet)**

**Authentication Server.**

**Id? ches**

**Enter response code for 70202: 04432234**

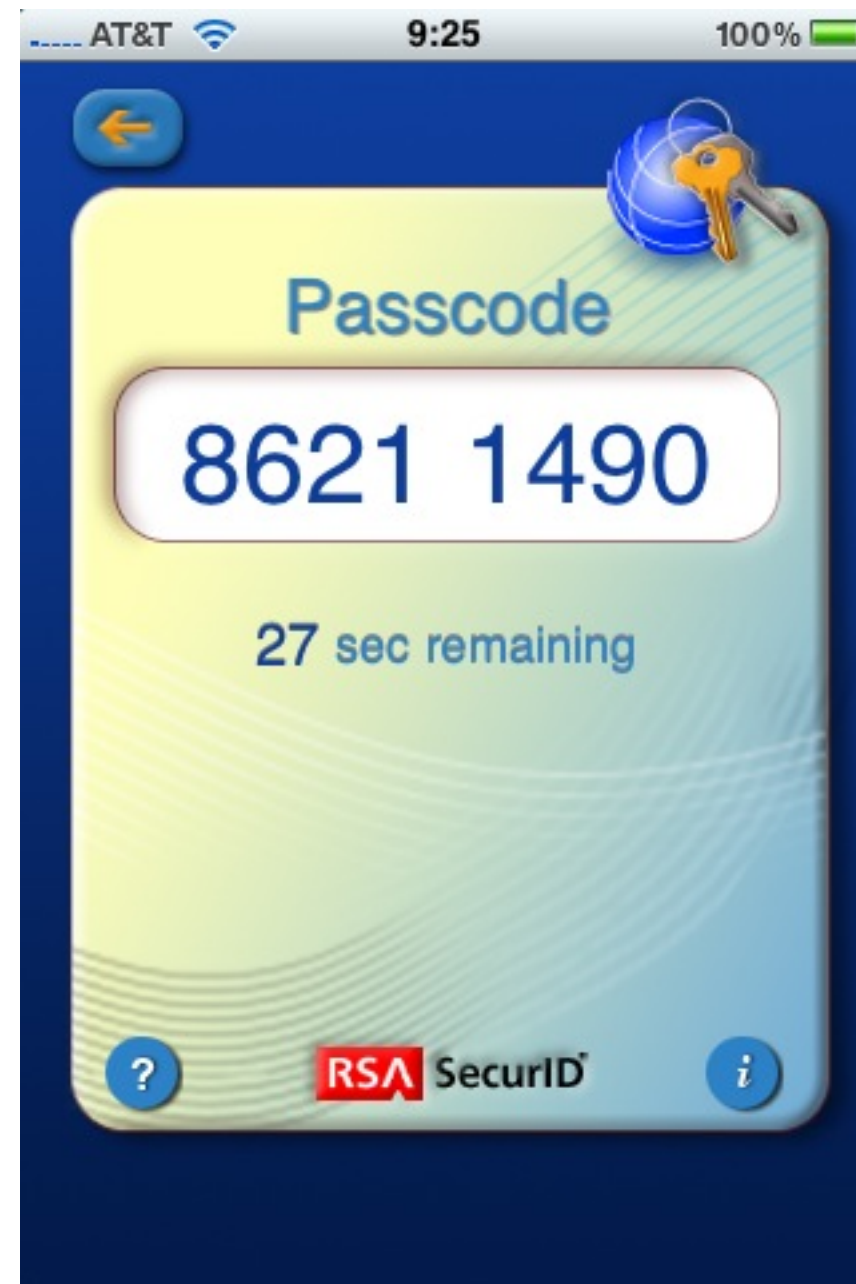
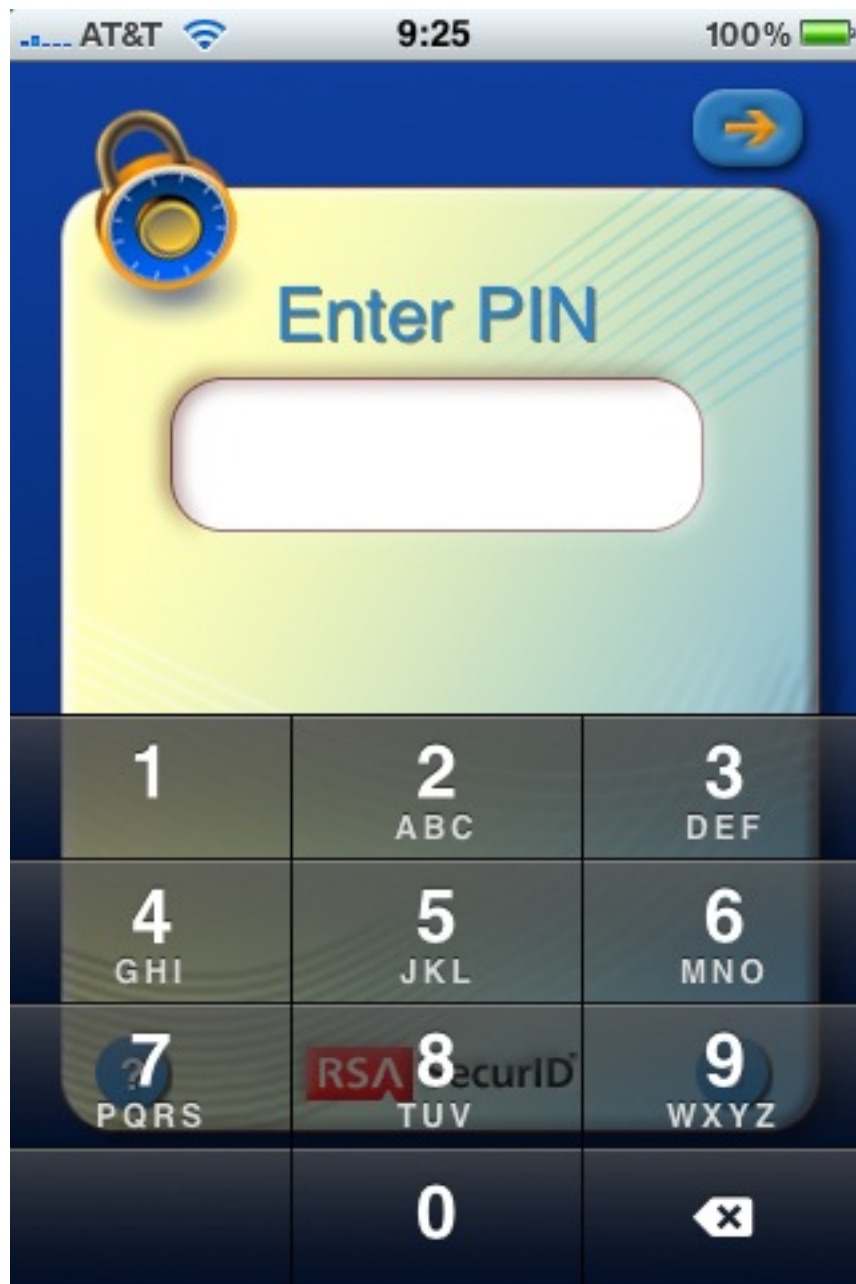
**Destination? cetus**

**\$**

# SecureID



# RSA Softkey



# Why aren't these ubiquitous?

- **Cheap devices available before 1990**
- **People hate:**
  - **Having to carry the device**
  - **Entering the challenge (why SNK lost)**
  - **Entering the response**
  - **Carrying multiple devices**

# Better Solutions

## **#2: Limiting guesses**

# Limiting guesses

- **This has worked for ATM PINs since the early 1970s!**
- **It requires an authentication server, or some means to shut off the card/account**
- **It replaces the *eye of newt* rules with...**



# The Non-moronic password rule!

**Pick something a friend, colleague won't  
guess in a few tries,  
and they can't figure out while watching you  
type it**

# Summary solution

- **Limited guesses and lock the account**
- **Non-moronic passwords**
- **Make locked accounts less painful**

# Grandma can understand and comply with this rule

- **It makes sense**
- **Now, dictionary words are okay**
- **Simpler passwords are easier to remember**
- **You probably don't have to write them down**

# Still Want Your Strong Passwords?

**Okay, fine. But let's make them fun, or at least easier to type (and tap)**

# 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/insult](http://www.cheswick.com/insult) (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 eccrasis  
You blotted kibble of unhygienic wild sheep spittle  
You hard-featured fistula of podagric macaque flux

# If you really need “high entropy” passwords

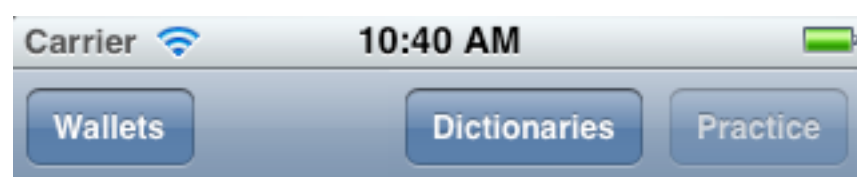
- **Not user-chosen, but user can veto, waiting for a “good one”**
  - **User-chosen phrases have much lower entropy**
- **They are going to write it down, for a while**
- **For daily use: who’s going to remember this over a year?**

# Words Are Better Than Eye-of-Newt

- **Much easier to type**
- **Spelling checking (iPhone) is your friend, not enemy**
- **Markus Jakobsson's *Fastwords***



**(105 demo)**



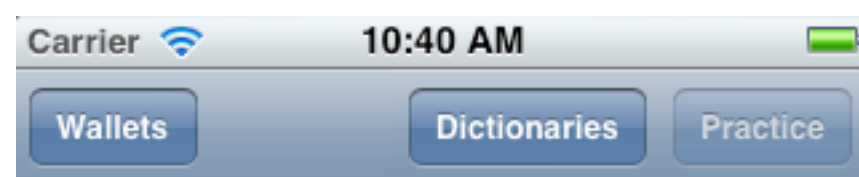
Wallet name:

Work factor: 80



problems sharing  
workshop holy legend  
gen equation

[Pick another key](#)



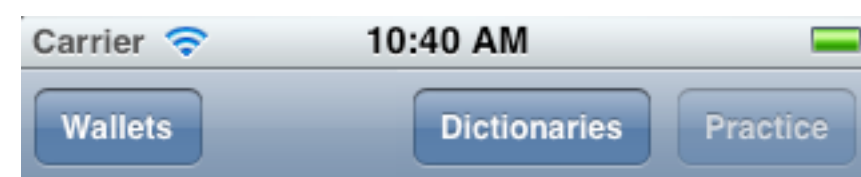
Wallet name:

Work factor: 80



monitor crooks cutter  
artaguetta enchanting  
decanted

[Pick another key](#)



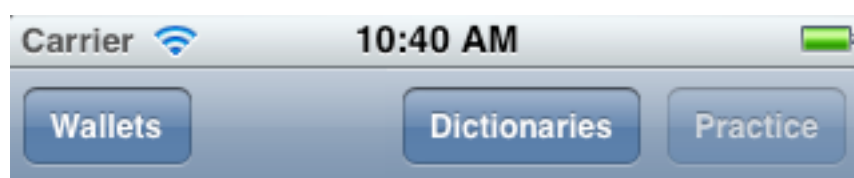
Wallet name:

Work factor: 80



marechal hobbler  
aurochs grinagog petiolar

[Pick another key](#)



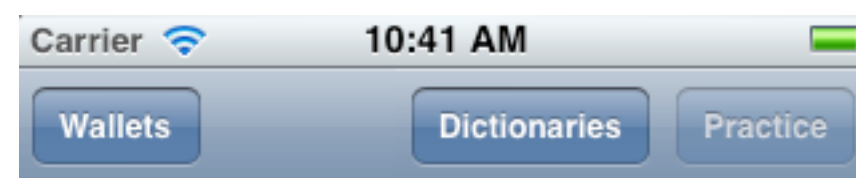
Wallet name:

Work factor: 105



can evening reach  
political applied whole  
without needs door  
member i

[Pick another key](#)



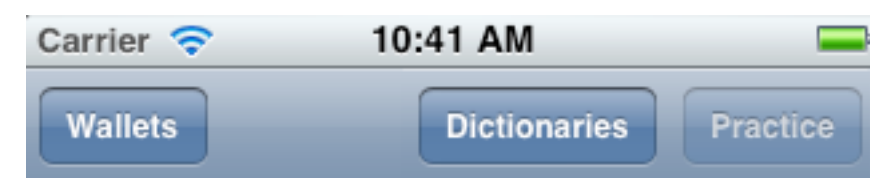
Wallet name:

Work factor: 105



building award days  
county rome why external  
ran states

[Pick another key](#)



Wallet name:

Work factor: 105



blokes hodgepodge  
melissa jannequin vying  
fha horseflesh

[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

**Frankly, I am sick of this!**

**Several solutions that work**

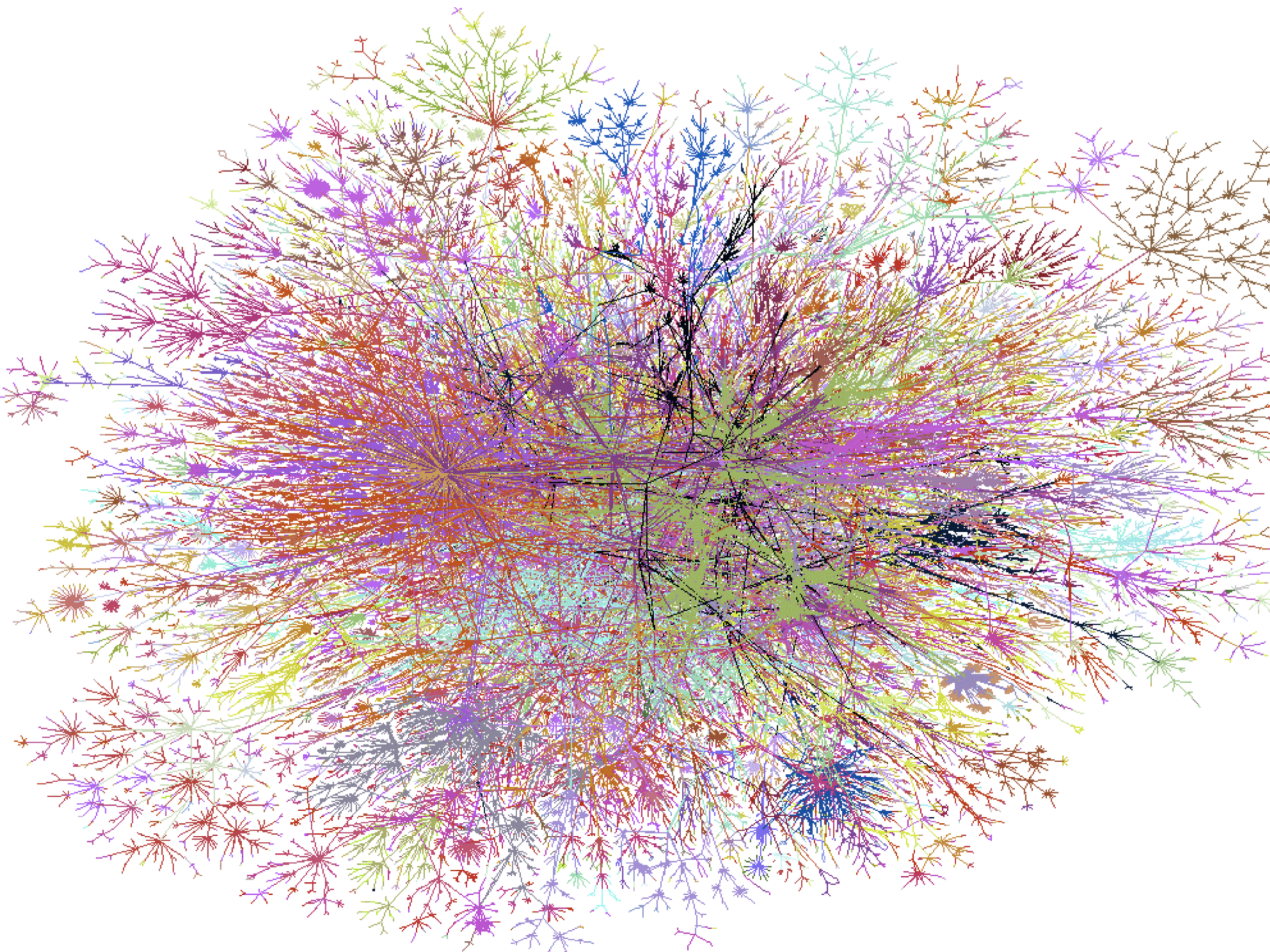


# **The Internet Mapping Project**

*What does the Internet look like?*  
*1997—2011*









# 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





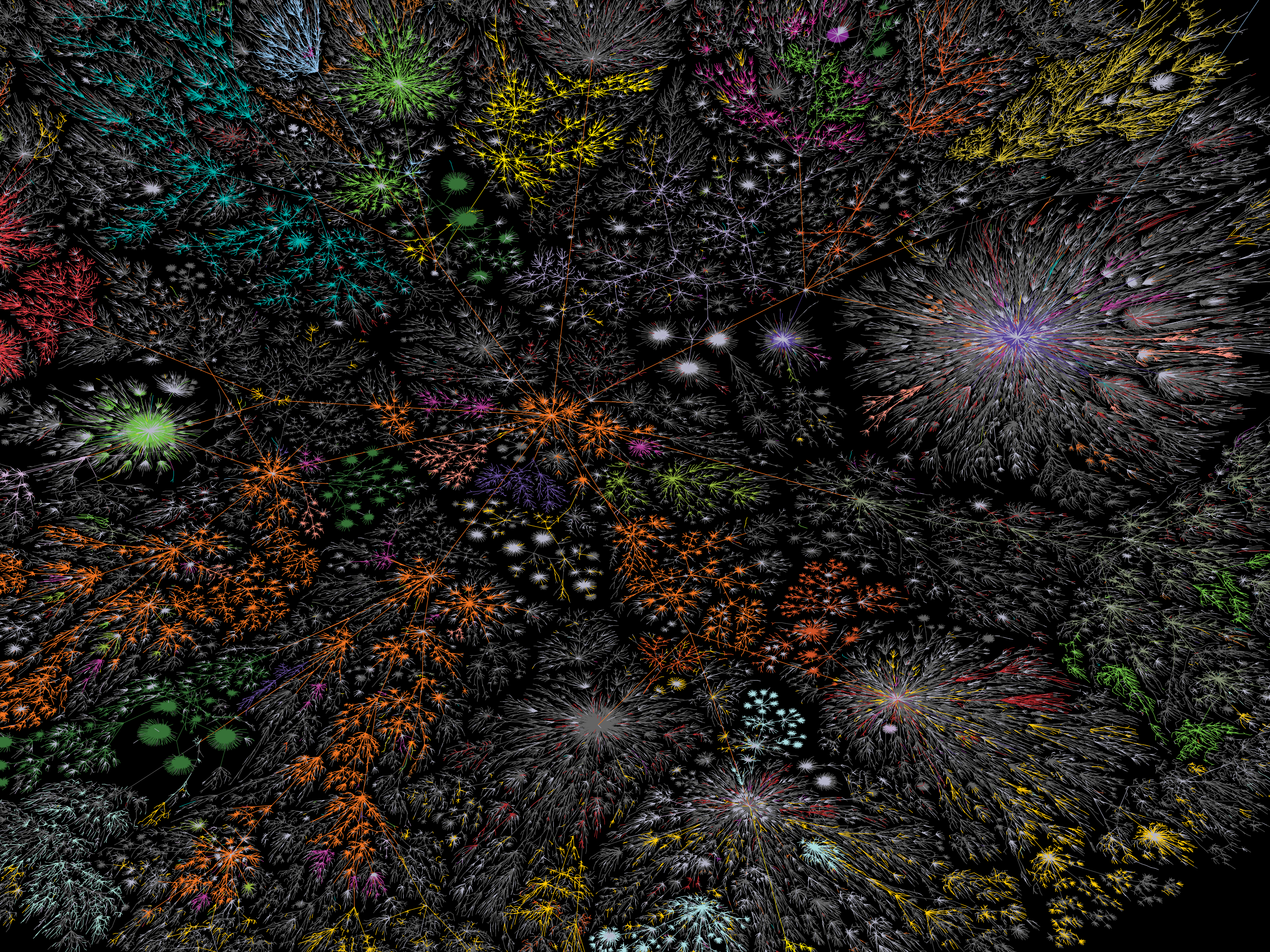
# Visualization of the layout algorithm

*Laying out an intranet*



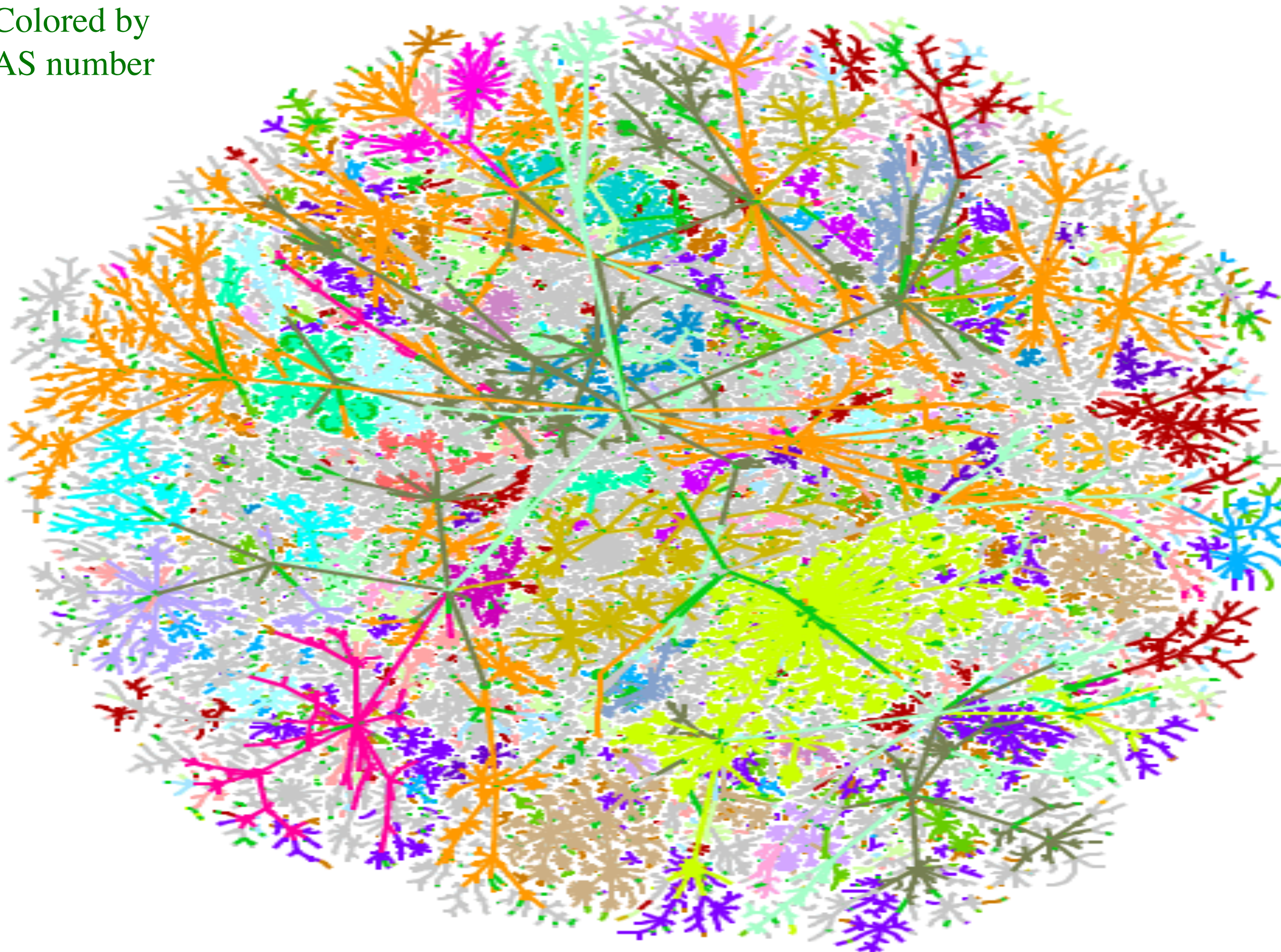








Colored by  
AS number



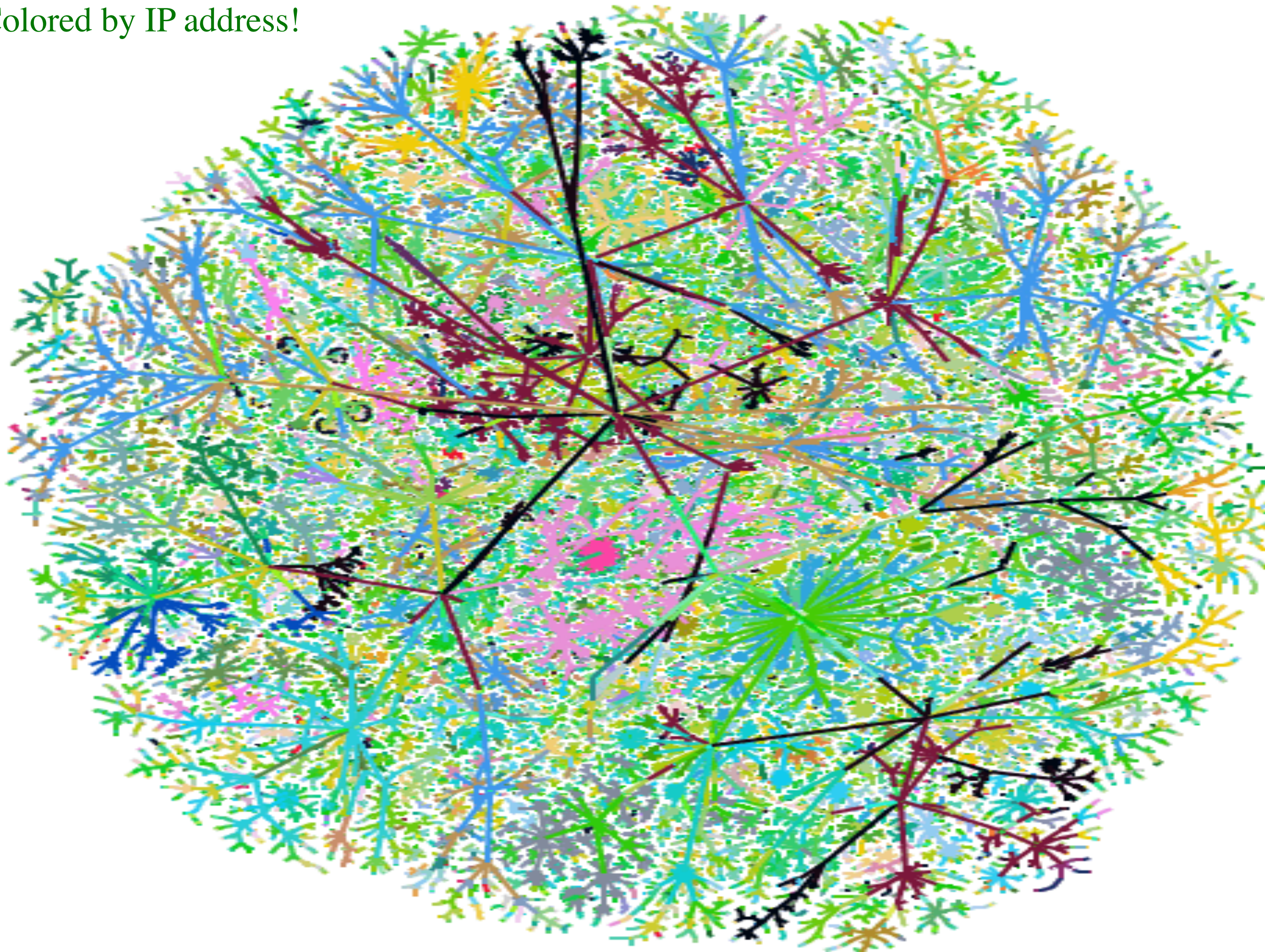


# Map Coloring

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

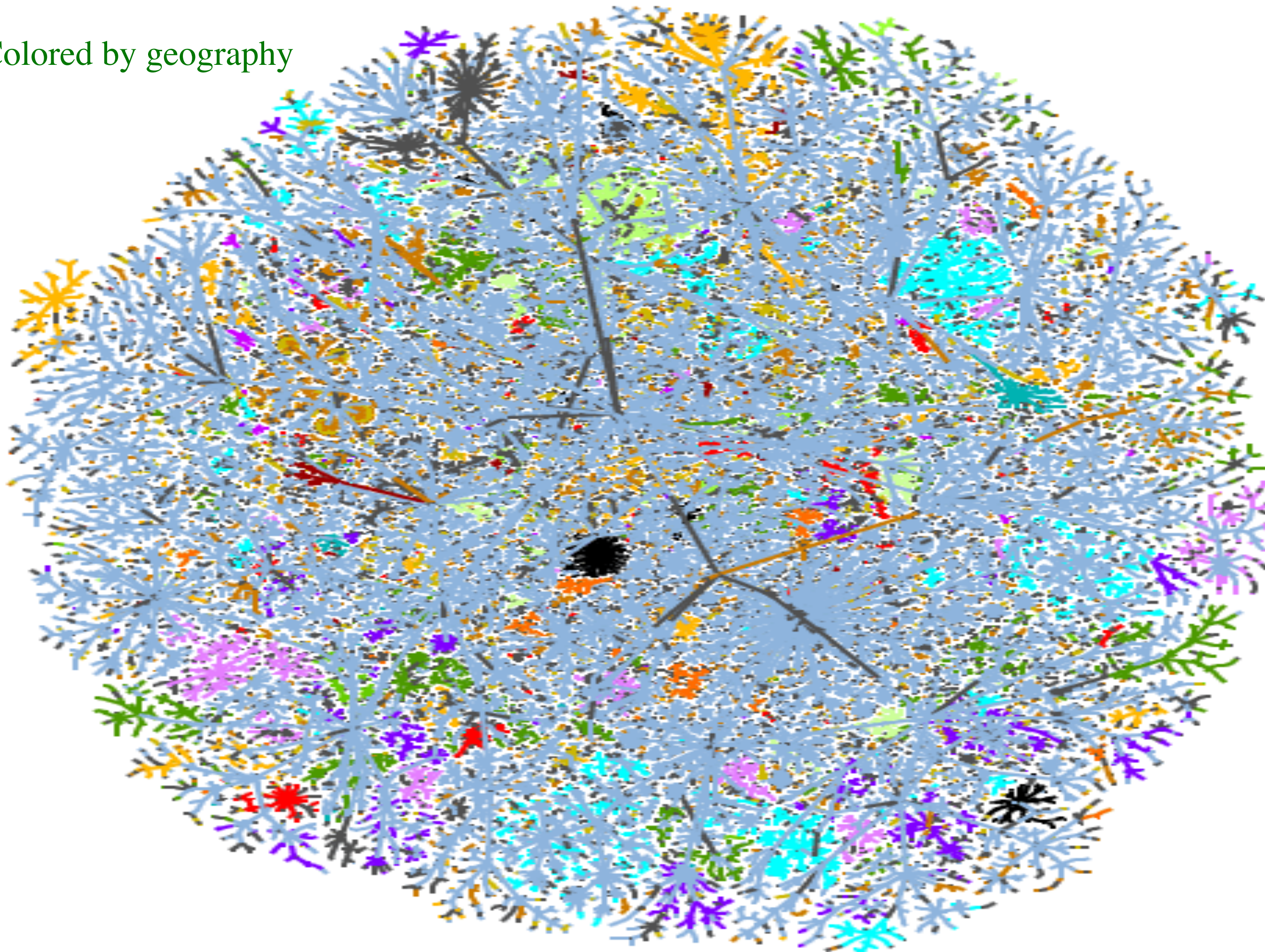


Colored by IP address!



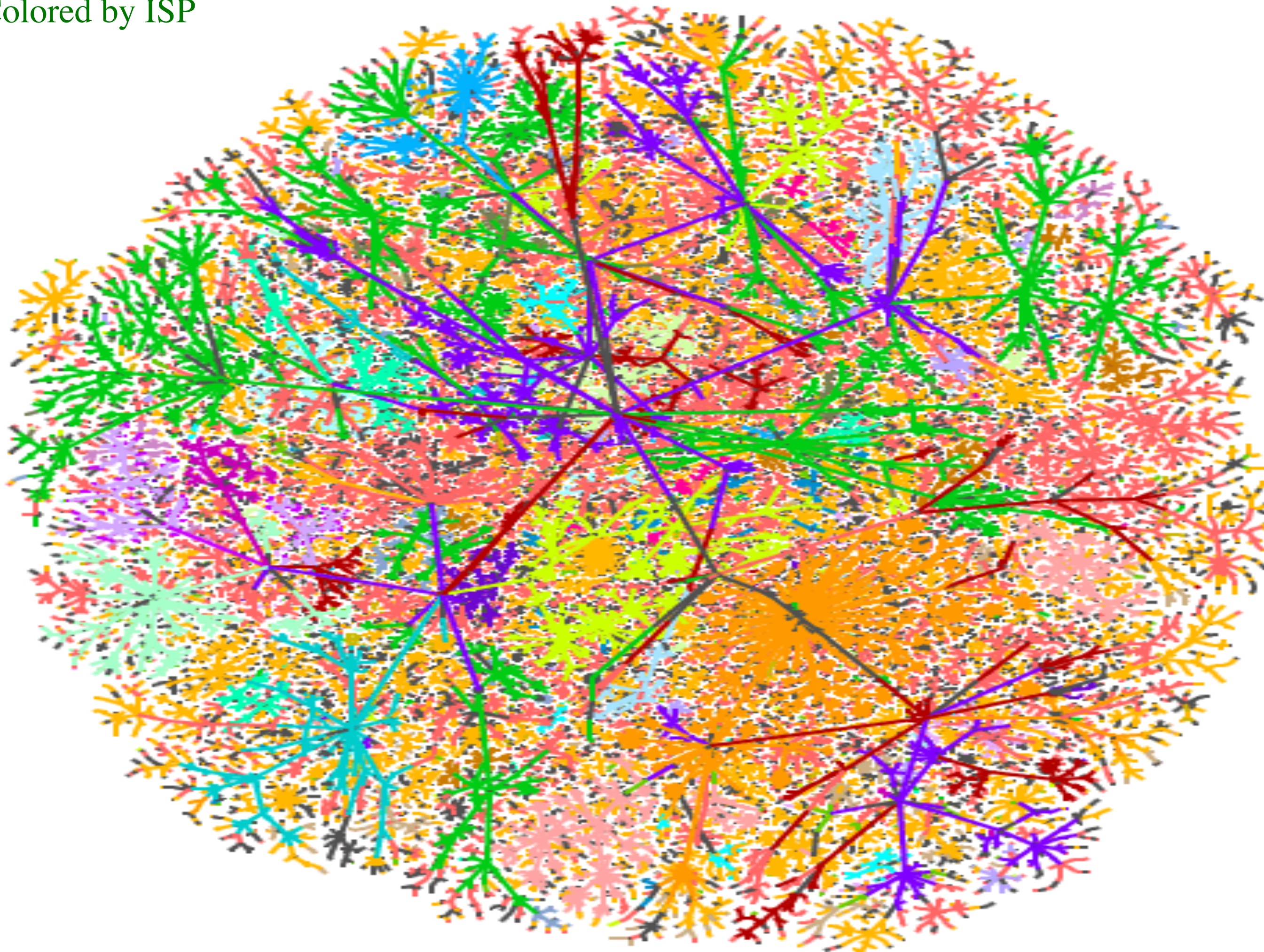


Colored by geography



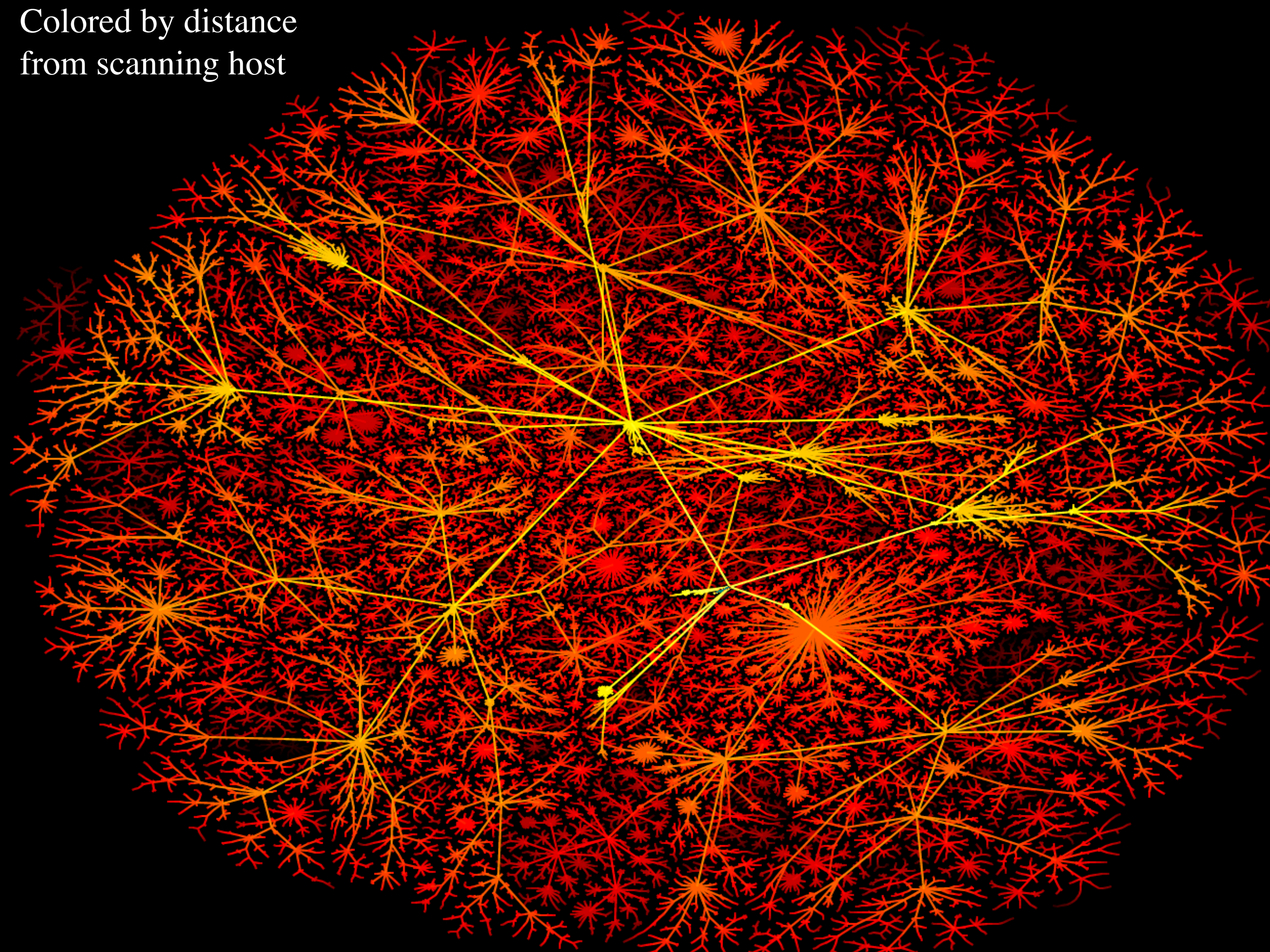


Colored by ISP

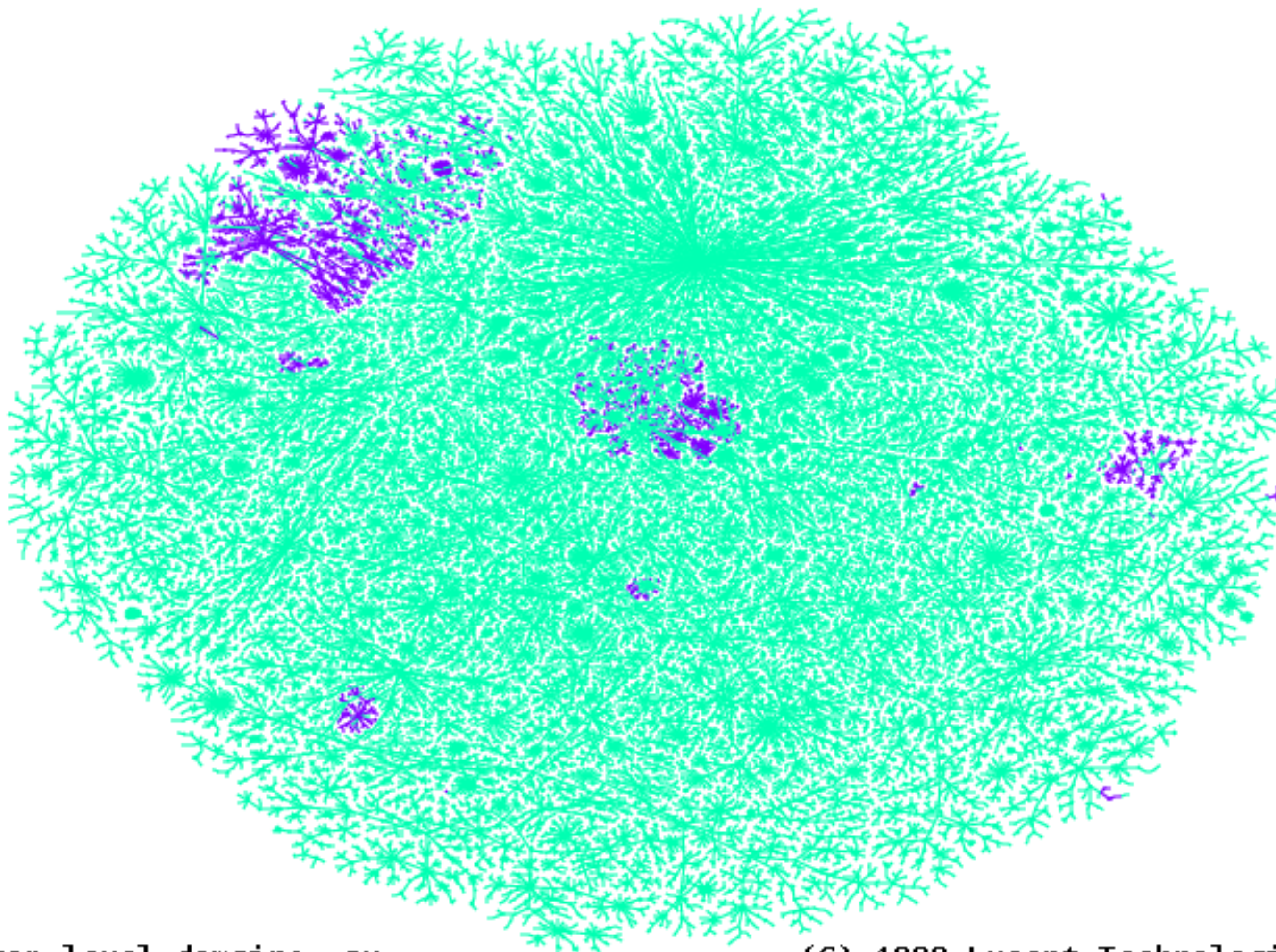




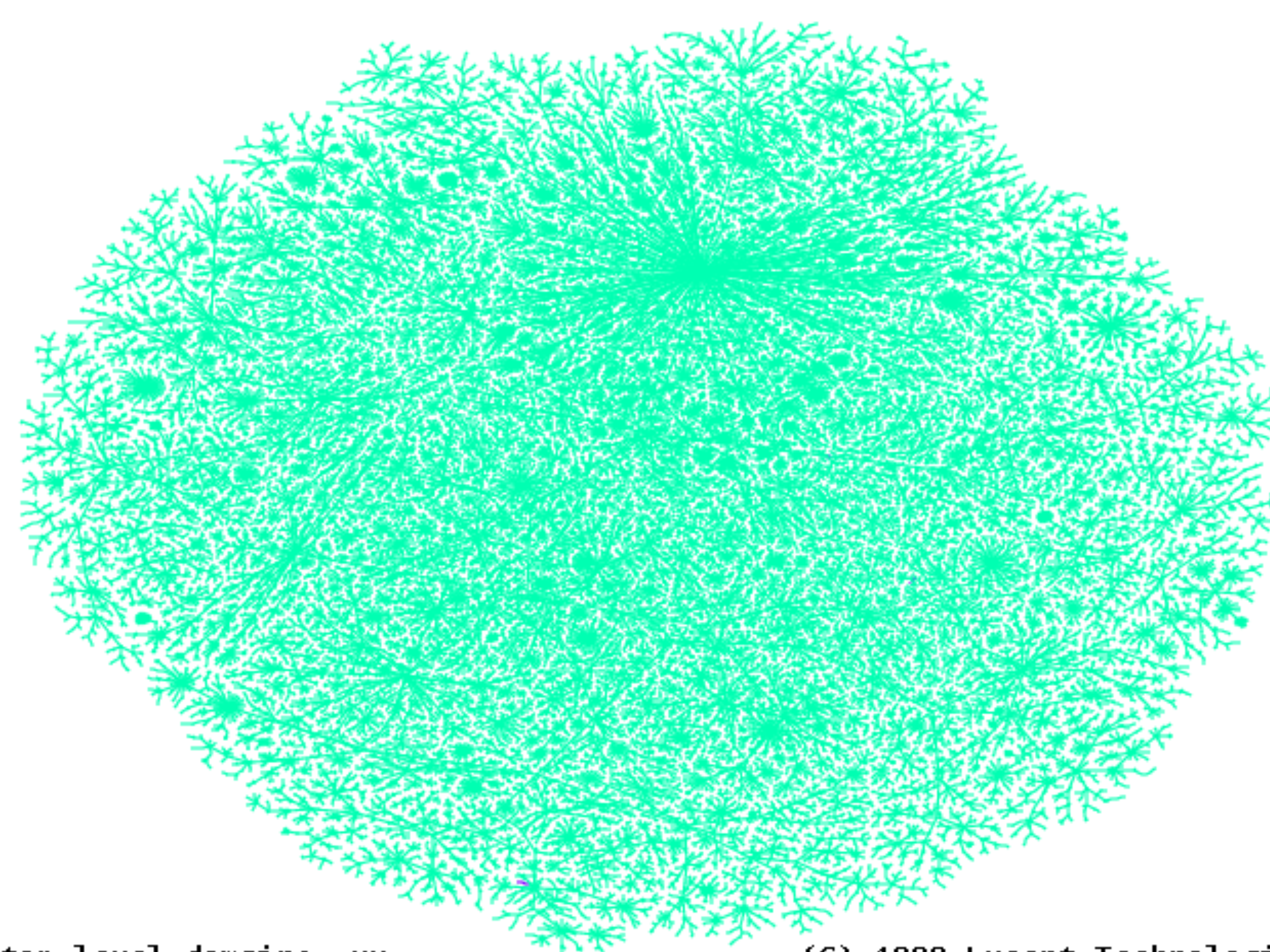
Colored by distance  
from scanning host















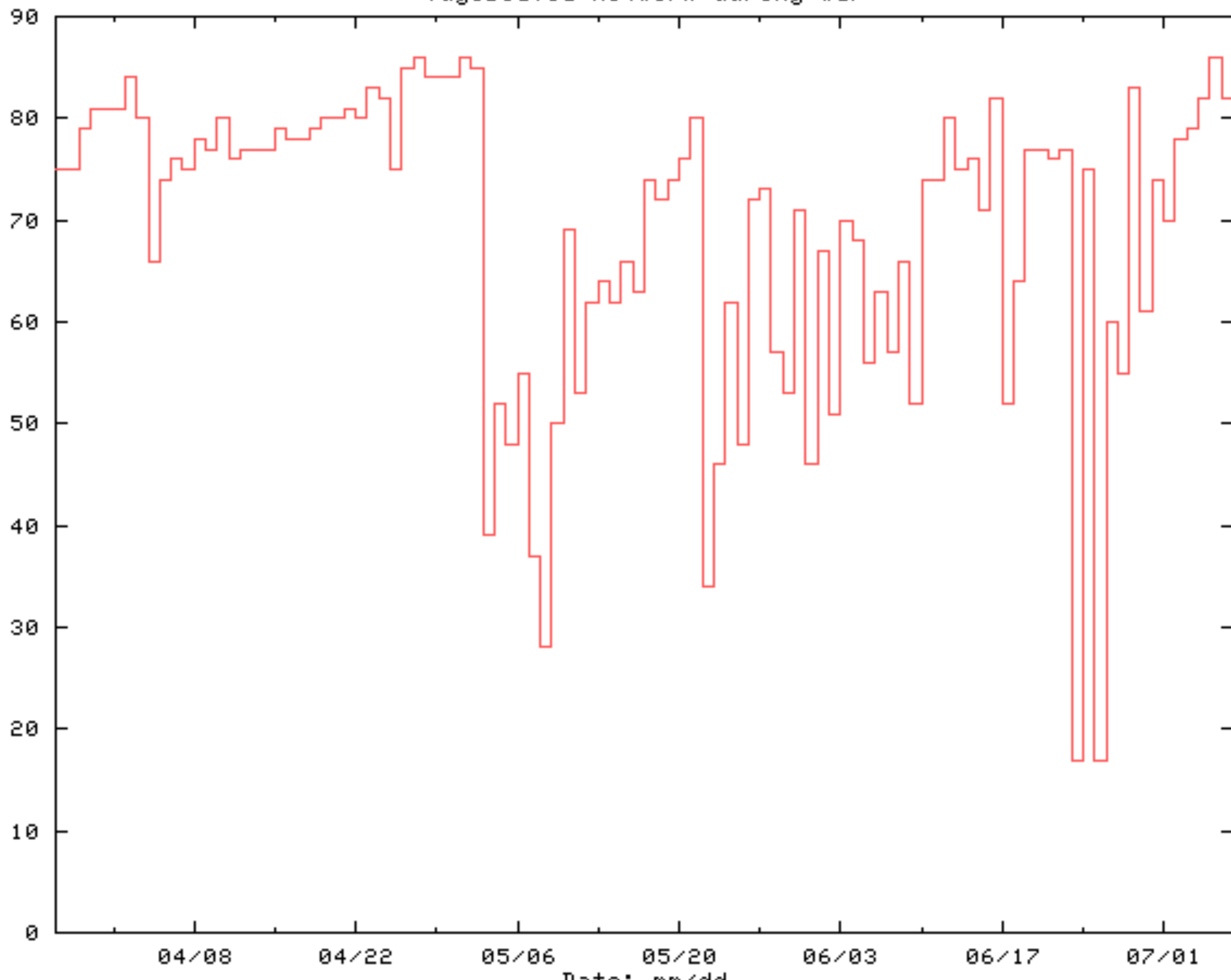
# Yugoslavia

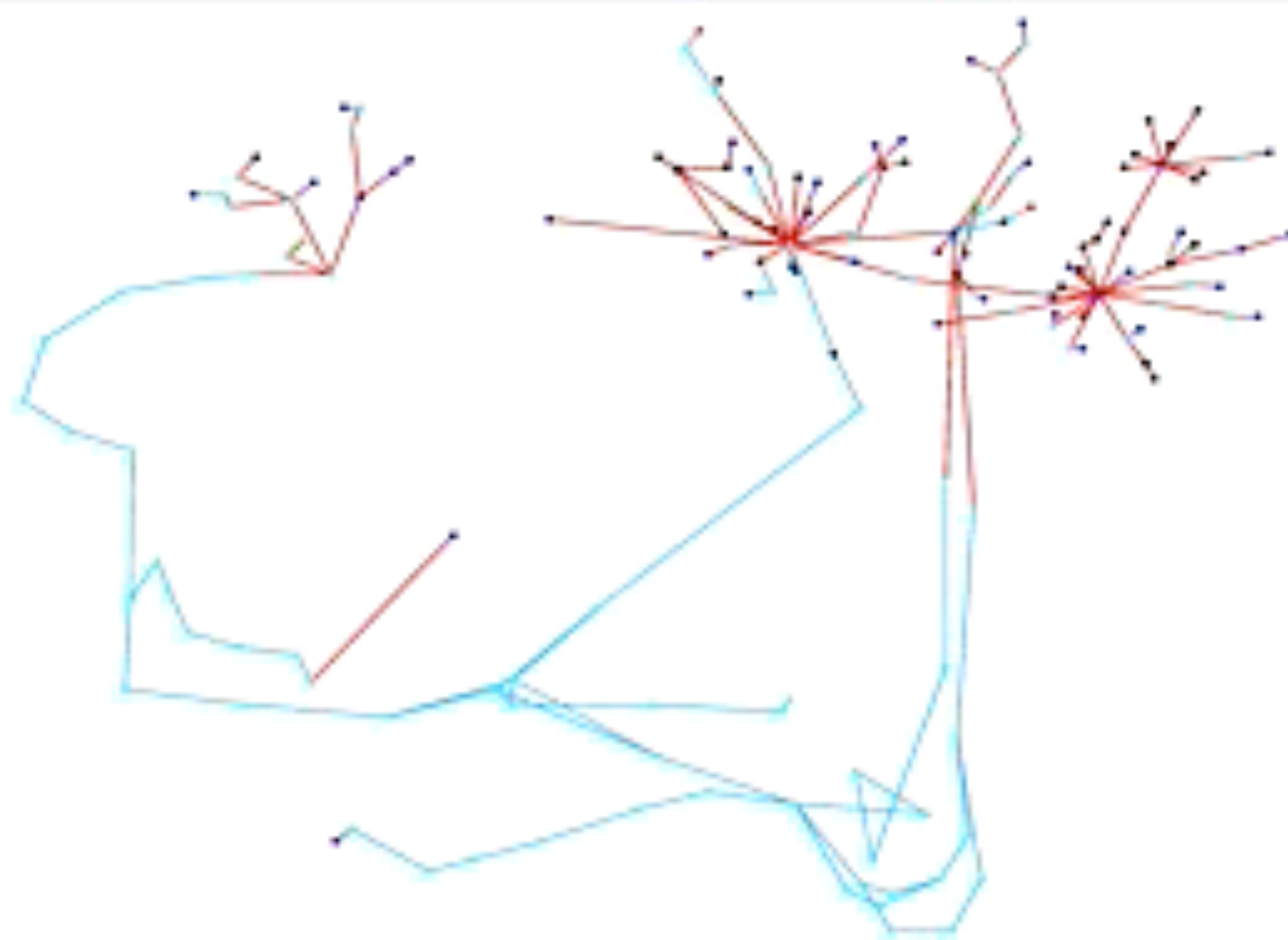
*An unclassified peek at a new  
battlefield*



Yugoslavia network during war

Routers detected

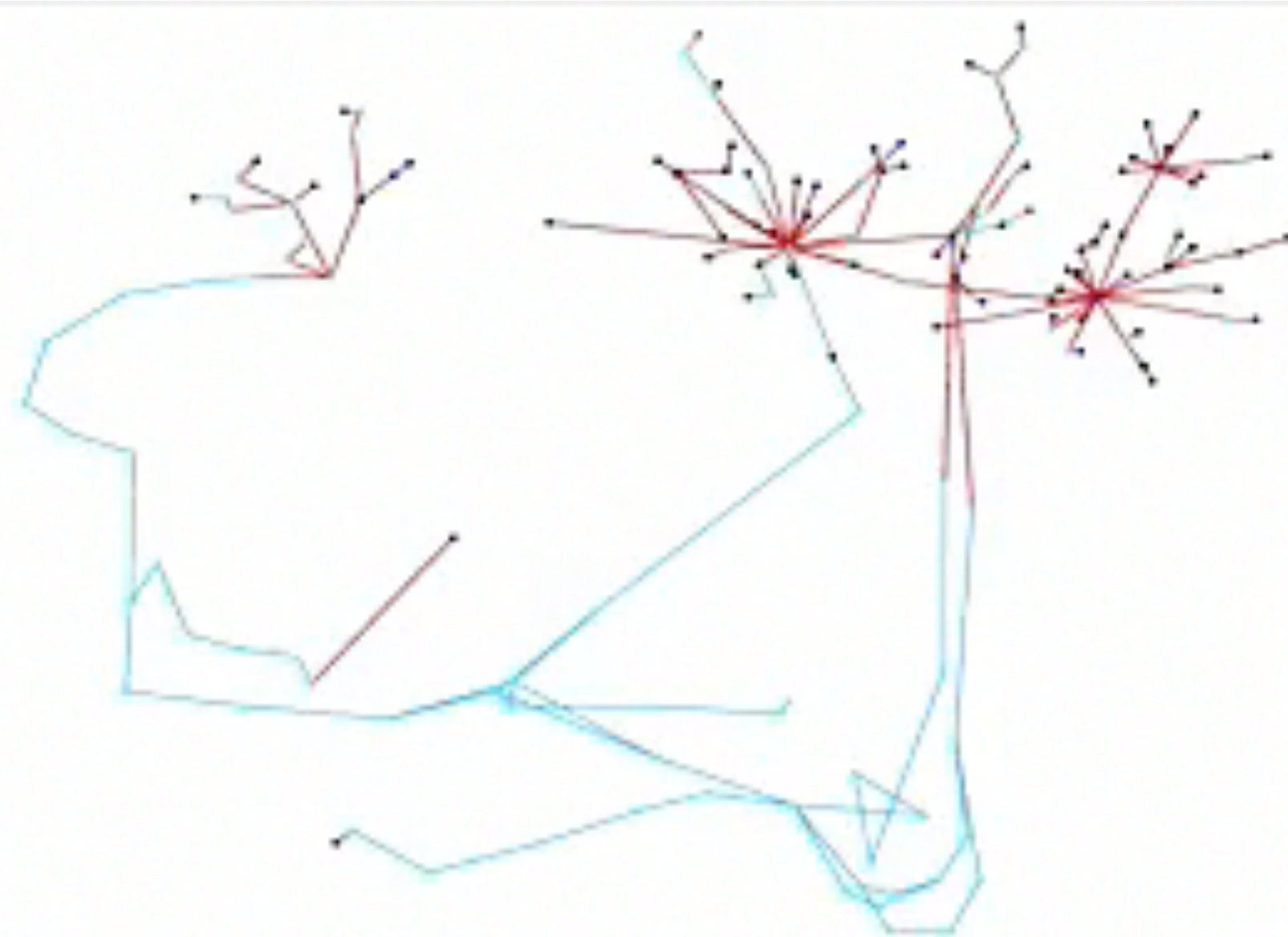




# Un film par Steve “Hollywood” Branigan...



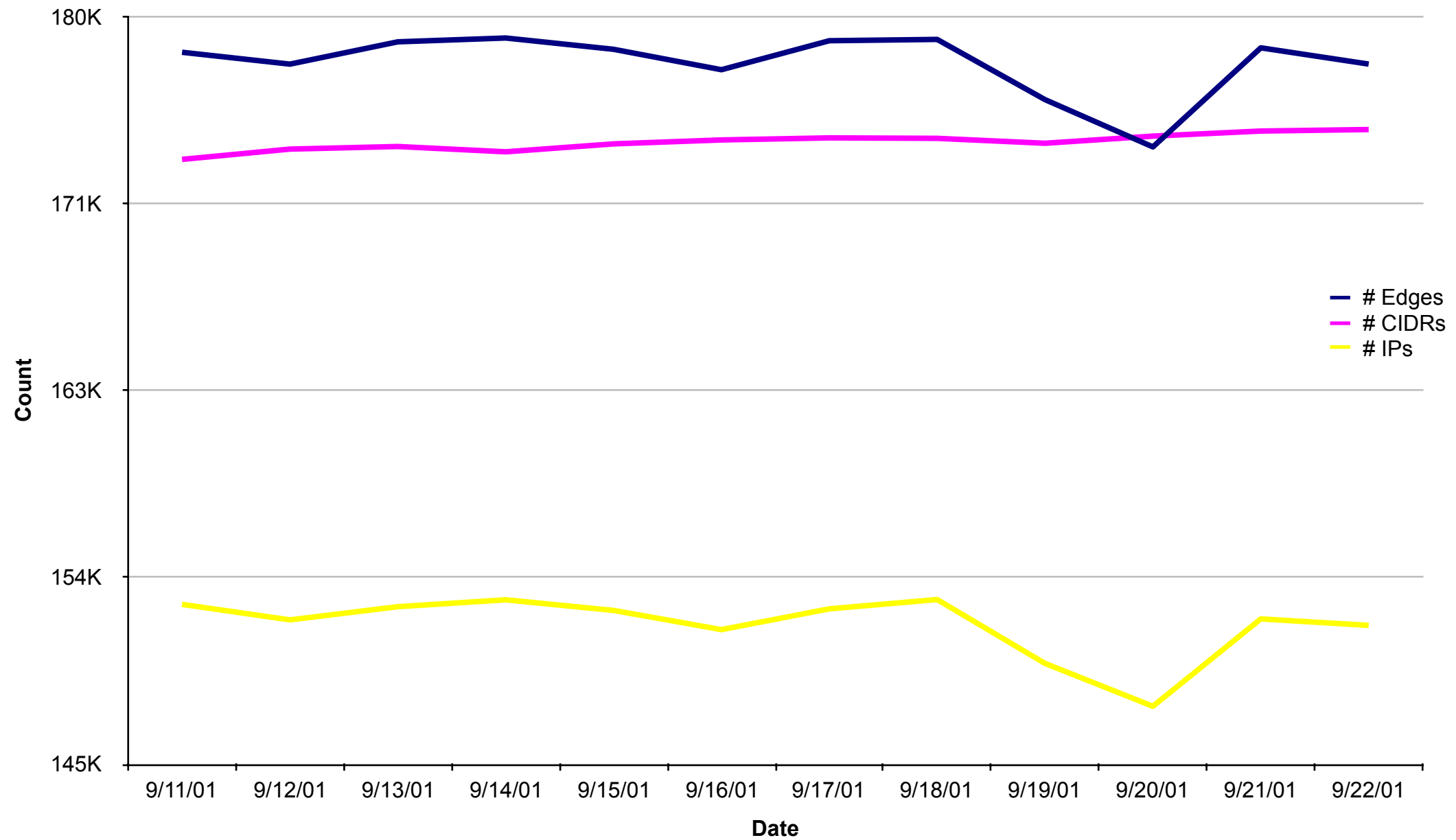




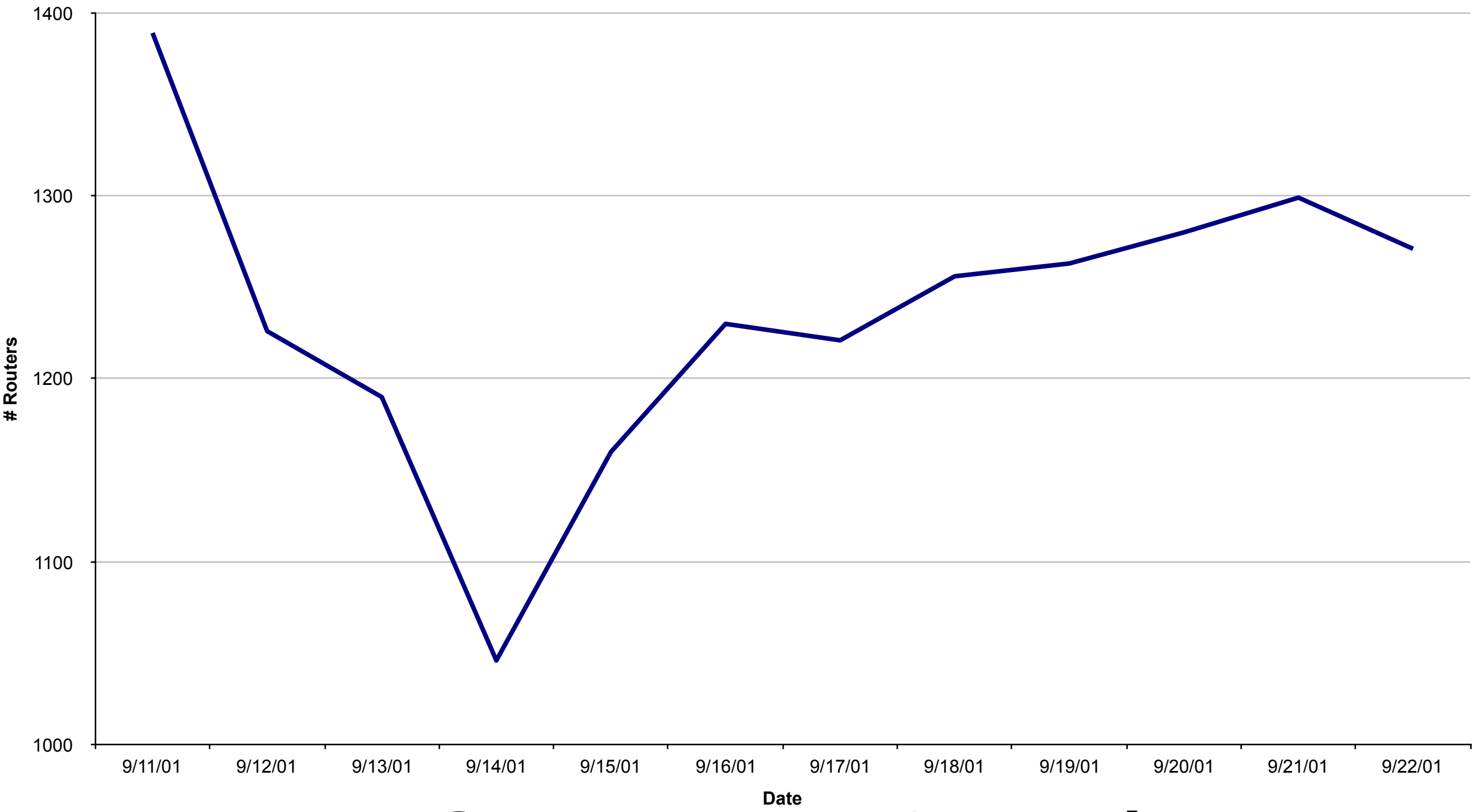
fin

# Serbian propaganda site found

- **Dead babies, “Hiroshima”, etc.**
- **Do I take it down?**
- **Cheswick needs a personal foreign policy**
- **At the time, this might have come as a surprise to the US State Department.**



# The Internet after 9/11

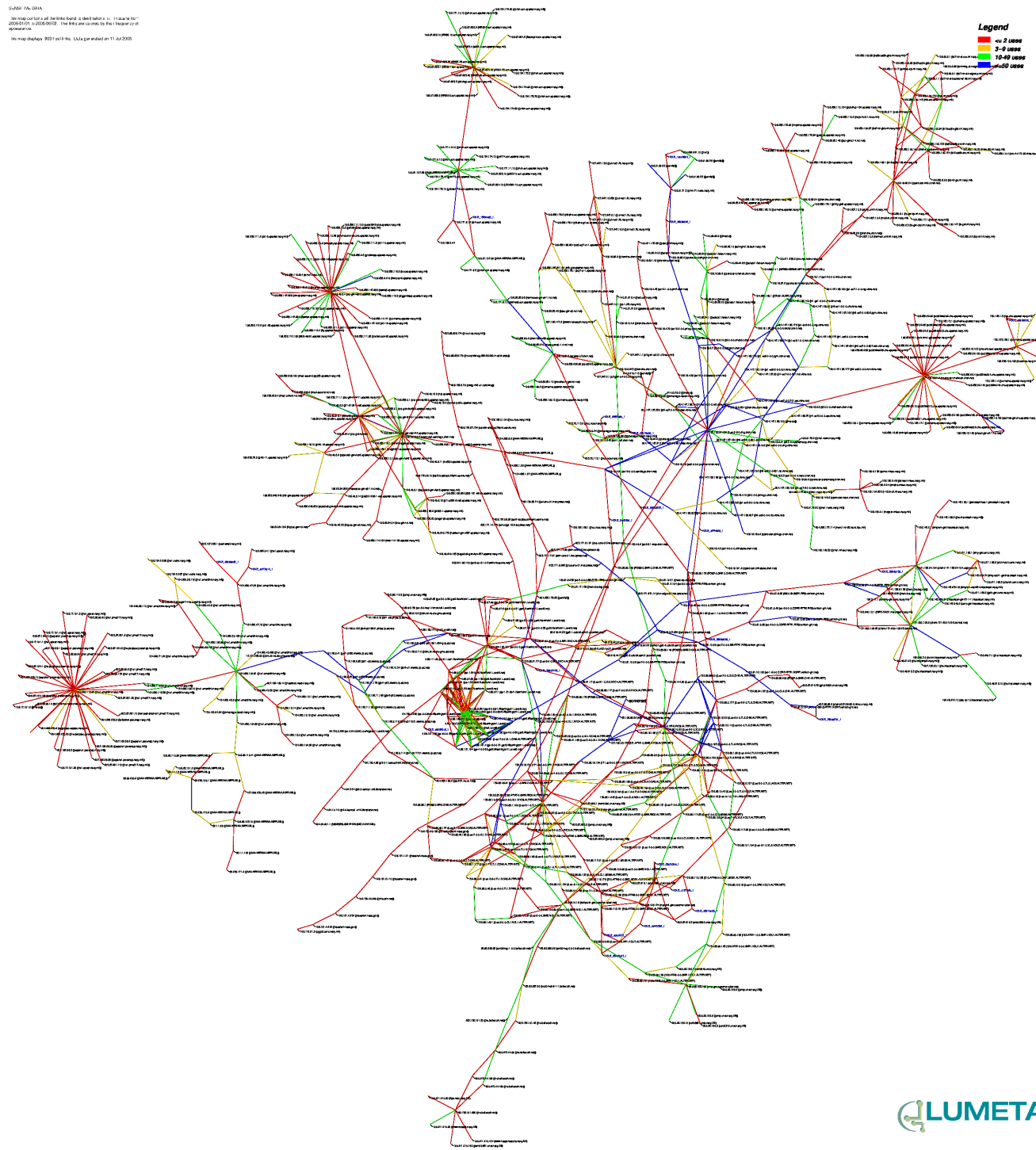


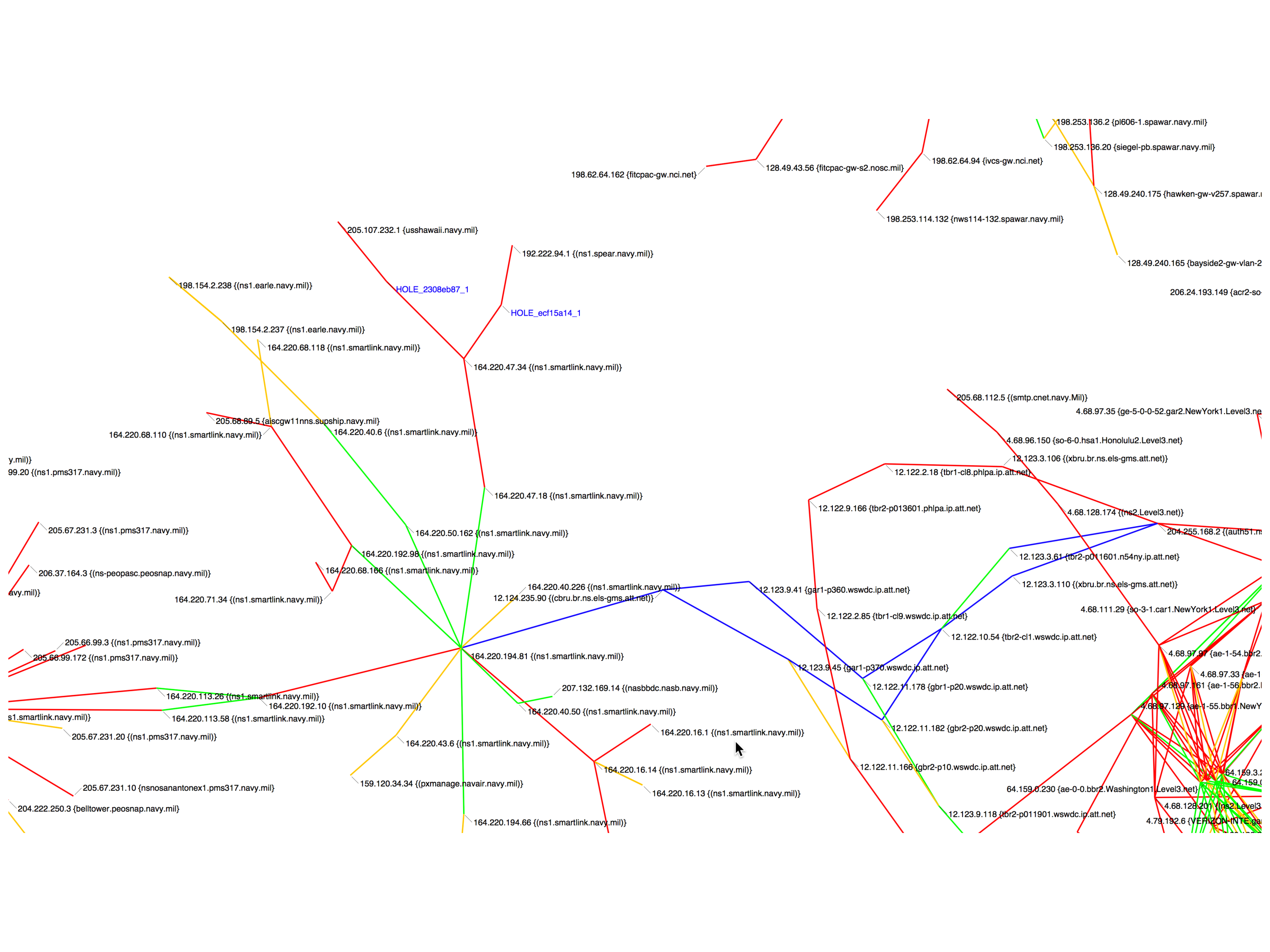
12 of about 56

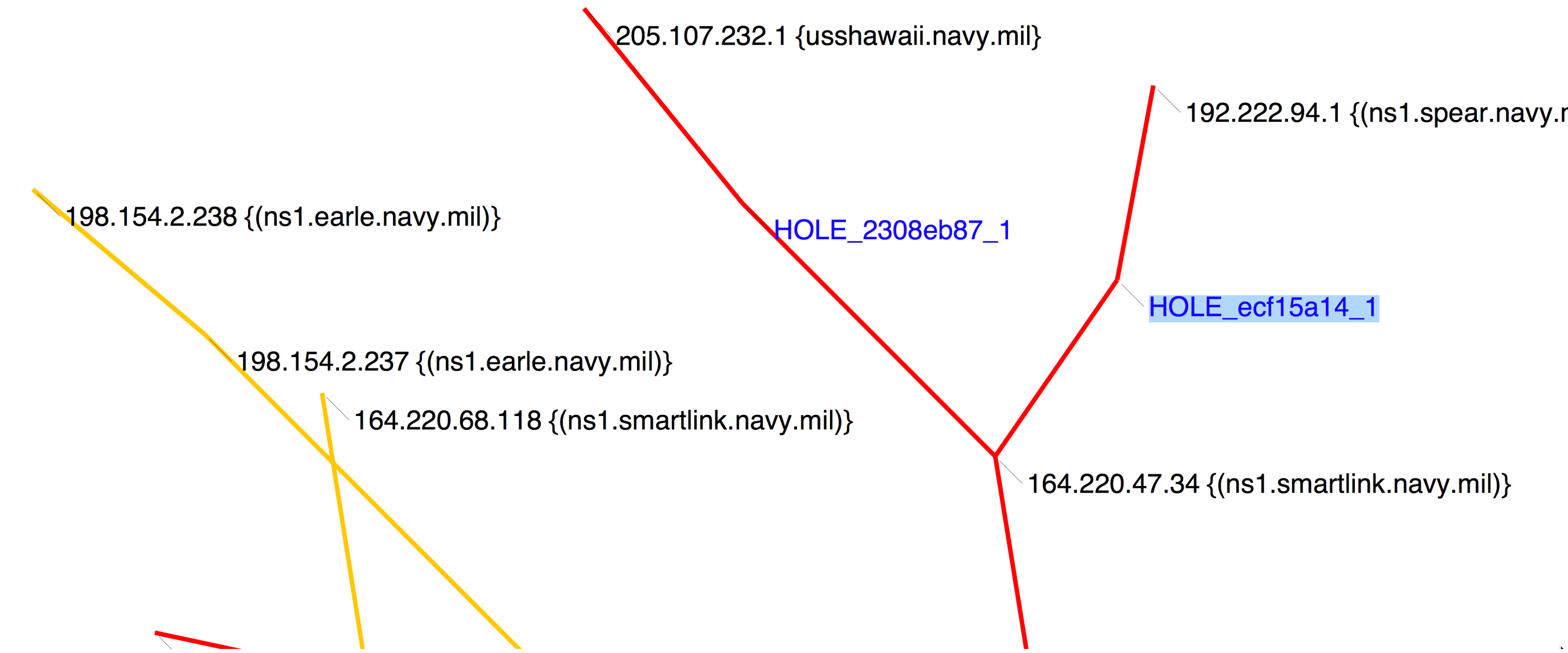
# NYC routers after 9/11

The map contains all the links found in this folder on 11/11/2005 from 2006/01/01 to 2006/06/02. The links are colored by this frequency of appearance.

The map displays 3037 links. Data generated on 11 Jul 2005.









# Fun With Research

**Bill Cheswick**  
**ches@cheswick.com**