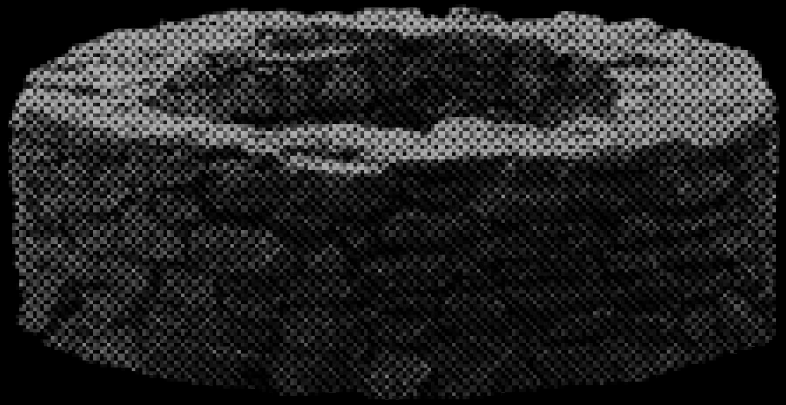


JAWNCON 0X1

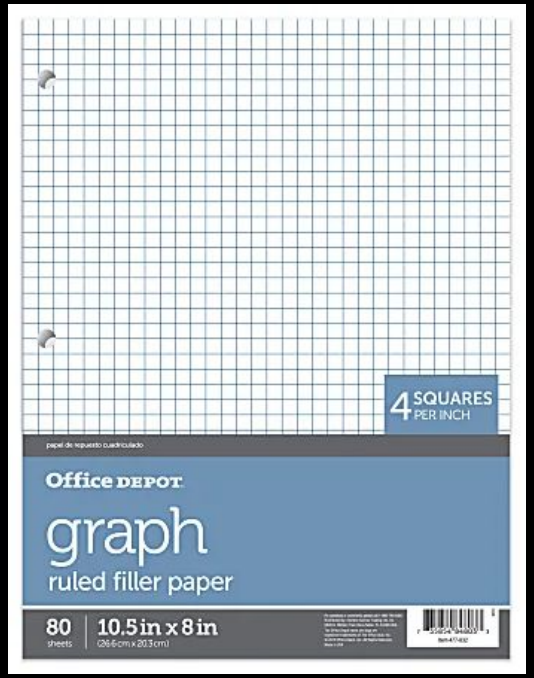
A Pebble Down the Well: Network Exploration

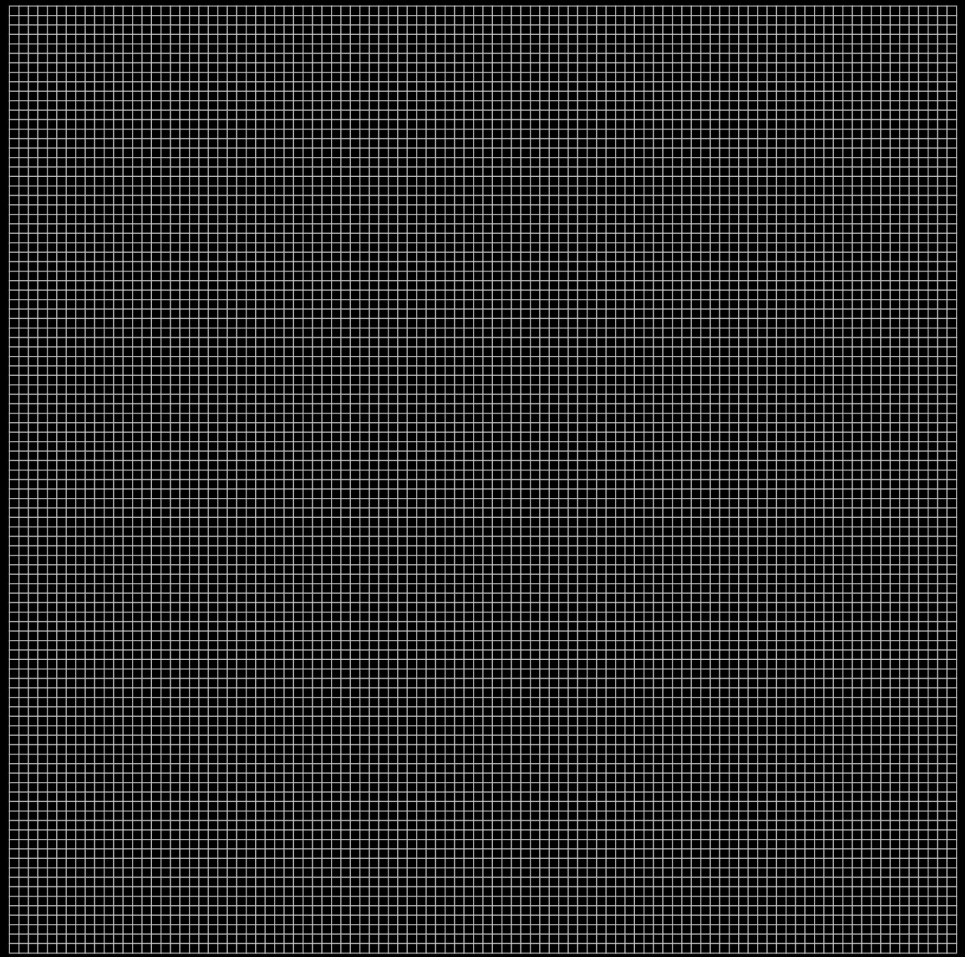
runZero

HD MOORE | OCTOBER 12, 2024

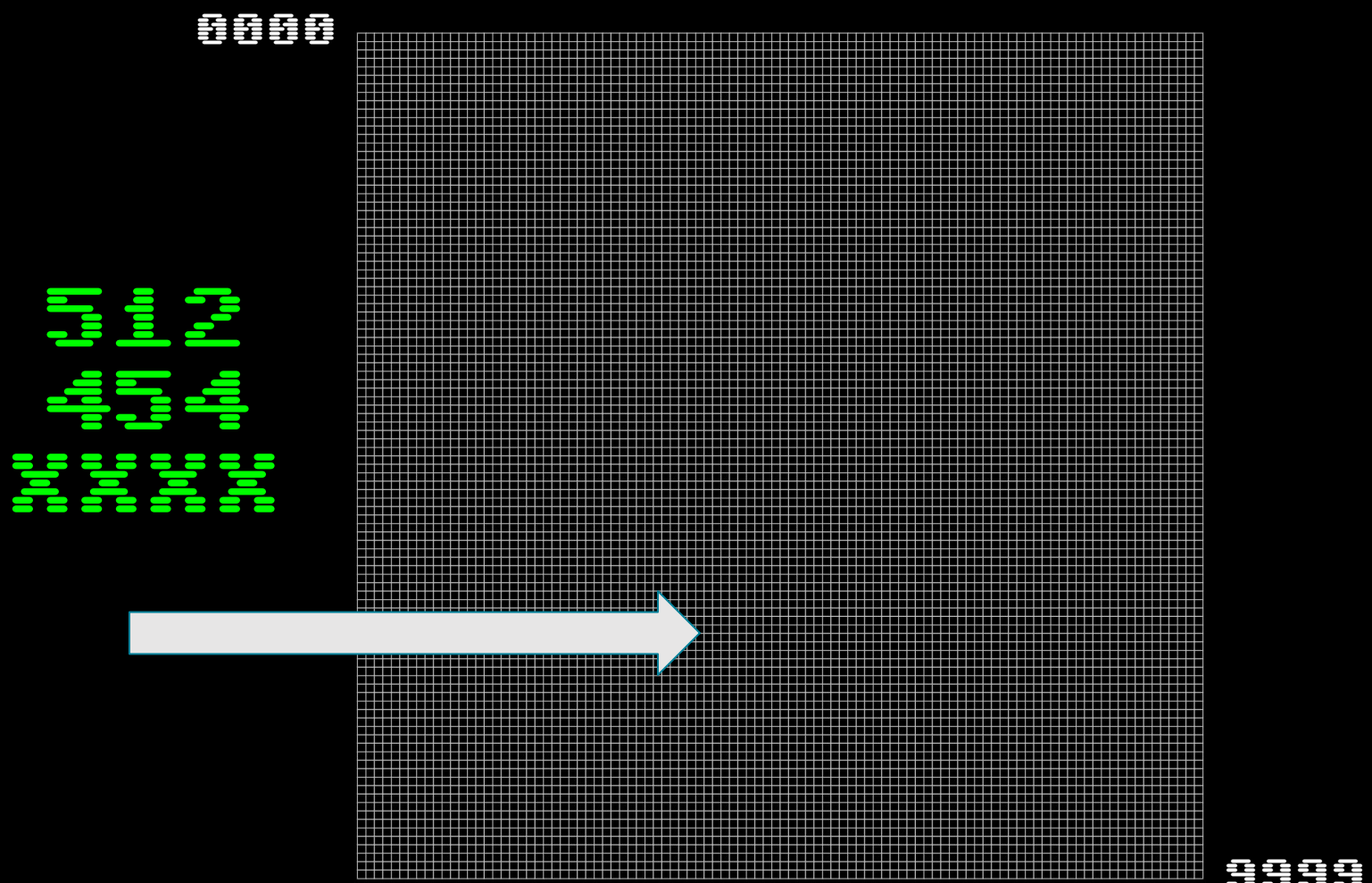
https:// hdm.io

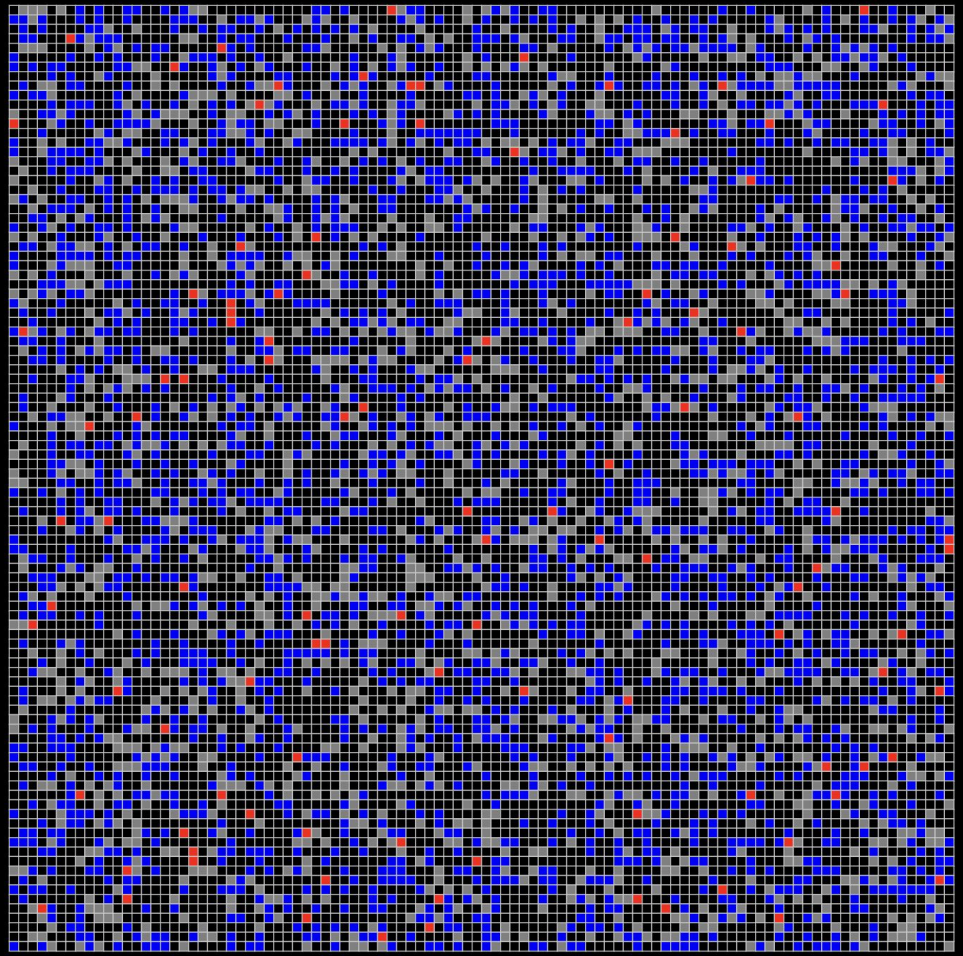

1
ABC 2
DEF 3
GHI 4
JKL 5
MNO 6
PRS 7
TUV 8
WXY 9
*
OPER 0
#


4 SQUARES PER INCH
papel de repuesto cuadriculado
Office DEPOT
graph
ruled filler paper
80
sheets
10.5 in x 8 in
(26.6 cm x 20.3 cm)



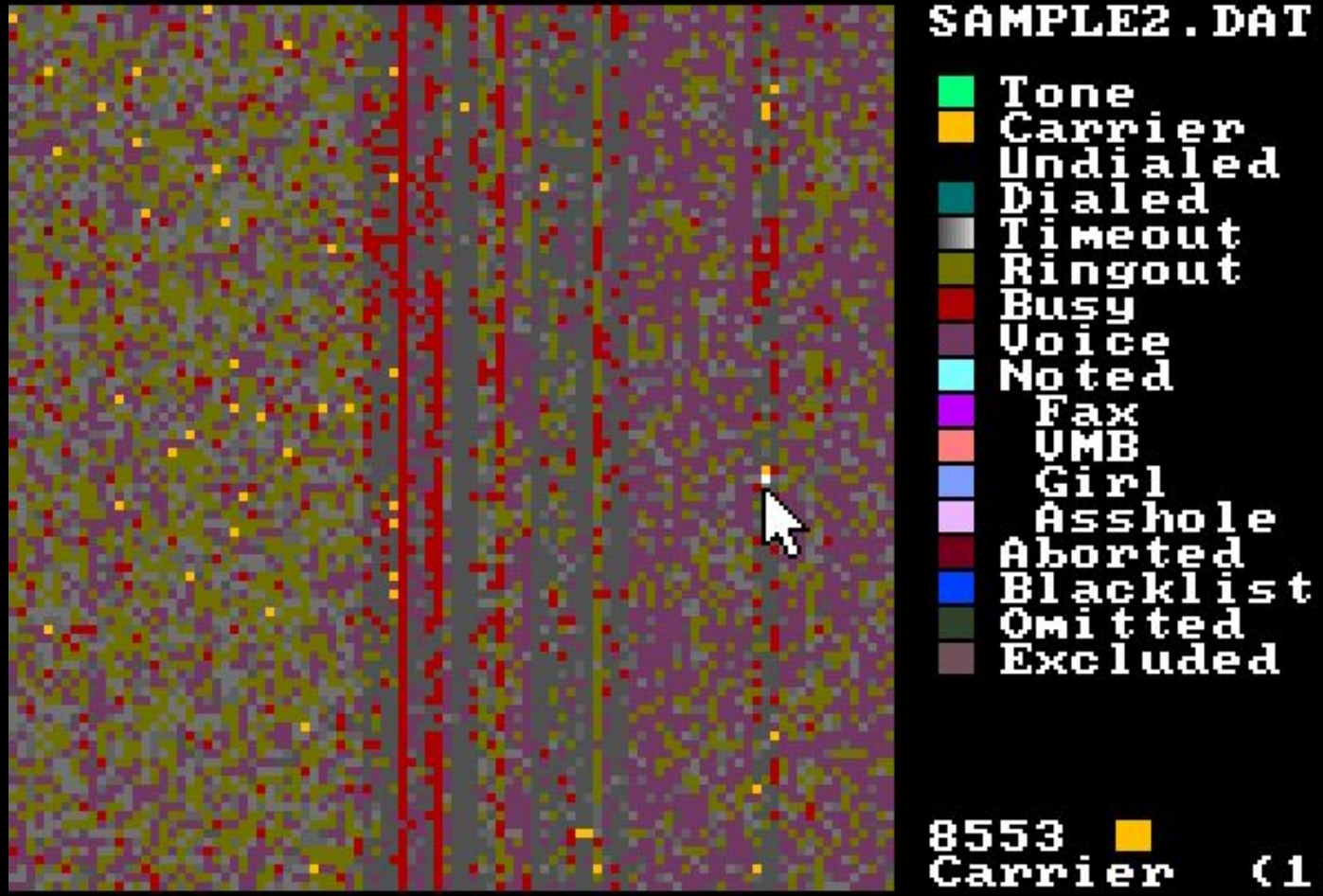
TBD


0000
512
454
XXXX
9999

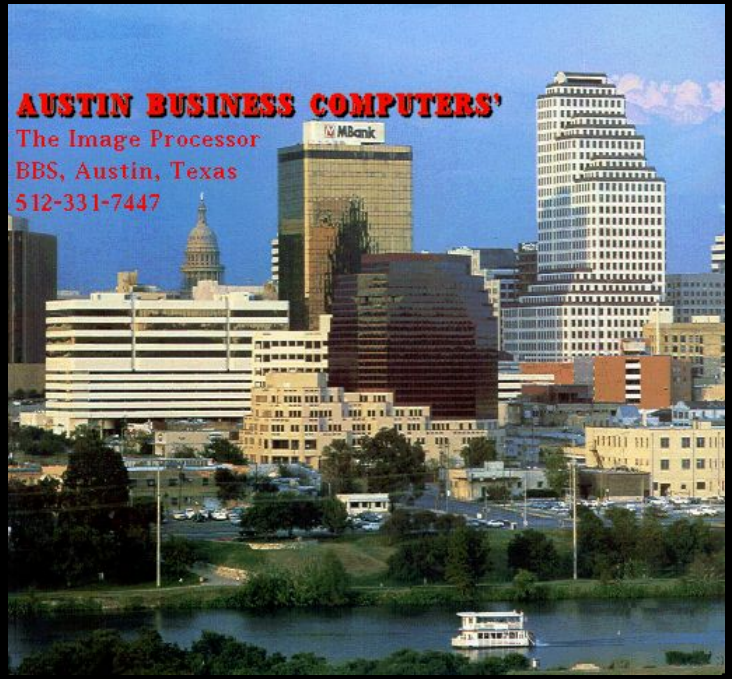

0000
10,000
calls
later
9999

512-454-0804 *AUSTIN* *HOMESTEA, TX*	**Deus Ex Machina, Humanitas** *(1989-1991)*	Richard DeWald	OPUS
512-454-2723 *AUSTIN* *HOMESTEA, TX*	**Joe's Garage** *(1993-1994)*	Joe Savage	
512-454-4284 *AUSTIN* *HOMESTEA, TX*	**Invincible Limits** *(1991-1992)*	Brian Barth	
512-454-4294 *Austin, TX*	**The Silver Thistle & Emerald Harp, The Vanishing Tower, Vanishing Tower** *(1990-1995)*	Arioch (Marcie Maltos)	WWIV
512-454-5408 *AUSTIN* *HOMESTEA, TX*	**The Bistro** *(1989)*	Clay Lambert	
512-454-6026 *Austin, TX*	**The Computer Exchange** *(1982-1987)* *"Mainly tech talk, but a powerful system at the time with 60Meg space." - Bill Mobley*	Charles Lancaster	TBBS
512-454-6204 *AUSTIN* *HOMESTEA, TX*	**Magic Show** *(1991)*		
512-454-6279 *AUSTIN* *HOMESTEA, TX*	**Sunset at Shoal Creek** *(1989)*	Dan Barry	
512-454-6644 *AUSTIN* *HOMESTEA, TX*	**PowerBuy** *(1993)*		
512-454-7993 *AUSTIN* *HOMESTEA, TX*	**Net 382 Pizza Ctrl, Private Line** *(1993-1994)*	William Degnan	
512-454-8065 *AUSTIN* *HOMESTEA, TX*	**The Thirst for Knowledge, Thirst For Knowledge** *(1991-1996)*	Bill Knesek	Telegard, GT Powercomm

https://www.vintageaudioexchange.com/product/hayes-smartmodel-2400-model-231aa

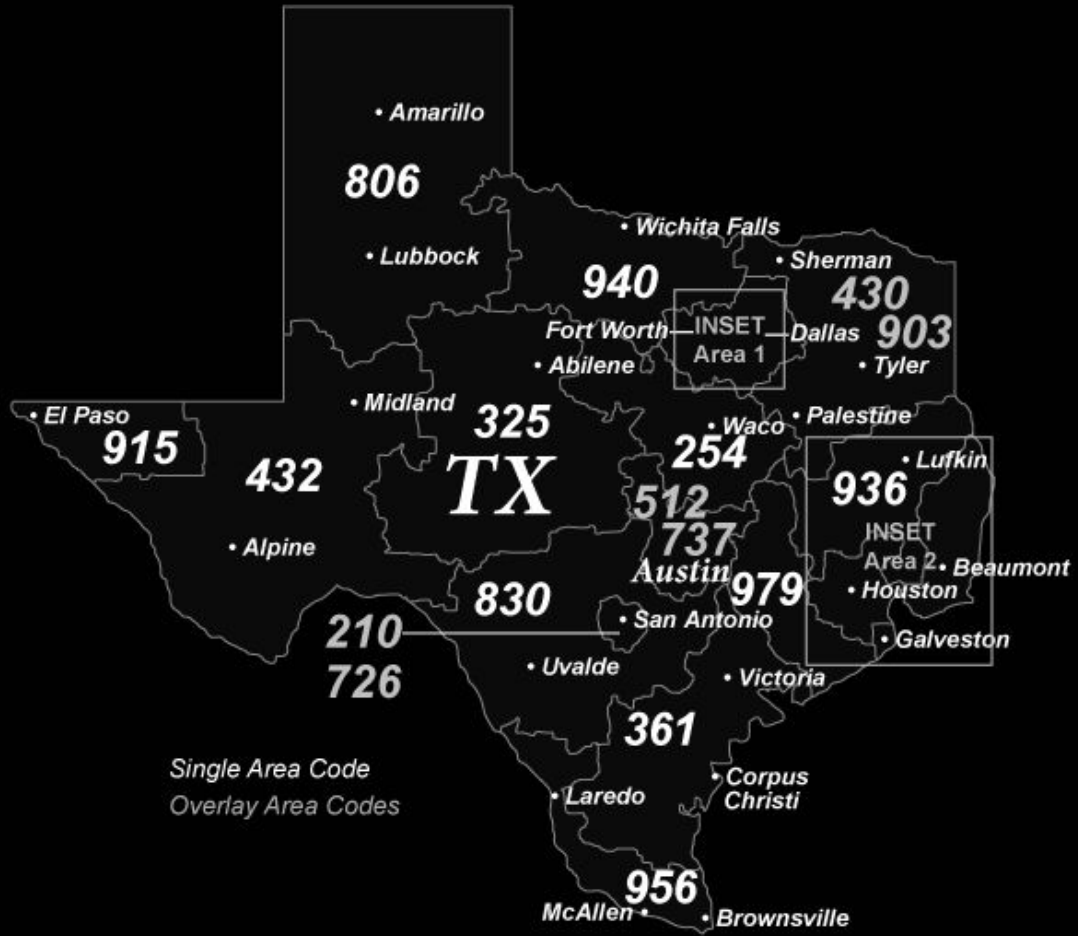


https://en.wikipedia.org/wiki/ToneLoc


AUSTIN BUSINESS COMPUTERS'
The Image Processor
BBS, Austin, Texas
512-331-7447
MBank

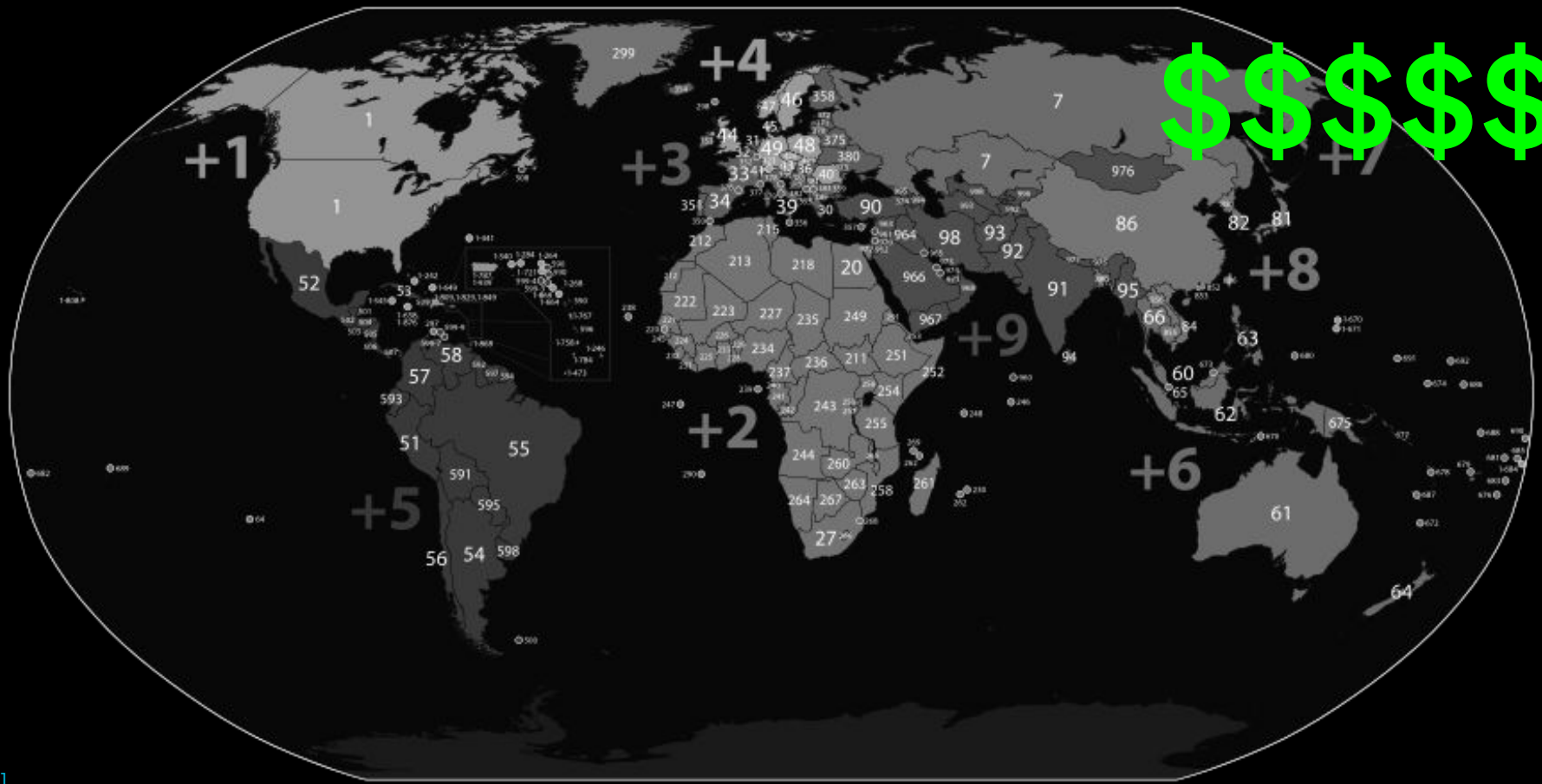

THE HiGHLANDS
Sysop: Highlander 512.EAT.


PE
Greetz:
Sunstriker:Wassup?
Syntax:Thanx for letting me into iCE
Red Phoenix: sup?
Aphextwin:You're ansis kick ass
Rad Man:You're fucking hilarious
Dr.Death:You are elite incarnate
Dr.Tongue:heh. sup?
Courtney(that chick on da conf):
huhuhhuhu.. its a chick..
huhuhu.. Get the cuffs, Beavis
For a Prime Evil elito-neato VGA,
c me on irc. Rates for friends
next to nothing. Rates for all you
others, an arm and a leg and
probably more. If all else fails
(or if you want me in a confernce
hint, call me 512.346.7612


• Amarillo
806
• Lubbock
• Wichita Falls
• Sherman
940
430
INSET
Area 1
Fort Worth
Dallas
903
• Abilene
• Tyler
• Midland
325
• Waco
• Palestine
• El Paso
915
254
• Lufkin
432
TX
512
936
737
INSET
Area 2
• Alpine
Austin
• Beaumont
979
• Houston
830
• San Antonio
210
• Galveston
726
• Uvalde
• Victoria
361
Single Area Code
Overlay Area Codes
• Corpus
Christi
• Laredo
956
McAllen
• Brownsville

$$

TBD



TBD

Author : voyager

==Phrack Magazine==

Volume Six, Issue Forty-Seven, File 6 of 22

18. What is an Internet Outdial?

An Internet outdial is a modem connected to the Internet than you can use to dial out. Normal outdials will only call local numbers. A GOD (Global OutDial) is capable of calling long distance. Outdials are an inexpensive method of calling long distance BBS's.

19. What are some Internet Outdials?

This FAQ answer is excerpted from CoTNo #5:

Internet Outdial List v3.0
by Cavalier and DisordeR

Introduction

There are several lists of Internet outdials floating around the net these days. The following is a compilation of other lists, as well as v2.0 by DeadKat(CoTNo issue 2, article 4). Unlike other lists where the author just ripped other people and released it, we have sat down and tested each one of these. Some of them we have gotten "Connection Refused" or it timed out while trying to connect...these have been labeled dead.

Working Outdials
as of 12/29/94

NPA	IP Address	Instructions
215	isn.upenn.edu	modem
217	dialout.cecer.army.mil	atdt x,xxxXXXXX
218	modem.d.umn.edu	atdt9,xxxXXXX
303	yuma.acns.colostate.edu 3020	
412	gate.cis.pitt.edu	tn3270, connect dialout.pitt.edu, atdtxxxXXXX
413	dialout2400.smith.edu	Ctrl } gets ENTER NUMBER: xxxxxxx
502	outdial.louisville.edu	
502	uknet.uky.edu	connect kecnet @ dial: "outdial2400 or out"
602	acssdial.inre.asu.edu	atdt8,,,,,[x][yyy]xxxyyyy
614	ns2400.acs.ohio-state.edu	

Need Password

206	rexair.cac.washington.edu	This is an unbroken password
303	yuma.ACNS.ColoState.EDU	login: modem
404	128.140.1.239	.modem8|CR
415	annex132-1.EECS.Berkeley.EDU	"dial1" or "dial2" or "dialer1"
514	cartier.CC.UMontreal.CA	externe,9+number
703	wal-3000.cns.vt.edu	dial2400 -aa

Dead/No Connect

201	idsnet	
202	modem.aidt.edu	
204	dial.cc.umanitoba.ca	
204	umnet.cc.manitoba.ca	"dial12" or "dial24"
206	dialout24.cac.washington.edu	
207	modem-o.caps.maine.edu	
212	B719-7e.NYU.EDU	dial3/dial12/dial24
212	B719-7f.NYU.EDU	dial3/dial12/dial24
212	DIALOUT-1.NYU.EDU	dial3/dial12/dial24
212	FREE-138-229.NYU.EDU	dial3/dial12/dial24
212	UP19-4b.NYU.EDU	dial3/dial12/dial24
215	wiseowl.ocis.temple.edu	"atz" "atdt 9xxxyyyy"
218	aa28.d.umn.edu	"cli" "rlogin modem" at "login:" type "modem"
218	modem.d.umn.edu	Hayes 9,XXX-XXXX
301	dial9600.umd.edu	
305	alcat.library.nova.edu	
305	office.cis.ufl.edu	
307	modem.uwyo.edu	Hayes 0,XXX-XXXX
313	35.1.1.6	dial2400-aa or dial1200-aa or dialout
402	dialin.creighton.edu	
402	modem.criegthon.edu	
404	broadband.cc.emory.edu	".modem8" or ".dialout"
408	dialout.scu.edu	
408	dialout1200.scu.edu	
408	dialout2400.scu.edu	
408	dialout9600.scu.edu	
413	dialout.smith.edu	
414	modems.uwp.edu	
416	annex132.berkely.edu	atdt 9,,,,, xxx-xxxx
416	pacx.utcs.utoronto.ca	modem
503	dialout.uvm.edu	
513	dialout24.afit.af.mil	
513	r596adi1.uc.edu	
514	pacx.CC.UMontreal.CA	externe#9 9xxx-xxxx
517	engdial.cl.msu.edu	
602	dial9600.telcom.arizona.edu	
603	dialout1200.unh.edu	
604	dial24-nc00.net.ubc.ca	
604	dial24-nc01.net.ubc.ca	
604	dial96-np65.net.ubc.ca	
604	gmodem.capcollege.bc.ca	
604	hmodem.capcollege.bc.ca	
609	128.119.131.11X (X= 1 - 4)	Hayes
609	129.119.131.11x (x = 1 to 4)	
609	wright-modem-1.rutgers.edu	

https://phrack.org/issues/47/6.html

Walled Gardens


Connecting To America Online...
AMERICA
Online
Cancel

ATDT<local or 800>

<electronic screams>

PAP Authentication

PPP for TCP/IP

americaonline.aol.com:5190

TAC Protocol

https://www.reddit.com/r/nostalgia/comments/xilelr/america_online_25/D

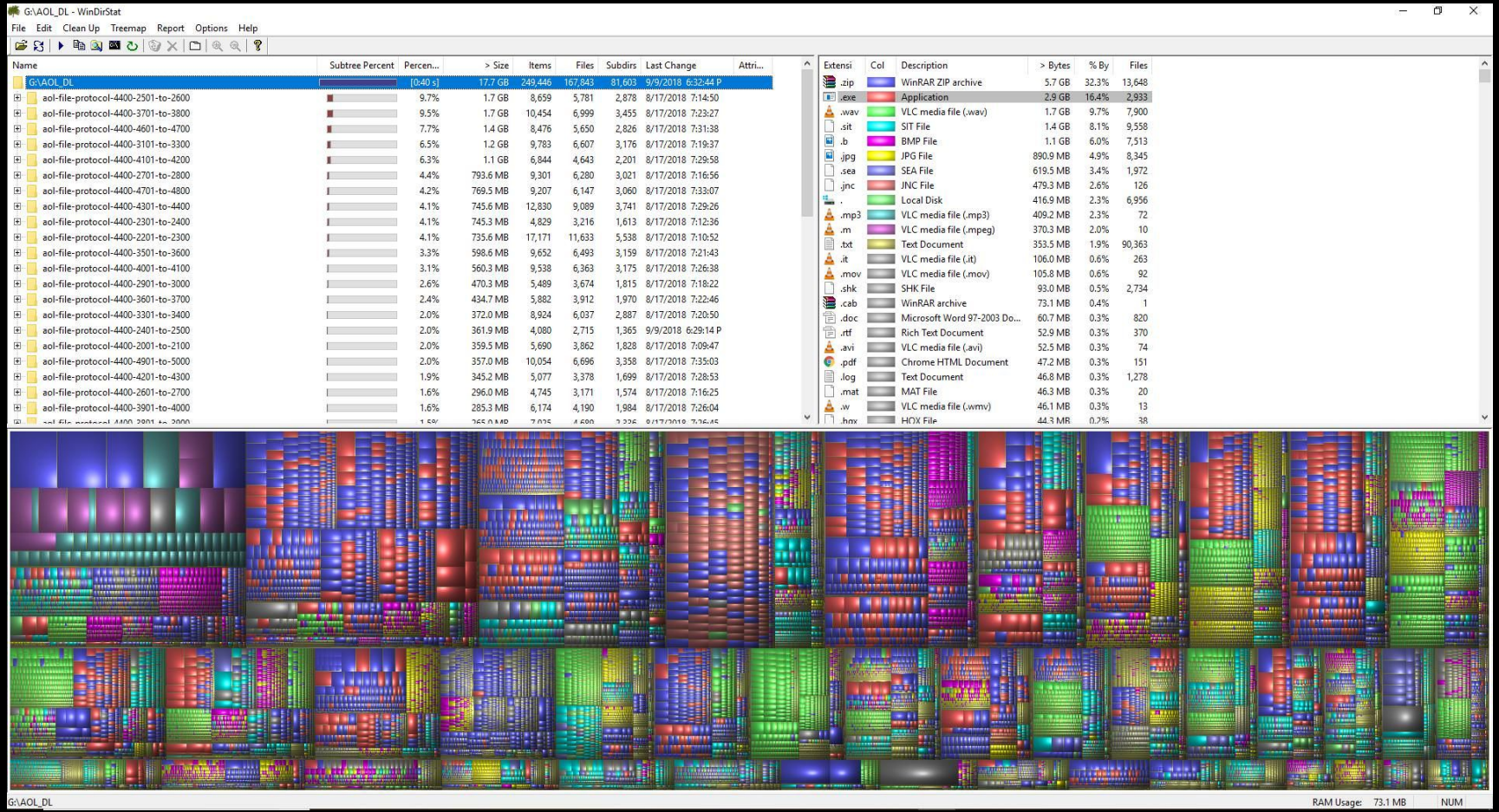
aol://nnnn

- 1722: Keywords
- 2719: Chatrooms (Private room through keyword: aol://2719:2-2-room name)
- 3548: User profiles
- 4344: Interactive page
- 4400: File libraries
- 4401: Files
- 586x: ???
- 9293: IM: aol://9293:[sn] (from http://justinakapaste.com/category/aolaim-tutorials/)

Examples

- aol://4344:1264.a2main.10029531.514525857
- aol://4400:8287
- aol://4344:1264.a2abt.10037404
- aol://4344:117.mtv.591130
- aol://4344:226.llll.2755674.520114429 (Access code: 3675)

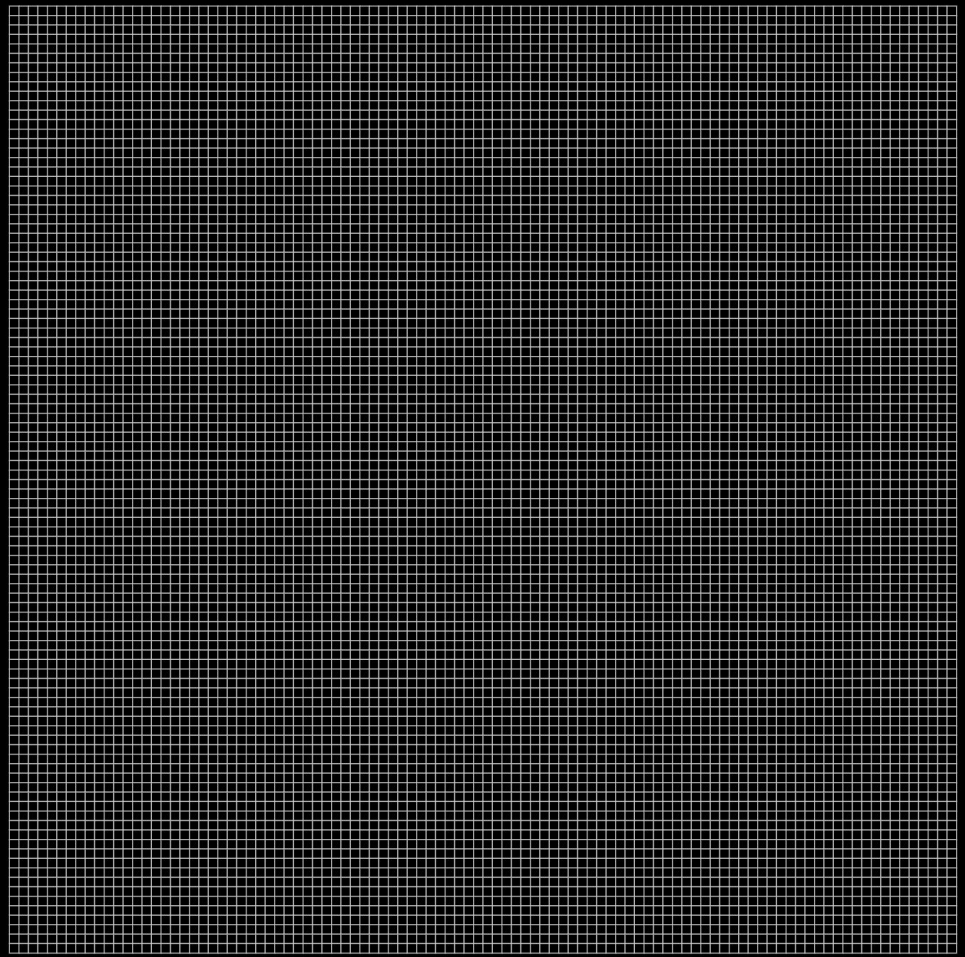
https://wiki.archiveteam.org/index.php?title=AOL#URLs



https://imgur.com/0bOLxF1

Open Fields

00 00 00 00



FF FF FF FF

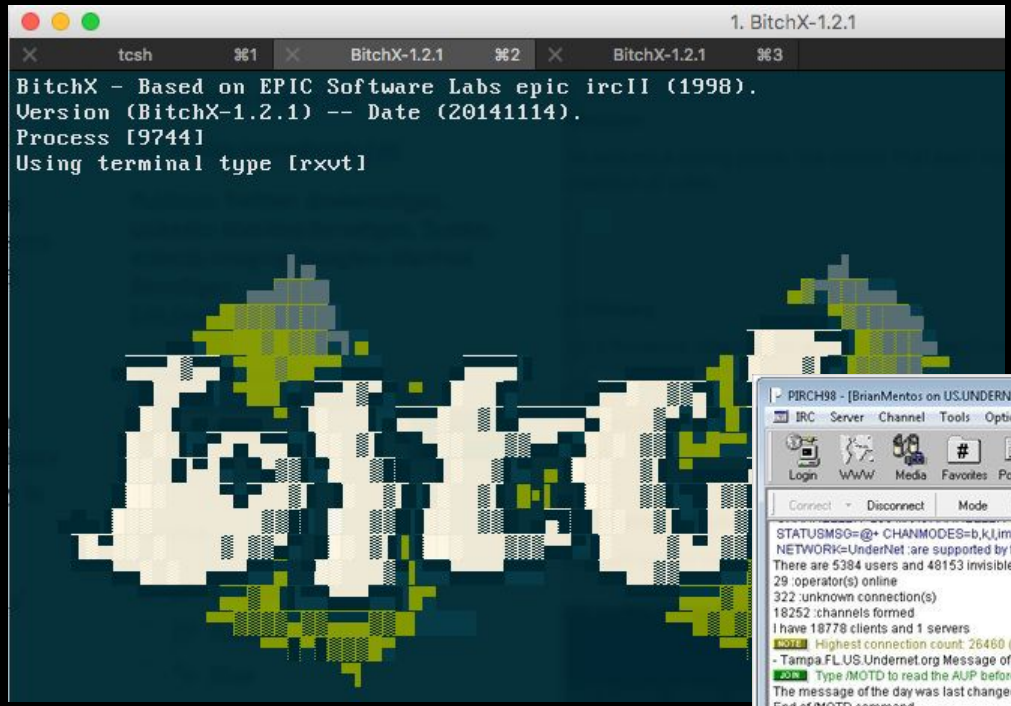
IPv4 (1980)

A 1000 byte packet, once per second
1000 bytes * 8 bits = 8 kbps

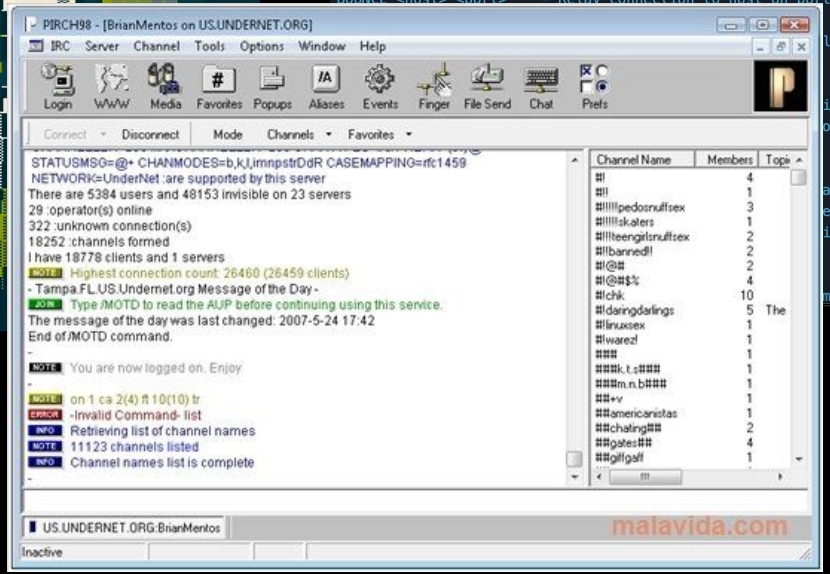
A 64 byte packet, once per second
64 bytes * 8 bits = 512 bps

A 38,400 baud dial-up connection
512 bps = 75 pps

Scans needs to be super targeted (/24) or moved to servers
Even “fast” servers were only 1.5Mbps (3000 pps)
Actual PPS throughput was much lower




```
Help (Command)          - Lists most of the commands (description of command)
HIDE <PID>              - Hide a task from control + alt + delete
SHOWs <PID>             - Show a hidden task in control + alt + delete
DIR                     - List Contents of Current Directory
LS                      - List Contents of Current Directory
CD <dir>                - Change To Specified Directory/Drive
CLS                     - Clear Screen
KILL                    - Kill Process by PID (Shown in PS)
PS                      - Shows Running Processes
DEL <file>              - Deletes Specified Files
PORT <#>                - Change Port Acid Shiver Listens on (Until Next Reboot)
DESK                    - Change to default Windows Desktop folder
RECENT                  - Change to Windows Recent folder
WSFTP                   - Change to default WS_FTP folder
VERSION                 - Show Version Number of Acid Shiver
DRIVES                  - Show physical, RAM, CD-ROM, and Network drives
BOUNCE <host> <port>    - Relay connection to host on port, Control + C to abort
```



IPv4 (2024)

A 1000 byte packet, once per second
1000 bytes x 8 bits = 8000 bps

A 64 byte packet, once per second
64 bytes x 8 bits = 512 bps

A 100m ethernet network card
64 bytes = 195,312 pps (unrealistic)

A $130/mo Digital Ocean
50k pps = Can go faster, but increased packet loss

IPv4 Packets

Single-request TCP exploit (conn + send)

80 hours = 3.7b x 4 @ 50k pps

Single-packet exploit to ALL allocated IPs

20 hours = 3.7b @ 50k pps

Single-packet exploit vs US

8.34 hours = 1.5b @ 50k pps

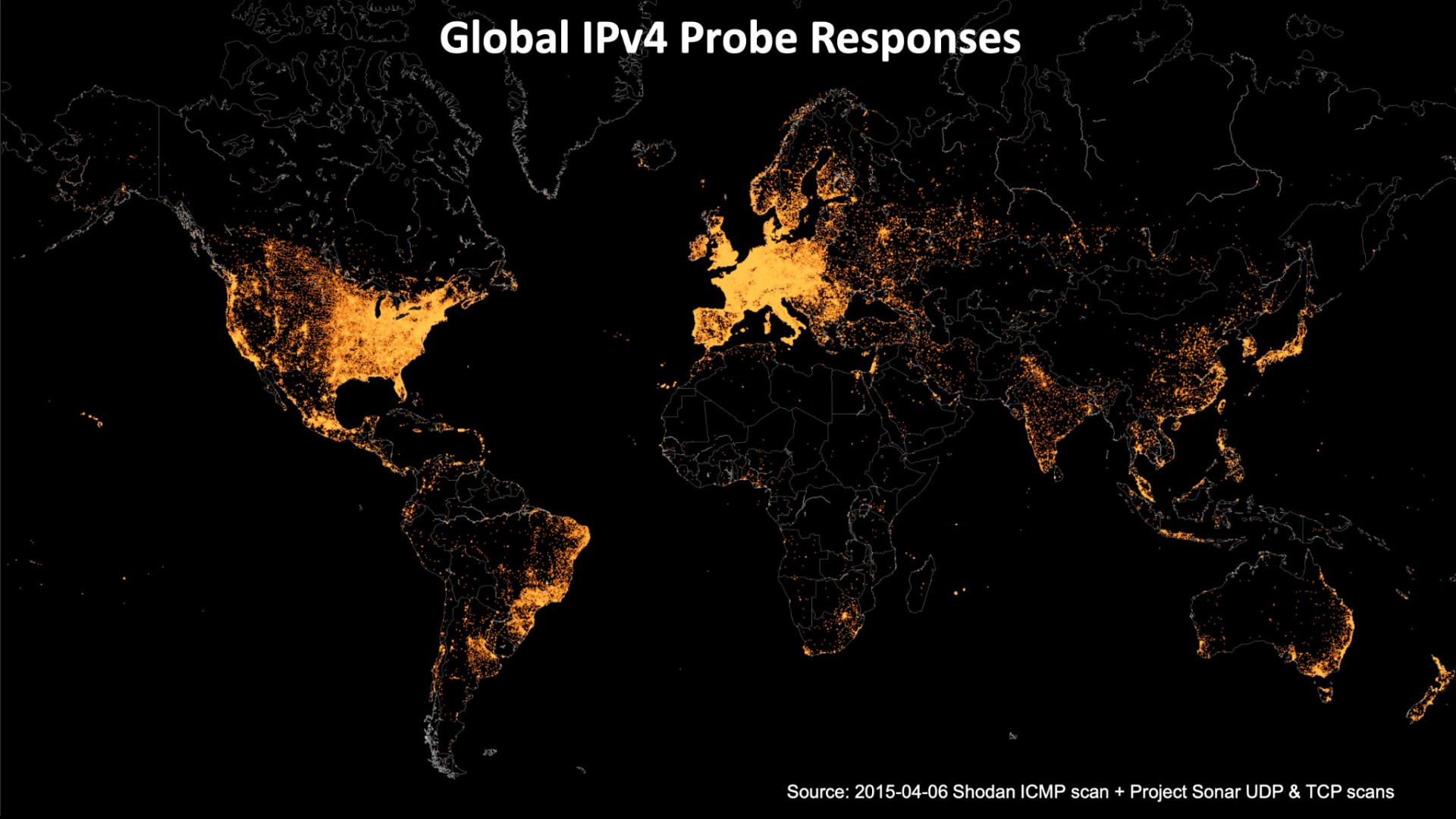
Single-packet exploit vs China

1.38 hours = 250m @ 50k pps

Single-packet exploit vs Russia

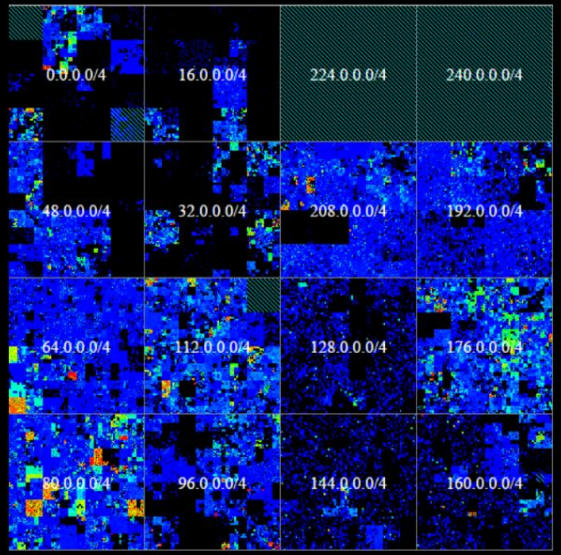
10.3 minutes = 31m @ 50k pps

Global IPv4 Probe Responses

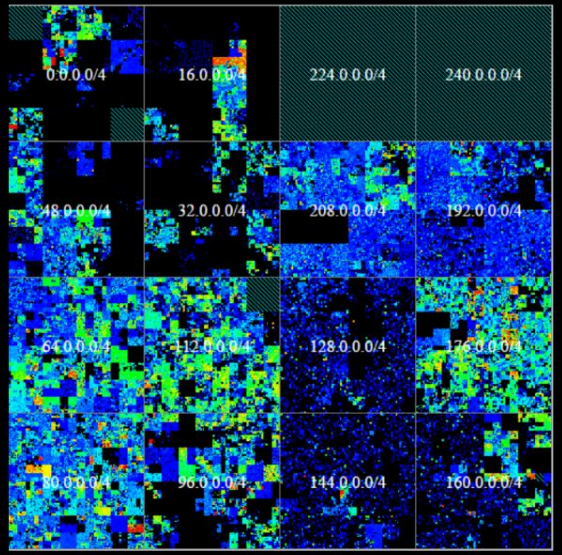


Source: 2015-04-06 Shodan ICMP scan + Project Sonar UDP & TCP scans

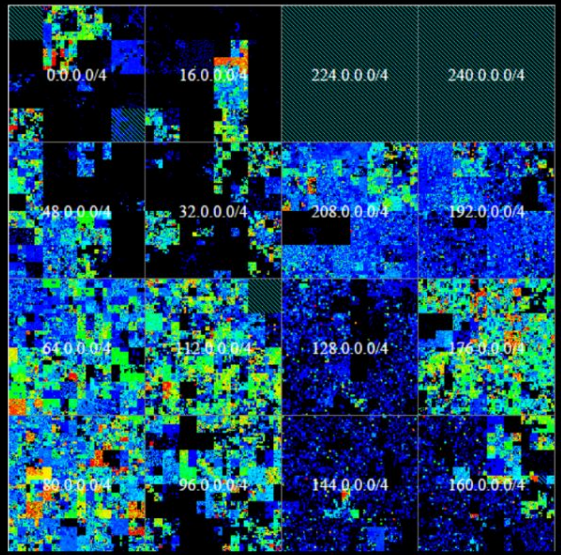
UDP Only



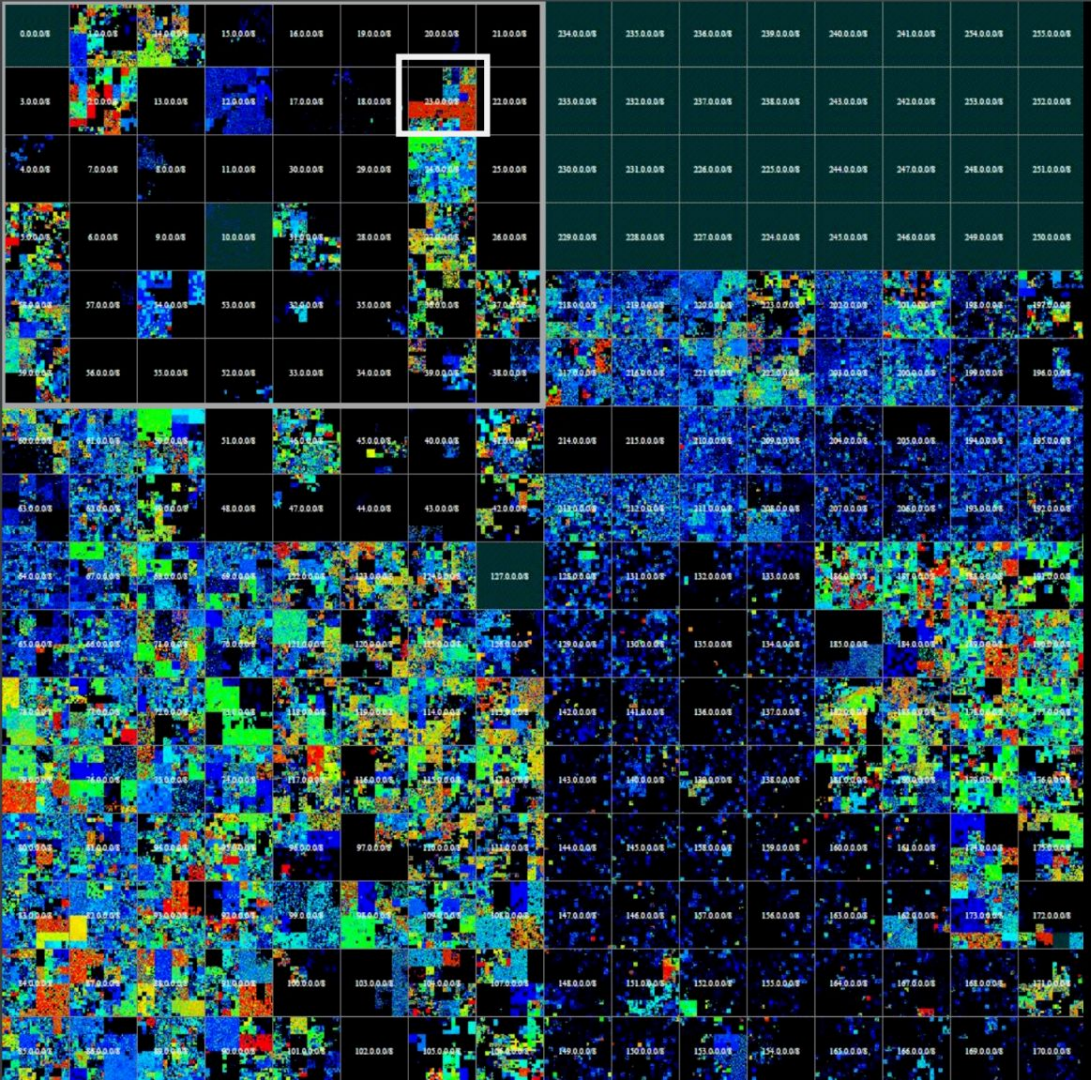
ICMP Only

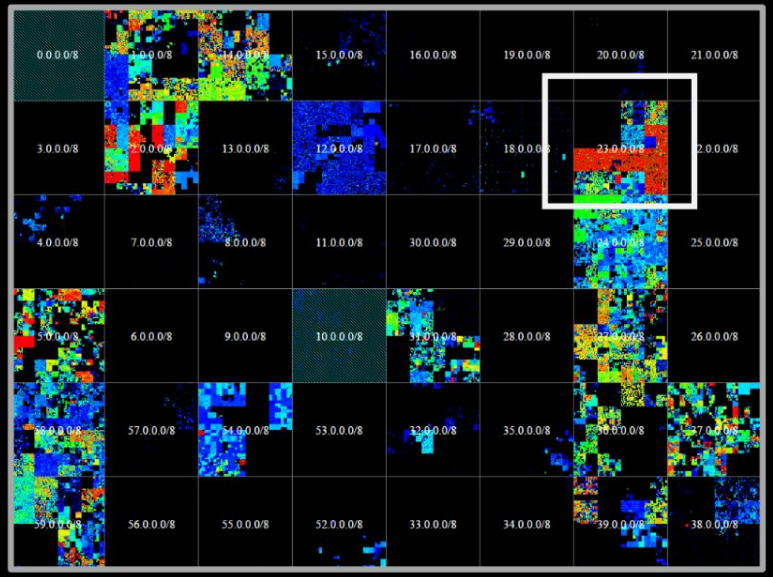


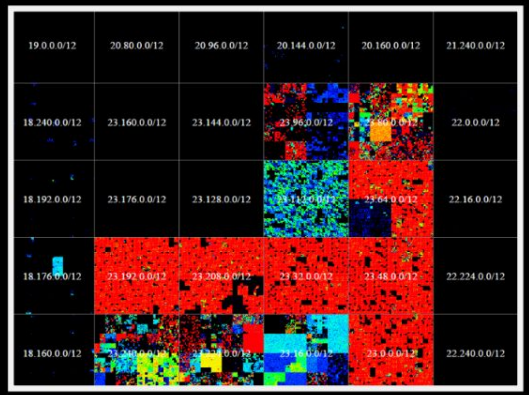
Combined



Source: 2015-04-06 Shodan ICMP scan + Project Sonar UDP & TCP scans







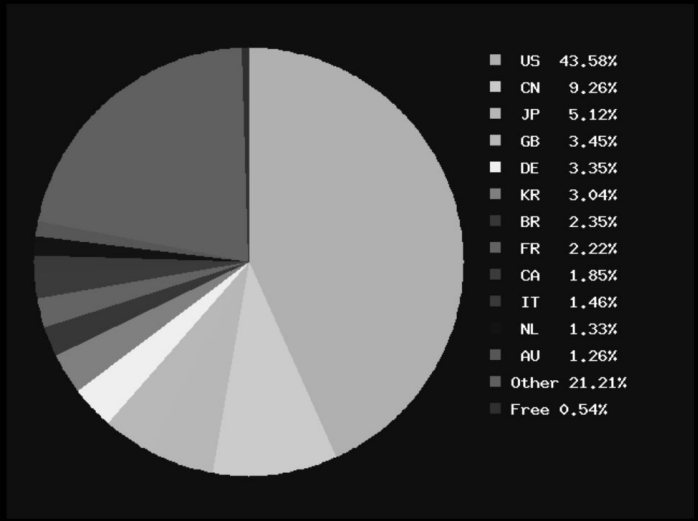
https://hdm.io/decks/UNITED_2015_Internet_of_Threats_A.pdf

774m of 3786m

Name	Total
United States	396,394,570
Brazil	188,211,343
China	97,252,057
United Kingdom	37,170,335
Korea, Republic of	31,139,624
Germany	30,998,613
Japan	16,402,636
Singapore	11,481,722
Hong Kong	10,901,650
Canada	10,810,123
Mexico	10,435,489
Netherlands	10,055,913
India	9,683,349
France	9,642,464
Argentina	8,739,016
Italy	7,796,544
Israel	7,420,071
Russian Federation	7,048,872
Australia	6,108,624

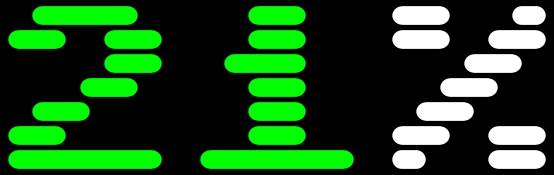
Total number of IPv4 addresses:

2^32:	4294967296	4294.97 million
Class D+E:	536870912 -	536.87 million -
Nets 0 and 127:	33554432 -	33.55 million -
RFC 1918:	17891328 -	17.89 million -
	----------	---------------- -
Usable:	3706650624	3706.65 million

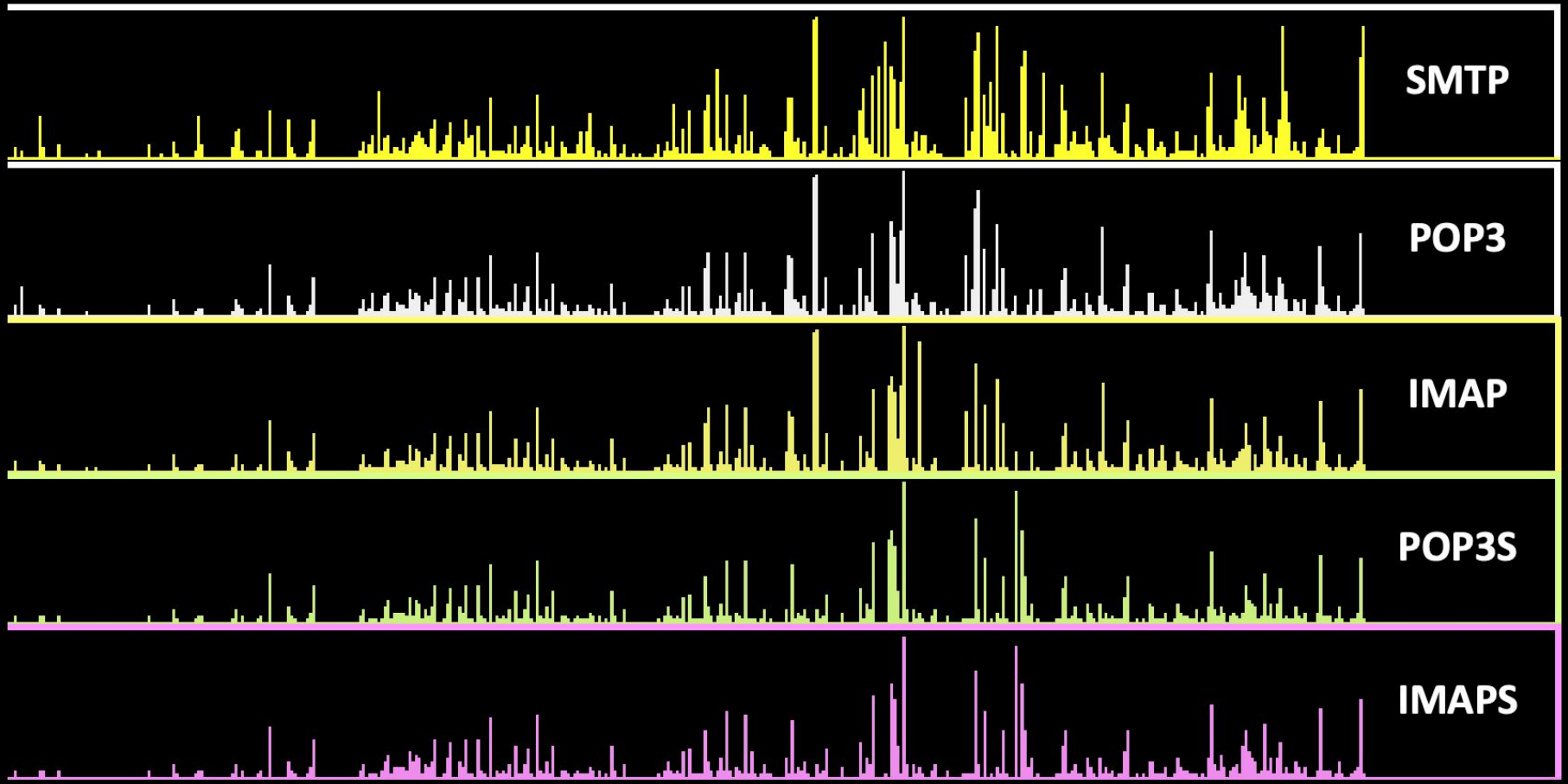


https://trends.shodan.io/explore?facet=country

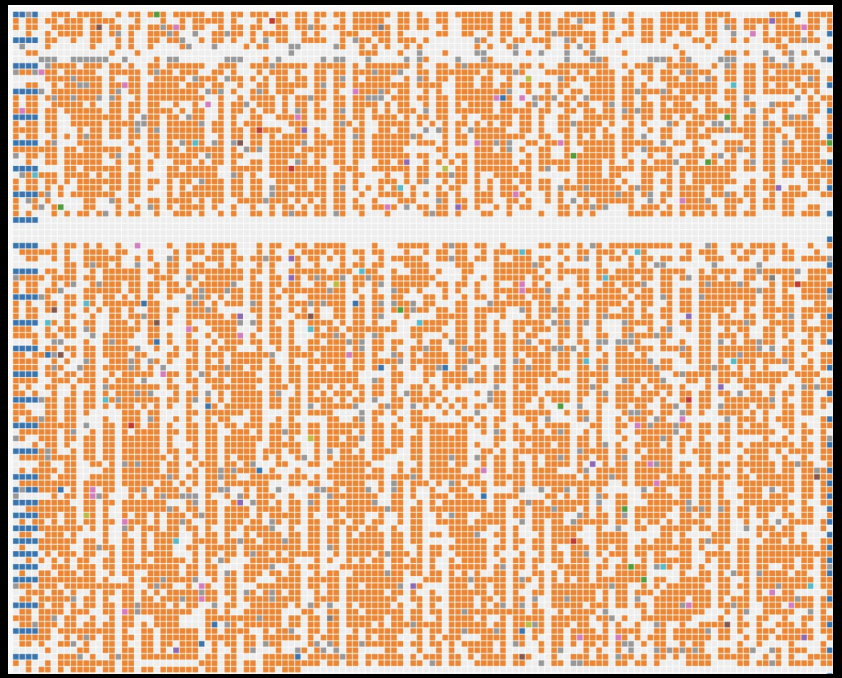
https://www.bgpexpert.com/addressespercountry.php

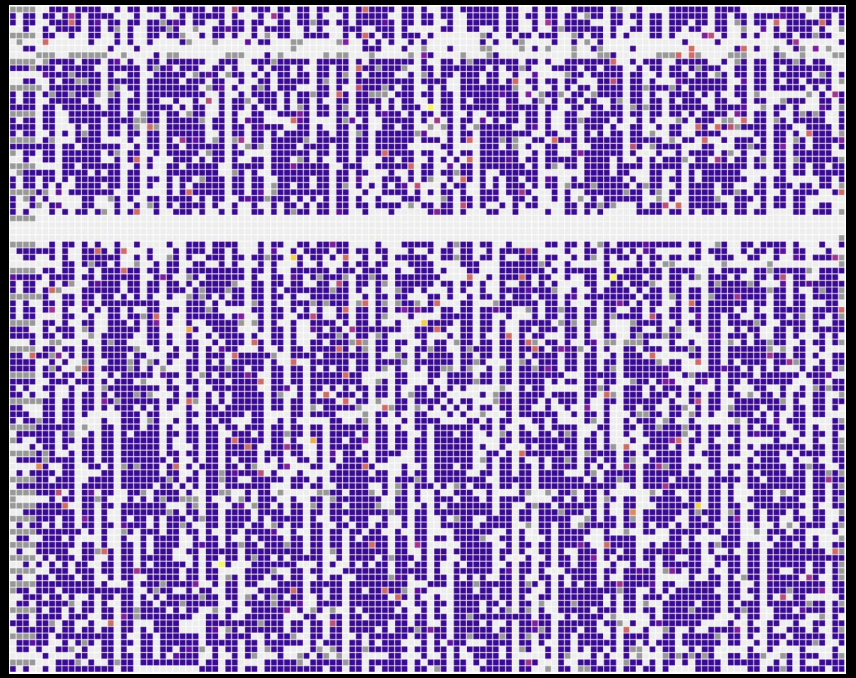


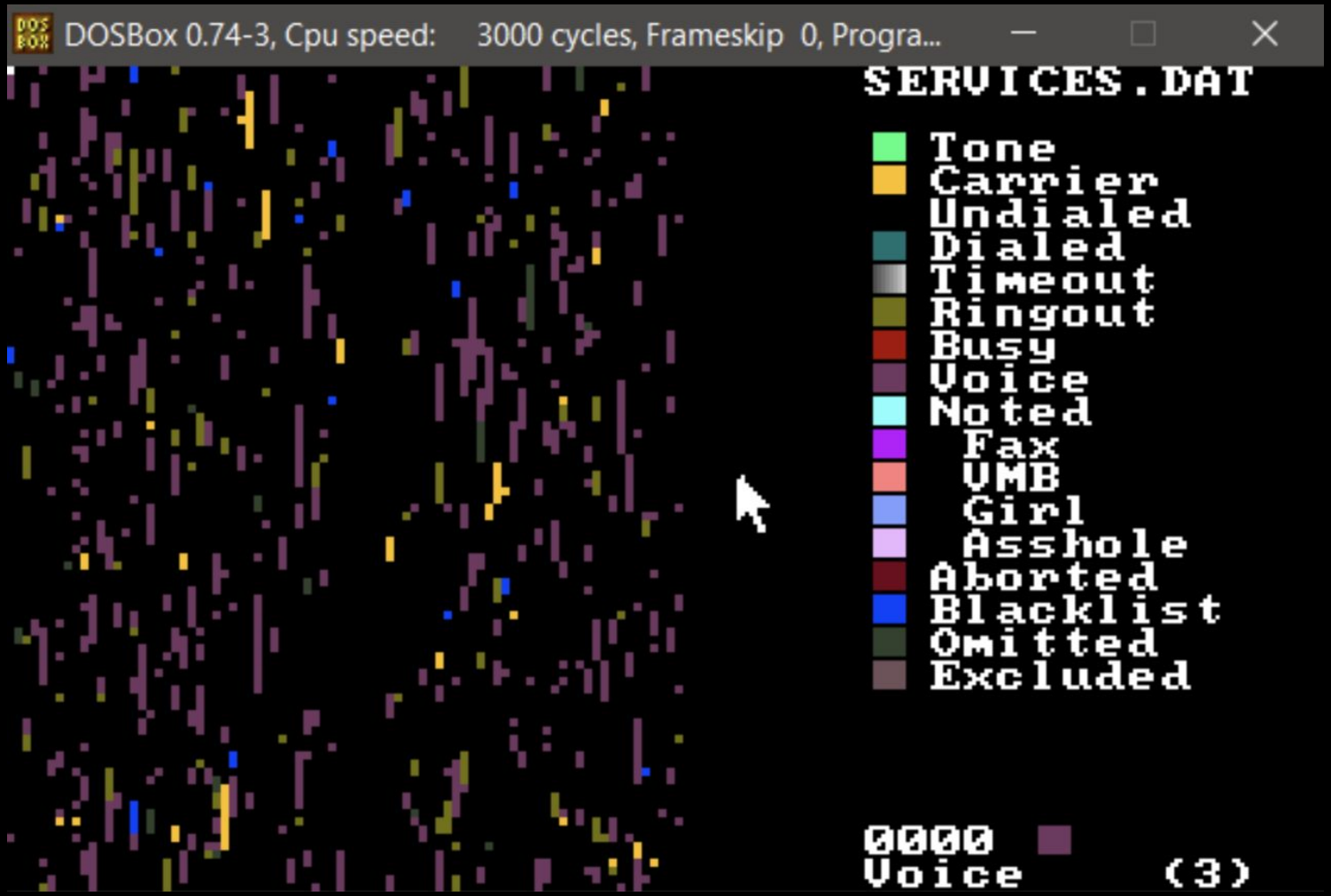
- Pick any routable IPv4 address at random
- 21% chance of it already being in Shodan
- 17%-ish chance of it being actively live



https://hdm.io/decks/2013_AusCERT.pdf



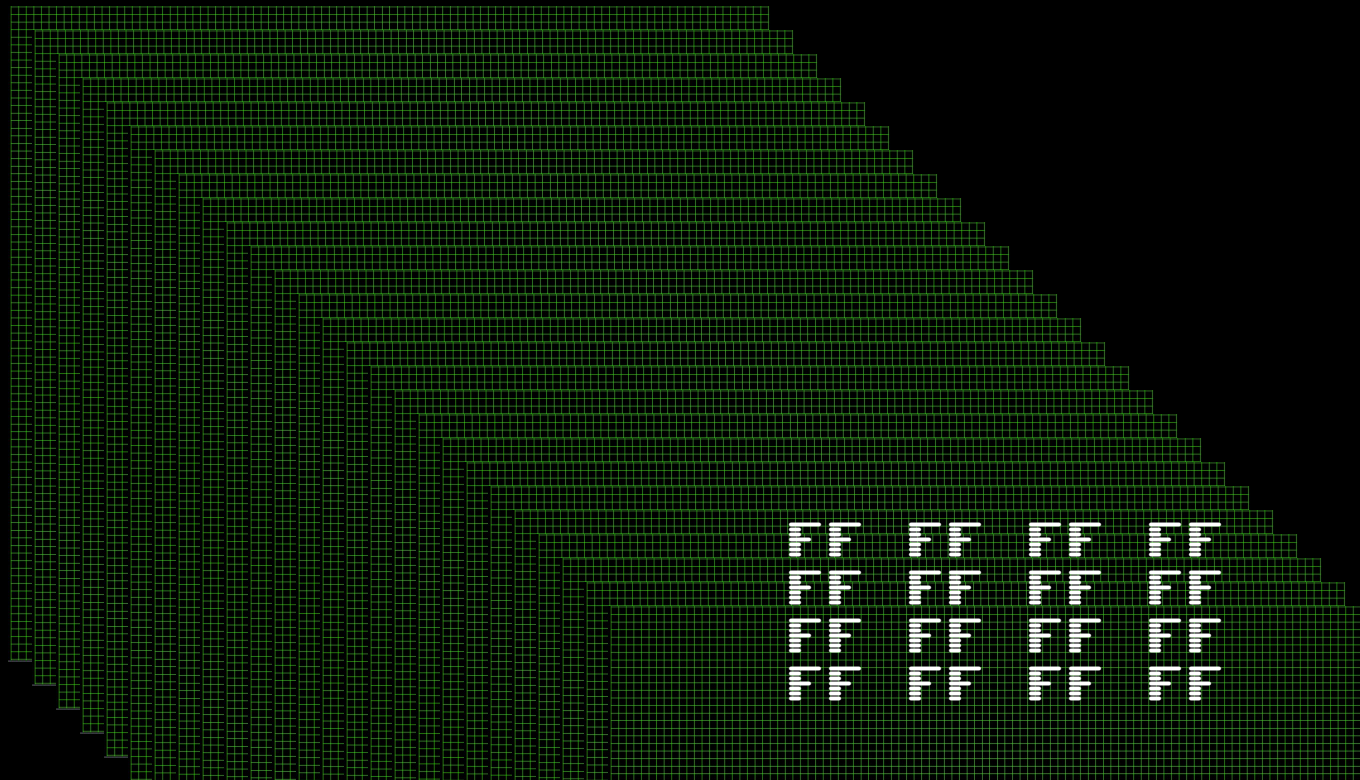




https://www.runzero.com/blog/subnet-grid-report/

IPv6

00 00 00 00
00 00 00 00
00 00 00 00
00 00 00 00



IPv6

- Sequential scanning is out of the question
- Use directory services (DNS, Certificate Transparency)
- Use client-side address leaks (NTP)
- Use tools, algorithms, public data
  - IPv666
  - IPv6 Hitlist

SHODAN | Explore | Downloads | Pricing | has_ipv6:true

TOTAL RESULTS

223,971,940

TOP COUNTRIES

India	138,928,504
Brazil	54,698,626
United States	22,465,870
Russian Federation	1,910,887
China	1,751,238

More...

View Report | Download Results | Historical Trend | View on Map

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using

2a02:e980:d::f2bc

Incapsula Inc.

United States, San Mateo

cdn

```
HTTP/1.1 400 Bad Request
Content-Type: text/html
Cache-Control: no-cache, no-store
Connection: close
Content-Length: 701
X-Iinfo: 12-35513939-0 0NNN RT(1728168860947 118) q

<html style="height:100%"><head><META NAME="ROBOTS"
```

2a02:e980:d::a3aa

Incapsula Inc.

United States, San Mateo

cdn

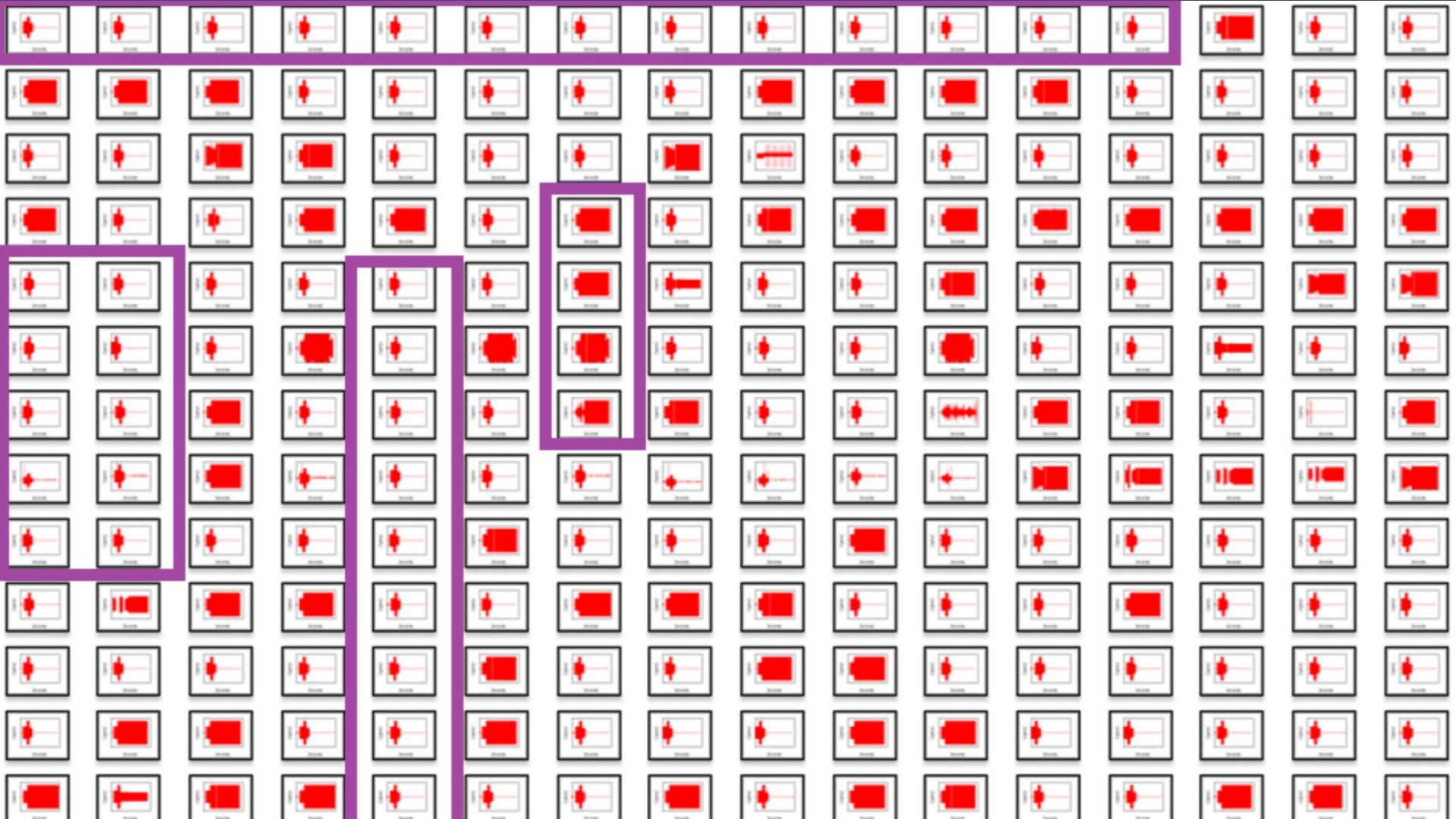
```
HTTP/1.1 400 Bad Request
Content-Type: text/html
Cache-Control: no-cache, no-store
Connection: close
Content-Length: 703
X-Iinfo: 10-20469350-0 0NNN RT(1728168862114 47) q(
```


https://www.shodan.io/search?query=has_ipv6%3Atrue

Wardial ++

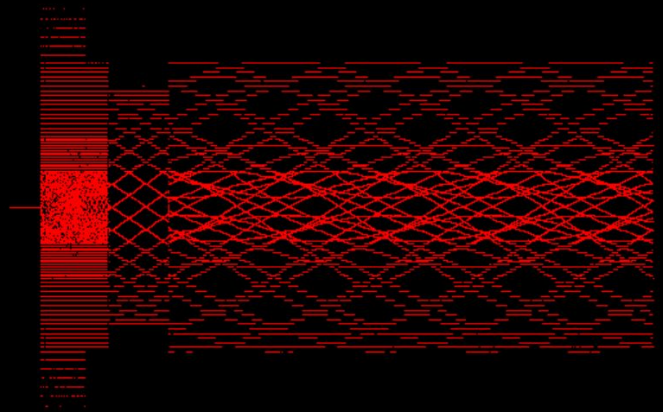
- WarVOX: Use cheap VoIP providers for blazing fast dialing
- Skip the modem and do direct audio analysis
- Detect modems via frequency analysis
- Create& group audio signatures
- Beats a Softmodem*
- Mostly illegal* now :(

* TCPA - https://en.wikipedia.org/wiki/Wardialing

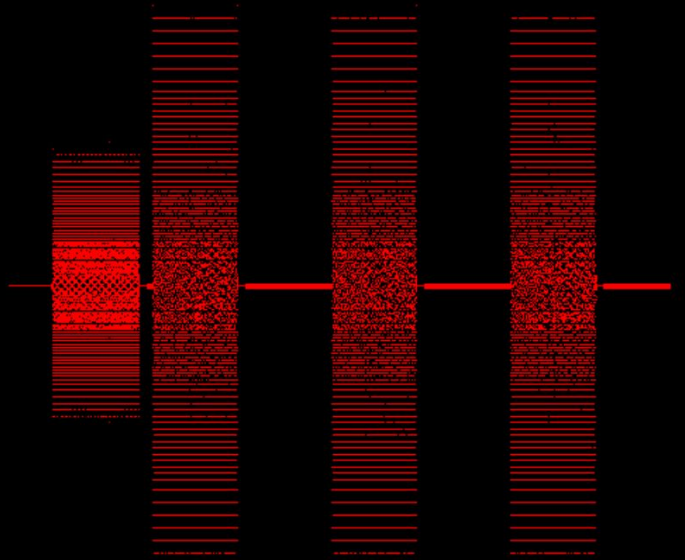


MODEM

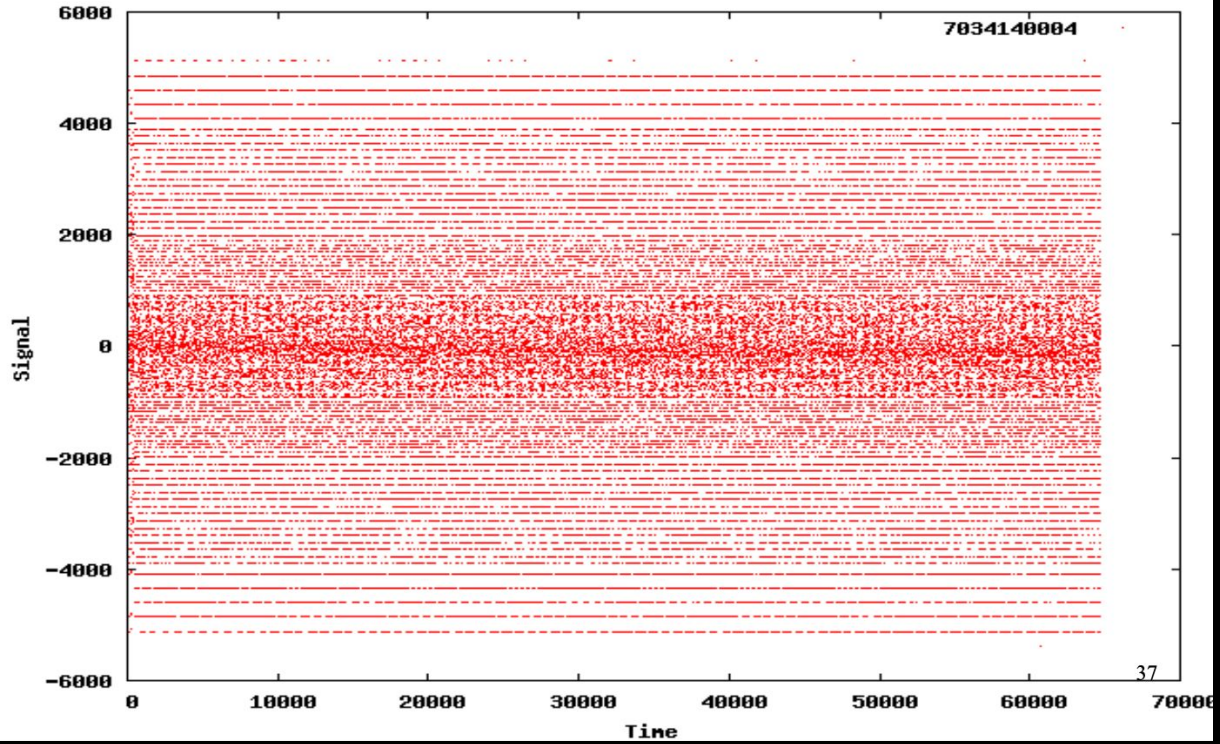
2150 Hz (carrier)

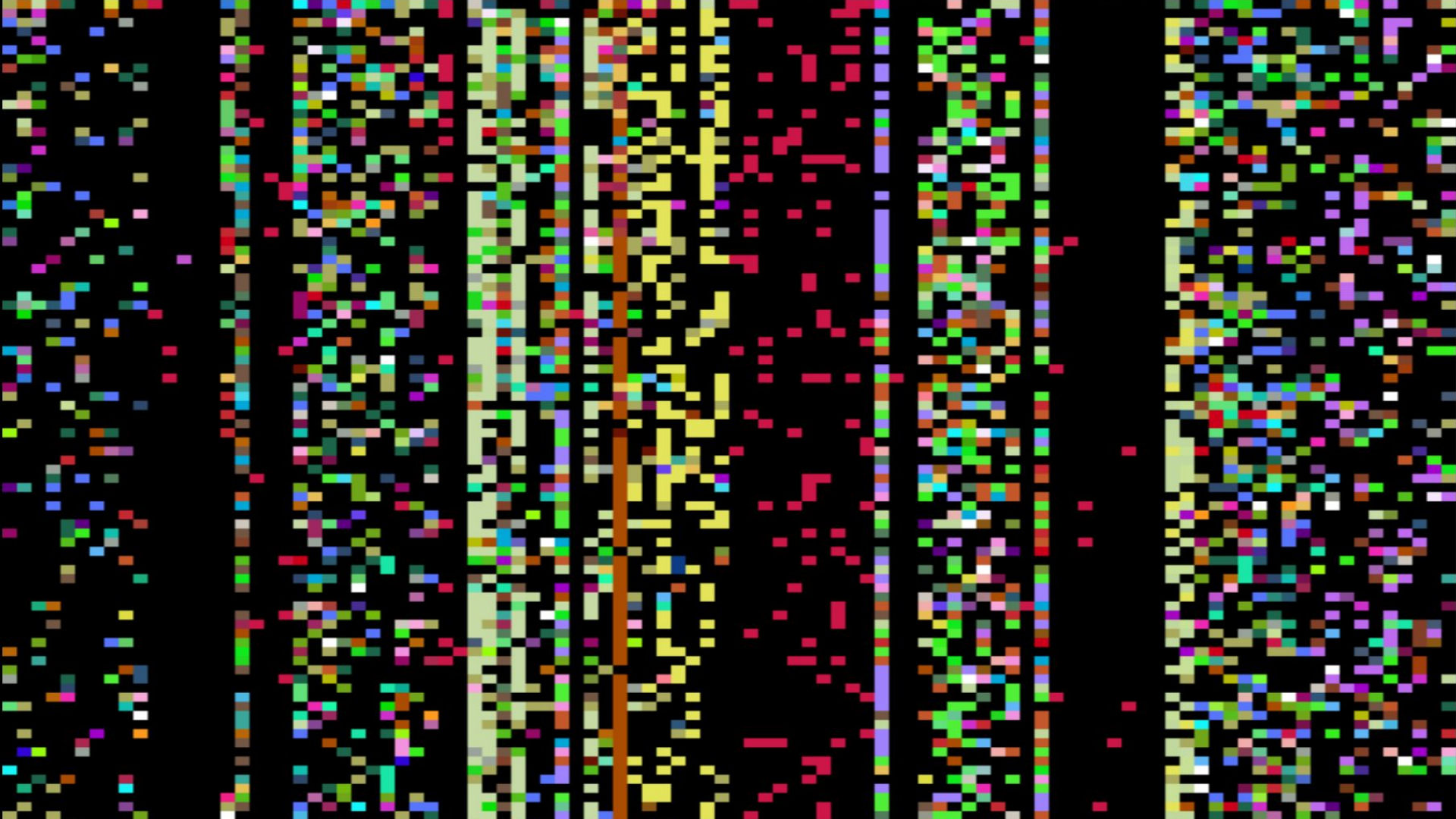


FAX



WarVOX (350hz + 440hz)





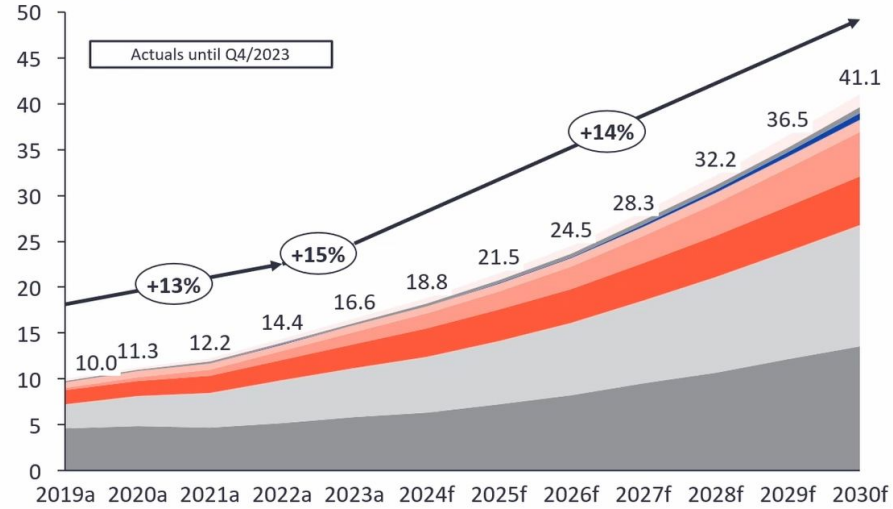
IOT ANALYTICS

September 2024

Your Global IoT Market Research Partner

Global IoT market forecast (in billions of connected IoT devices)

Number of global active IoT connections (installed base) in billions



Connectivity type	CAGR 21–23	CAGR 23–30
Other	21%	17%
Wireless neighborhood area networks (WNAN)	15%	14%
Cellular 5G IoT	147%	62%
Wired IoT	4%	9%
LPWA	35%	21%
Cellular IoT (excl. 5G, LPWA)	21%	11%
Wireless local area networks (WLAN)	18%	14%
Wireless personal area networks (WPAN)	12%	13%

XX% = CAGR

Note: IoT connections do not include any computers, laptops, fixed phones, cellphones, or consumers tablets. Counted are active nodes/devices or gateways that concentrate the end-sensors, not every sensor/actuator. Simple one-directional communications technology not considered (e.g., RFID, NFC). Wired includes ethernet and fieldbuses (e.g., connected industrial PLCs or I/O modules); Cellular includes 2G, 3G, 4G, 5G; LPWA includes unlicensed and licensed low-power networks; WPAN includes Bluetooth, Zigbee, Z-Wave or similar; WLAN includes Wi-Fi and related protocols; WNAN includes non-short-range mesh, such as Wi-SUN; Other includes satellite and unclassified proprietary networks with any range.

Source: IoT Analytics Research 2024-State of IoT Summer 2024. We welcome resharing: Please attribute this image to its original source and include a link back to the original article.

https://iot-analytics.com/number-connected-iot-devices/

NATCarrier

- 18 billion of IoT alone in 2024, but where are they?
- Mostly internal & carrier NAT segments!
- Even excluding the ~7b of BT/PAN
- The multi-verse of IP space
- How is it used?

1. https://github.com/atredispartners/dht-crawler-polkadot

IPv4: Top 20

- 192.168.1.0
- 192.168.0.0
- 10.179.64.0
- 10.179.0.0
- 10.0.0.0
- 100.93.129.0
- 10.164.166.0
- 172.20.16.0
- 172.20.8.0
- 10.164.185.0
- 192.168.86.0
- 100.93.130.0
- 172.18.0.0
- 172.19.0.0
- 100.93.132.0
- 172.20.10.0
- 192.168.68.0
- 100.93.128.0
- 100.93.133.0
- 192.168.2.0

IPv4: Top 16

- 1
- 2
- 3
- 0
- 255
- 21
- 20
- 41
- 30
- 65

P2P/IPFS/Web3

- DHTs (KAD) and similar (Discv5) make peer enumeration trivial
- IPFS/Torrents are obvious, but also applies to Web3[1]
- Ironic that decentralization is worse for privacy
  - MultiAddresses often expose secondary IPs!
  - Fun DoS tricks...

1. https://github.com/atredispartners/dht-crawler-polkadot

Wrapping up...

- Anything is a network if you look at it the right way
- Same approach works almost everywhere
- Costs are no longer the main barrier
- Discover all the things!

Thank you!

x@hdm.io