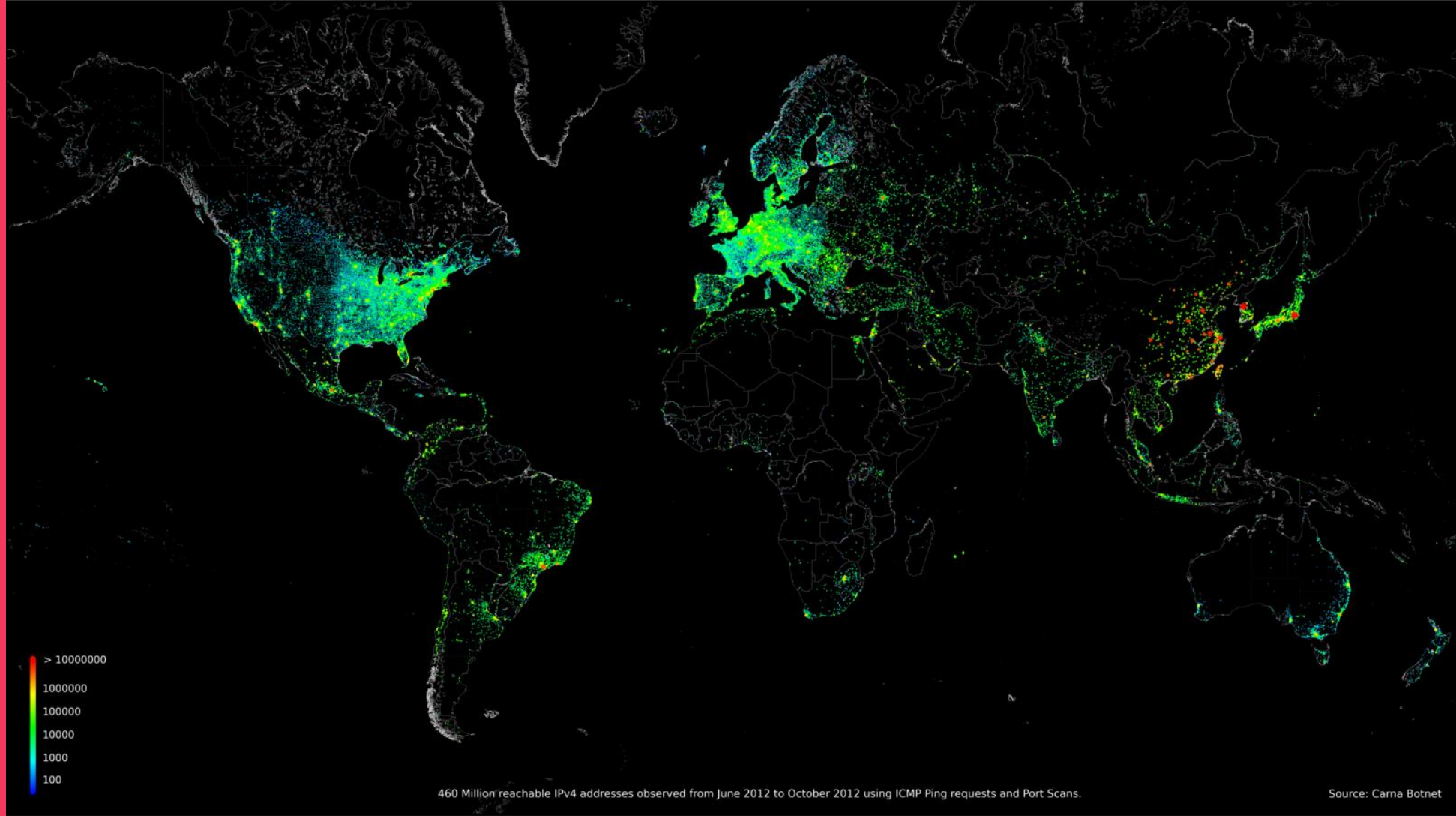


2012 internet census

jeff crowell

cs558 – spring 2013

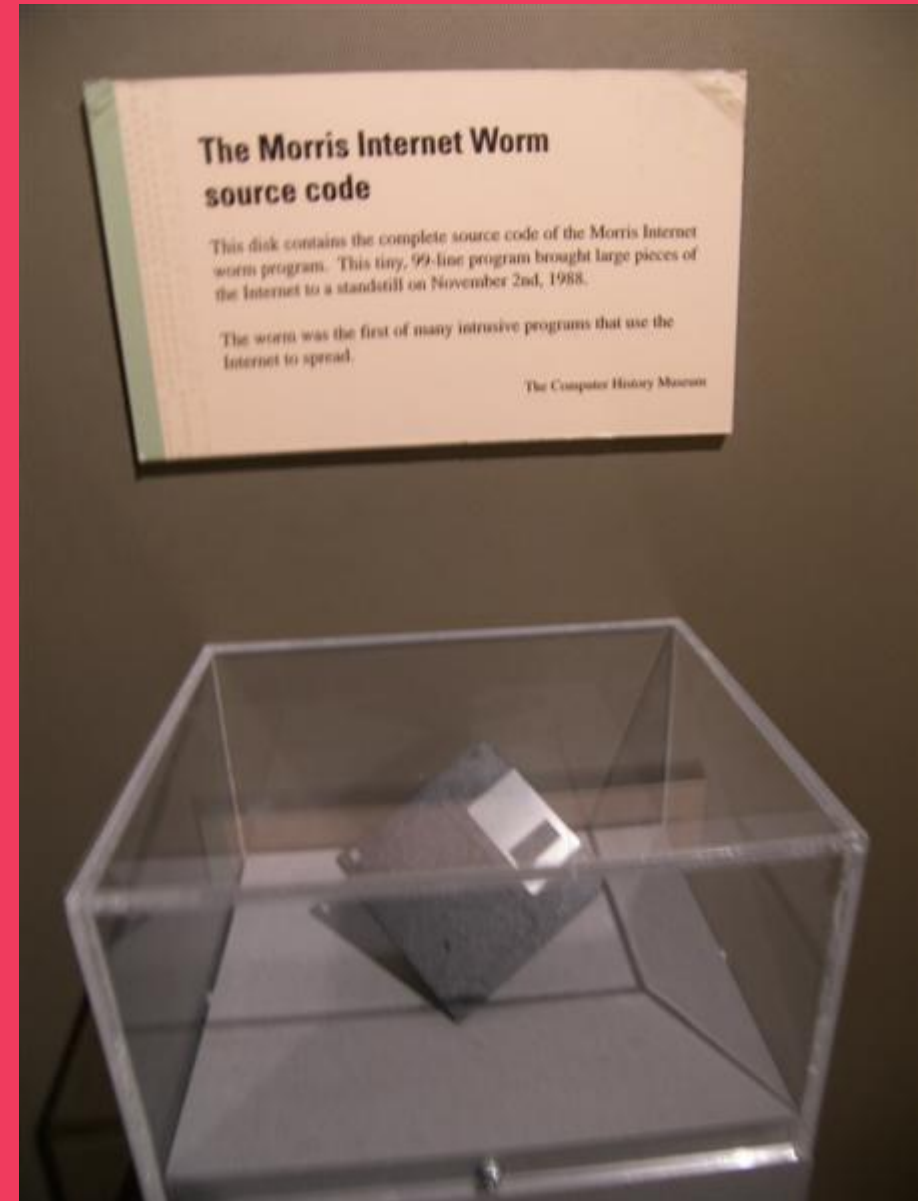


heatmap of all 460,000,000 ipv4 addresses

source: 2013 census

history

- 1988 First Internet Worm
- Morris Worm
- Goal => Gauge Size of the Internet
- Exploited debug hole in UNIX sendmail
- Infected 6,000 Machines
- Punishment
 - 3 years probation
 - 400 Hours Community Service
 - \$10,000 Fine



2012 carna botnet

- Goal => map all ipv4 IP addresses
- A “last chance” at mapping all IP before IPv6 becomes standard
 - Ipv6 = 340 Sextillion addresses
 - IPv4 = “only” 3,706,452,992 public addresses

“be nice”

- Be as unobtrusive as possible
- Non-persistent
- Low priority
- Don't capture traffic 😊
- “respect privacy”



how it works

- Part 1: scans given address space for “open” telnet connections
 - root:root, admin:admin, ...
- Find machine? Great! Drop Listener binary
- Part 2: Scanner manager, sends ip ranges to be scanned and uploads scan results to specified IP address. Stopped deployment after 30k machines.

infrastructure

- Unlike most botnets, not C&C, directly accessible from internet.
- “Middle Nodes”
 - Most powerful devices take client data, store it for the master server
- Each node gets “part id” “starting ip” “stepwidth” and “end ip” for coordination, addresses broken up to 240k jobs, each with 15k addresses

Software

- Binary - Portable! : 46-90kb (SMALL)
 - 9 Architectures, ARM/MIPS/x86/others
- Backend API
 - API, called by Python scripts
 - Web interface PHP
- Database
 - BIG DATA
 - Hadoop/PIG -> MapReduce
- No source released

Scans

- ICMP – *faaaaaaaast* – probe ipv4 in under a day
 - 52billion pings
- Reverse DNS
 - Who has <IP ADDRESS> to biggest 16 DNS Servers (Google, Level3,...) 10.5b records

```
{13-04-10 20:00}lostwoods:~ jeff% host 168.122.193.53
53.193.122.168.in-addr.arpa domain name pointer park509-0b01-dhcp53.bu.edu.
```

- Nmap
 - Heavier than ping/dns, only on the more powerful MIPS machines
 - Syn scan of top 100 ports, 85 service probes
 - Service Probes
- Traceroute
 - Targets can't run linux/no shell, could only do ping/traceroute
 - Small, limited resources, not that useful.

```
{13-04-10 19:45}enggrid1:~ crowell% traceroute raxcity.com
traceroute to raxcity.com (168.122.193.53), 30 hops max, 40 byte packets
 1 cumm024-0b08net-gw.bu.edu (128.197.115.1)  1.420 ms  1.405 ms  1.392 ms
 2 comm595-core-aca01-gi2-2-cumm024-dist-aca01-gi5-2.bu.edu (128.197.254.205)  1.232 ms  1.224 ms  1.232 ms
 3 comm595-core-res01-gi1-2-comm595-core-aca01-gi1-2.bu.edu (128.197.254.74)  1.576 ms  1.589 ms  1.597 ms
 4 park520-dist-res01-gi5-2-comm595-core-res01-gi-2-4.bu.edu (128.197.254.246)  1.200 ms  1.246 ms  1.252 ms
 5 park509-0b01-dhcp53.bu.edu (168.122.193.53)  0.991 ms  1.096 ms  1.324 ms
```


Target: raxcity.com

Profile: Intense scan

Scan

Cancel

Command: nmap -T4 -A -v raxcity.com

Hosts

Services

Nmap Output

Ports / Hosts

Topology

Host Details

Scans

OS

Host

raxcity.com (1)

nmap -T4 -A -v raxcity.com

Details

```

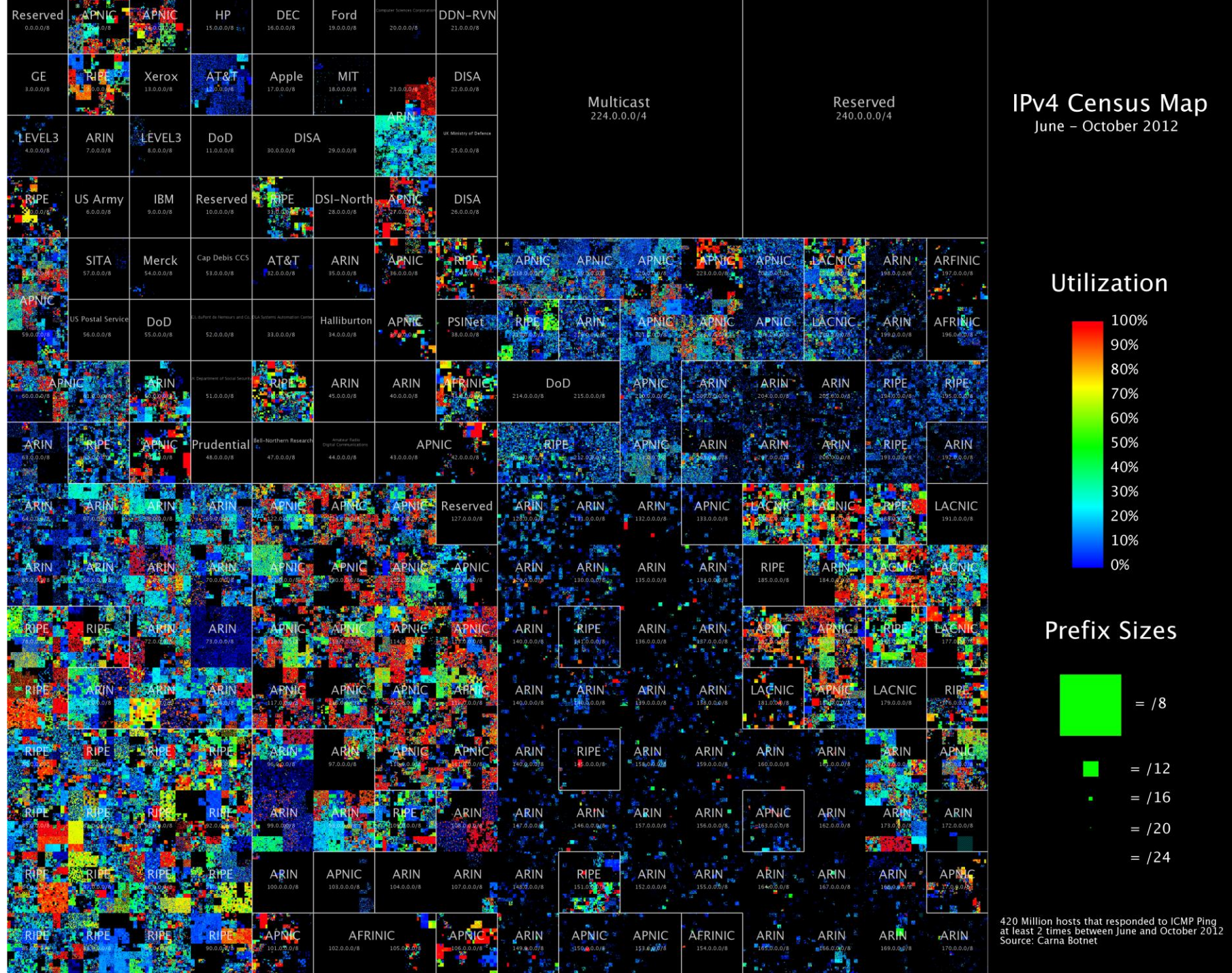
Initiating OS detection (try #1) against raxcity.com (168.122.193.53)
Retrying OS detection (try #2) against raxcity.com (168.122.193.53)
Initiating Traceroute at 20:17
Completed Traceroute at 20:17, 3.03s elapsed
NSE: Script scanning 168.122.193.53.
Initiating NSE at 20:17
Completed NSE at 20:18, 30.13s elapsed
Nmap scan report for raxcity.com (168.122.193.53)
Host is up (0.0080s latency).
rDNS record for 168.122.193.53: park509-0b01-dhcp53.bu.edu
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh           OpenSSH 6.0p1 Debian 4 (protocol 2.0)
|_ ssh-hostkey: 1024 06:af:7c:a2:4d:4e:08:d3:0b:88:d3:2d:29:93:9e:34
(DSA)
|_ 2048 94:f1:2f:0f:07:ea:a6:08:92:55:1f:dc:a5:59:2d:98 (RSA)
|_ 256 fa:63:c0:89:5b:fa:ab:a6:78:66:53:8e:b2:af:d1:57 (ECDSA)
80/tcp    open  http         Apache httpd 2.2.22 ((Debian))
|_ http-methods: OPTIONS GET HEAD POST
|_ http-title:
9001/tcp  open  tor-orport?
10000/tcp open  http         MiniServ 1.620 (Webmin httpd)
|_ http-favicon: Unknown favicon MD5: C5C3376517454BC9DB00555602B7BD67
|_ http-git: 0
|_ http-methods: No Allow or Public header in OPTIONS response (status
code 200)
|_ http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
|_ ndmp-version:
|_ ERROR: Failed to get host information from server

```

< Filter Hosts >

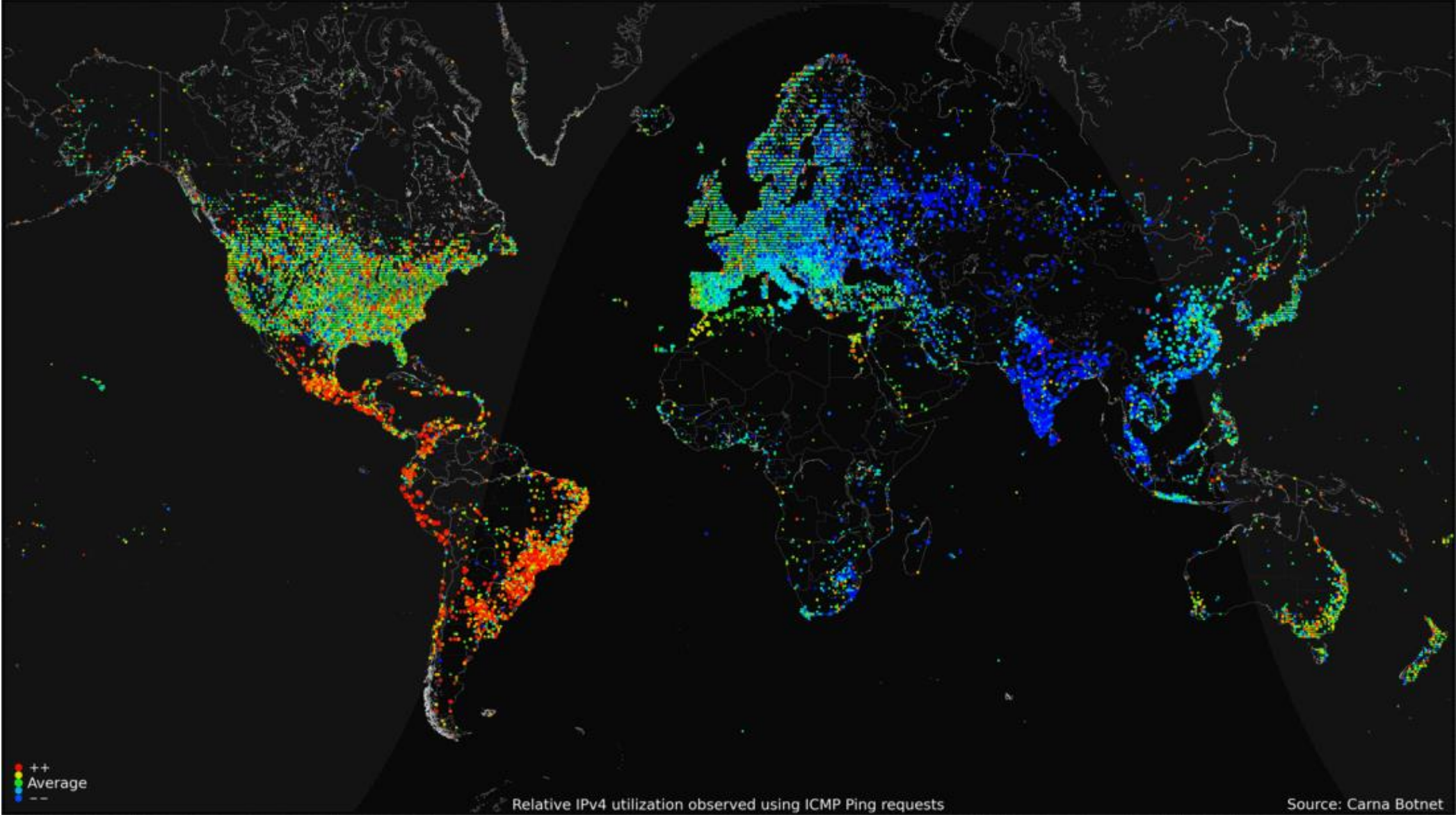
Interesting Stats

- .NET = Most popular TLD for reverse DNS RRs
- Apache holds 20% of web servers in the world on Port 80
- HP LaserJet P2055 ~2.71% of all Web Connected Printers
- How Big?
 - 420M responded to pings
 - 36M with open ports that did not respond to pings
 - 450M “Definitely” in use
 - 141M closed ports/no ping, firewalled ranges, unknown if computer
 - 591M “in use”
 - 729M only have reverse DNS records, no probe response
 - 1.3 B IP addresses
 - 2.3 B unused?
- Data is free to analyze ~1TB
 - <http://internetcensus2012.bitbucket.org/download.html>



Reserved 0.0.0.0/8	APNIC 1.0.0.0/8	APNIC 2.0.0.0/8	HP 15.0.0.0/8	DEC 16.0.0.0/8	Ford 19.0.0.0/8	DDN-RVN 20.0.0.0/8	21.0.0.0/8									
GE 3.0.0.0/8	RIPE 4.0.0.0/8	Xerox 13.0.0.0/8	AT&T 14.0.0.0/8	Apple 17.0.0.0/8	MIT 18.0.0.0/8	23.0.0.0/8	DISA 22.0.0.0/8									
LEVEL3 4.0.0.0/8	ARIN 7.0.0.0/8	LEVEL3 8.0.0.0/8	DoD 11.0.0.0/8	DISA 30.0.0.0/8	29.0.0.0/8	ARIN 32.0.0.0/8	UK Ministry of Defence 25.0.0.0/8									
RIPE 5.0.0.0/8	US Army 6.0.0.0/8	IBM 9.0.0.0/8	Reserved 10.0.0.0/8	RIPE 31.0.0.0/8	DSI-North 28.0.0.0/8	APNIC 37.0.0.0/8	DISA 26.0.0.0/8									
APNIC 59.0.0.0/8	SITA 57.0.0.0/8	Merck 54.0.0.0/8	Cap Debis CCS 53.0.0.0/8	AT&T 32.0.0.0/8	ARIN 35.0.0.0/8	APNIC 36.0.0.0/8	RIPE 34.0.0.0/8	APNIC 218.0.0.0/8	APNIC 219.0.0.0/8	APNIC 220.0.0.0/8	APNIC 223.0.0.0/8	APNIC 224.0.0.0/8	LACNIC 225.0.0.0/8	ARIN 198.0.0.0/8	ARFINIC 197.0.0.0/8	
US Postal Service 56.0.0.0/8	DoD 55.0.0.0/8	Department of Homeland Security 52.0.0.0/8	Halliburton 33.0.0.0/8	ARIN 34.0.0.0/8	APNIC 38.0.0.0/8	PSINet 39.0.0.0/8	RIPE 40.0.0.0/8	ARIN 41.0.0.0/8	APNIC 42.0.0.0/8	APNIC 43.0.0.0/8	APNIC 44.0.0.0/8	LACNIC 45.0.0.0/8	ARIN 199.0.0.0/8	AFRINIC 196.0.0.0/8		
APNIC 60.0.0.0/8	ARIN 61.0.0.0/8	APNIC 62.0.0.0/8	Prudential 48.0.0.0/8	Bell-Northern Research 47.0.0.0/8	APNIC 44.0.0.0/8	APNIC 43.0.0.0/8	APNIC 42.0.0.0/8	DoD 214.0.0.0/8	215.0.0.0/8	APNIC 216.0.0.0/8	ARIN 217.0.0.0/8	ARIN 218.0.0.0/8	ARIN 219.0.0.0/8	ARIN 220.0.0.0/8	RIPE 194.0.0.0/8	RIPE 195.0.0.0/8
ARIN 64.0.0.0/8	ARIN 65.0.0.0/8	ARIN 66.0.0.0/8	ARIN 67.0.0.0/8	APNIC 68.0.0.0/8	APNIC 69.0.0.0/8	APNIC 70.0.0.0/8	Reserved 127.0.0.0/8	ARIN 128.0.0.0/8	ARIN 129.0.0.0/8	ARIN 130.0.0.0/8	ARIN 131.0.0.0/8	APNIC 132.0.0.0/8	LACNIC 133.0.0.0/8	LACNIC 134.0.0.0/8	RIPE 188.0.0.0/8	LACNIC 191.0.0.0/8
ARIN 68.0.0.0/8	ARIN 69.0.0.0/8	ARIN 70.0.0.0/8	ARIN 71.0.0.0/8	APNIC 72.0.0.0/8	APNIC 73.0.0.0/8	APNIC 74.0.0.0/8	APNIC 75.0.0.0/8	ARIN 76.0.0.0/8	ARIN 77.0.0.0/8	ARIN 78.0.0.0/8	ARIN 79.0.0.0/8	ARIN 80.0.0.0/8	RIPE 185.0.0.0/8	ARIN 184.0.0.0/8	LACNIC 183.0.0.0/8	LACNIC 182.0.0.0/8
RIPE 76.0.0.0/8	RIPE 77.0.0.0/8	ARIN 78.0.0.0/8	ARIN 79.0.0.0/8	APNIC 80.0.0.0/8	APNIC 81.0.0.0/8	APNIC 82.0.0.0/8	APNIC 83.0.0.0/8	ARIN 140.0.0.0/8	RIPE 141.0.0.0/8	ARIN 142.0.0.0/8	ARIN 143.0.0.0/8	ARIN 144.0.0.0/8	ARIN 145.0.0.0/8	ARIN 146.0.0.0/8	ARIN 147.0.0.0/8	ARIN 148.0.0.0/8
RIPE 84.0.0.0/8	RIPE 85.0.0.0/8	RIPE 86.0.0.0/8	RIPE 87.0.0.0/8	ARIN 88.0.0.0/8	ARIN 89.0.0.0/8	APNIC 90.0.0.0/8	APNIC 91.0.0.0/8	ARIN 149.0.0.0/8	ARIN 150.0.0.0/8	ARIN 151.0.0.0/8	ARIN 152.0.0.0/8	ARIN 153.0.0.0/8	ARIN 154.0.0.0/8	ARIN 155.0.0.0/8	ARIN 156.0.0.0/8	ARIN 157.0.0.0/8
RIPE 92.0.0.0/8	RIPE 93.0.0.0/8	RIPE 94.0.0.0/8	RIPE 95.0.0.0/8	ARIN 96.0.0.0/8	ARIN 97.0.0.0/8	ARIN 98.0.0.0/8	ARIN 99.0.0.0/8	ARIN 158.0.0.0/8	ARIN 159.0.0.0/8	ARIN 160.0.0.0/8	ARIN 161.0.0.0/8	ARIN 162.0.0.0/8	ARIN 163.0.0.0/8	ARIN 164.0.0.0/8	ARIN 165.0.0.0/8	ARIN 166.0.0.0/8
RIPE 96.0.0.0/8	RIPE 97.0.0.0/8	RIPE 98.0.0.0/8	RIPE 99.0.0.0/8	ARIN 100.0.0.0/8	APNIC 103.0.0.0/8	ARIN 104.0.0.0/8	ARIN 107.0.0.0/8	ARIN 149.0.0.0/8	RIPE 151.0.0.0/8	ARIN 152.0.0.0/8	ARIN 153.0.0.0/8	ARIN 164.0.0.0/8	ARIN 167.0.0.0/8	ARIN 168.0.0.0/8	ARIN 169.0.0.0/8	APNIC 170.0.0.0/8
RIPE 100.0.0.0/8	RIPE 101.0.0.0/8	RIPE 102.0.0.0/8	RIPE 103.0.0.0/8	APNIC 102.0.0.0/8	AFRINIC 103.0.0.0/8	APNIC 105.0.0.0/8	ARIN 106.0.0.0/8	ARIN 149.0.0.0/8	ARIN 150.0.0.0/8	ARIN 151.0.0.0/8	AFRINIC 154.0.0.0/8	ARIN 165.0.0.0/8	ARIN 166.0.0.0/8	ARIN 167.0.0.0/8	ARIN 168.0.0.0/8	ARIN 169.0.0.0/8

Geolocation of Ips
from
maxmind.com
database



http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Morris_worm.html

https://en.wikipedia.org/wiki/Morris_worm

<http://www.nbcnews.com/technology/technolog/hacker-maps-internet-enslaving-thousands-vulnerable-machines-1C8979106>

<http://internetcensus2012.bitbucket.org/paper.html>

<http://seclists.org/fulldisclosure/2013/Mar/166>

http://www.theregister.co.uk/2013/03/19/carna_botnet_ipv4_internet_map/print.html

http://gawker.com/5991667/this-illegally-made-incredibly-mesmerizing-animated-gif-is-what-the-internet-looks-like?utm_campaign=socialflow_gawker_facebook&utm_source=gawker_facebook&utm_medium=socialflow