LASCON

runZero

Hacker Numerology

HD Moore

LASCON OCTOBER 27, 2024 AUSTIN, TX

bell¿ngcat

This presentation is dedicated to Bellingcat, who hold authorities accountable for human rights abuses, world-world, at extreme personal risk, through open source research.

https://Bellingcat.com/

Now serving…

- You receive ticket number 74
- What does this tell you?
- Now serving number 82
- Now serving number 85
- Now serving number 67

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

Every thing has an identifier

- Credit cards
- Documents
- Babies
- Patents
- Cables
- Passports
- Phones
- Cars
- Pets
- Receipts
- Web requests
- PINs

> “ Now serving customer 1729880287601 ...

Most identifiers are short

- Entering long numbers is a hassle and error-prone
- The result is that identifiers are *dense*
- Information is encoded everywhere

Ex: Social security numbers

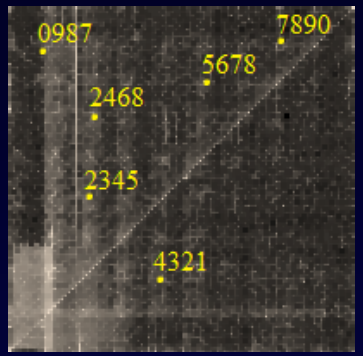
- The first set of three digits is called the Area Number
- The second set of two digits is called the Group Number
- The final set of four digits is the Serial Number

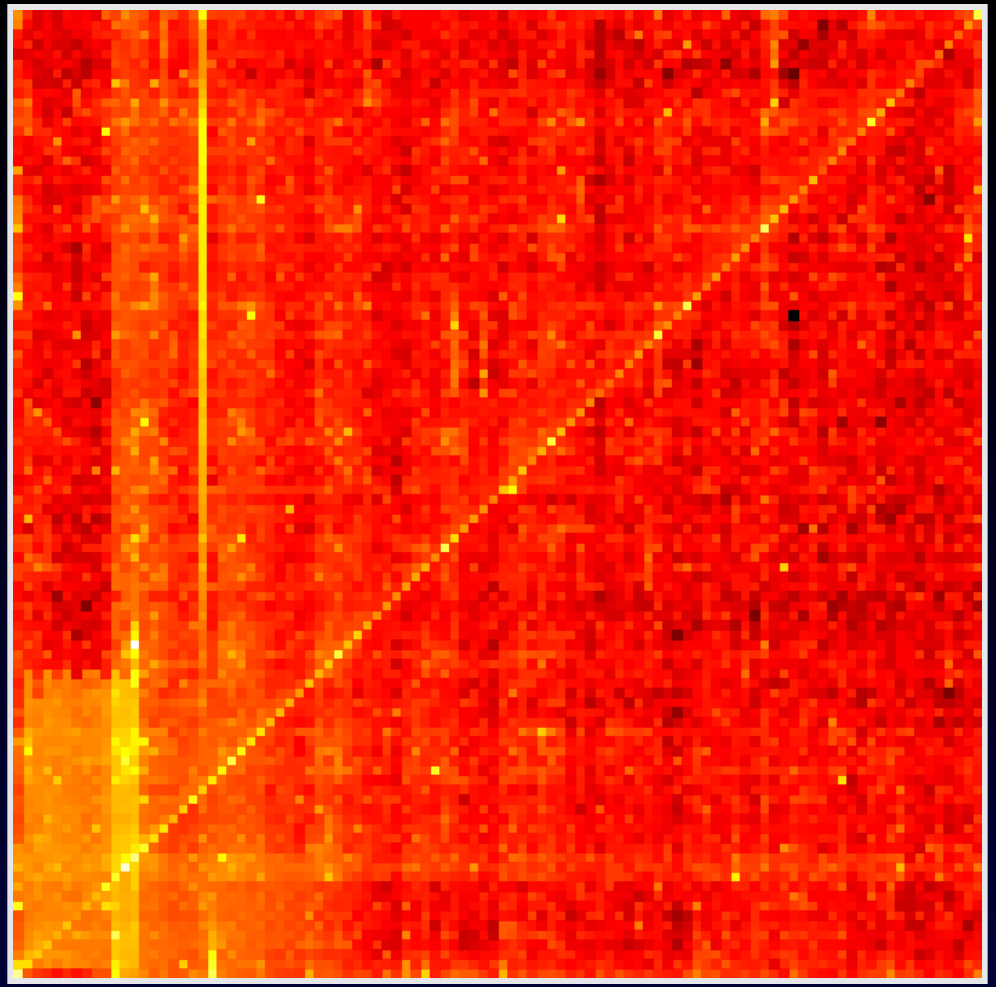
https://www.ssa.gov/employer/ssnvhighgroup.htm

PINs

- User-chosen IDs are the worst
- Short and predictable

Statistically, one third of all codes can be guessed by trying just 61 distinct combinations!





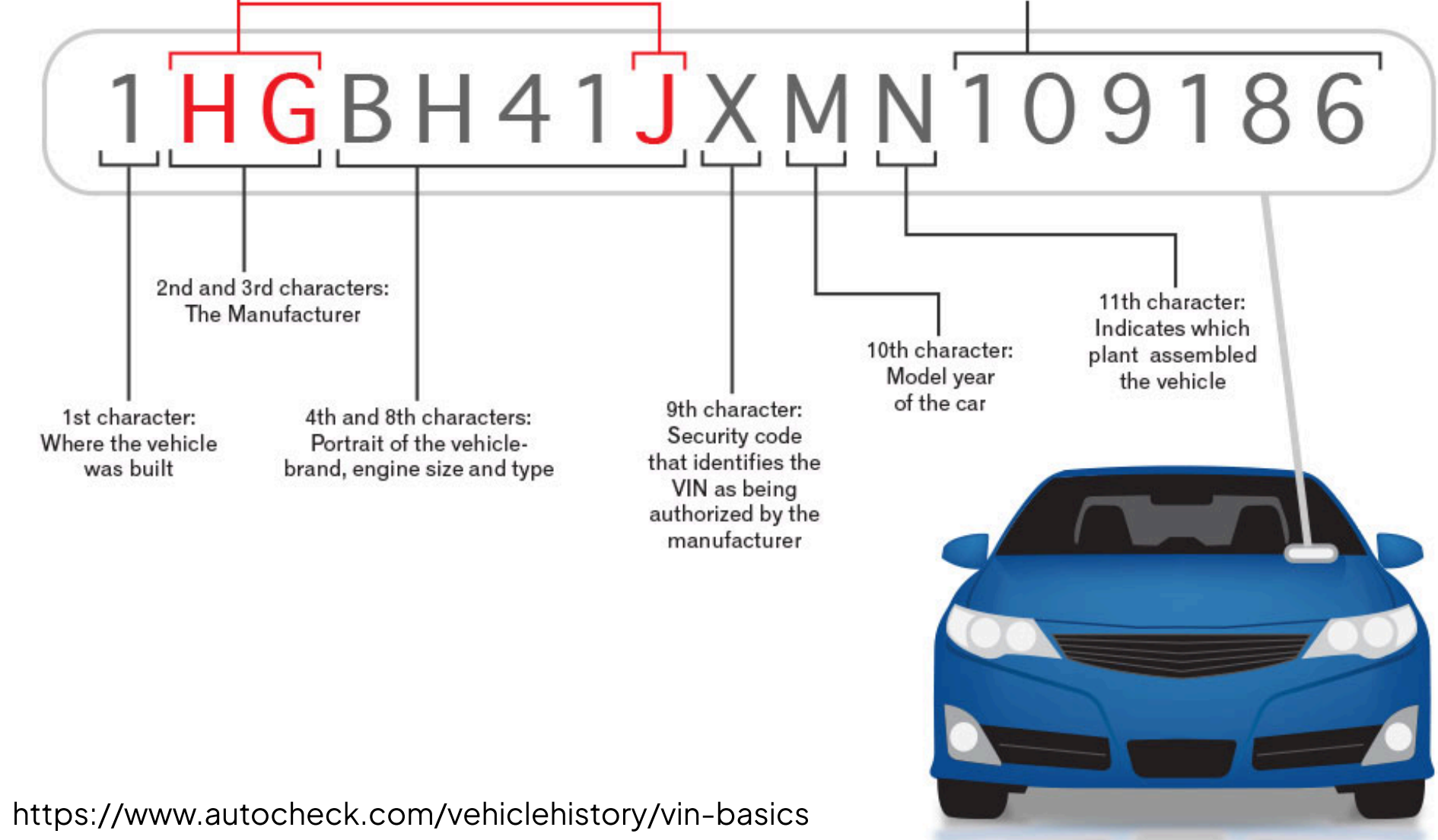
http://www.datagenetics.com/blog/september32012/

Every identifier is also a number

- Dell service tags are in the form of HGJSQY1
- This is a Base36 (0–9A-Za-z) encoded decimal number
- This converts to Express ID 380–060–125–21
- Flatten this to decimal 38,006,012,521

Identifiers often include categories, sequence numbers, and checksums

Vehicle Identification Numbers are a great example



https://www.autocheck.com/vehiclehistory/vin-basics

Identifiers are information-rich

- IDs often tell us the location, time of creation and rate of change
- IDs often represent real-world system limitations
- Even a small sample set can define the range
- Why does this matter?

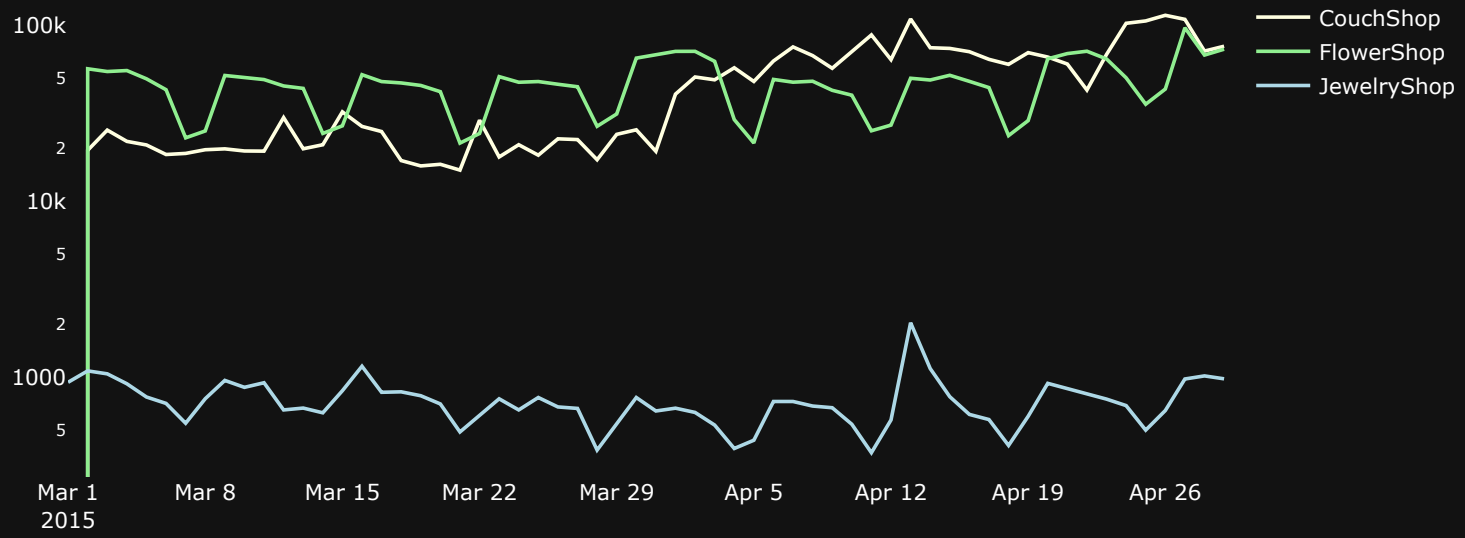
Missing ACLs are not just for the web

- Insecure Direct Object References (IDOR), everywhere!
- ID discovery enables data leaks and abuse

runZero

Business intelligence

- Even minor leaks expose granular data over time
- Oracle Commerce (ATG) DYN_USER_ID cookies



Application defense

- Understanding identifiers is critical to security
- Sequential? Predictable? Encoded?

Not always obvious...

- `ba209999-0c6c-11d2-97cf-00c04f8eea45`
- `1998-06-25 20:40:26.586562.5 UTC`
- `MAC Address 00:c0:4f:8e:ea:45`
- `UUID v1 (Dell Desktop)`

Identifier Discovery

Discovery process

1. A sample identifier to seed discovery
2. An action to resolve an ID to attributes
3. A system to record the results
4. A method to correlate attributes

Telephone networks

1. A sample identifier to seed discovery

   555-454-9600

2. An action to resolve an ID to attributes

   Call the number and record the response

3. A system to record the results

   A notebook

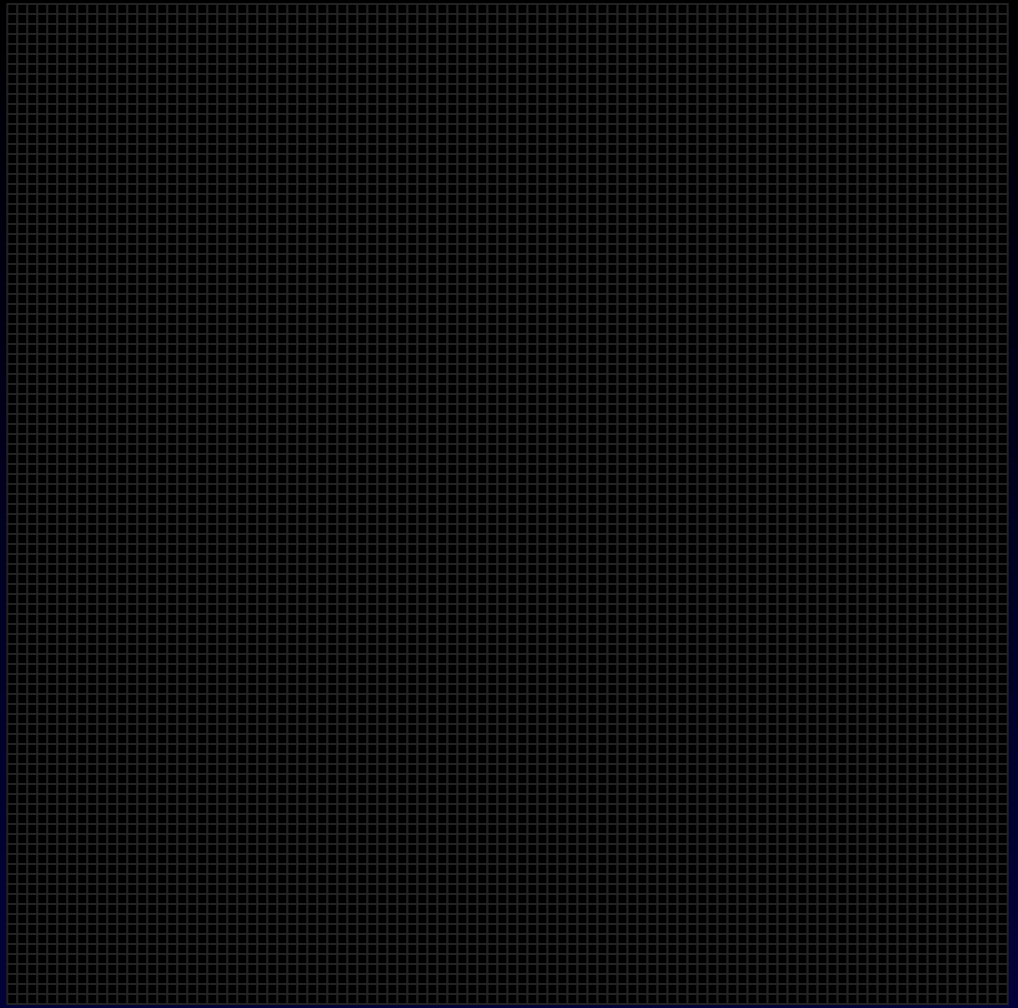
4. A method to correlate attributes

   Link numbers with similar attributes


Hayes
FOR USE WITH HAYES
UNITS MARKED 8.5 VAC
SMARTMODEM 2400
Hayes
HS
AA
CD
OH
RD
SD
TR
MR

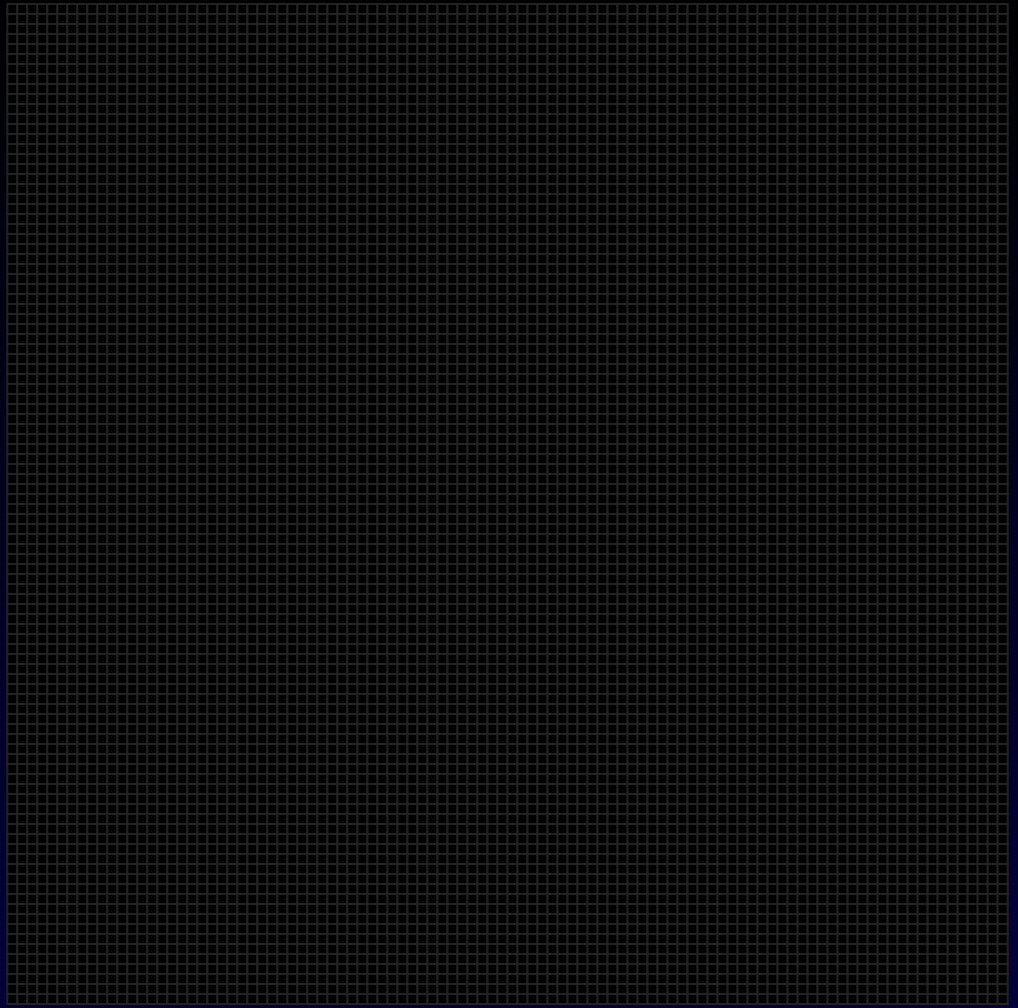
555-454-XXXX

- 10,000 numbers to a block



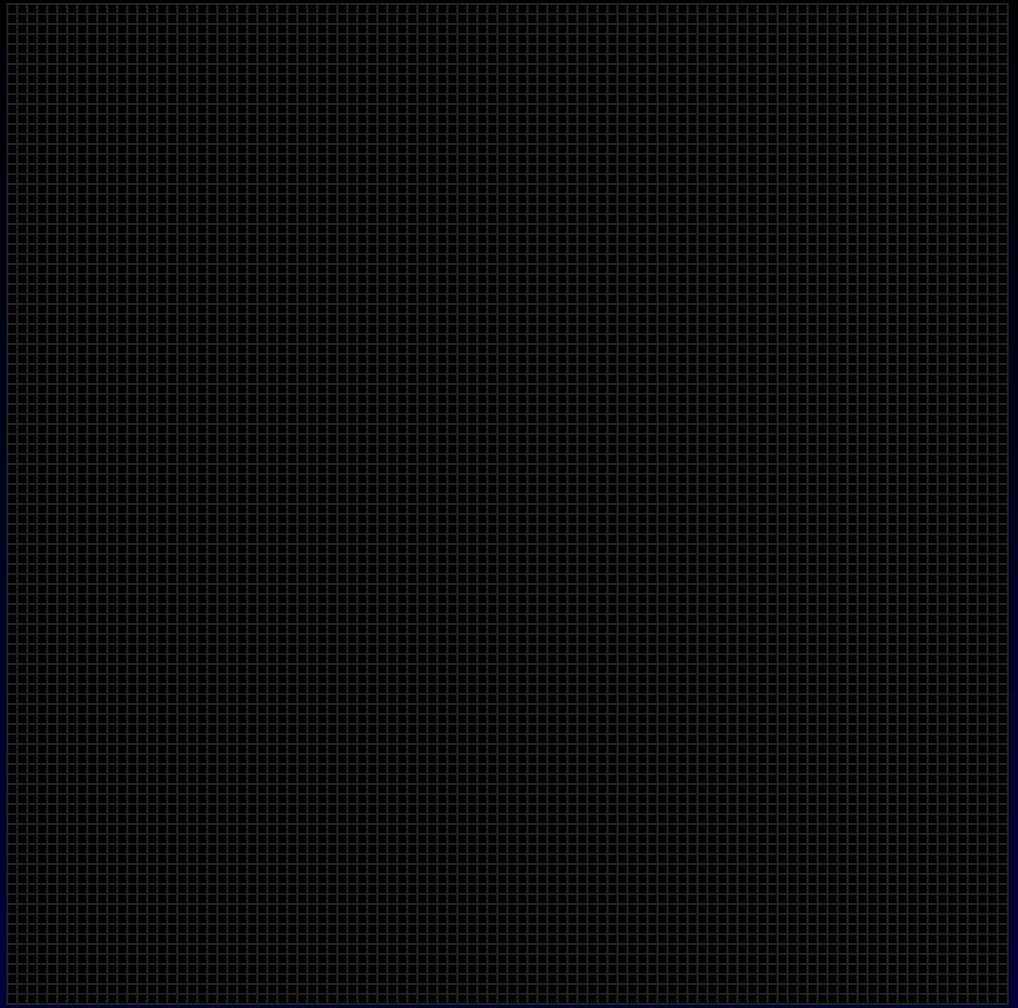
555-454-XXXX

- 10,000 numbers to a block
- Each call takes 30 seconds



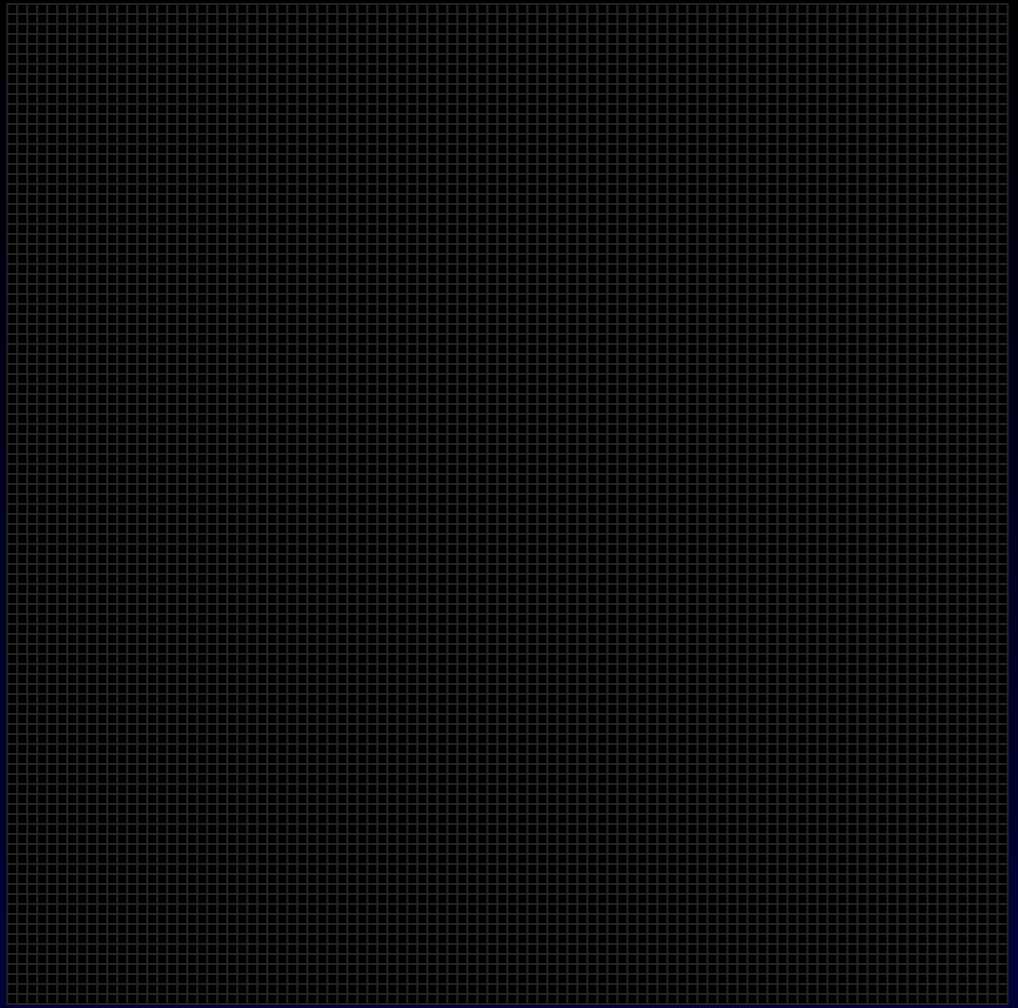
555-454-XXXX

- 10,000 numbers to a block
- Each call takes 30 seconds
- 83 hours to dial every line



555-454-XXXX

- 10,000 numbers to a block
- Each call takes 30 seconds
- 83 hours to dial every line
- Patterns appear quickly



Discovery process (IPv4)

1. A sample identifier to seed discovery

   192.168.0.5

2. An action to resolve an ID to attributes

   Scan the address for services and fingerprints

3. A system to record the results

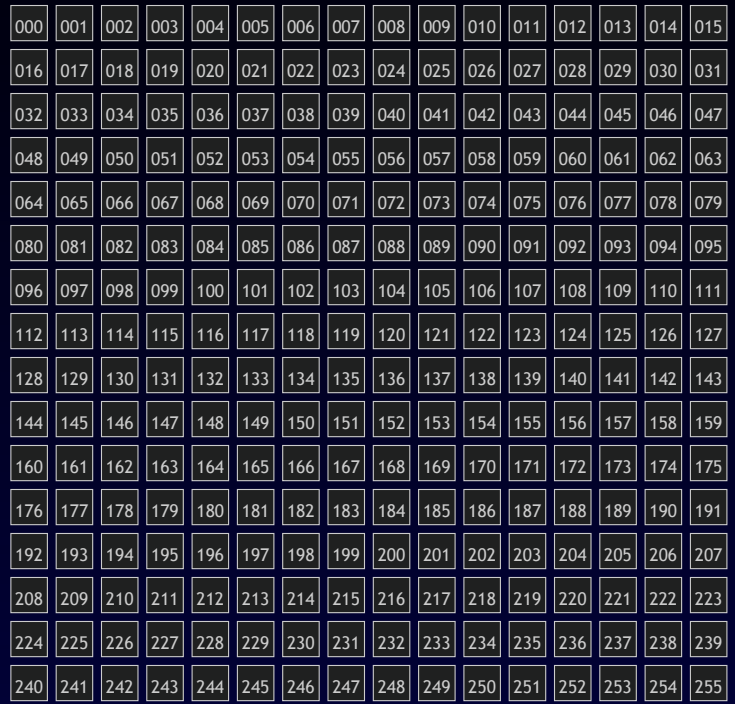
   A markdown file

4. A method to correlate attributes

   Color addresses based on fingerprint

192.168.0.0/24

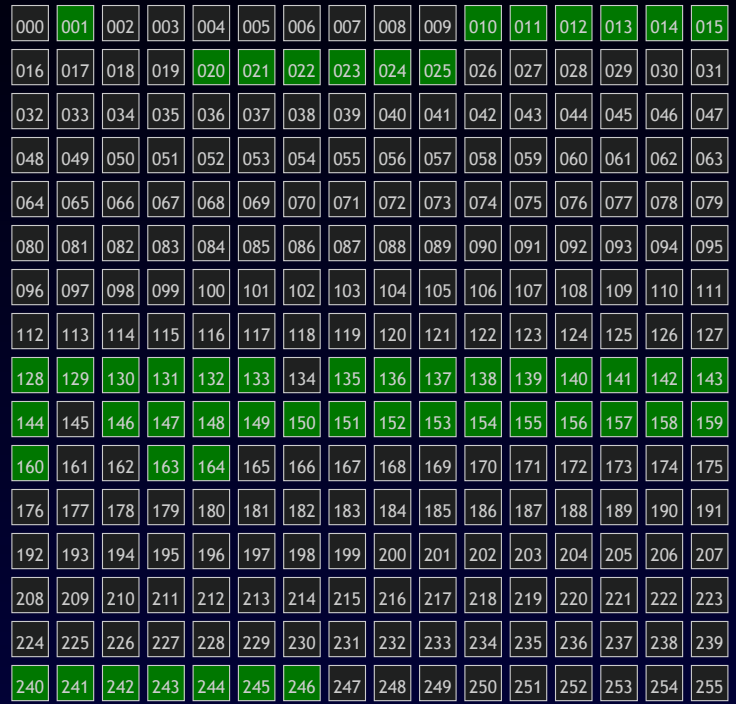
- 256 numbers to a block



runZero

192.168.0.0/24

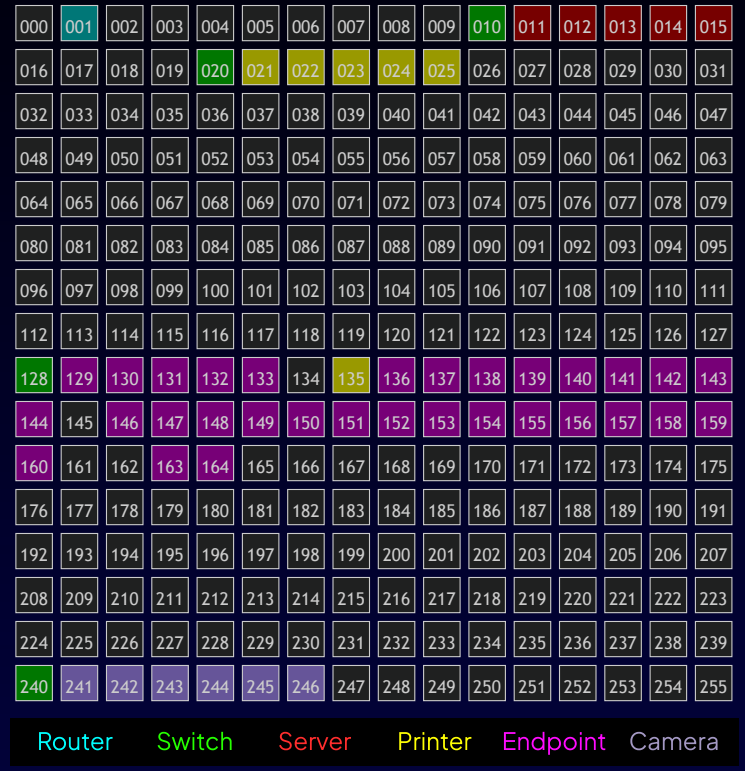
- 256 numbers to a block
- Each IP takes a few seconds
- A minute or so to scan every IP



runZero

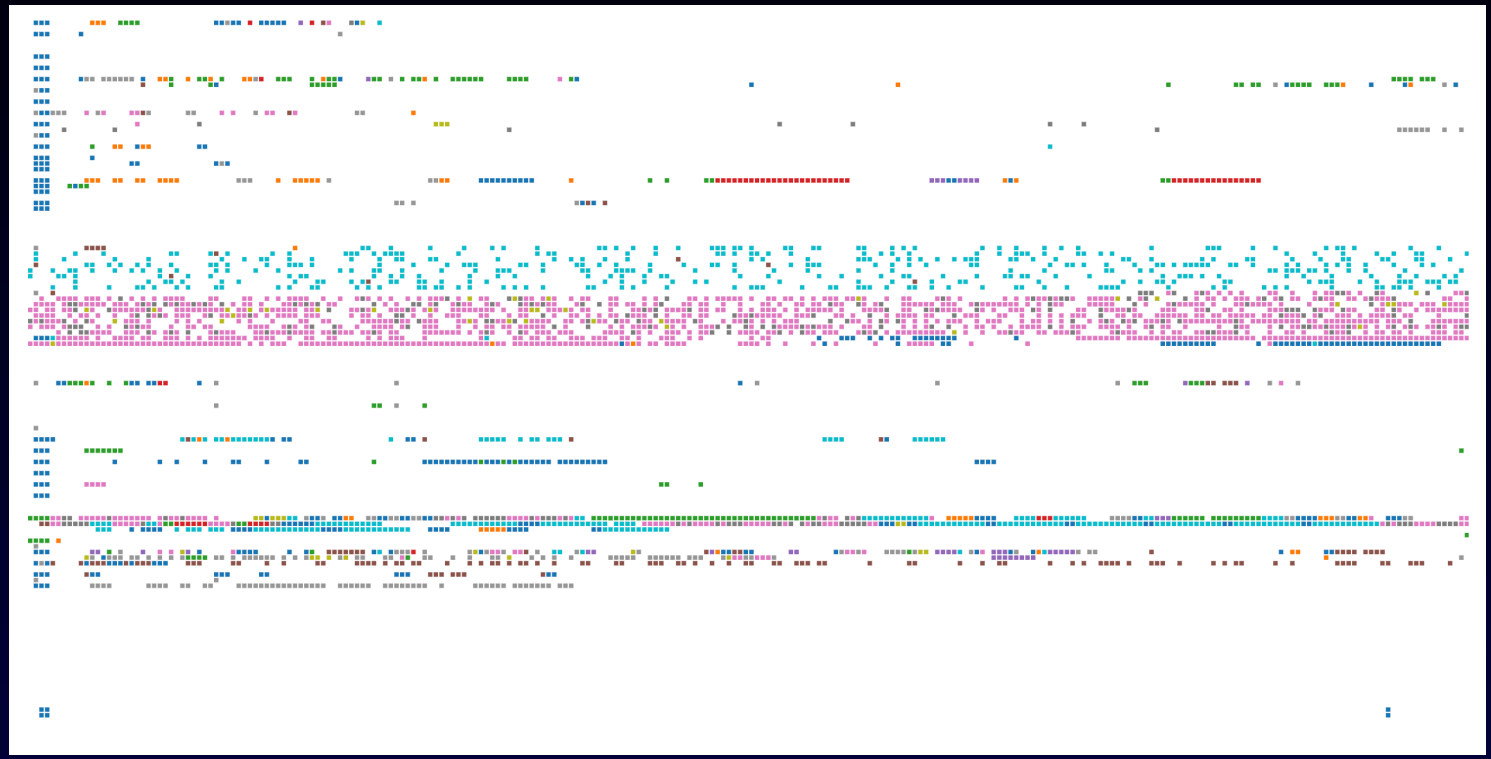
192.168.0.0/24

- 256 numbers to a block
- Each IP takes a few seconds
- A minute or so to scan every IP
- Patterns also appear quickly

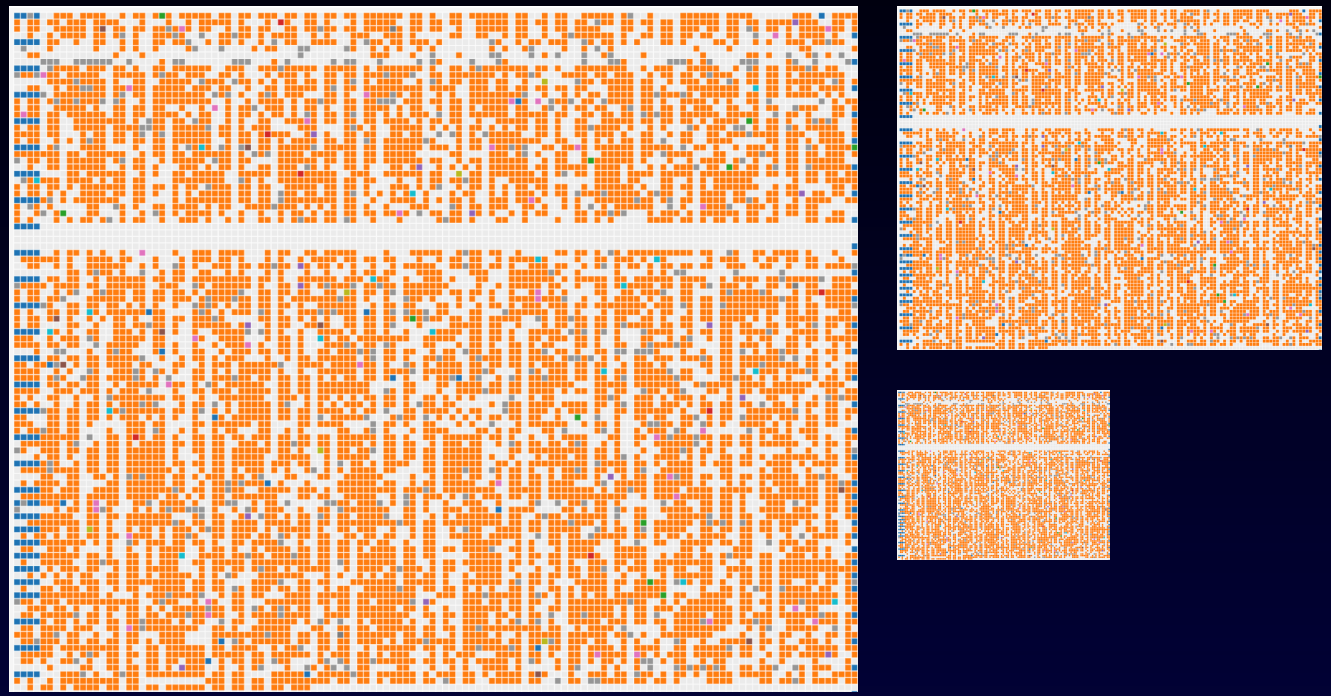


runZero

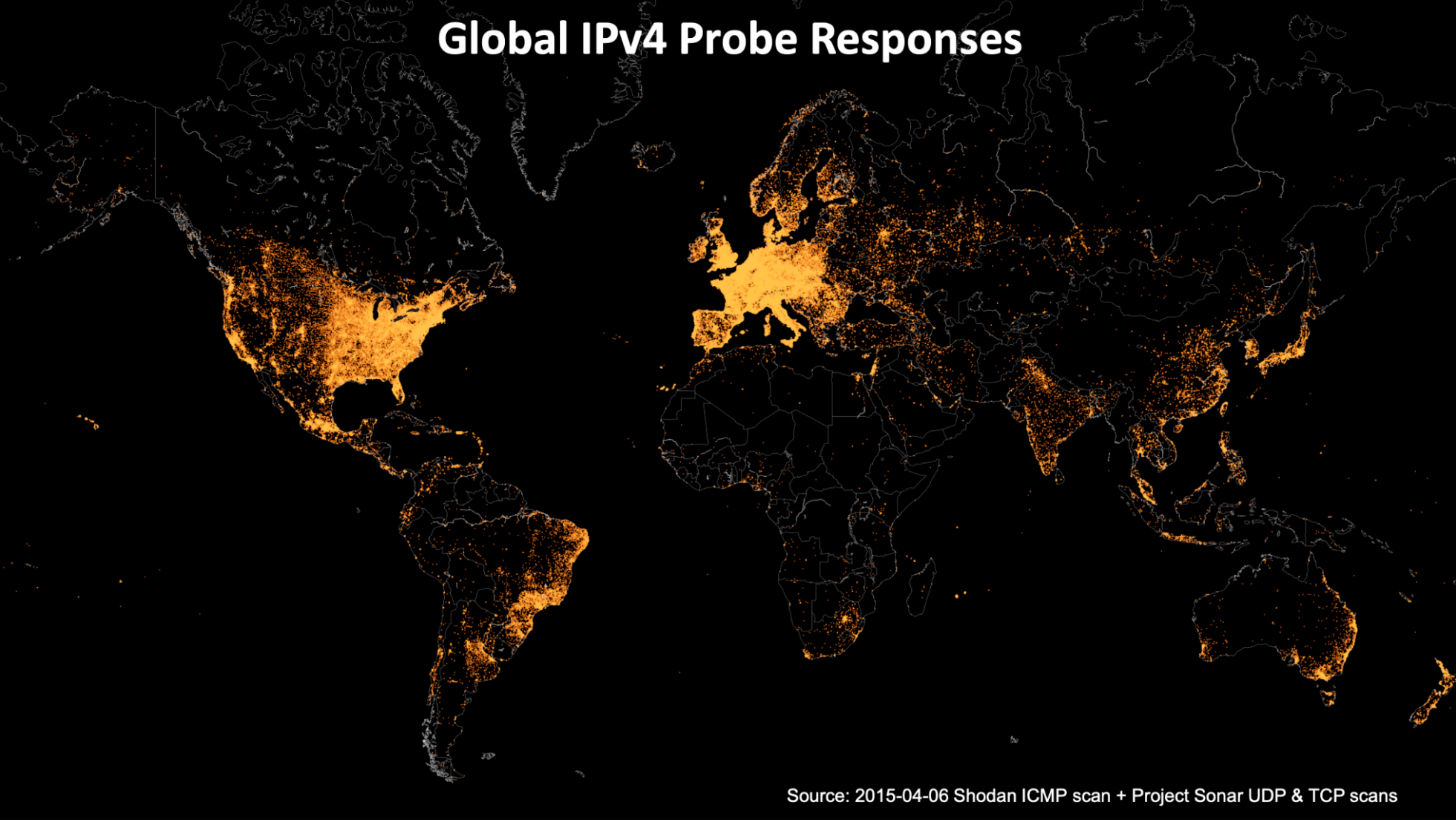
Enterprise internal



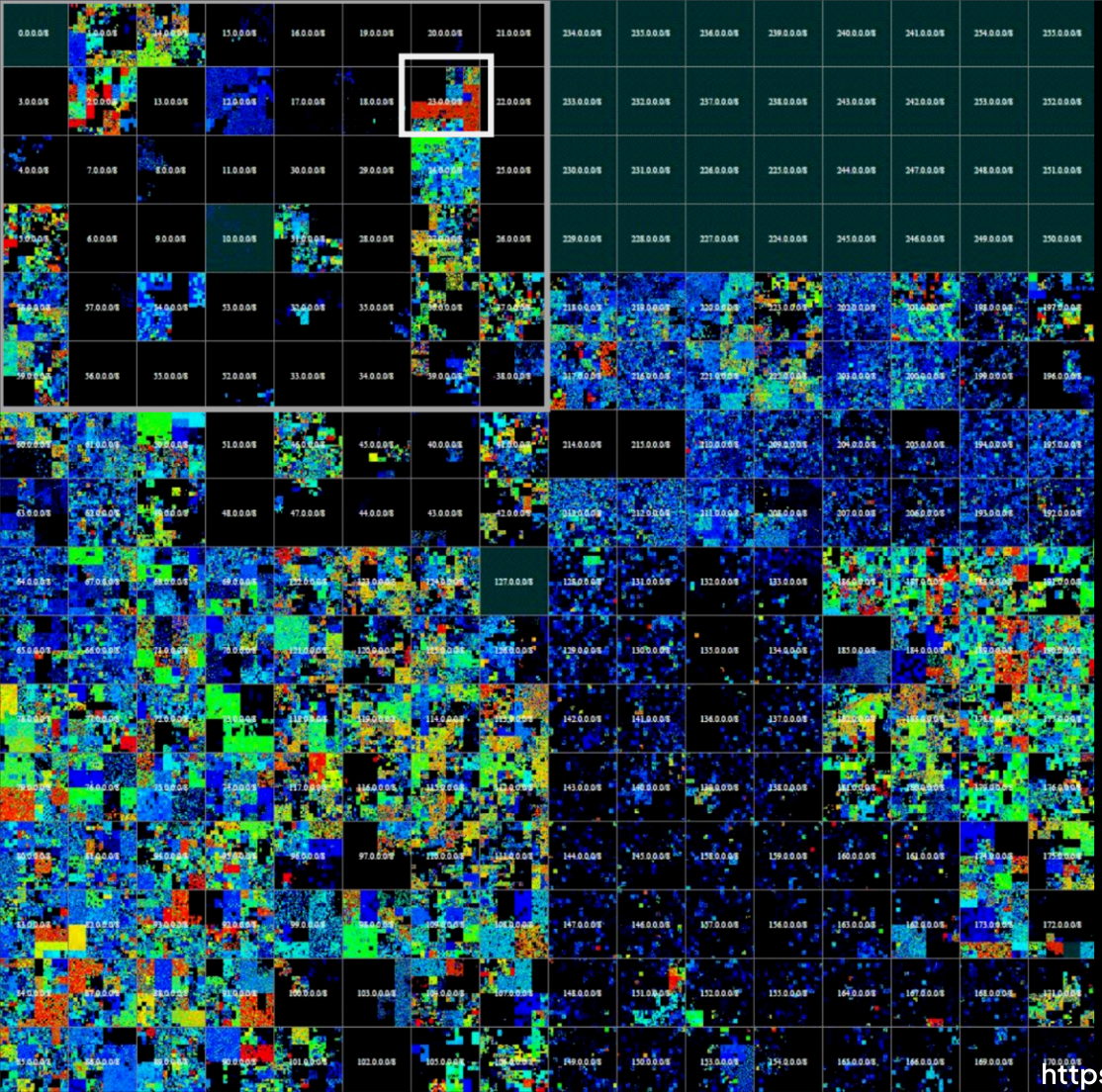
Public IPv4

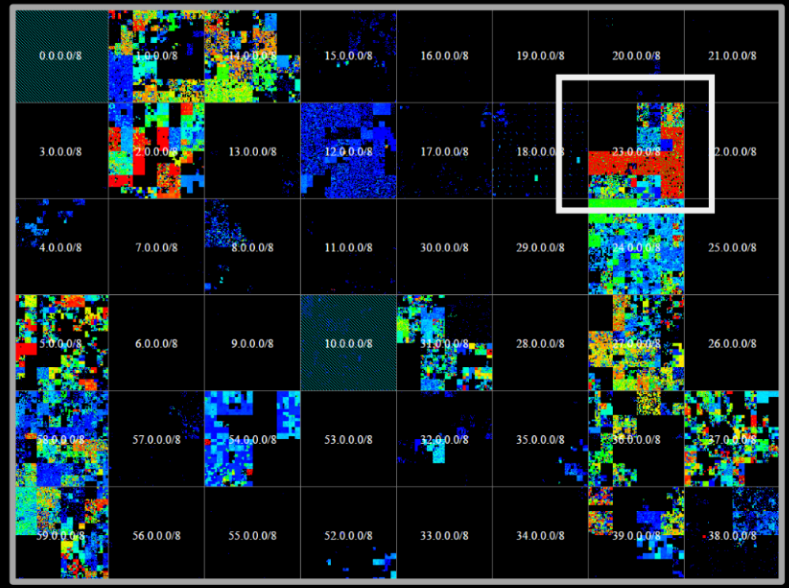


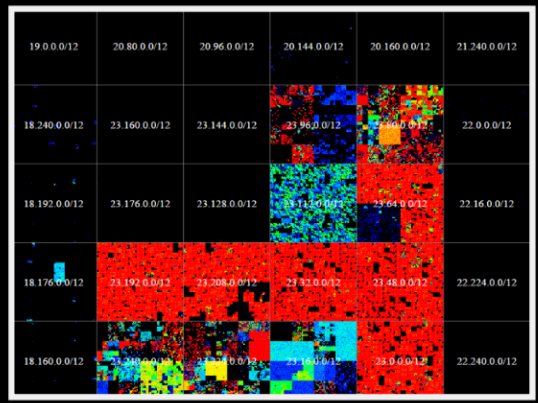
Global IPv4 Probe Responses



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







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

IPv4 is full, go home

3.7b of 4.3b

of IPv4 is routable

774m of 3706m

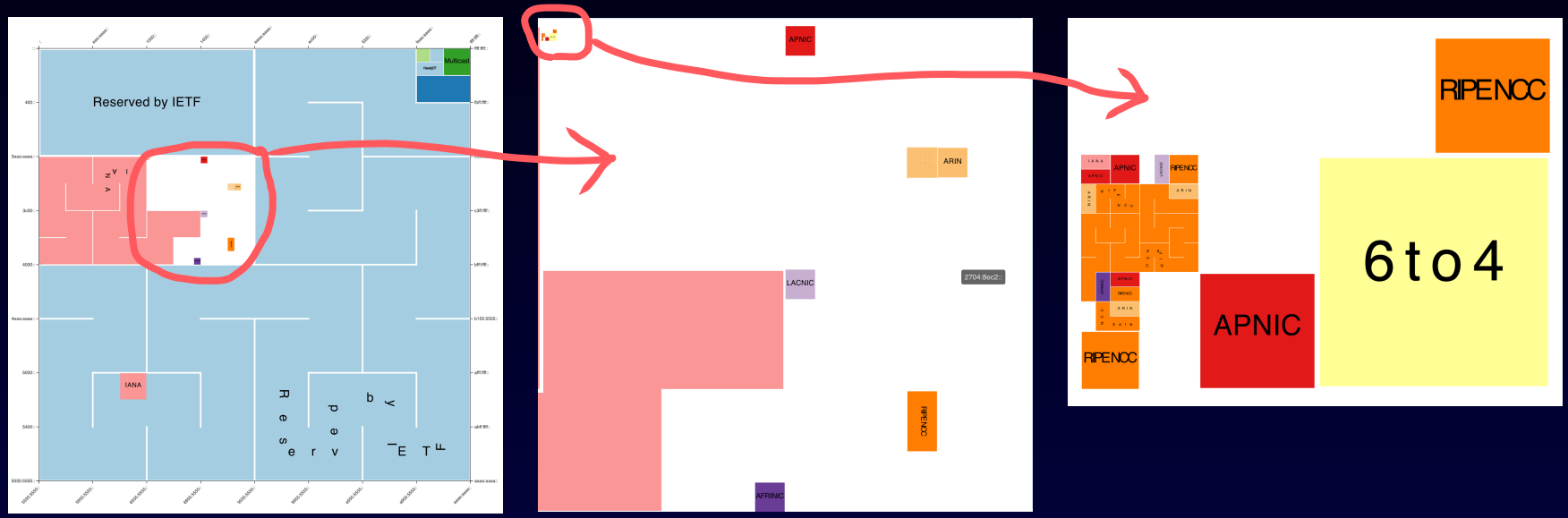
is already in Shodan

17% chance

of any IPv4 being live

IPv6 is the opposite (128 bits)

- Every host gets IPv4 ^ 2 addresses
- Range-based discovery doesn't work



https://observablehq.com/@vasturiano/hilbert-map-of-ipv6-address-space

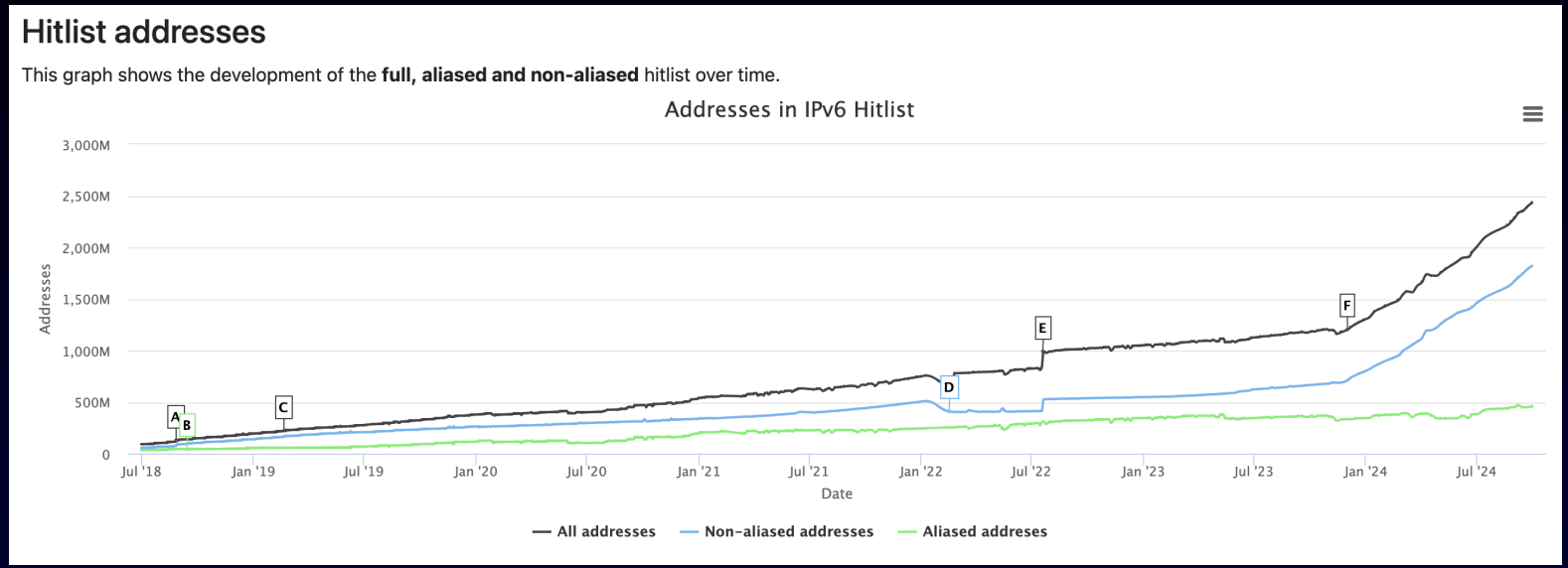
IPv6 link-local

- Local IPv6 discovery is trivial

```
sh-3.2# ping6 ff02::1%en0

PING6(56=40+8+8 bytes) fe80::bd:7caa:2daa:c6b8%en0 ⟶ ff02::1%en0
16 bytes from fe80::bd:7caa:2daa:c6b8%en0, icmp_seq=0 hlim=64 time=6.111 ms
16 bytes from fe80::f6e2:c6ff:fea8:ca34%en0, icmp_seq=0 hlim=64 time=12.431 ms
16 bytes from fe80::76ac:b9ff:fe5b:eca4%en0, icmp_seq=0 hlim=64 time=16.818 ms
16 bytes from fe80::f690:eaff:fe00:823f%en0, icmp_seq=0 hlim=64 time=20.237 ms
16 bytes from fe80::1c5a:a22:eac6:bf31%en0, icmp_seq=0 hlim=64 time=22.755 ms
16 bytes from fe80::d217:69ff:feb0:cf03%en0, icmp_seq=0 hlim=64 time=112.749 ms
16 bytes from fe80::eac7:4fff:fe04:c4ea%en0, icmp_seq=0 hlim=64 time=211.174 ms
16 bytes from fe80::fa0f:f9ff:fe87:b909%en0, icmp_seq=0 hlim=64 time=212.109 ms
16 bytes from fe80::5660:9ff:fe9e:f9ea%en0, icmp_seq=0 hlim=64 time=217.347 ms
16 bytes from fe80::1042:8d8d:771b:3535%en0, icmp_seq=0 hlim=64 time=241.916 ms
16 bytes from fe80::4661:32ff:fe12:494f%en0, icmp_seq=0 hlim=64 time=242.435 ms
16 bytes from fe80::d6f5:47ff:fe21:fc1%en0, icmp_seq=0 hlim=64 time=242.821 ms
16 bytes from fe80::4661:32ff:fe1d:4d79%en0, icmp_seq=0 hlim=64 time=254.185 ms
16 bytes from fe80::10b6:ff9a:de65:8e87%en0, icmp_seq=0 hlim=64 time=263.771 ms
16 bytes from fe80::1c8d:ddec:c48a:5721%en0, icmp_seq=0 hlim=64 time=264.057 ms
```

Public IPv6 is an art

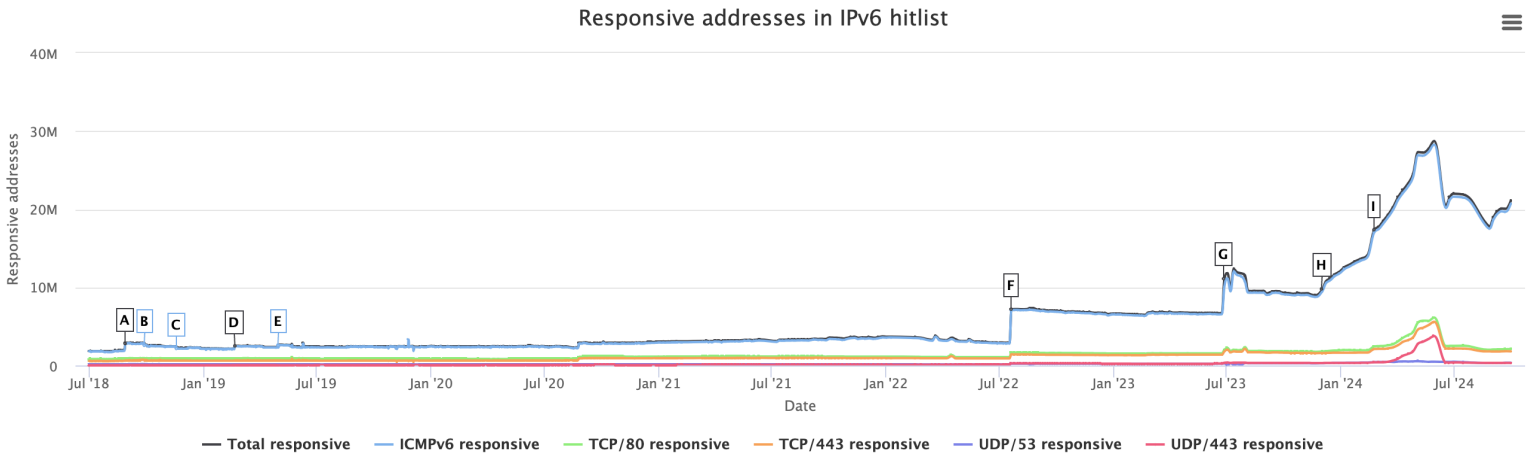


https://ipv6hitlist.github.io/

IPv6 hitlist results

Responsive addresses

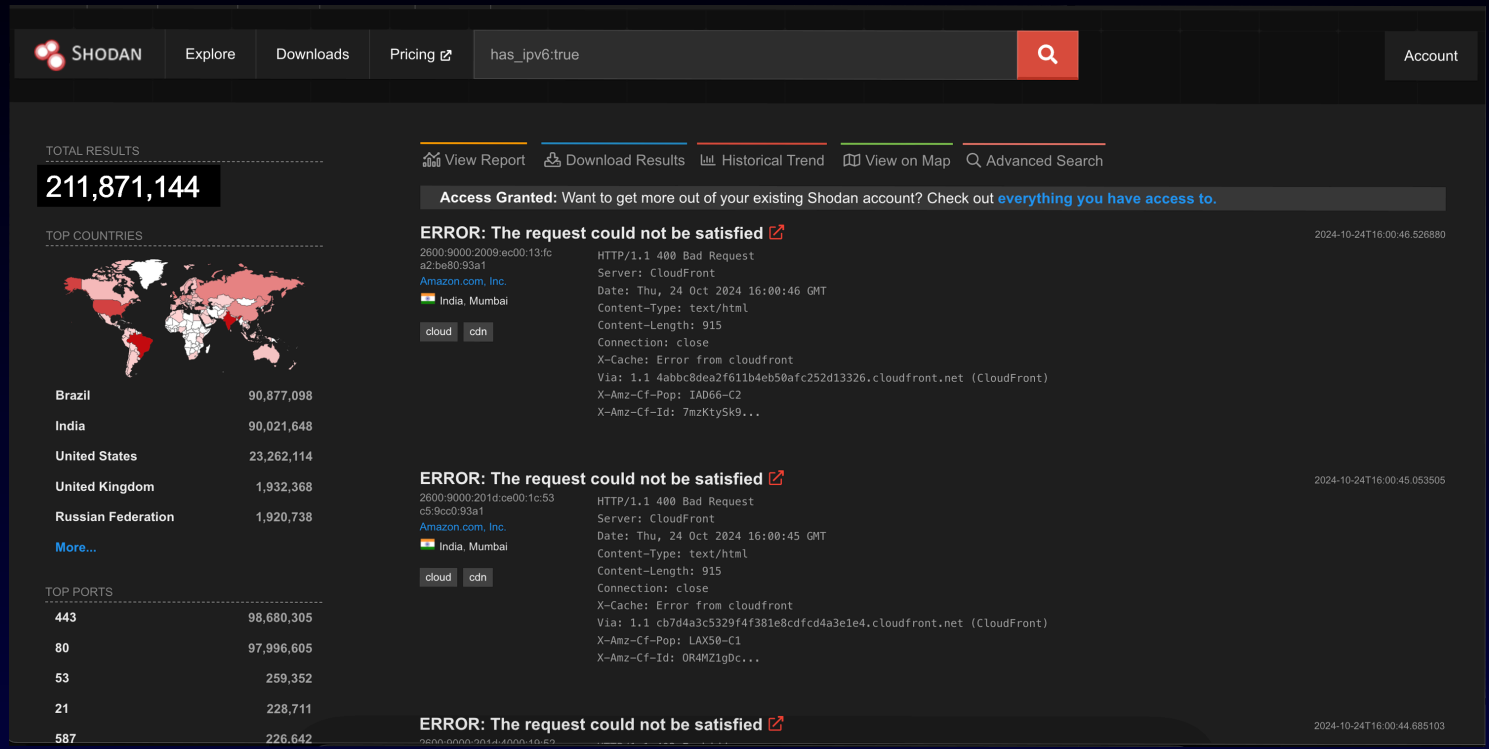
Here, the development of the **different protocol responses** over time is shown. We scan five different protocols, an additional graph shows the amount of IP addresses which respond to at least one of the protocols.



https://ipv6hitlist.github.io/

runZero

Shodan wins!



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

Universally unique identifiers

`1ef7e299-fa25-4f65-afca-ee27cc61b843`

- 128 bits, like IPv6, multiple versions, and everywhere
- Random-looking, but often richly encoded

UUID versions

```
v1: f270fa6e-9214-11ef-b864-00c04f8eea45
v2: 000003e8-921b-21ef-9400-325096b39f47
v3: 3a232406-35ad-39bb-8b78-3b7b3624a768
v4: 9c5b94b1-35ad-49bb-b118-8e8fc24abf80
v5: da81c735-c250-58bc-b407-89ecef772215
v6: 1e65ced7-cdcb-679d-8405-c8bcc8a0b1fd
v7: 0192bf28-cf17-72f6-a0ee-c48769f6a408
v8: 9c5b94b1-35ad-89bb-b118-8e8fc24abf80
```

Version/Variant

Timestamp

MAC/Node

MD5/SHA

Random

Vendor

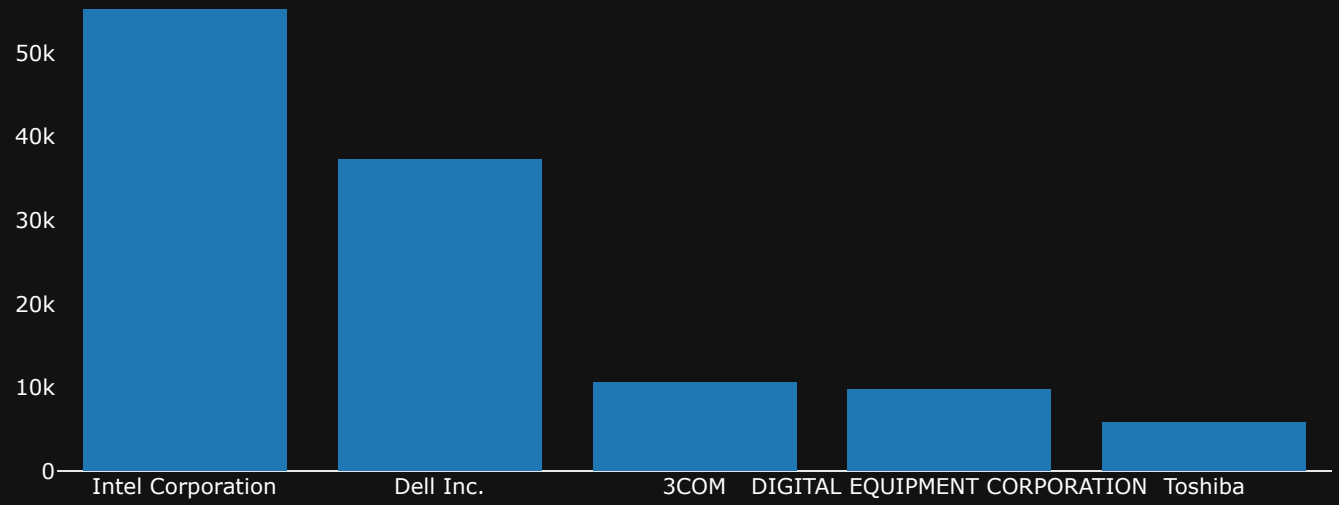
Sources of UUIDs

- Web requests (BurpSuite + UUID Detector[1])
- Microsoft Office file formats (docID)
- Windows registry & binaries
- Database record IDs

1. https://github.com/PortSwigger/uuid-detector

Windows registry

- Dump all UUID/GUIDs from the Windows registry
- Extract UUID v1/v2 nodes, convert to MACs



UUID v7 adoption

- UUID v4 effectively replaced UUID v1
- UUID v4 isn't great for sharding
- UUID v7 helps, but at a cost
- 48-bit ts with ms precision
- Expect to see it soon!

`0192bf28-cf17-72f6-a0ee-c48769f6a408`

https://aws.amazon.com/blogs/database/implement-uuidv7-in-amazon-rds-for-postgresql-using-trusted-language-extensions/

MAC addresses

- Associated with Ethernet, WiFi, & Bluetooth
- 48–bits (6 bytes), but prefix-allocated
- Currently ~53,000 prefixes
- Prefix lengths vary

```
30:20:4b:00:01:02 (L)
18:c3:f4:10:01:02 (M)
00:1b:c5:00:40:02 (S)
```

MAC history

- Companies (and people) purchase a prefix from IEEE
- As devices are shipped, new prefixes are added
- IEEE records the owner & address
- Historical data requires work
  - https://github.com/hdm/mac-ages/

30:20:4b:00:01:02

Huawei on 2024-10-23

Data mining MACs

- MACs are exposed via SNMP, mDNS, NetBIOS, and more
- Sometimes via unlikely avenues
- Odd scan on ports 987 & 9302

```
SRCH * HTTP/1.1
device-discovery-protocol-version:00030010
```

PlayStations!


```
{
  "type": "result",
  "ts": 1729755767731551726,
  "host": "141.41.34.20",
  "port": "9302",
  "proto": "udp",
  "probe": "psdisco",
  "info": {
    "psdisco.code": "200",
    "psdisco.id": "5C96669DAB01",
    "psdisco.name": "PS5-912",
    "psdisco.protoVersion": "00030010",
    "psdisco.requestPort": "997",
    "psdisco.status": "Ok",
    "psdisco.sysVersion": "10010000",
    "psdisco.type": "PS5"
  }
}
```


- The ID `5C96669DAB01` looks familiar...

PlayStations MACs

5C:96:66:9D:AB:01

Sony Interactive Entertainment on 2021-08-27

PlayStation status

Firmware

43288 10200006
33216 12008011
2765 10010000
2397 11520011
1606 11508011
694 11020001
367 11008001
311 09008031
279 10508011
177 10010001
172 09600004
135 10710001
90 10000046
63 09600011
54 09030001
37 09400008
33 06720001
29 09200005

Applications

2466 YouTube
615 Netflix
354 Call of Duty®
303 Fortnite
285 Prime Video
243 EA SPORTS FC 25
176 Grand Theft Auto V
129 Apex Legends
123 Disney+
120 eFootball™
102 Twitch
99 Hulu
93 原神
78 Max
69 Red Dead Redemption 2
68 Overwatch 2
60 TubiTV
60 Crunchyroll

Summary

- Short identifiers are pervasive and dangerous
- Long identifiers provide precise tracking
- Fun data is everywhere!

LASCON

runZero

Thank you!

hdm @ runZero.com