Visual Tools for Security: is there a There There?

Bill Cheswick
AT&T Labs - Research
Shannon Labs
ches@research.att.com
http://www.cheswick.com/ches/

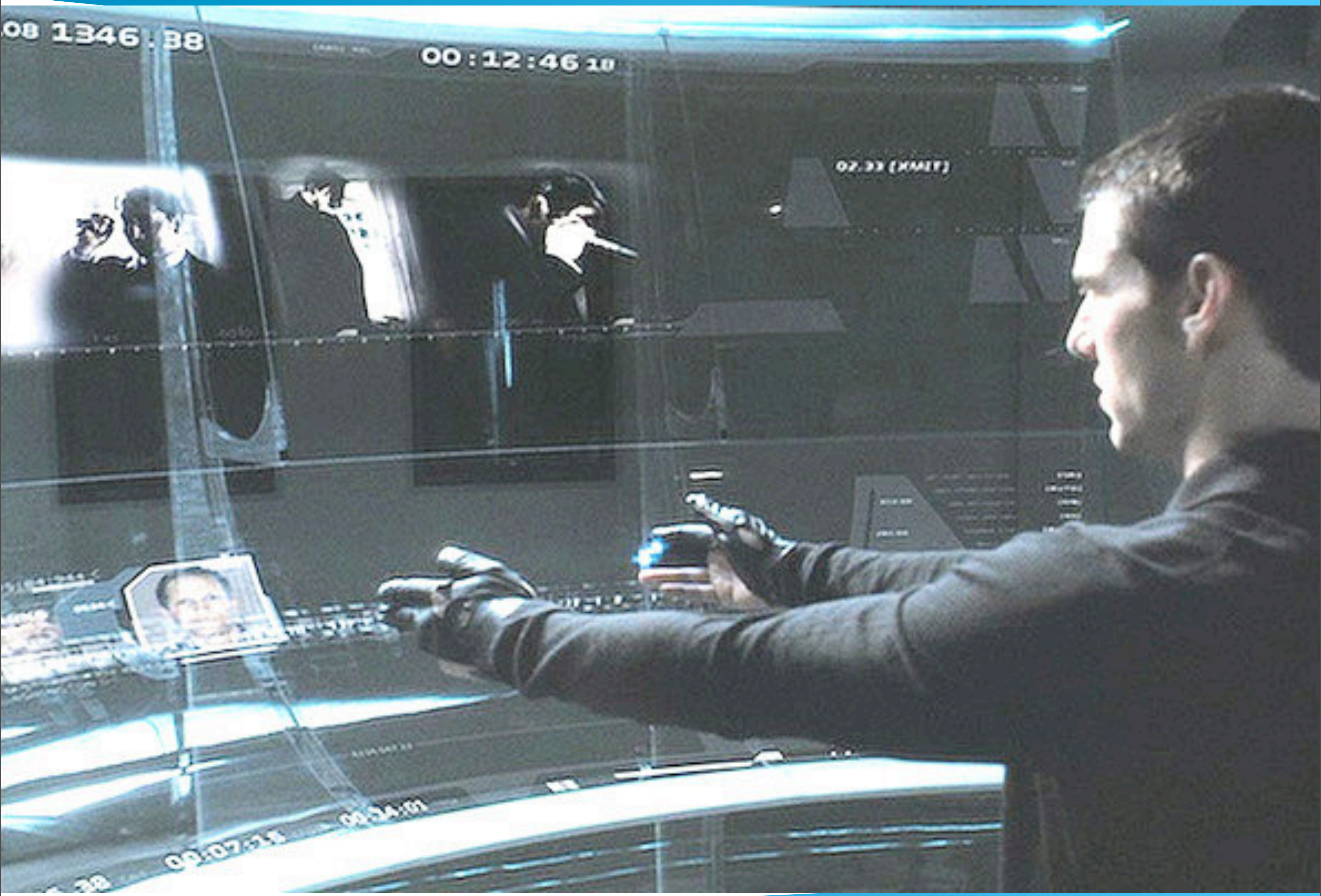
Not الكتاّ Lucent Bell Labs

Limitations

- I know more about security than visualization
- The *Related Works* portion of this talk would be weak.
- I'll be around all week: feel free to set me straight

The Case for Visualization

- Complex software, networks, and network traffic are way too much for a human to grok
- Visual input offers high bandwidth and native mental skills
    - other inputs too
- Modern hardware: offering new opportunities to experiment


08 1346 38
00:12:46 18
02.33 (XMIT)
00:07:15
00:34:01

Johnny Chung Lee (CMU)

Saturn V mission control

NORAD: War Games (1983)

NORAD, 9/11

AT&T GNOC

AT&T GNOC

GNOC
THE ONLY WAY TO EAT
SNOOP DOGG, JT THE BIGGA FIGGA
MISTAH F.A.B., ANDRE NICKATINA, SAN QUINN
CLOUDYMINDZ, TEAM GUTTA AND MORE !!

Accenture Global Network Ops

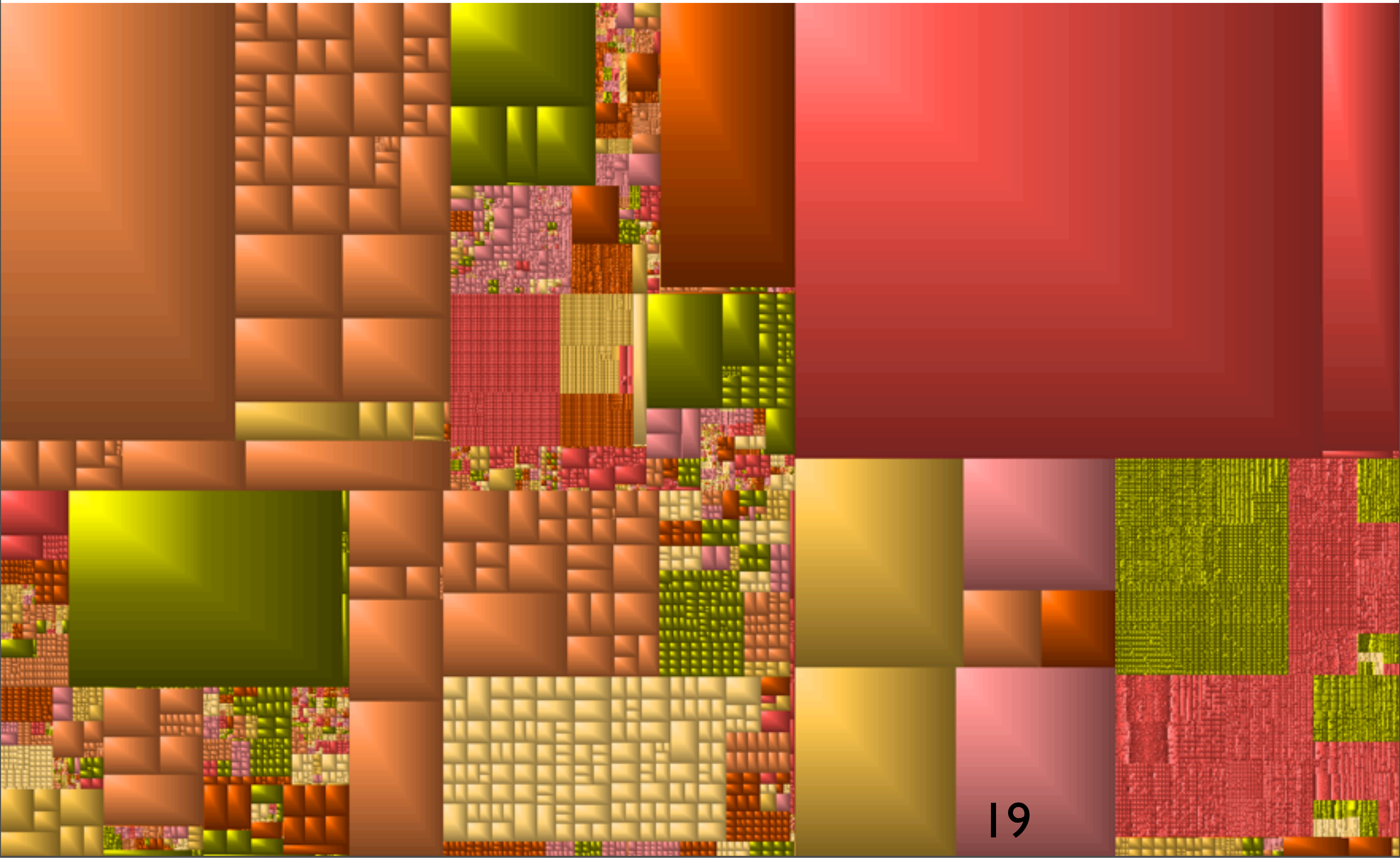
I’ve seen a lot of ideas

- and lots of startups
- but actual deployment seems to be lagging
- Microsoft hasn’t changed much in Windows
- Mac has cover views and multitouch is coming to all
- Cooliris

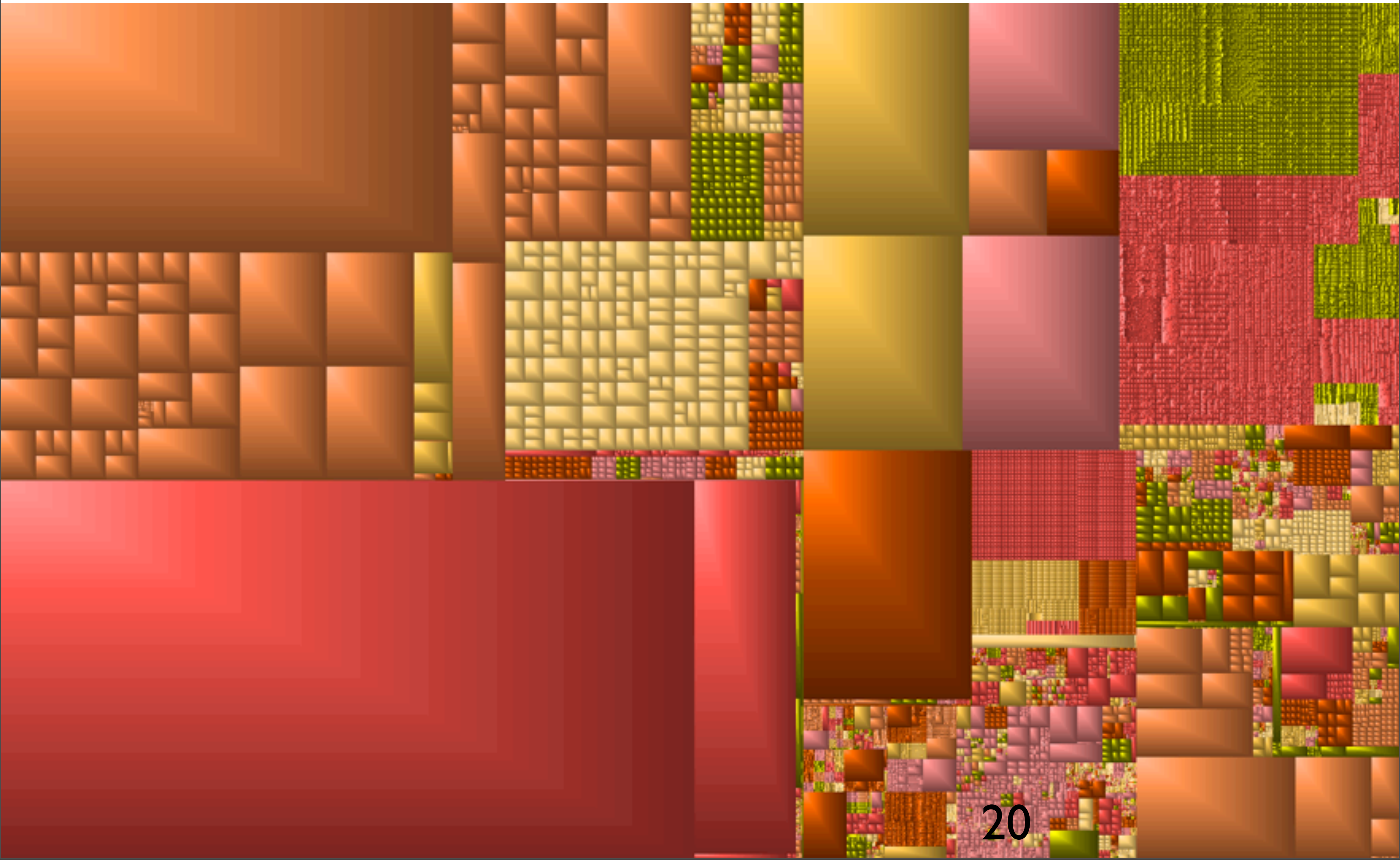
Case in point: treemap

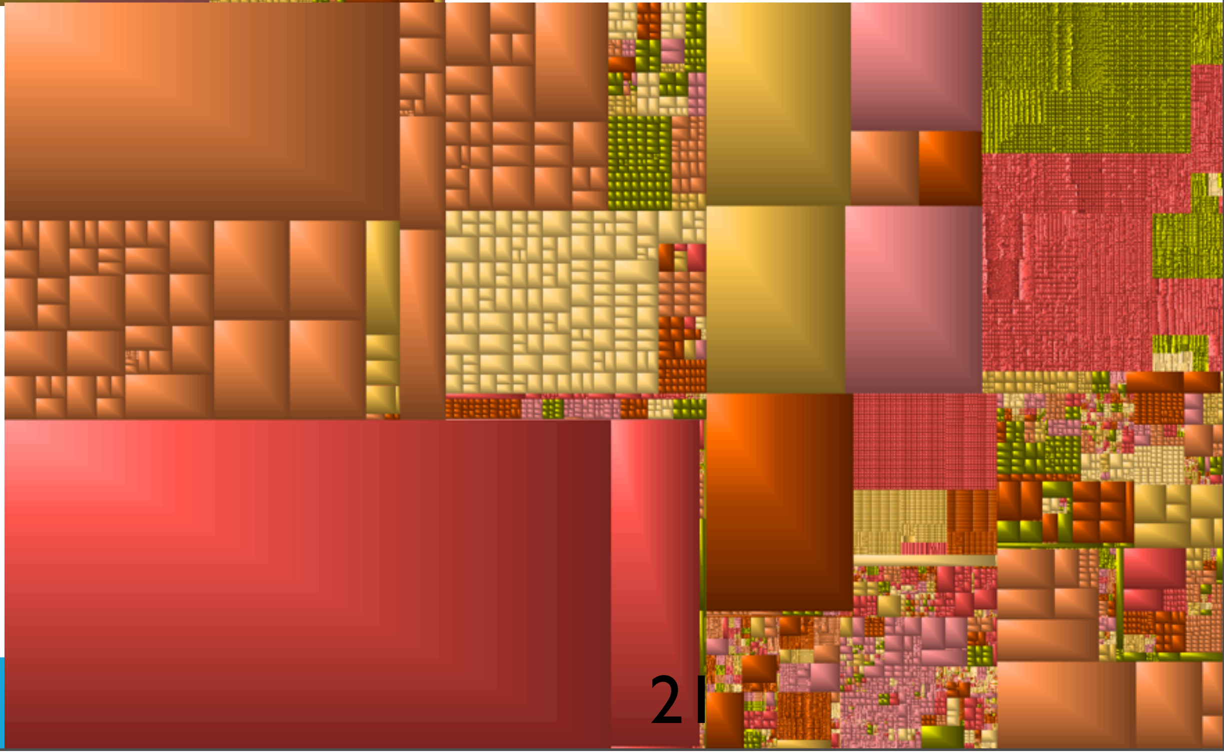
- Treemap came out in 1992. Not widely adopted.
- treemap on the Mac

Before



After



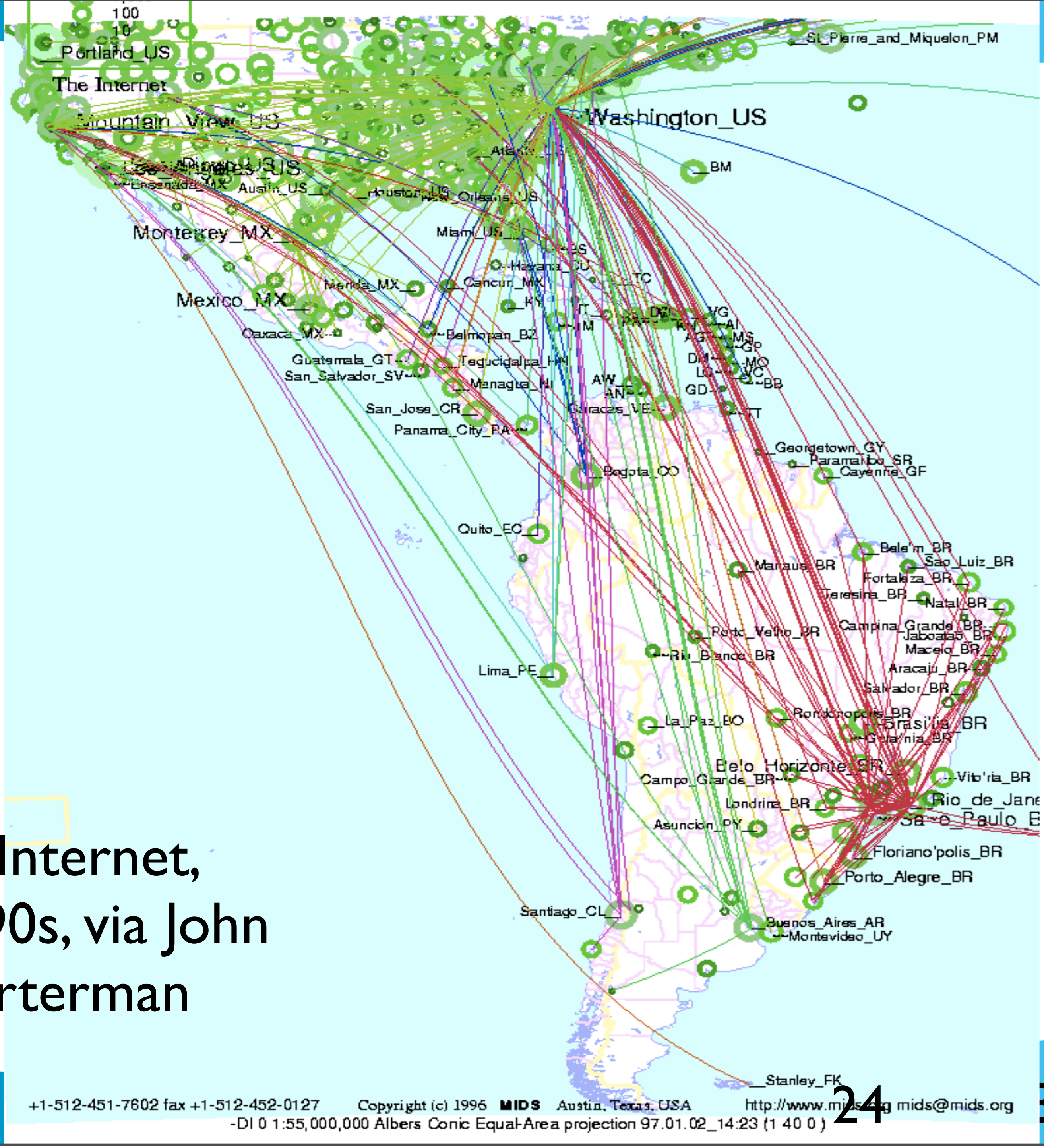


Problems

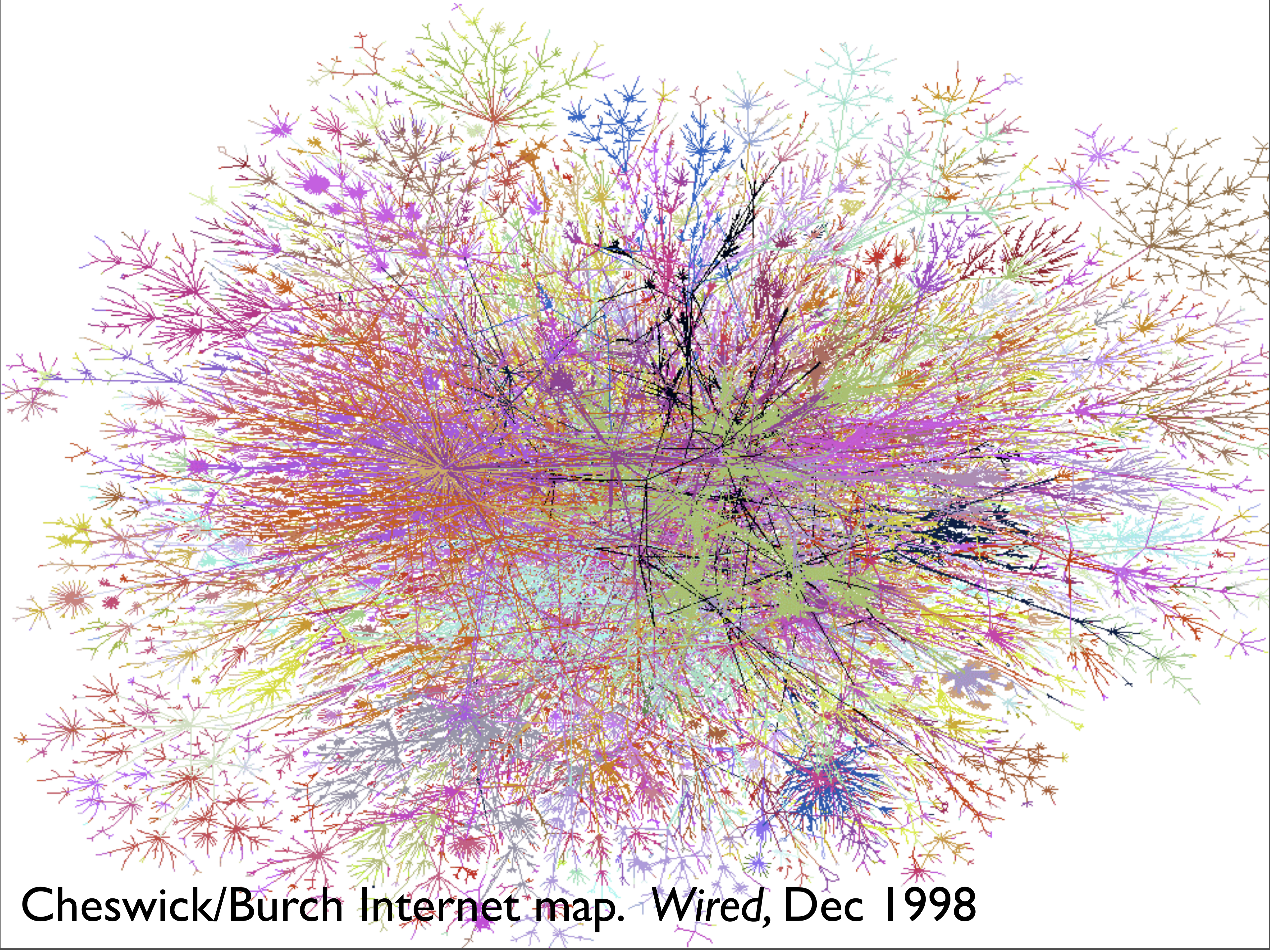
- The layout is made in arbitrary space
- Evolution to new arbitrary space is not shown
- The removed areas are not shown
- Both destroy context

This is a crude use, it may be unfair

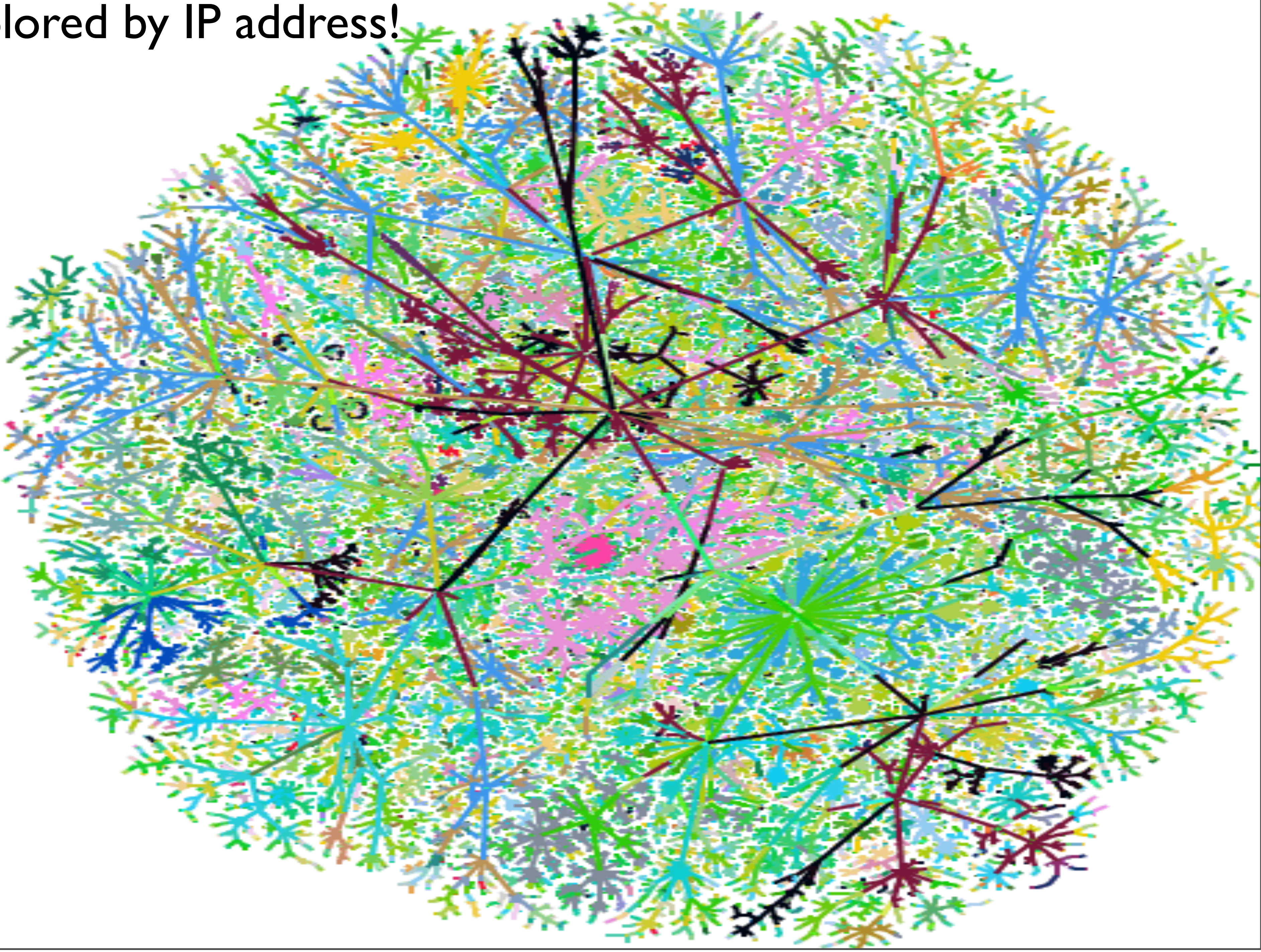
- I just grabbed a tool and used it
- The tool, and these ideas, would be more useful, and maybe adopted



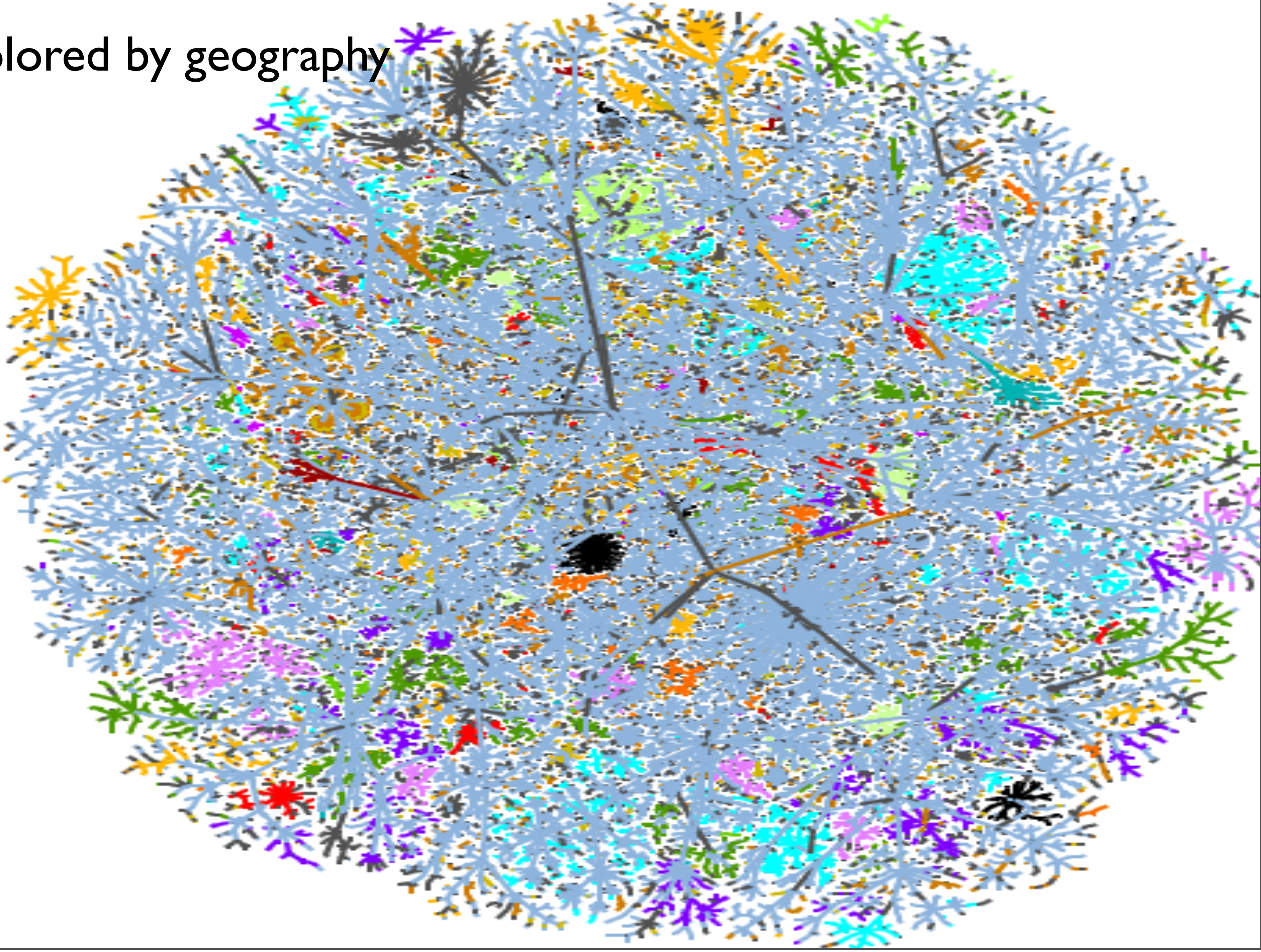
The Internet, mid-1990s, via John Quarterman



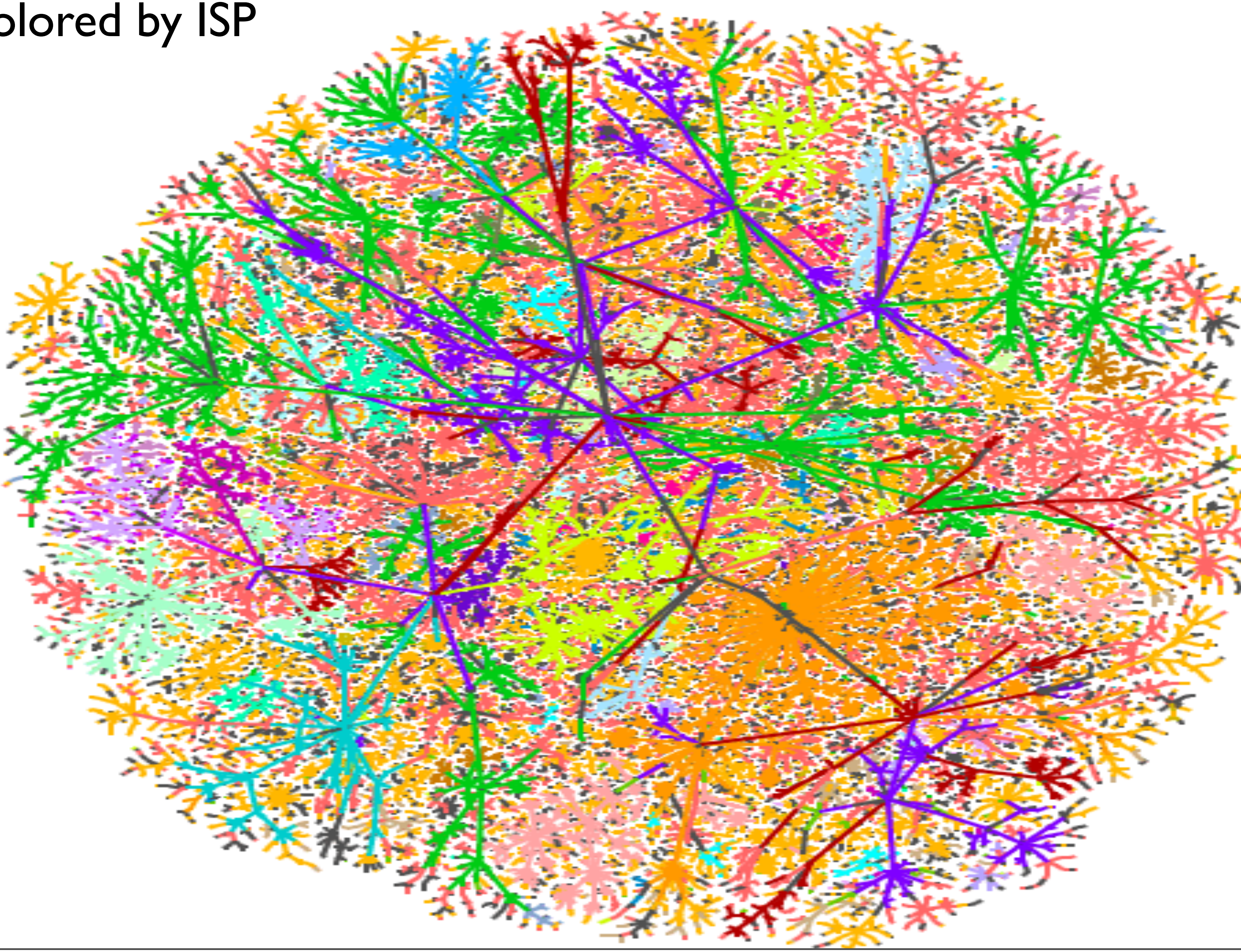
Cheswick/Burch Internet map. *Wired,* Dec 1998 olored by IP address!

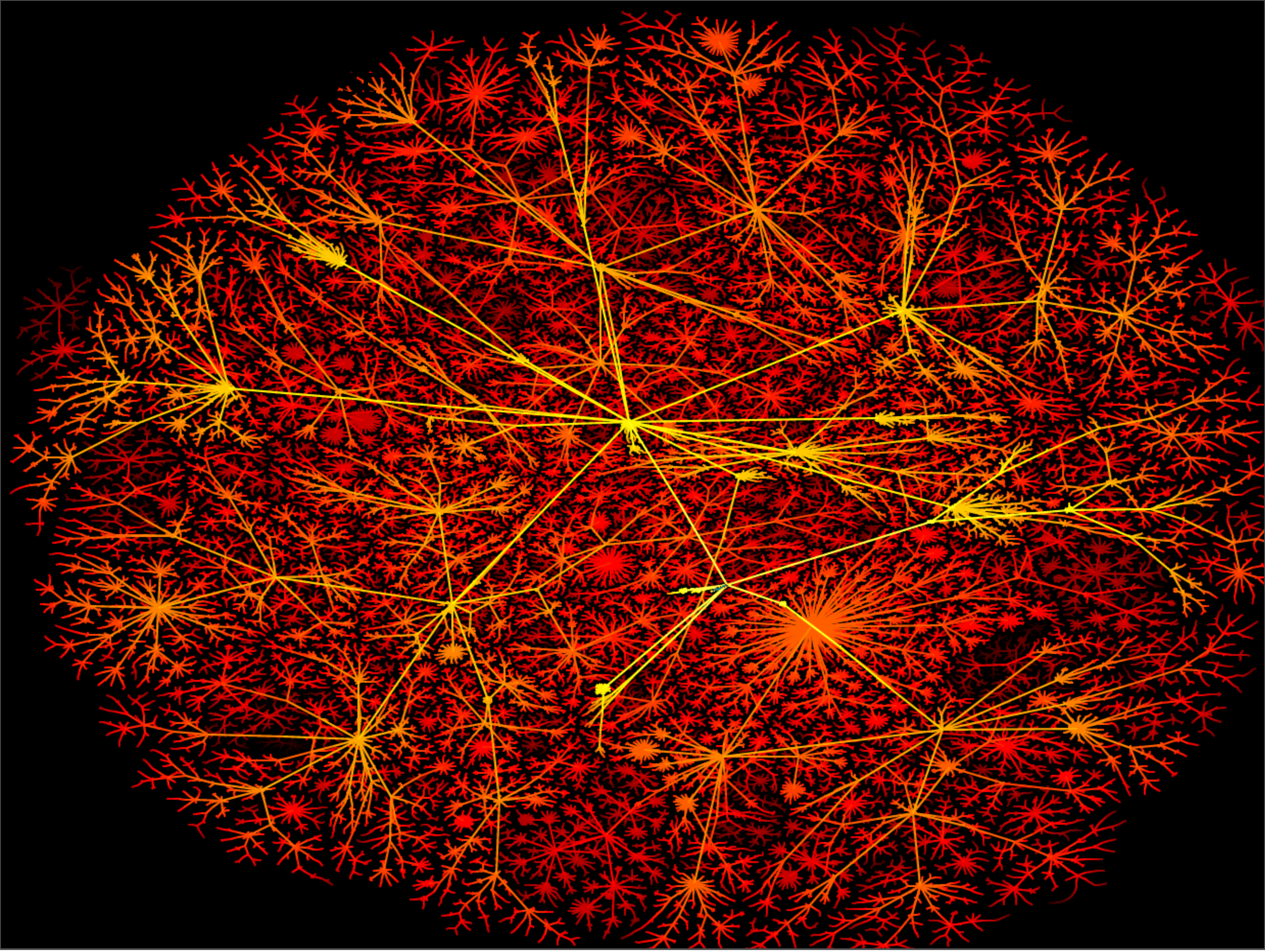


olored by geography



Colored by ISP

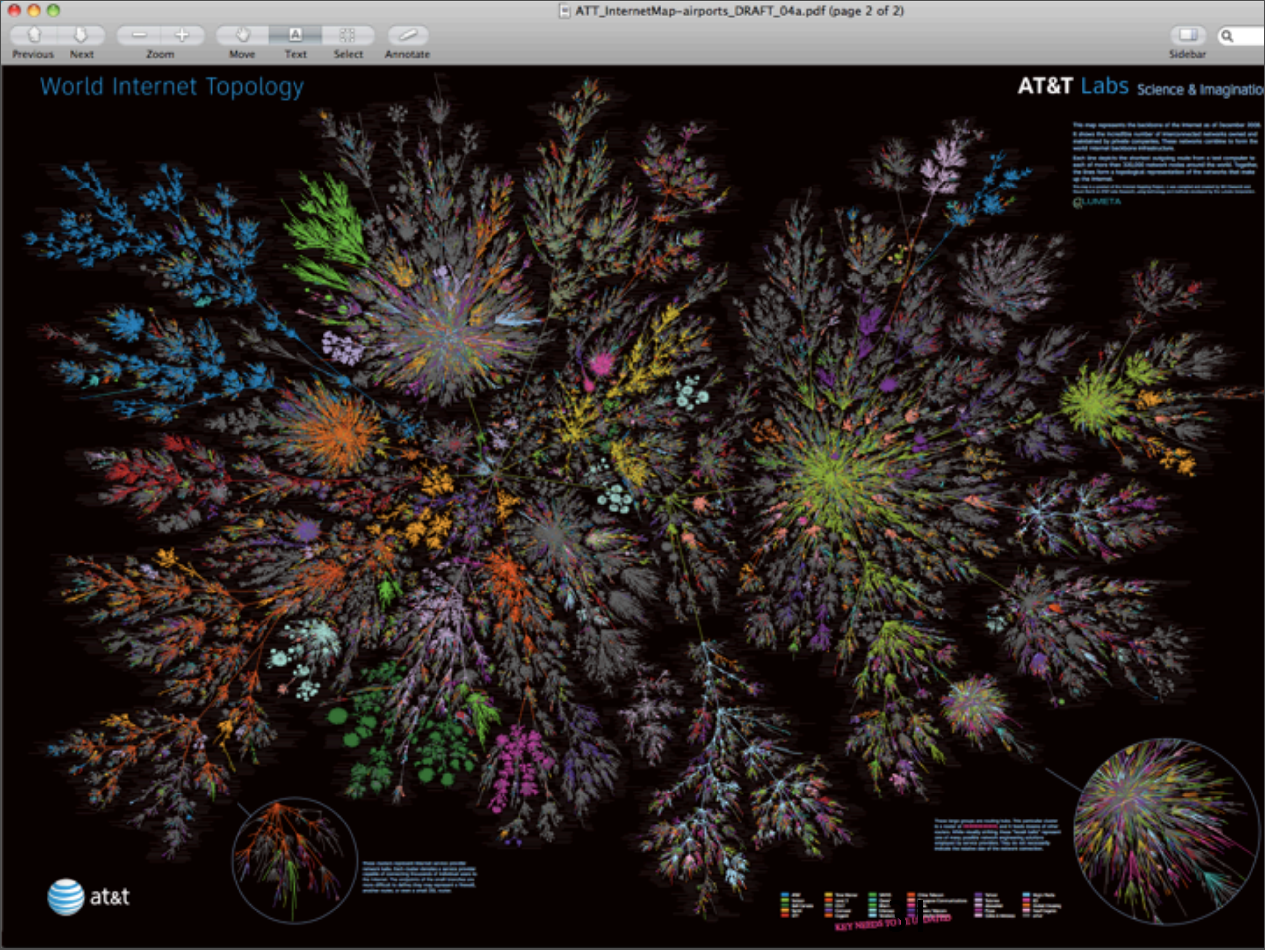




All of these are cheats

- They are minimum spanning trees of all the data
- about 35% of the raw data is discarded
- For some uses, that doesn't matter

at&t

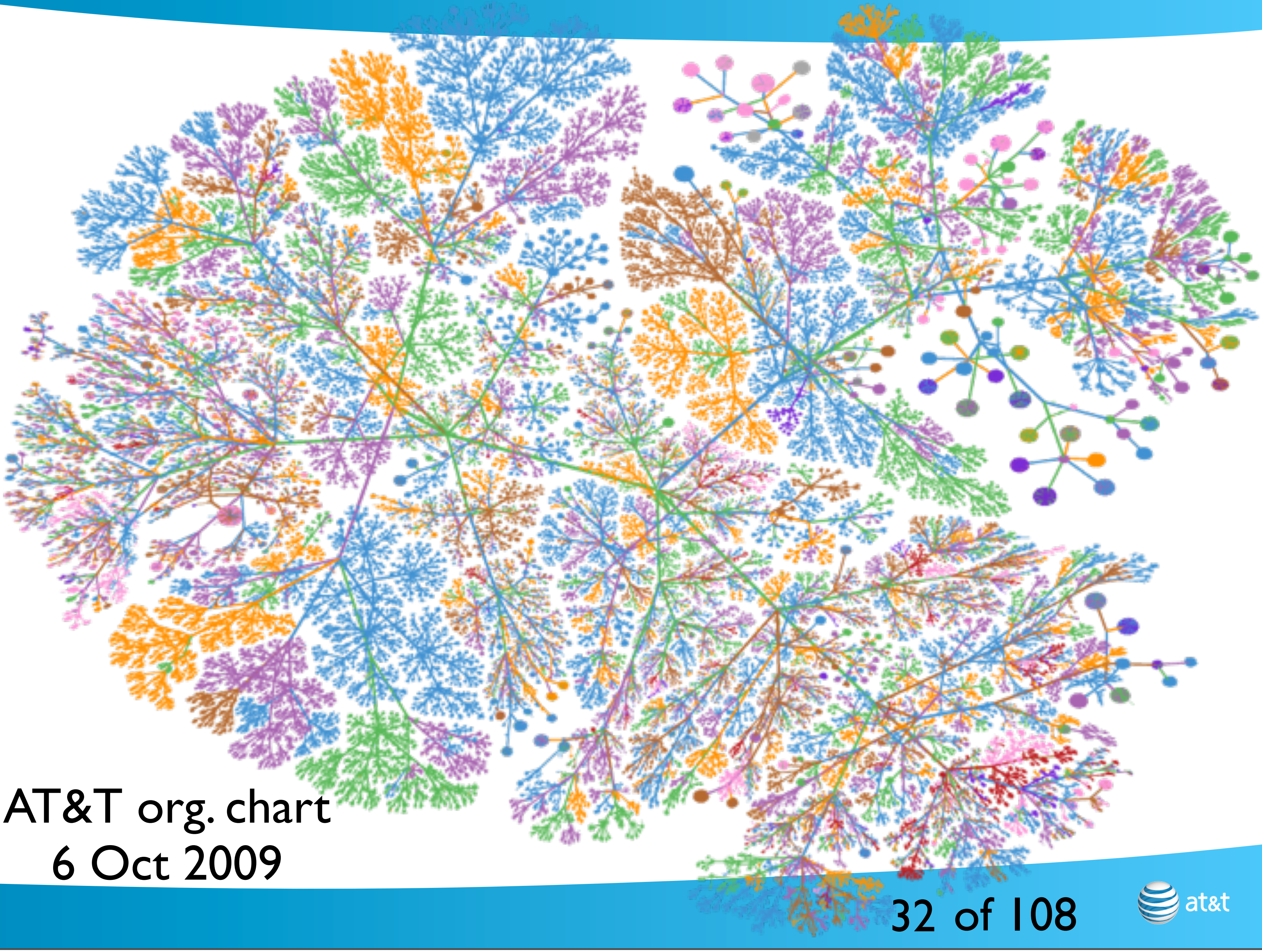


This map represents the backbone of the Internet as of December 2008.

It shows the incredible number of interconnected networks owned and maintained by private companies. These networks combine to form the world Internet backbone infrastructure.

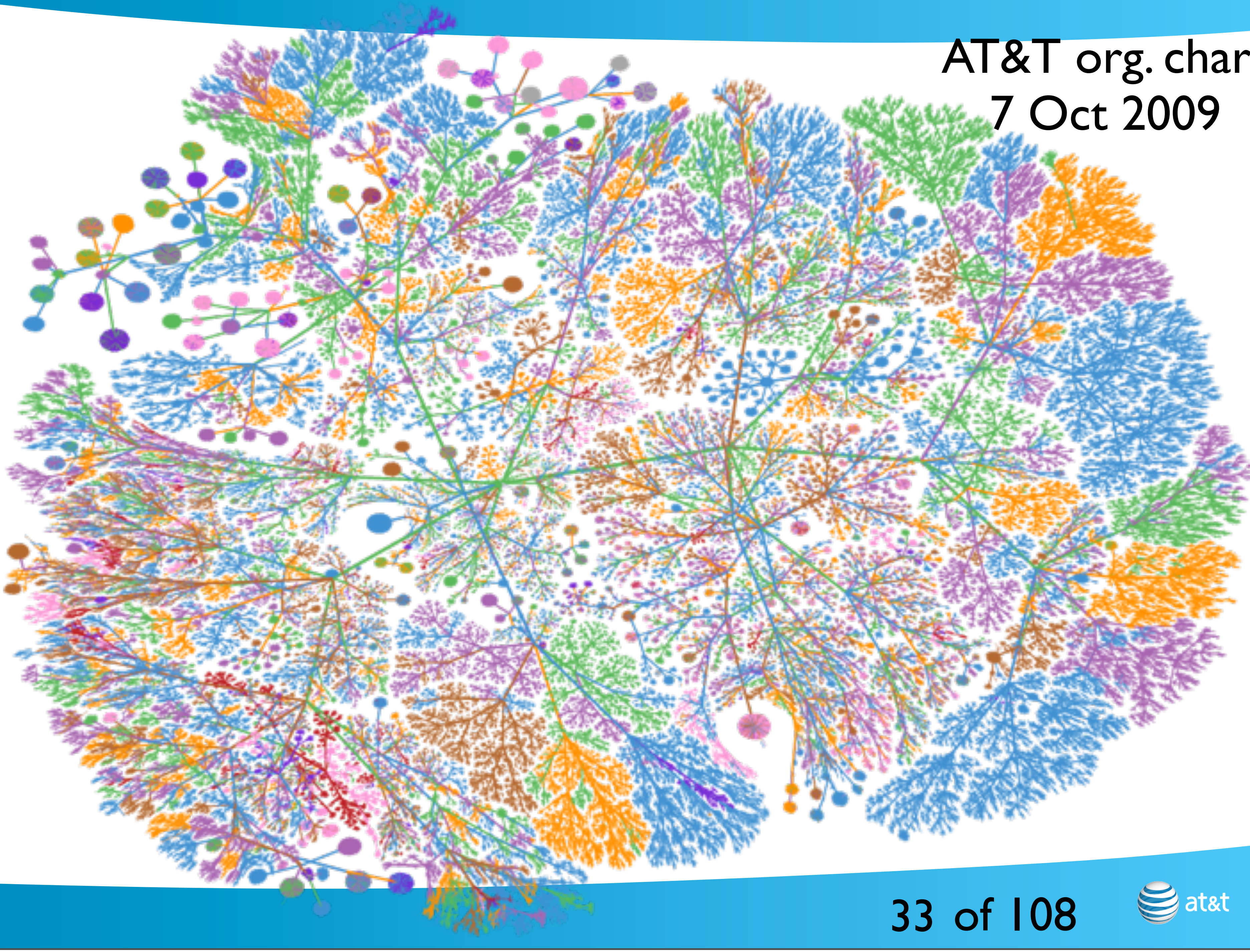
Each line depicts the shortest outgoing route from a test computer to each of more than 330,000 network nodes around the world. Together, the lines form a topological representation of the networks that make up the Internet.

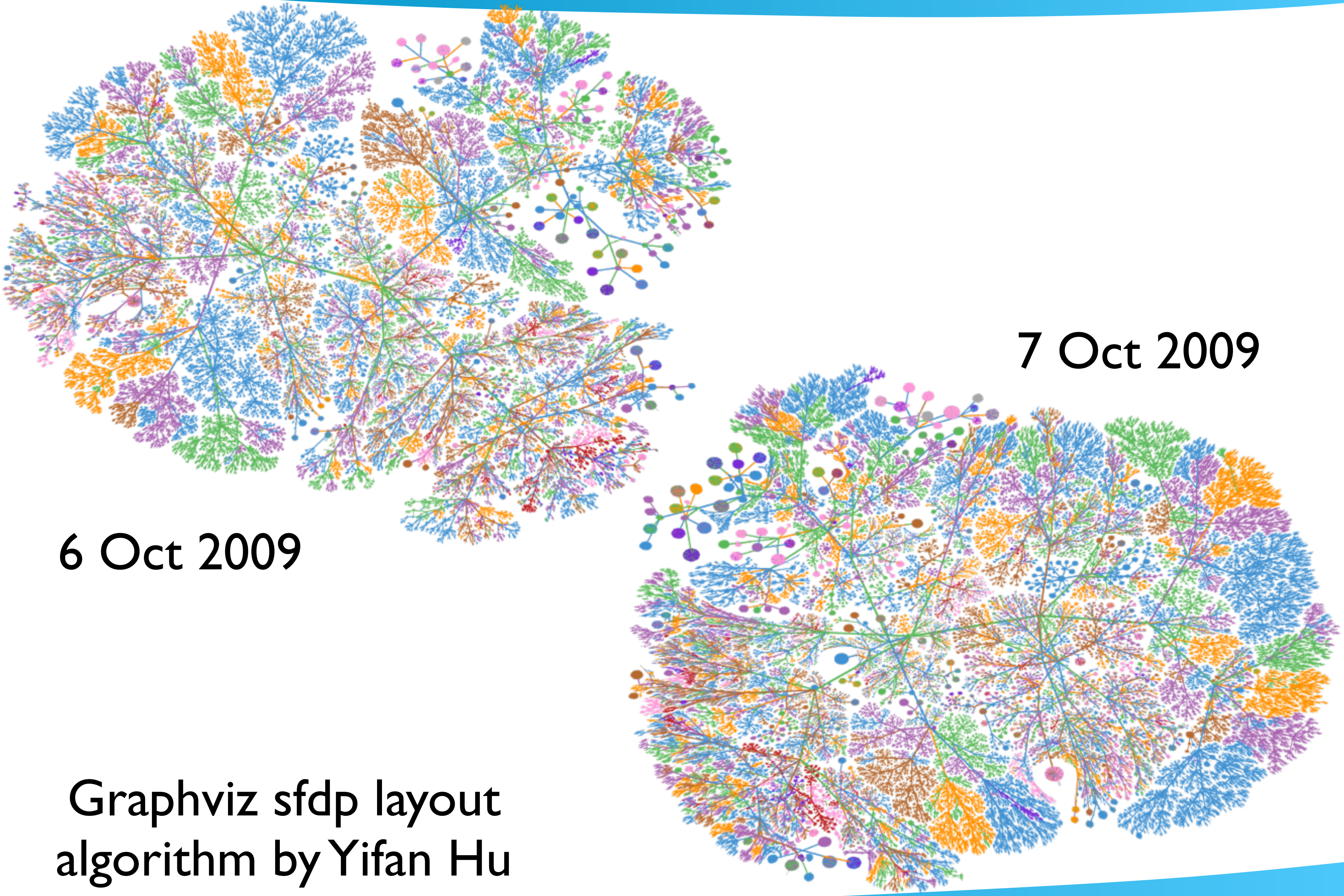
[illegible]



AT&T org. chart
6 Oct 2009

AT&T org. chart
7 Oct 2009





6 Oct 2009

7 Oct 2009

Graphviz sfdp layout algorithm by Yifan Hu

Consistency helps the user

- Consistent layouts would be very helpful, especially in arbitrary spaces
- Incremental layouts ought to be available

Implementations are often idiosyncratic

- Implemented in unusual systems, like Mathematica, or strange shell loops
- RUMINT is okay if you are running Windows, but what if you don't trust Windows
- Many network administrators prefer Linux or FreeBSD

Fancy solutions can hinder adoption

- Peep (The Network Auralizer), *Gilfix and Couch*, LISA 2000
- “This system combines network state information from multiple data sources, by mixing audio signals into a single audio stream in real time.”
- This is a very cool idea

Peep

- *n.b.* audio is a kind of visualization
- Needs to be easy and install and try out
- Needs to have good security properties when running

How Do You Measure Security?

- Generals and CIOs want to know. So do insurance companies

When you can measure what you are speaking about, and express it in numbers, you know something about it. But when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind: it may be the beginning of knowledge, but you have scarcely. . . advanced to the state of science.

- Lord Kelvin

Measuring security

- Safes: withstand 30 minutes of prying
- Nuclear weapons: resistance to misuse
- Computers: withstands x hours of attack by y people of z capability?

Many want to measure computer security

- change one bit in a gigabyte of programs? Two bits? Measure security brittleness?
- Trusecure: there always seems to be a human judge at one step

Some places to measure security

1. OS security: gaining privilege from a user's account
2. Network services security: gaining access to a networked computer
3. Attack surface, and code dependencies
4. Network topological security: gaining access to network access to a host

Measuring Network Access Security

```
netstat -an | wc -l
```

Win ME

```
Active Connections - Win ME

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1032         0.0.0.0:0              LISTENING
  TCP    223.223.223.10:139     0.0.0.0:0              LISTENING
  UDP    0.0.0.0:1025           *:*
  UDP    0.0.0.0:1026           *:*
  UDP    0.0.0.0:31337          *:*
  UDP    0.0.0.0:162            *:*
  UDP    223.223.223.10:137     *:*
  UDP    223.223.223.10:138     *:*
```

Win 2K

```
Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1029           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1036           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1078           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1080           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1086           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:6515           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:139          0.0.0.0:0              LISTENING
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1038           *:*
  UDP    0.0.0.0:6514           *:*
  UDP    0.0.0.0:6515           *:*
  UDP    127.0.0.1:1108         *:*
  UDP    223.223.223.96:500     *:*
  UDP    223.223.223.96:4500    *:*
```

Win XP pre-SP2

```
Proto  Local Address          Foreign Address        State
 TCP    ches-pc:epmap          ches-pc:0              LISTENING
 TCP    ches-pc:microsoft-ds   ches-pc:0              LISTENING
 TCP    ches-pc:1025           ches-pc:0              LISTENING
 TCP    ches-pc:1036           ches-pc:0              LISTENING
 TCP    ches-pc:3115           ches-pc:0              LISTENING
 TCP    ches-pc:3118           ches-pc:0              LISTENING
 TCP    ches-pc:3470           ches-pc:0              LISTENING
 TCP    ches-pc:3477           ches-pc:0              LISTENING
 TCP    ches-pc:5000           ches-pc:0              LISTENING
 TCP    ches-pc:6515           ches-pc:0              LISTENING
 TCP    ches-pc:netbios-ssn    ches-pc:0              LISTENING
 TCP    ches-pc:3001           ches-pc:0              LISTENING
 TCP    ches-pc:3002           ches-pc:0              LISTENING
 TCP    ches-pc:3003           ches-pc:0              LISTENING
 TCP    ches-pc:5180           ches-pc:0              LISTENING
 UDP    ches-pc:microsoft-ds   *:*
 UDP    ches-pc:isakmp         *:*
 UDP    ches-pc:1027           *:*
 UDP    ches-pc:3008           *:*
 UDP    ches-pc:3473           *:*
 UDP    ches-pc:6514           *:*
 UDP    ches-pc:6515           *:*
 UDP    ches-pc:netbios-ns     *:*
 UDP    ches-pc:netbios-dgm    *:*
 UDP    ches-pc:1900           *:*
 UDP    ches-pc:ntp            *:*
 UDP    ches-pc:1900           *:*
 UDP    ches-pc:3471           *:*
```

Guiding security principle for servers

- “You’ve got to get out of the game.” - Fred Grampp
- “Best block is not be there.” - Mr. Miyagi, Karate Kid 2

Measuring network security

- netstat -an
  - doesn't show the efforts of firewalls
- nmap output?

My FreeBSD machine

```
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address
tcp4       0      0  *.22
tcp6       0      0  *.22
```

Microsoft wasn’t the first

SGI Irix

```
ftp     stream  tcp     nowait  root    /v/gate/ftpd
telnet  stream  tcp     nowait  root    /usr/etc/telnetd
shell   stream  tcp     nowait  root    /usr/etc/rshd
login   stream  tcp     nowait  root    /usr/etc/rlogind
exec    stream  tcp     nowait  root    /usr/etc/rexecd
finger  stream  tcp     nowait  guest   /usr/etc/fingerd
bootp   dgram   udp     wait    root    /usr/etc/bootp
tftp    dgram   udp     wait    guest   /usr/etc/tftpd
ntalk   dgram   udp     wait    root    /usr/etc/talkd
tcpmux  stream  tcp     nowait  root    internal
echo    stream  tcp     nowait  root    internal
discard stream  tcp     nowait  root    internal
chargen stream  tcp     nowait  root    internal
daytime stream  tcp     nowait  root    internal
time    stream  tcp     nowait  root    internal
echo    dgram   udp     wait    root    internal
discard dgram   udp     wait    root    internal
chargen dgram   udp     wait    root    internal
daytime dgram   udp     wait    root    internal
time    dgram   udp     wait    root    internal
sgi-dgl stream  tcp     nowait  root/rcv dgld
uucp   stream  tcp      nowait  root    /usr/lib/uucp/uucpd
```

SGI Irix (cont.)

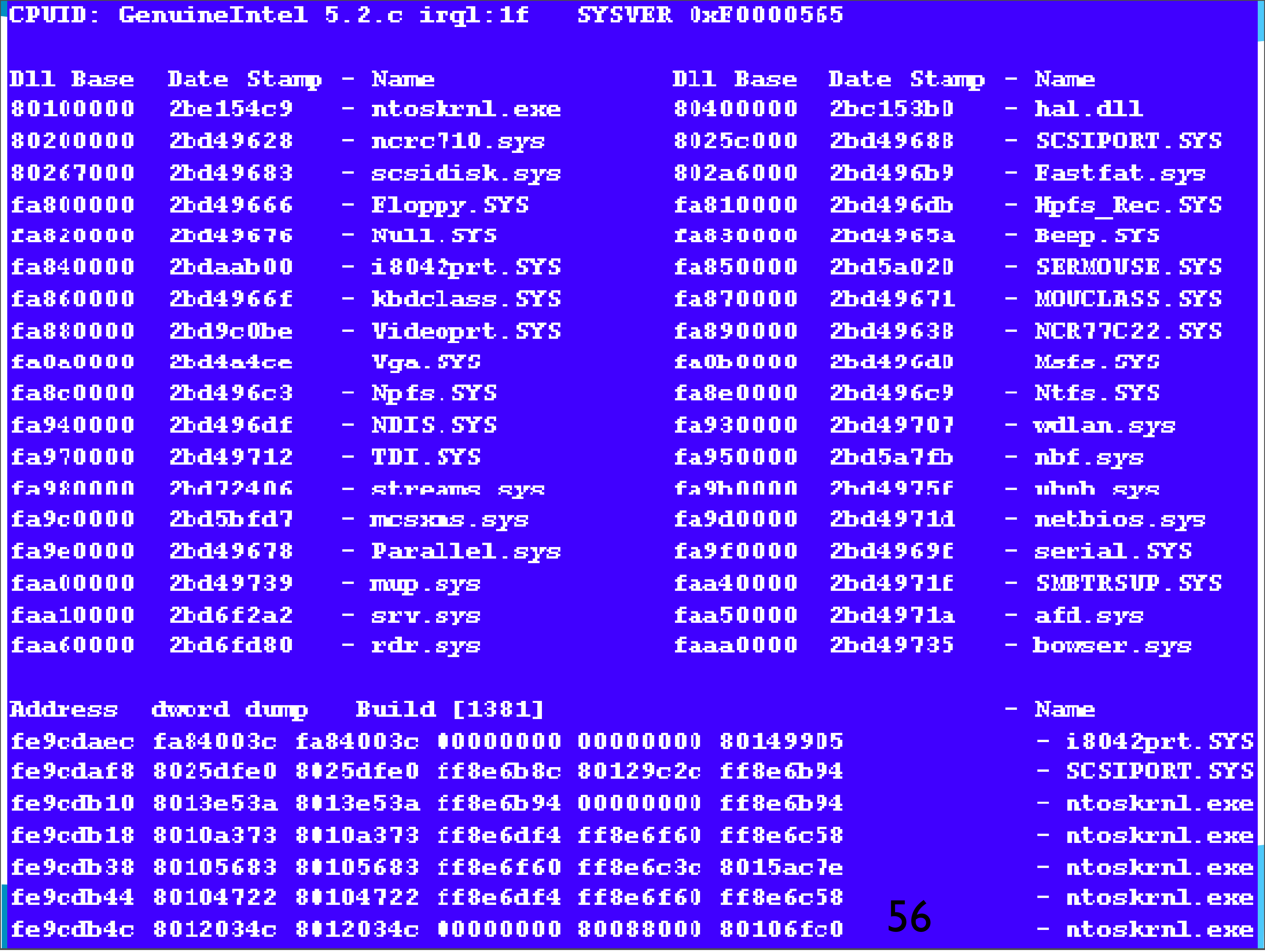
```
mountd/1    stream  rpc/tcp wait/lc    root    rpc.mountd
mountd/1    dgram   rpc/udp wait/lc    root    rpc.mountd
sgi_mountd/1 stream rpc/tcp wait/lc    root    rpc.mountd
sgi_mountd/1 dgram  rpc/udp wait/lc    root    rpc.mountd
rstatd/1-3  dgram   rpc/udp wait       root    rpc.rstatd
walld/1     dgram   rpc/udp wait       root    rpc.rwalld
rusersd/1   dgram   rpc/udp wait       root    rpc.rusersd
rquotad/1   dgram   rpc/udp wait       root    rpc.rquotad
sprayd/1    dgram   rpc/udp wait       root    rpc.sprayd
bootparam/1 dgram   rpc/udp wait       root    rpc.bootparamd
sgi_videod/1 stream rpc/tcp wait       root    ?videod
sgi_fam/1   stream  rpc/tcp wait       root    ?fam
sgi_snoopd/1 stream rpc/tcp wait       root    ?rpc.snoopd
sgi_pcsd/1  dgram   rpc/udp wait       root    ?cvpcsd
sgi_pod/1   stream  rpc/tcp wait       root    ?podd
tcpmux/sgi_scanner stream tcp nowait   root    ?scan/net/scannerd
tcpmux/sgi_printer stream tcp nowait   root    ?print/printerd
9fs         stream  tcp     nowait     root    /v/bin/u9fs u9fs
webproxy    stream  tcp     nowait     root    /usr/local/etc/webserv
```

Measuring OS privilege escalation

- Moving from user privileges to root
- Much too easy, in my judgement
  - Prefer single-user machines
  - *Not* the right answer in many research environments

Unix Host Security

```
find / -perm -4000
-user root -print |
wc -l
```



```
CPUID: GenuineIntel 5.2.c irql:1f    SYSVER 0xF0000565

Dll Base  Date Stamp - Name               Dll Base  Date Stamp - Name
80100000  2be154c9   - ntoskrnl.exe       80400000  2bc153b0   - hal.dll
80200000  2bd49628   - ncrc710.sys        8025c000  2bd49688   - SCSIPORT.SYS
80267000  2bd49683   - scsidisk.sys       802a6000  2bd496b9   - Fastfat.sys
fa800000  2bd49666   - Floppy.SYS         fa810000  2bd496db   - Hpfs_Rec.SYS
fa820000  2bd49676   - Null.SYS           fa830000  2bd4965a   - Beep.SYS
fa840000  2bdaab00   - i8042prt.SYS       fa850000  2bd5a020   - SERMOUSE.SYS
fa860000  2bd4966f   - kbdclass.SYS       fa870000  2bd49671   - MOUCLASS.SYS
fa880000  2bd9c0be   - Videoprt.SYS       fa890000  2bd49638   - NCR77C22.SYS
fa0a0000  2bd4a4ce     Vga.SYS            fa0b0000  2bd496d0     Msfs.SYS
fa8c0000  2bd496c3   - Npfs.SYS           fa8e0000  2bd496c9   - Ntfs.SYS
fa940000  2bd496df   - NDIS.SYS           fa930000  2bd49707   - wdlan.sys
fa970000  2bd49712   - TDI.SYS            fa950000  2bd5a7fb   - nbf.sys
fa980000  2bd72406   - streams.sys        fa9b0000  2bd4975f   - ubnb.sys
fa9c0000  2bd5bfd7   - mcsxms.sys         fa9d0000  2bd4971d   - netbios.sys
fa9e0000  2bd49678   - Parallel.sys       fa9f0000  2bd4969f   - serial.SYS
faa00000  2bd49739   - mup.sys            faa40000  2bd4971f   - SMBTRSUP.SYS
faa10000  2bd6f2a2   - srv.sys            faa50000  2bd4971a   - afd.sys
faa60000  2bd6fd80   - rdr.sys            faaa0000  2bd49735   - bowser.sys

Address  dword dump   Build [1381]                             - Name
fe9cdaec fa84003c fa84003c 00000000 00000000 80149905          - i8042prt.SYS
fe9cdaf8 8025dfe0 8025dfe0 ff8e6b8c 80129c2c ff8e6b94          - SCSIPORT.SYS
fe9cdb10 8013e53a 8013e53a ff8e6b94 00000000 ff8e6b94          - ntoskrnl.exe
fe9cdb18 8010a373 8010a373 ff8e6df4 ff8e6f60 ff8e6c58          - ntoskrnl.exe
fe9cdb38 80105683 80105683 ff8e6f60 ff8e6c3c 8015ac7e          - ntoskrnl.exe
fe9cdb44 80104722 80104722 ff8e6df4 ff8e6f60 ff8e6c58          - ntoskrnl.exe
fe9cdb4c 8012034c 8012034c 00000000 80088000 80106fc0          - ntoskrnl.exe
```

```
/bin/rcp
/sbin/ping
/sbin/ping6
/sbin/shutdown
/usr/X11R6/bin/Xwrapper
/usr/X11R6/bin/xterm
/usr/X11R6/bin/Xwrapper-4
/usr/bin/keyinfo
/usr/bin/keyinit
/usr/bin/lock
/usr/bin/crontab
/usr/bin/opieinfo
/usr/bin/opiepasswd
/usr/bin/rlogin
/usr/bin/quota
/usr/bin/rsh
/usr/bin/su
/usr/bin/lpq
/usr/bin/lpr
/usr/bin/lprm
/usr/bin/chpass
/usr/bin/login
/usr/bin/passwd
/usr/bin/at
/usr/bin/ypchsh
/usr/bin/ypchfn
/usr/bin/ypchpass
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/yppasswd
/usr/bin/batch
/usr/bin/atrm
/usr/bin/atq
/usr/local/bin/screen
/usr/local/bin/sudo
/usr/local/bin/lppasswd
/usr/sbin/mrinfo
/usr/sbin/mtrace
/usr/sbin/ppp
/usr/sbin/pppd
/usr/sbin/sliplogin
/usr/sbin/timedc
/usr/sbin/traceroute
/usr/sbin/traceroute6
```

Remove the ones I never Use

“You should never be vulnerable to a weakness of a feature you do not use” - Microsoft security directive

Remove the Services I Never Use

```
/bin/rcp
/sbin/ping
/sbin/ping6
/sbin/shutdown
/usr/X11R6/bin/Xwrapper
/usr/X11R6/bin/xterm
/usr/X11R6/bin/Xwrapper-4
/usr/bin/keyinfo
/usr/bin/keyinit
/usr/bin/lock
/usr/bin/crontab
/usr/bin/opieinfo
/usr/bin/opiepasswd
/usr/bin/rlogin
/usr/bin/quota
```

```
/usr/bin/rsh
/usr/bin/su
/usr/bin/lpq
/usr/bin/lpr
/usr/bin/lprm
/usr/bin/chpass
/usr/bin/login
/usr/bin/passwd
/usr/bin/at
/usr/bin/ypchsh
/usr/bin/ypchfn
/usr/bin/ypchpass
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/yppasswd
```

```
/usr/bin/batch
/usr/bin/atrm
/usr/bin/atq
/usr/local/bin/screen
/usr/local/bin/sudo
/usr/local/bin/
lppasswd
/usr/sbin/mrinfo
/usr/sbin/mtrace
/usr/sbin/ppp
/usr/sbin/pppd
/usr/sbin/sliplogin
/usr/sbin/timedc
/usr/sbin/traceroute
/usr/sbin/traceroute6
```

Least Privilege

```
/sbin/ping
/sbin/ping6
/usr/X11R6/bin/xterm
/usr/X11R6/bin/Xwrapper-4
/usr/bin/crontab
/usr/bin/su
/usr/bin/lpq
/usr/bin/lpr
/usr/bin/lprm
/usr/bin/login
/usr/bin/passwd
/usr/bin/at
/usr/bin/chsh
/usr/bin/atrm
/usr/bin/atq
/usr/local/bin/sudo
/usr/sbin/traceroute
/usr/sbin/traceroute6
```

```
/usr/X11R6/bin/Xwrapper-4
/usr/bin/su
/usr/bin/passwd
/usr/bin/chsh
/usr/local/bin/sudo
```

```
AIX 4.2                 & 242   & a staggering number \\
BSD/OS 3.0              & 78              \\
FreeBSD 4.3             & 42    & someone's guard machine\\
FreeBSD 4.3             & 47    & 2 appear to be third-party\\
FreeBSD 4.5             & 43    & see text for closer analysis \\
HPUX A.09.07            & 227   & about half may be special for this host
Linux (Mandrake 8.1)    & 39    & 3 appear to be third-party \\
Linux (Red Hat 2.4.2-2) & 39    & 2 third-party programs \\
Linux (Red Hat 2.4.7-10)        & 31    & 2 third-party programs\\
Linux (Red Hat 5.0)     & 59          \\
Linux (Red Hat 6.0)     & 38    & 2--4 third-party \\
Linux 2.0.36            & 26    & approved distribution for one university
Linux 2.2.16-3          & 47               \\
Linux 7.2               & 42          \\
NCR Intel 4.0v3.0       & 113   & 34 may be special to this host \\
NetBSD 1.6              & 35          \\
SGI Irix 5.3            & 83          \\
SGI Irix 5.3            & 102         \\
Sinux 5.42c1002         & 60    & 2 third-party programs\\
Sun Solaris 5.4         & 52    & 6 third-party programs\\
Sun Solaris 5.6         & 74    & 11 third-party programs\\
Sun Solaris 5.8         & 70    & 6 third-party programs\\
Sun Solaris 5.8         & 82    & 6 third-party programs\\
Tru64 4.0r878           & 72    & \\
```

The “Attack Surface”

- Code visualization
- Code dependencies

I have no idea how to visualize the code attack surface

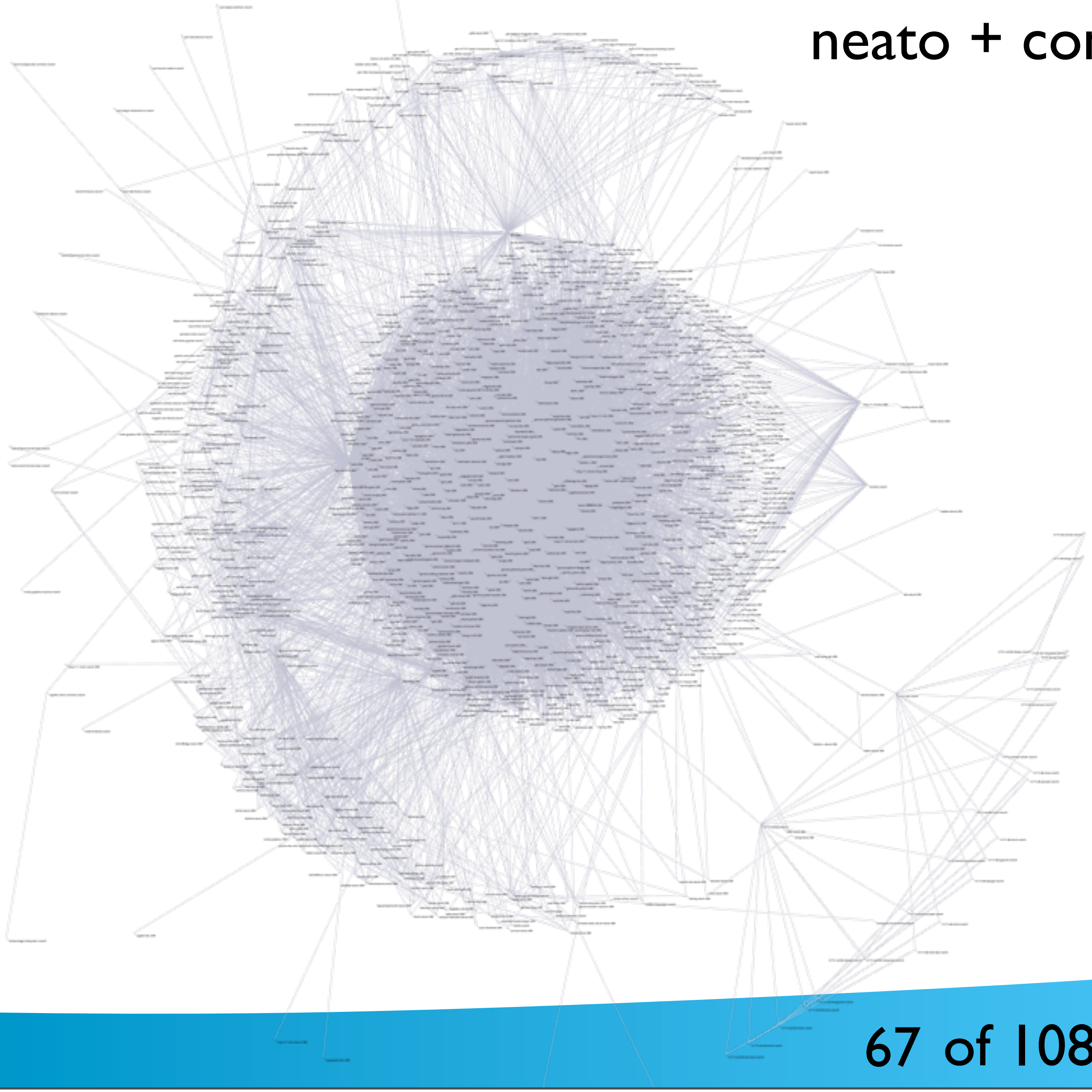
- I deem it *impossible*

Mythtv backend
Fedora Core 10

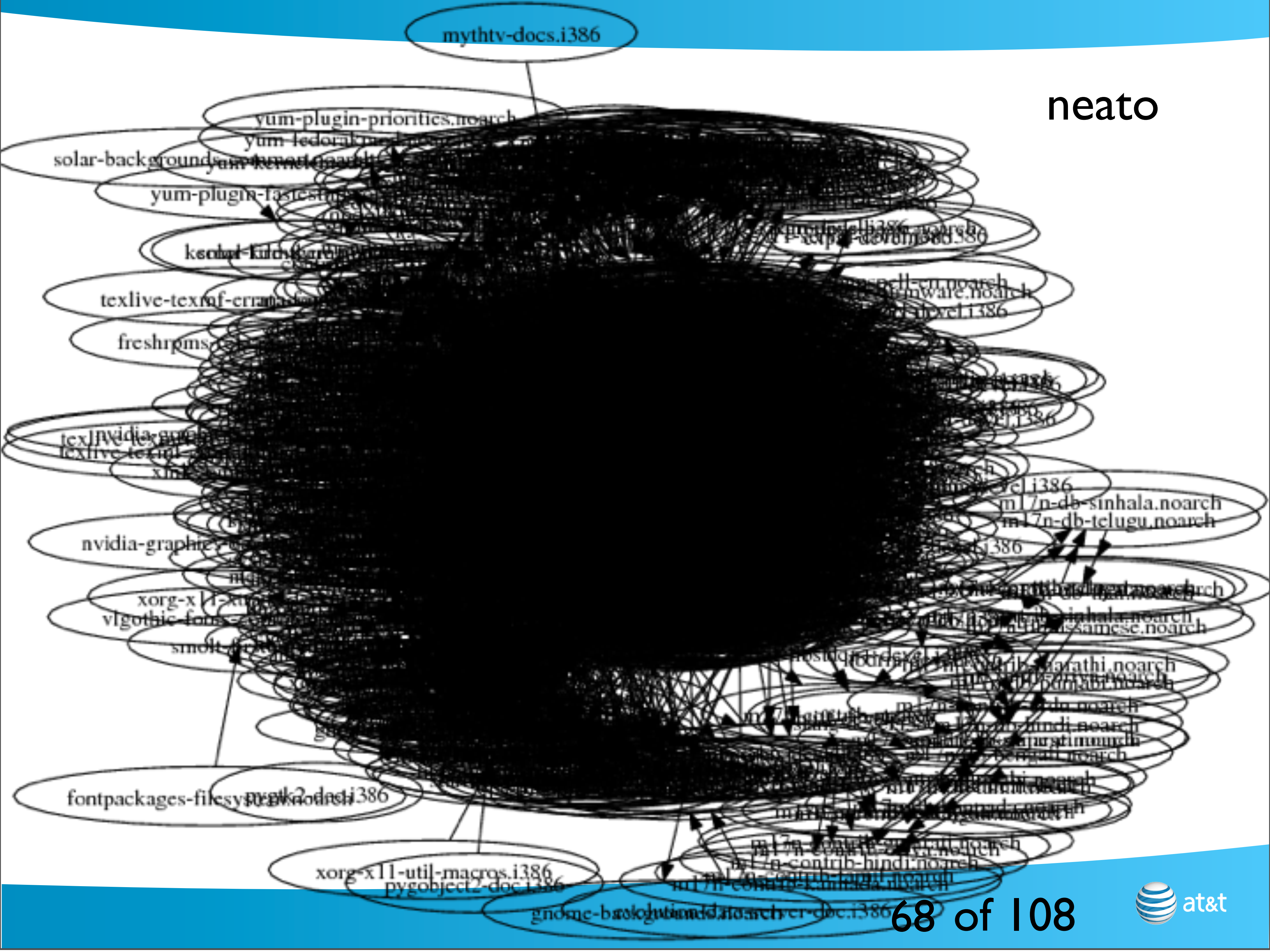
```
ypbind.i386                          3:1.20.4-11.fc10                    installed
yum.noarch                           3.2.23-3.fc10                       installed
yum-fedorakmod.noarch                1.1.19-1.fc10                       installed
yum-kernel-module.noarch             1.1.19-1.fc10                       installed
yum-metadata-parser.i386             1.1.2-10.fc10                       installed
yum-plugin-fastestmirror.noarch      1.1.22-1.fc10                       installed
yum-plugin-kmdl.noarch               0.8-11.fc10                         installed
yum-plugin-priorities.noarch         1.1.22-1.fc10                       installed
yum-utils.noarch                     1.1.22-1.fc10                       installed
zd1211-firmware.noarch               1.4-1                               installed
zenity.i386                          2.24.1-1.fc10                       installed
zip.i386                             2.31-6.fc9                          installed
zlib.i386                            1.2.3-18.fc9                        installed
zlib-devel.i386                      1.2.3-18.fc9                        installed
zoneminder.i386                      1.23.3-2.fc10                       installed
zvbi.i386                            0.2.30-1.fc9                        installed
btvs:~$ yum list installed | wc -l
1447
```

sfdp

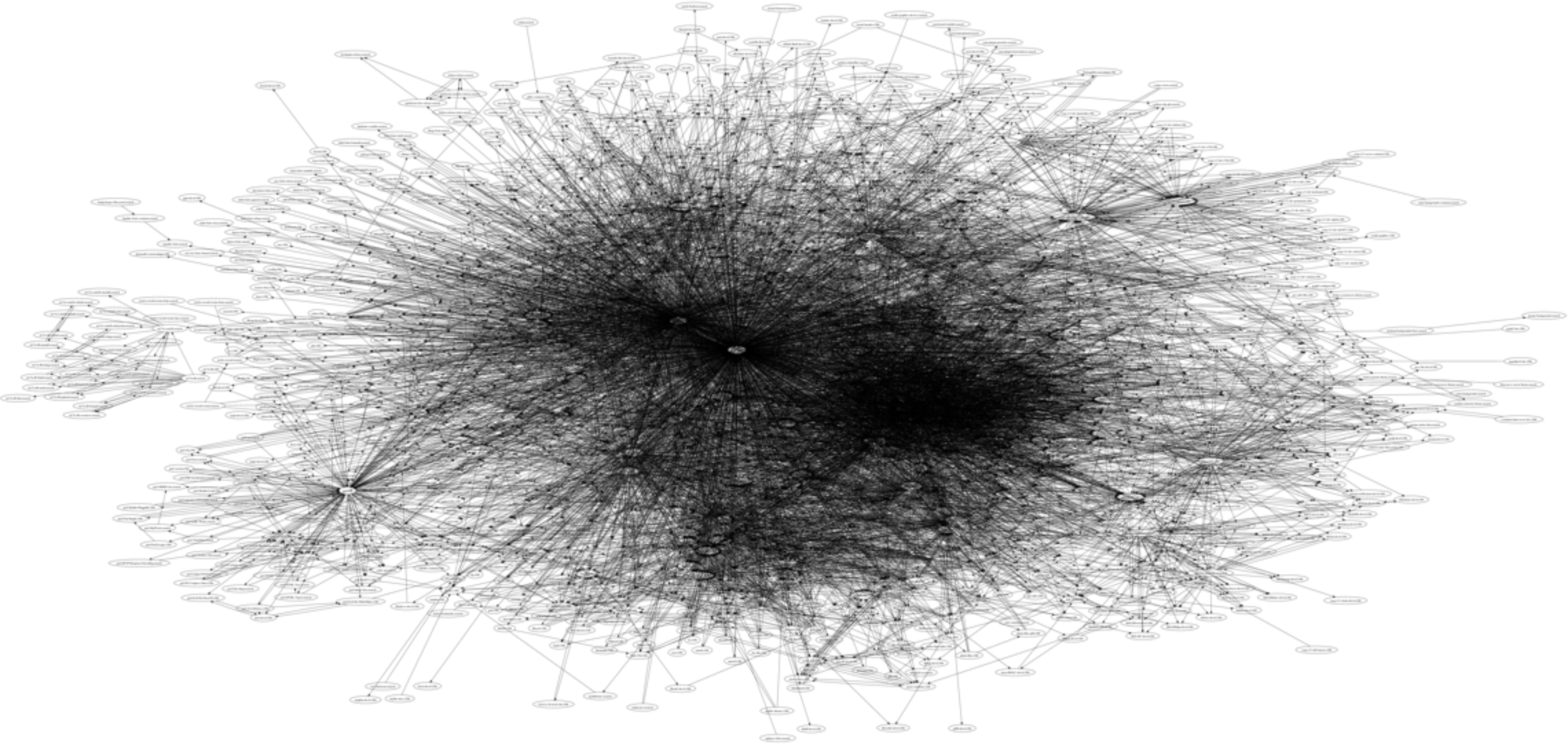
neato + concentrate



neato

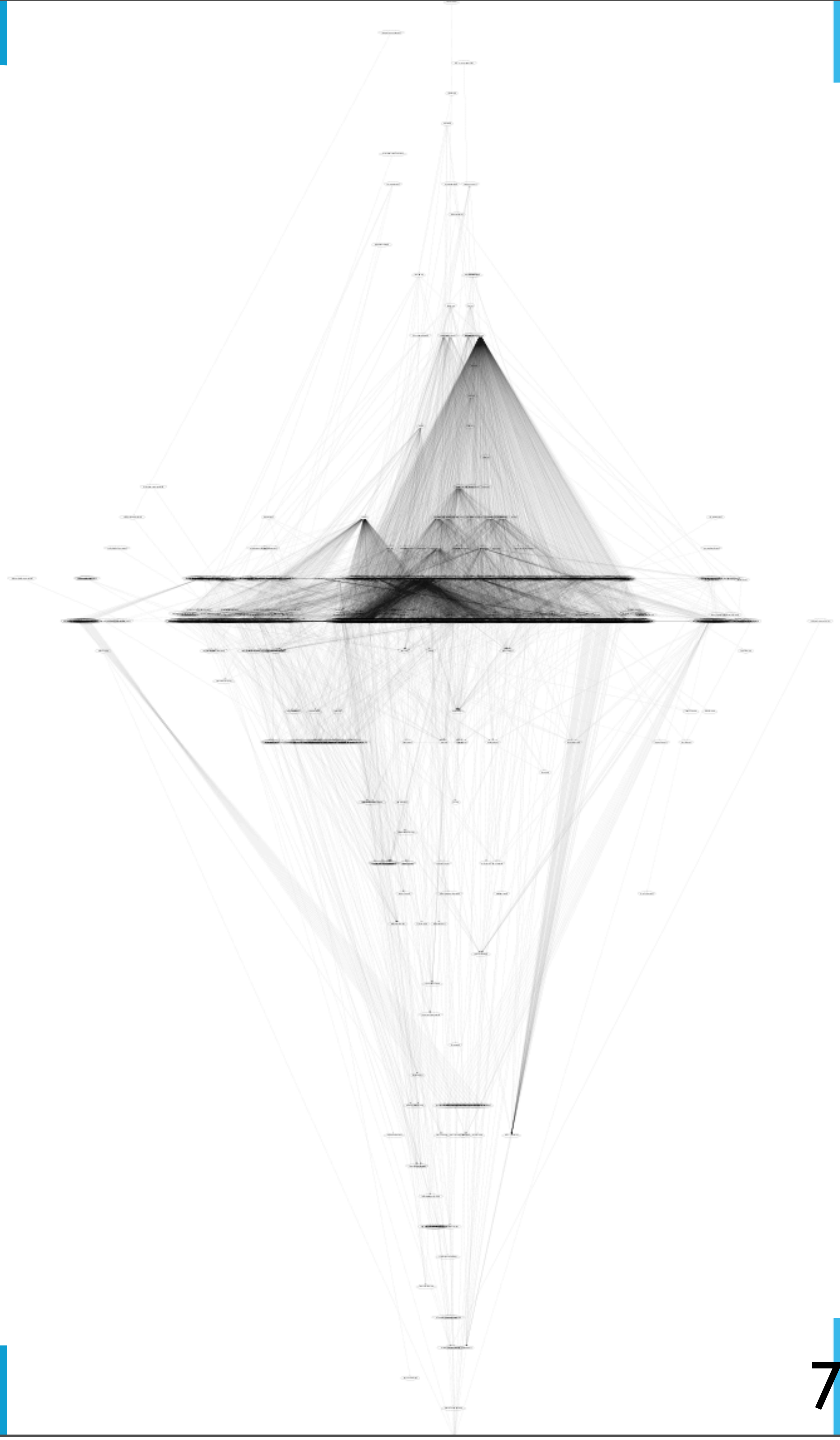

mythtv-docs.i386
yum-plugin-priorities.noarch
solar-backgrounds
yum-plugin-fastestmirror
texlive-texmf-errata
freshrpms
nvidia-graphics
xorg-x11
vlgothic-fonts
smolt
fontpackages-filesystem.noarch
gtk2-docs.i386
xorg-x11-util-macros.i386
pygobject2-doc.i386
gnome-backgrounds.noarch
m17n-db-sinhala.noarch
m17n-db-telugu.noarch
m17n-db-assamese.noarch
m17n-db-marathi.noarch
m17n-db-punjabi.noarch
m17n-contrib-hindi.noarch
m17n-contrib-tamil.noarch
m17n-contrib-kannada.noarch

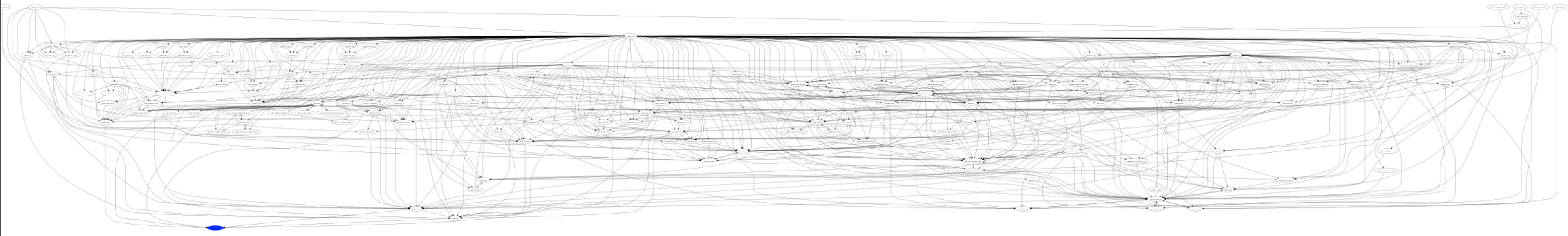
sfdp



What I really care about

- Dangerous software as dependencies
- e.g. mythweb -> PHP
- PHP is the source of most break-ins on many or most *nix machines



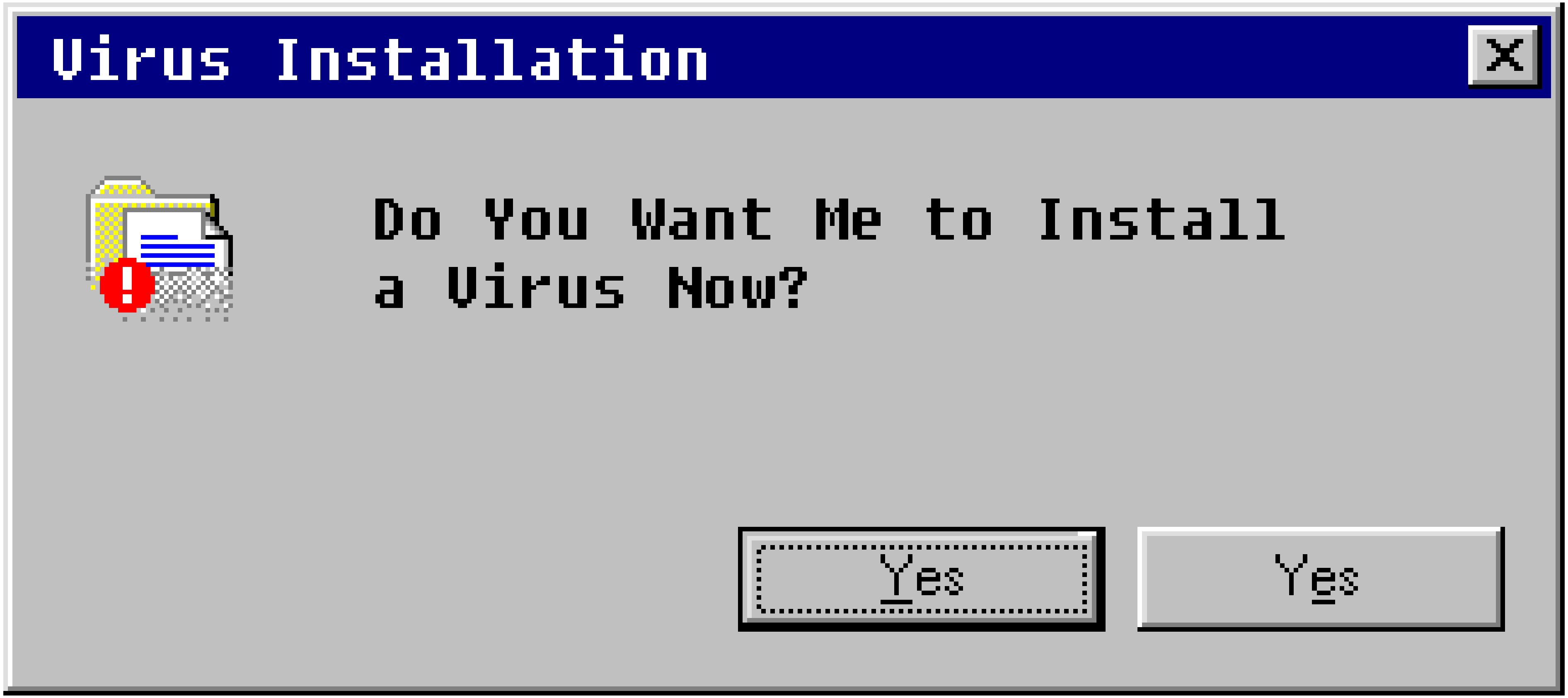


To do

- A dependency graph of typical or specific Linux systems, annotated with security opinions or code analysis, could be helpful
- Ditto for *bsd "port" dependencies

Bozo in the Chair

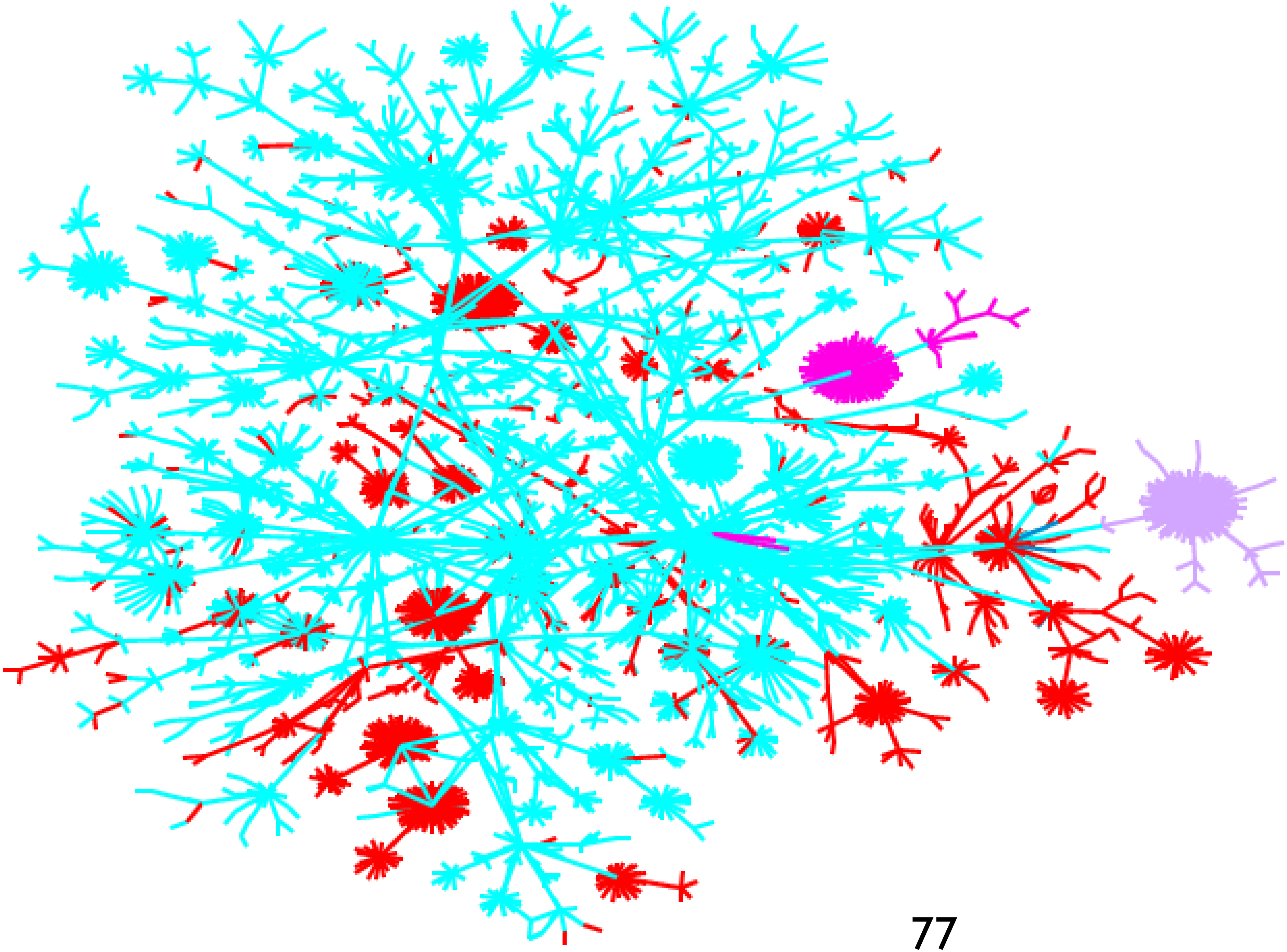
- These attacks will continue indefinitely
- Attackers' ingenuity is endless

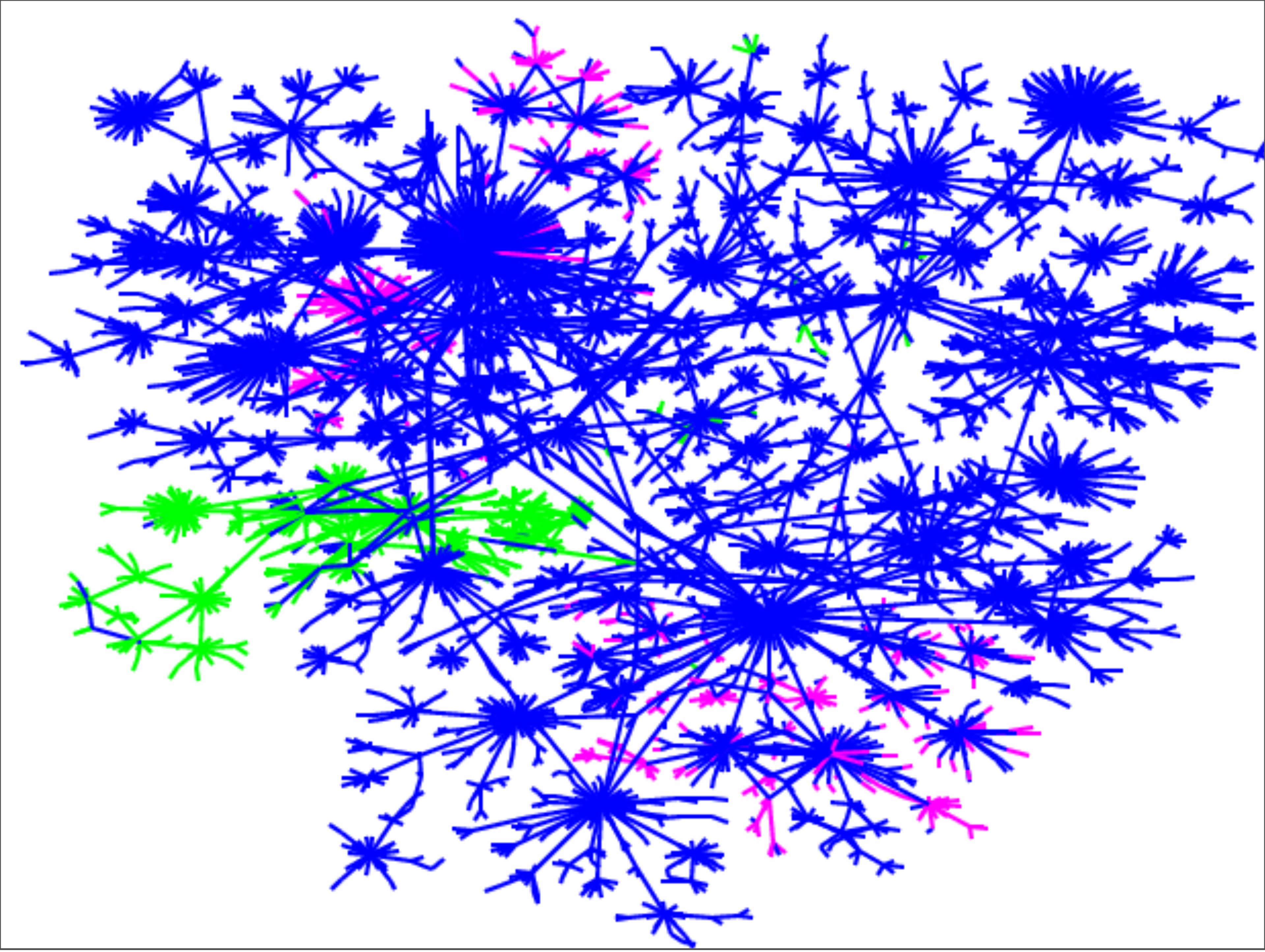


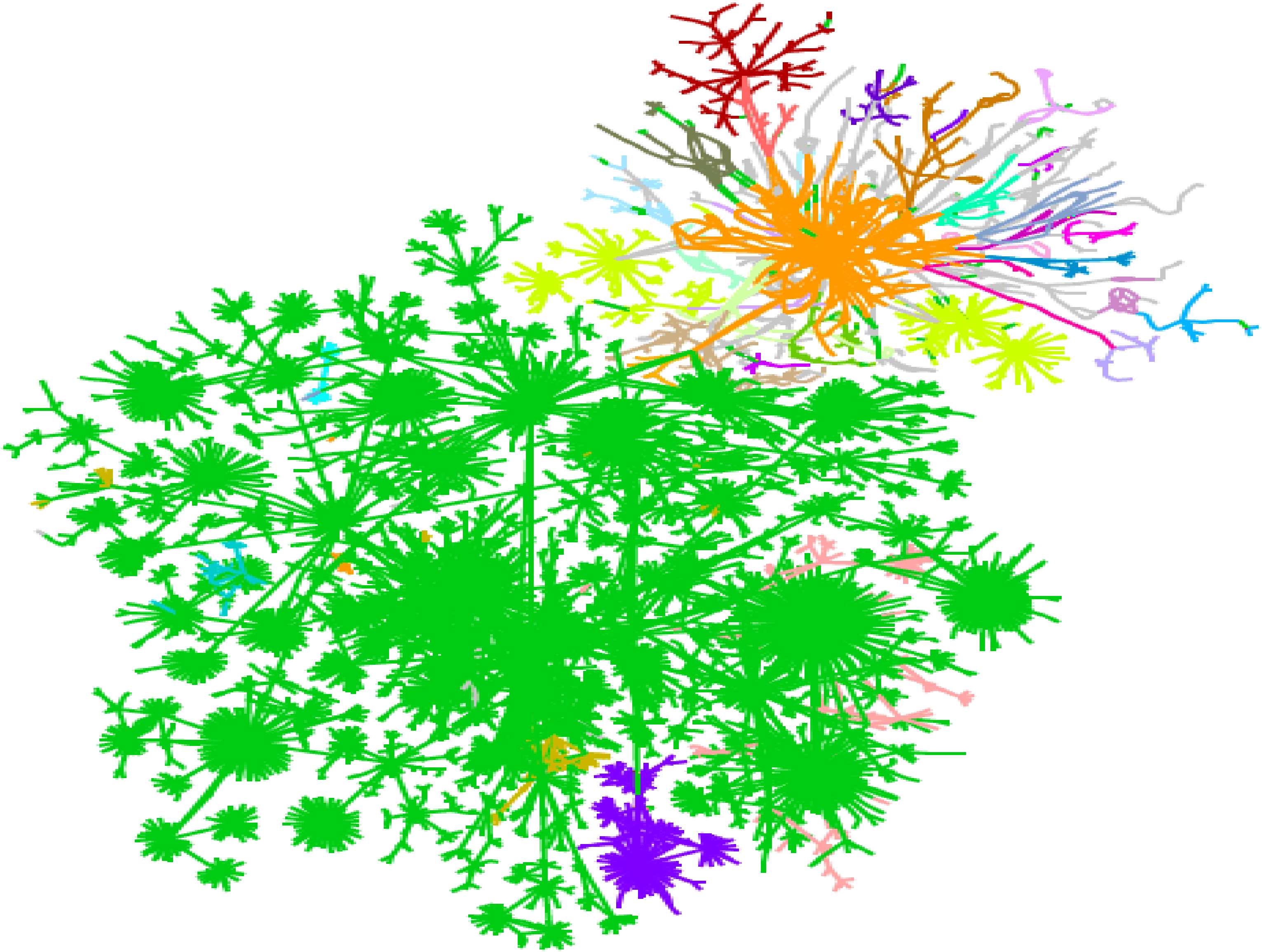
Virus Installation

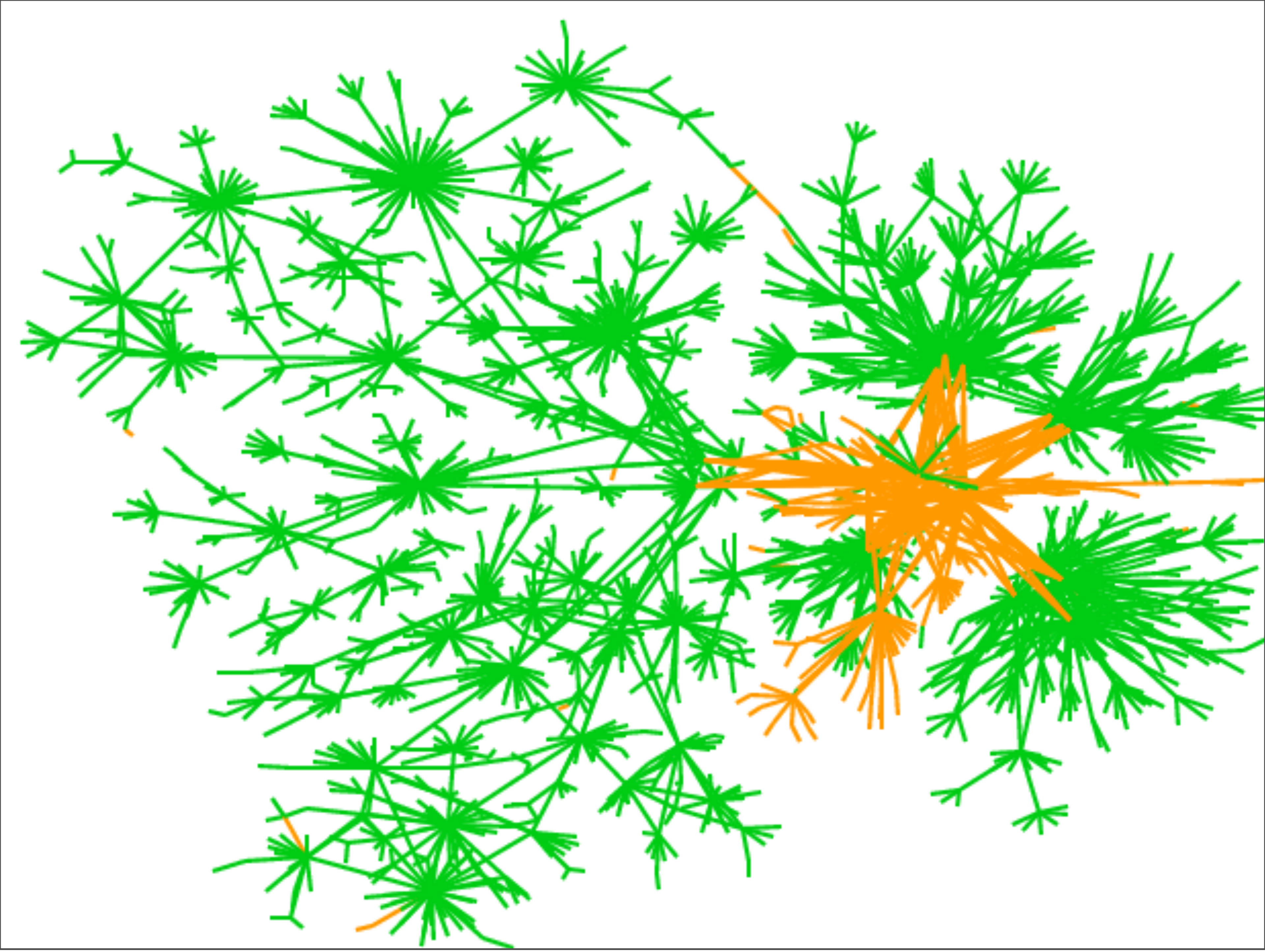
Do You Want Me to Install
a Virus Now?

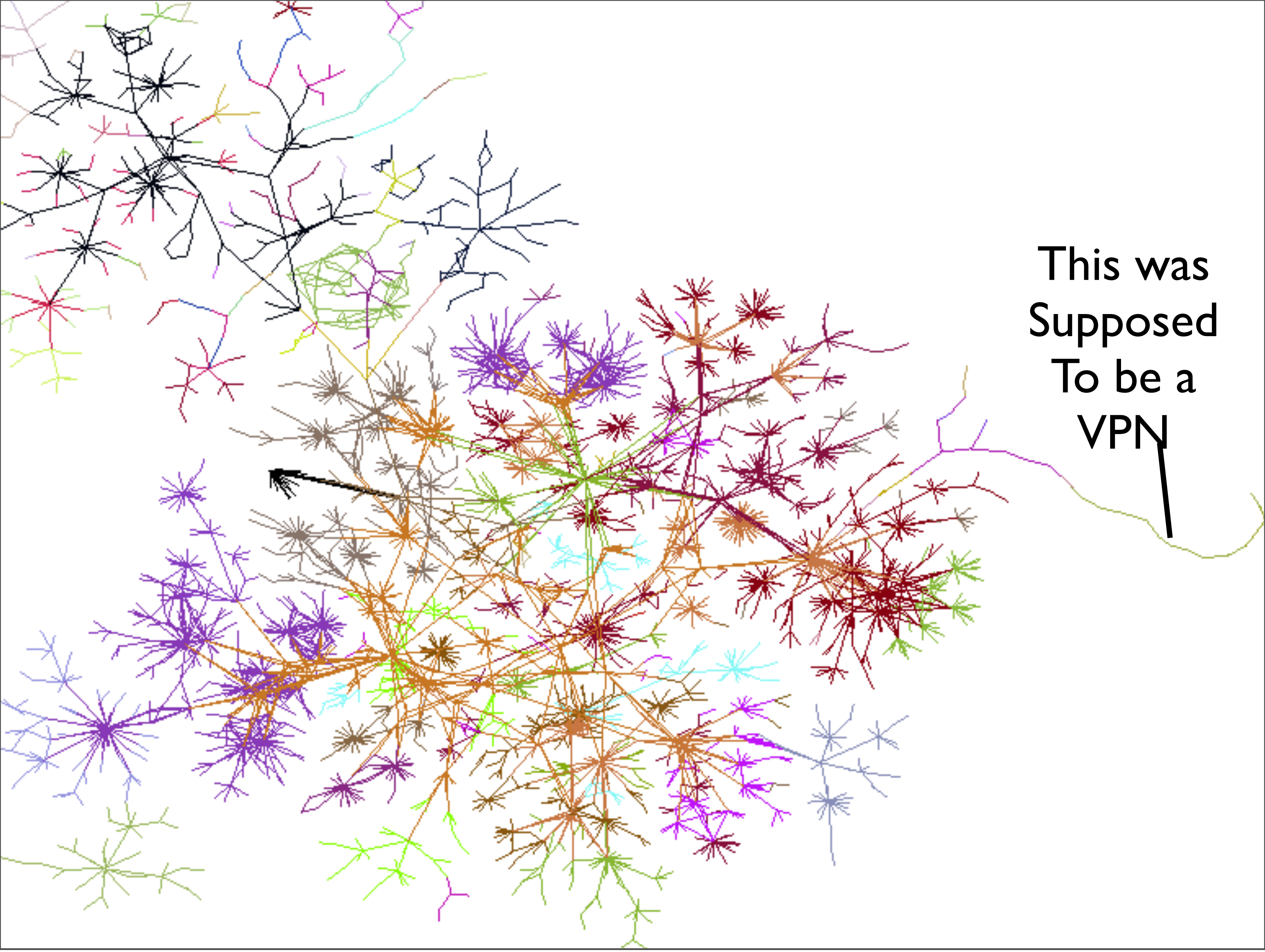
Network Topological Security



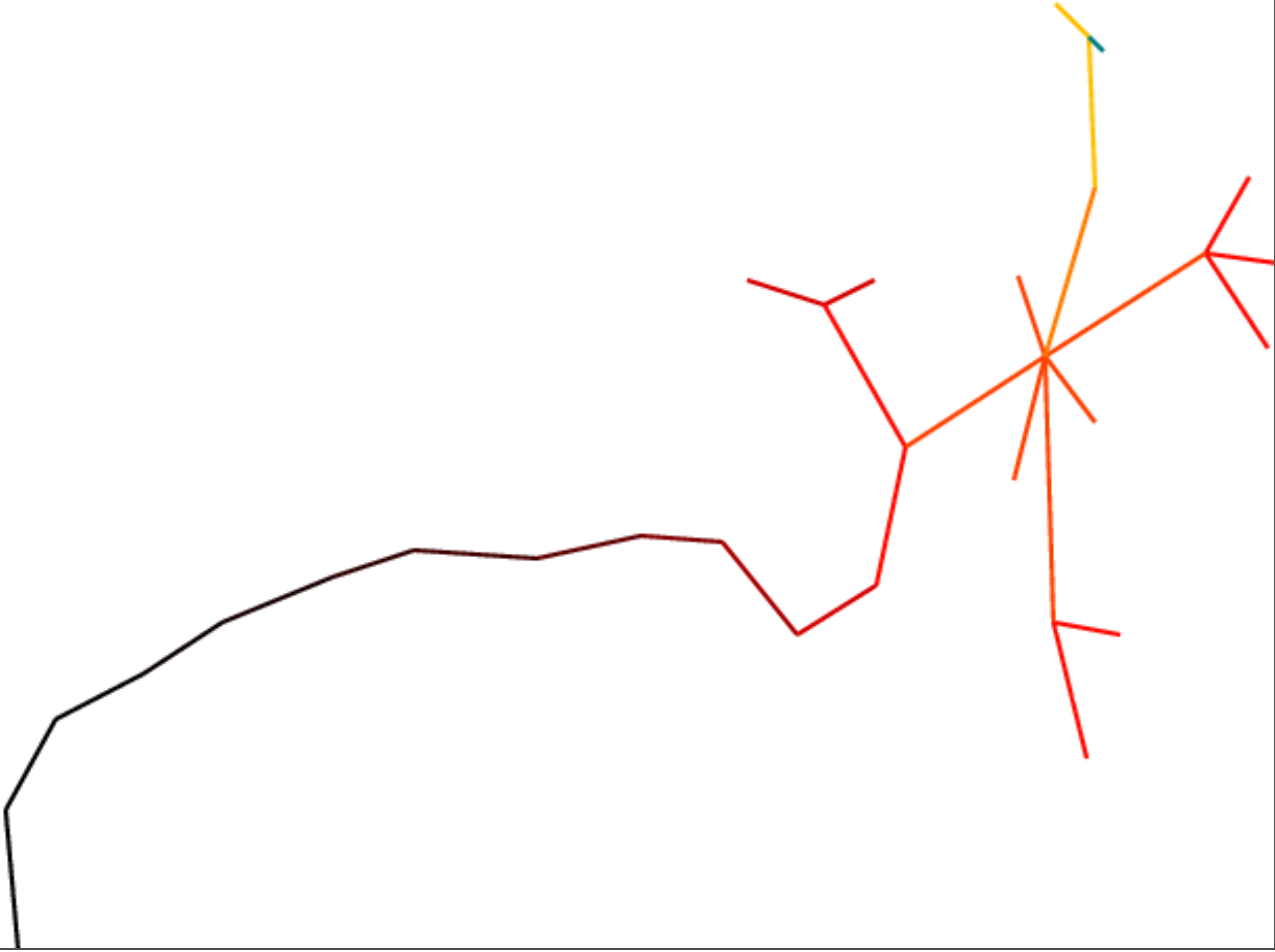


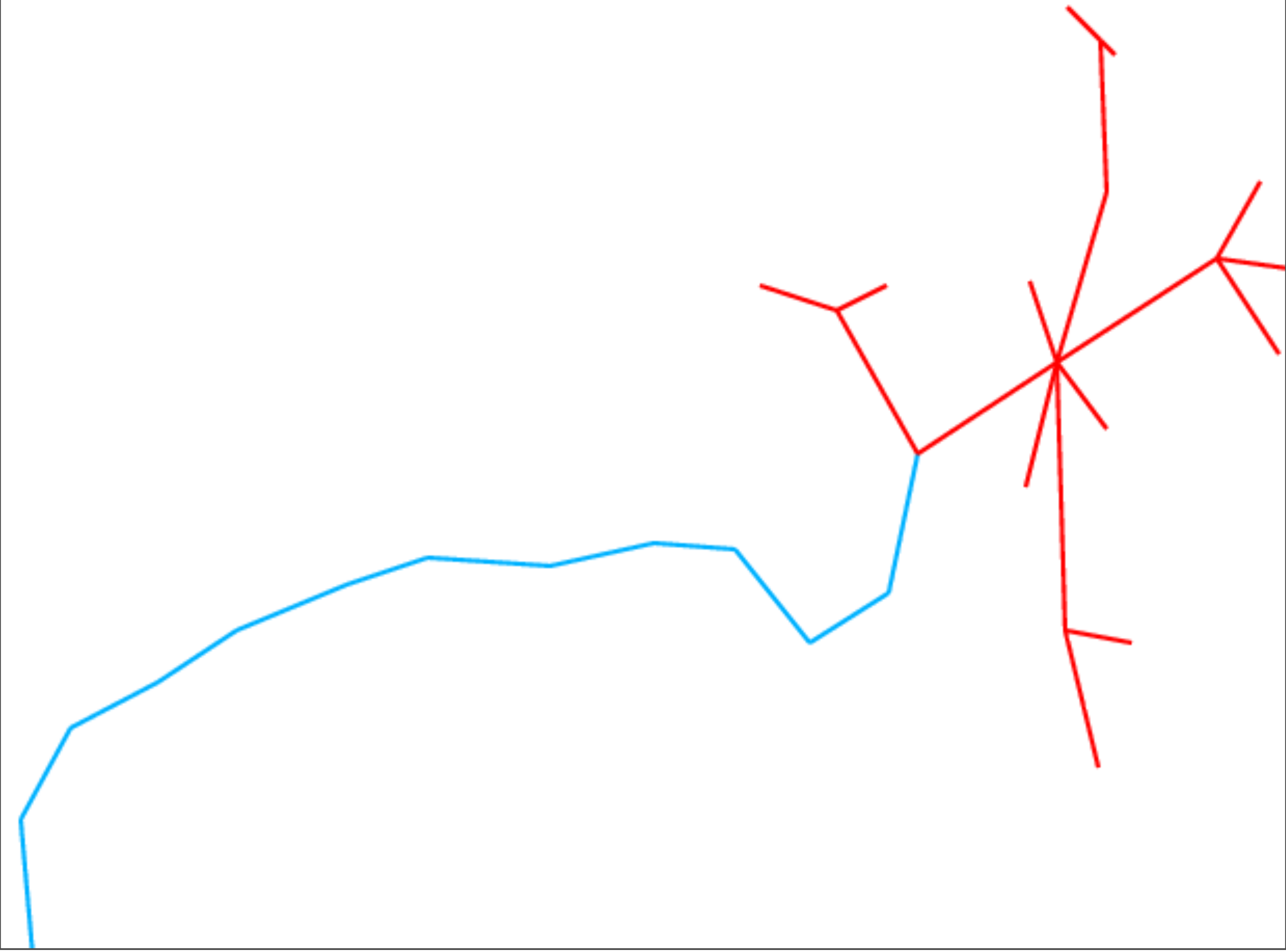






This was
Supposed
To be a
VPN





Lessons from Lumeta

1997 - 2006 (for me)

The Special Sauce

- Internet and intranet maps
- Leak detection
- (Also a cool firewall analysis program by Wool and Meyer)

Spun off from Bell Labs/ Lucent

- Oct 1, 2000. Worse timing than now, maybe
- Big companies wanted it, but at what price?
- Would our visualization algorithm do okay on alien intranets?
- What was a competitor going to look like?

Some hard parts

- displaying data as information: 3 versions
- limited by needing web reports
- technical audience had special concerns
- getting colors right

Sales resistance

- Competitor was for the dollars, not the product
- Remediation costs lots more than discovery
- Non-technical companies
- Some Just Did Not Want To Know

“Can you improve my ROI?”

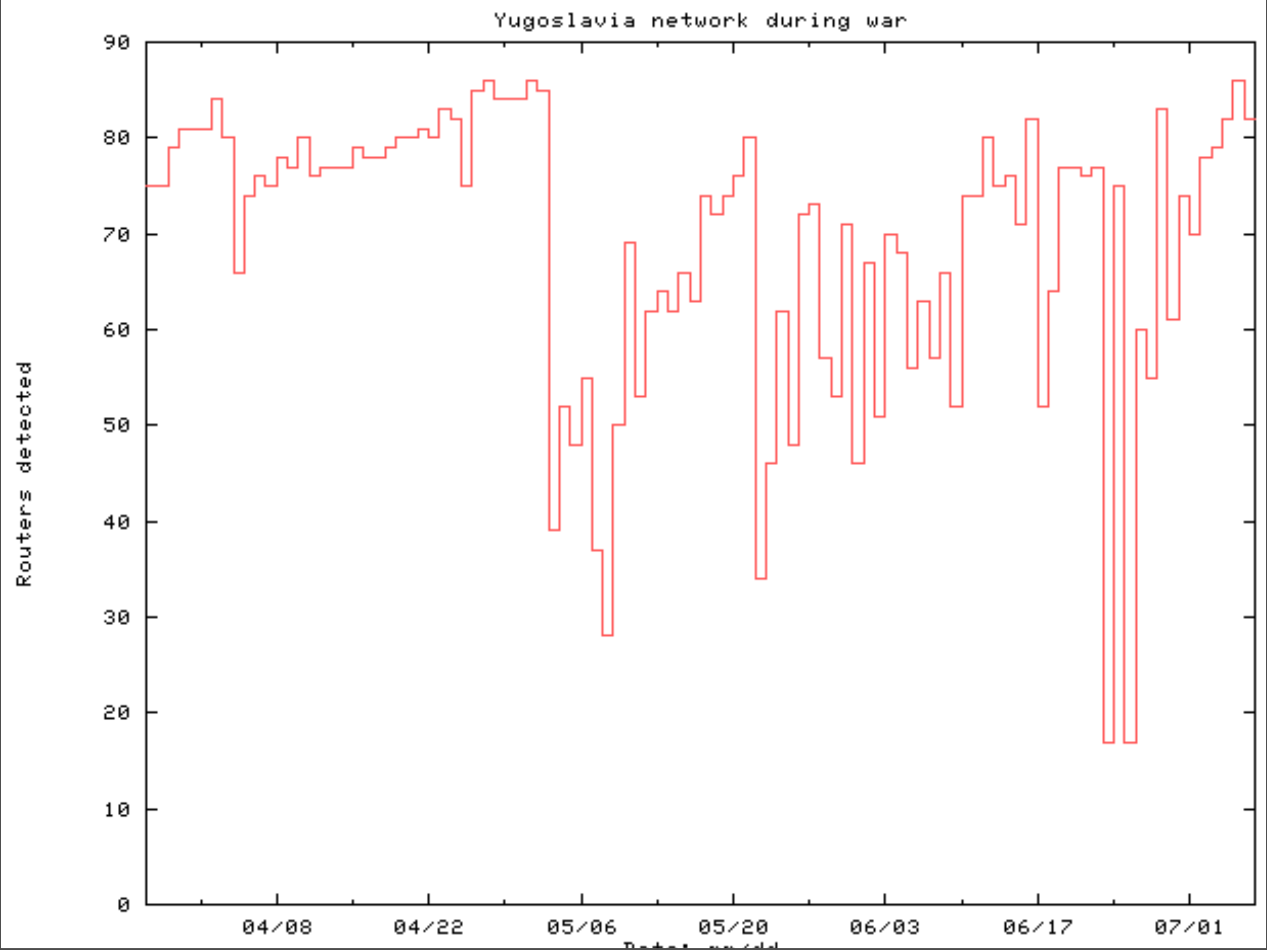
Nice to have

or

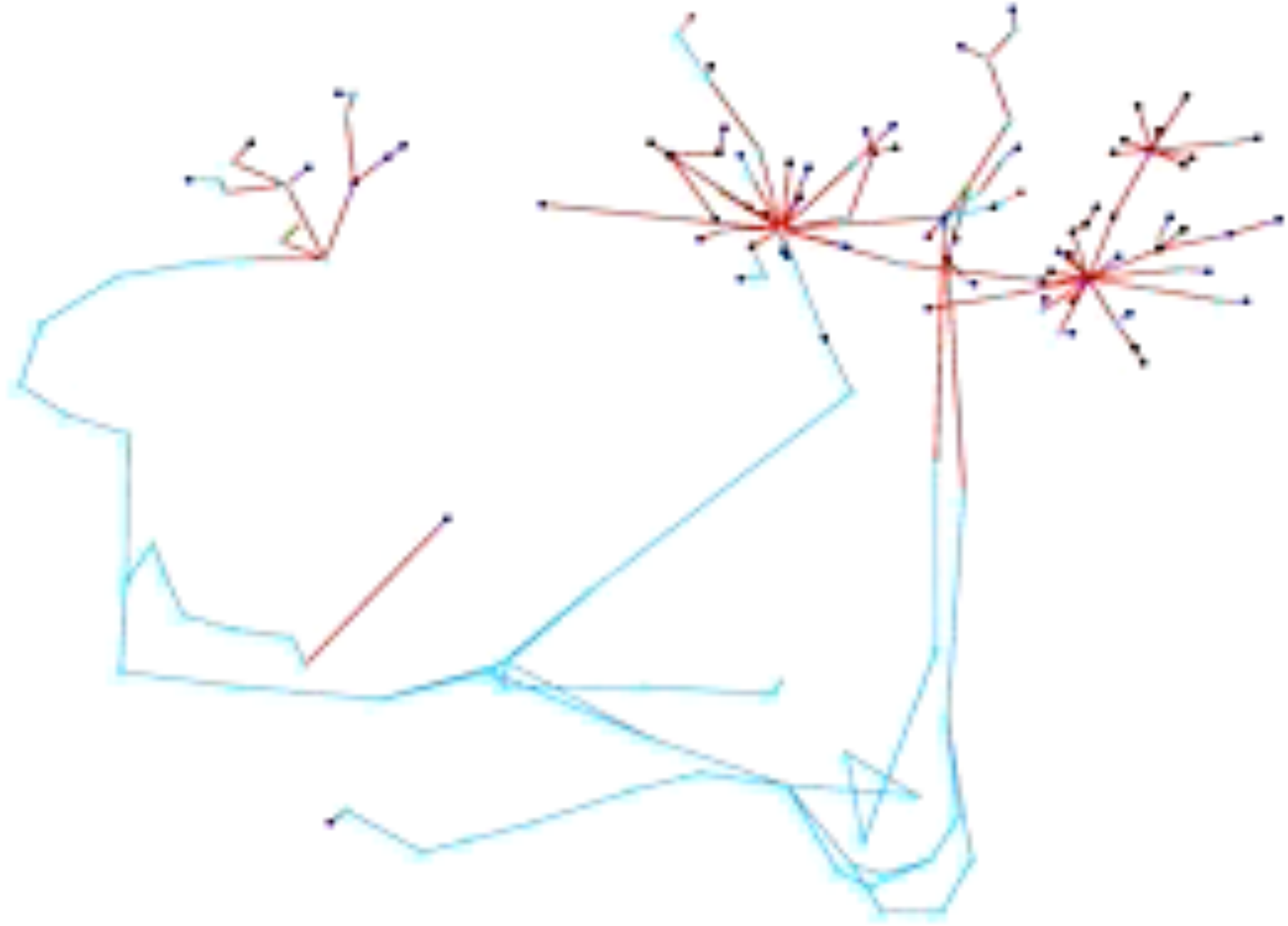
Gotta have

Yugoslavia

An unclassified peek at a new battlefield


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

Un film par Steve "Hollywood" Branigan...



05/01/1999

fin

Visualization of the layout algorithm

Laying out the Internet graph

Visualization of the layout algorithm

Laying out an intranet

A small experiment

- Time visualization
  - I haven't seen this done well yet
- Incremental layouts
  - not generally available
- (demo here)

Layout Programs

- Tend to be self-contained, and weird
- Burch/Cheswick was a combination of C, called in a shell script
- Others tend to be more monolithic
- A procedure call would be nice. Also, use multicore CPUs.

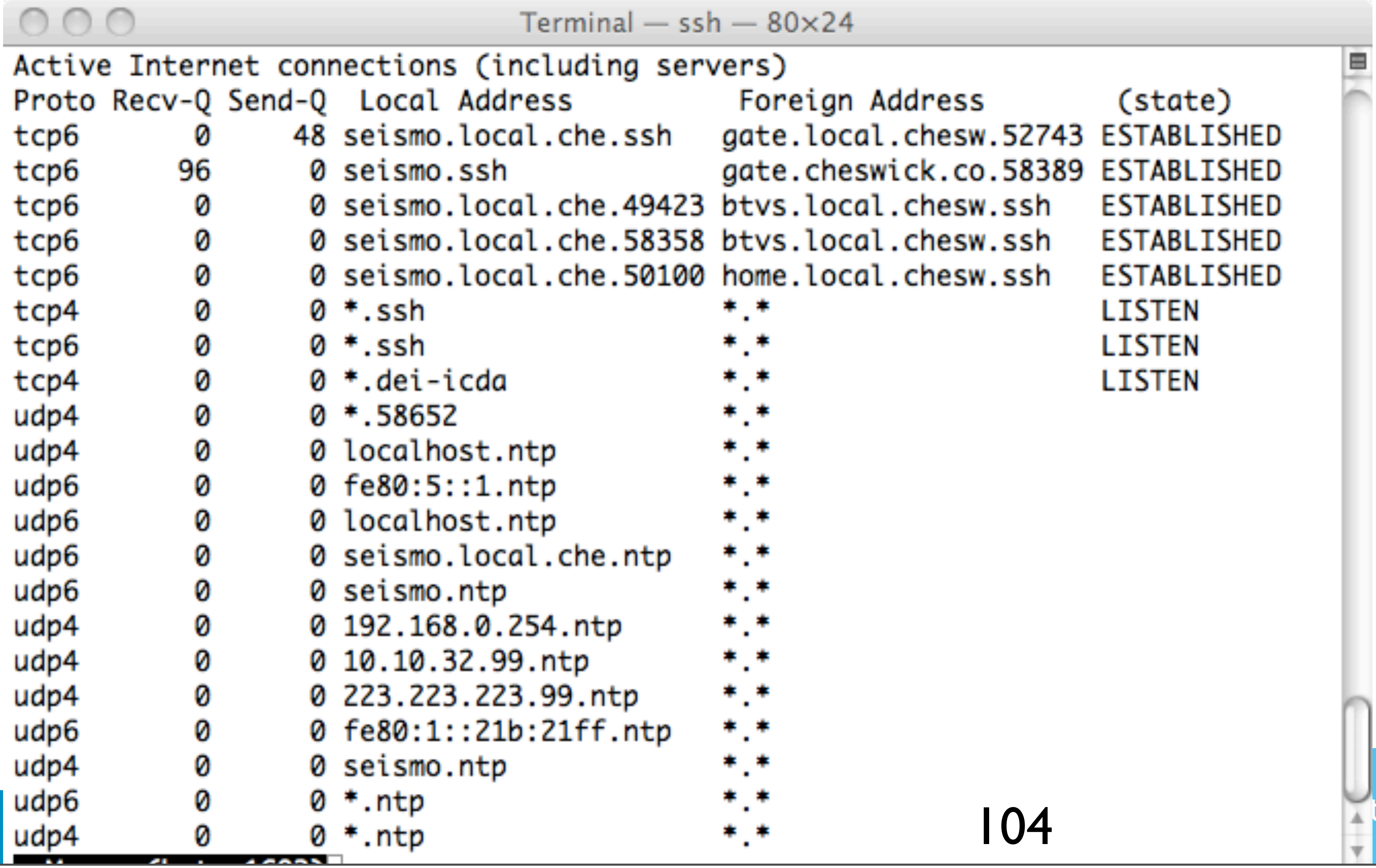
Other visualizations

- zitvis?
- groanalarm (patent pending)

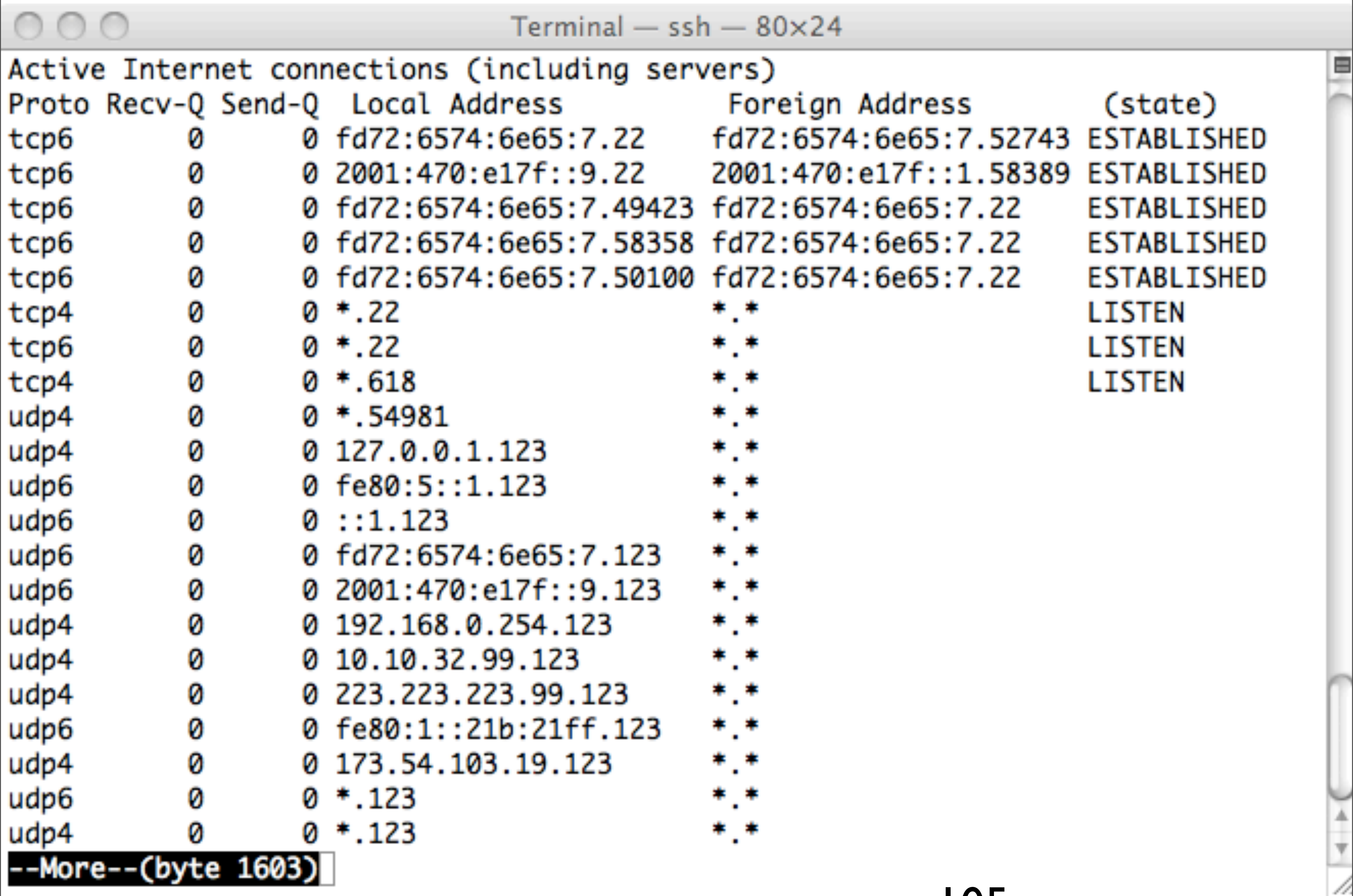
I hate the Hilbert layout

- Everything is adjacent.
- Big deal, I miss the big picture
- Maybe I am just grumpy

Troubles coming: IPv6



```
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp6       0     48  seismo.local.che.ssh   gate.local.chesw.52743 ESTABLISHED
tcp6      96      0  seismo.ssh             gate.cheswick.co.58389 ESTABLISHED
tcp6       0      0  seismo.local.che.49423 btvs.local.chesw.ssh   ESTABLISHED
tcp6       0      0  seismo.local.che.58358 btvs.local.chesw.ssh   ESTABLISHED
tcp6       0      0  seismo.local.che.50100 home.local.chesw.ssh   ESTABLISHED
tcp4       0      0  *.ssh                  *.*                    LISTEN
tcp6       0      0  *.ssh                  *.*                    LISTEN
tcp4       0      0  *.dei-icda             *.*                    LISTEN
udp4       0      0  *.58652                *.*
udp4       0      0  localhost.ntp          *.*
udp6       0      0  fe80:5::1.ntp          *.*
udp6       0      0  localhost.ntp          *.*
udp6       0      0  seismo.local.che.ntp   *.*
udp6       0      0  seismo.ntp             *.*
udp4       0      0  192.168.0.254.ntp      *.*
udp4       0      0  10.10.32.99.ntp        *.*
udp4       0      0  223.223.223.99.ntp     *.*
udp6       0      0  fe80:1::21b:21ff.ntp   *.*
udp4       0      0  seismo.ntp             *.*
udp6       0      0  *.ntp                  *.*
udp4       0      0  *.ntp                  *.*
```



```
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp6       0      0  fd72:6574:6e65:7.22    fd72:6574:6e65:7.52743 ESTABLISHED
tcp6       0      0  2001:470:e17f::9.22    2001:470:e17f::1.58389 ESTABLISHED
tcp6       0      0  fd72:6574:6e65:7.49423 fd72:6574:6e65:7.22    ESTABLISHED
tcp6       0      0  fd72:6574:6e65:7.58358 fd72:6574:6e65:7.22    ESTABLISHED
tcp6       0      0  fd72:6574:6e65:7.50100 fd72:6574:6e65:7.22    ESTABLISHED
tcp4       0      0  *.22                   *.*                    LISTEN
tcp6       0      0  *.22                   *.*                    LISTEN
tcp4       0      0  *.618                  *.*                    LISTEN
udp4       0      0  *.54981                *.*
udp4       0      0  127.0.0.1.123          *.*
udp6       0      0  fe80:5::1.123          *.*
udp6       0      0  ::1.123                *.*
udp6       0      0  fd72:6574:6e65:7.123   *.*
udp6       0      0  2001:470:e17f::9.123   *.*
udp4       0      0  192.168.0.254.123      *.*
udp4       0      0  10.10.32.99.123        *.*
udp4       0      0  223.223.223.99.123     *.*
udp6       0      0  fe80:1::21b:21ff.123   *.*
udp4       0      0  173.54.103.19.123      *.*
udp6       0      0  *.123                  *.*
udp4       0      0  *.123                  *.*
--More--(byte 1603)
```

Summary

- Better engineering and usability may improve adoption of these tools
- Cool makes a paper, but often not a sale
- The infiltration of gamers may change things, but the target audience is usually very tech savvy, and even geeky

Visual Tools for Security: is there a There There?

Bill Cheswick
AT&T Labs - Research
Shannon Labs
ches@research.att.com
http://www.cheswick.com/ches/