black hat BRIEFINGS
AUGUST 6-7, 2025
MANDALAY BAY / LAS VEGAS

Exploiting DNS for Stealthy User Tracking

Béla Genge, Ioan Pădurean, Dan Macovei

Béla GENGE

Senior Security Researcher

IoT security, vulnerability research

Scientist at heart

Ioan PĂDUREAN

Junior Security Researcher

Applied ML techniques, IoT security

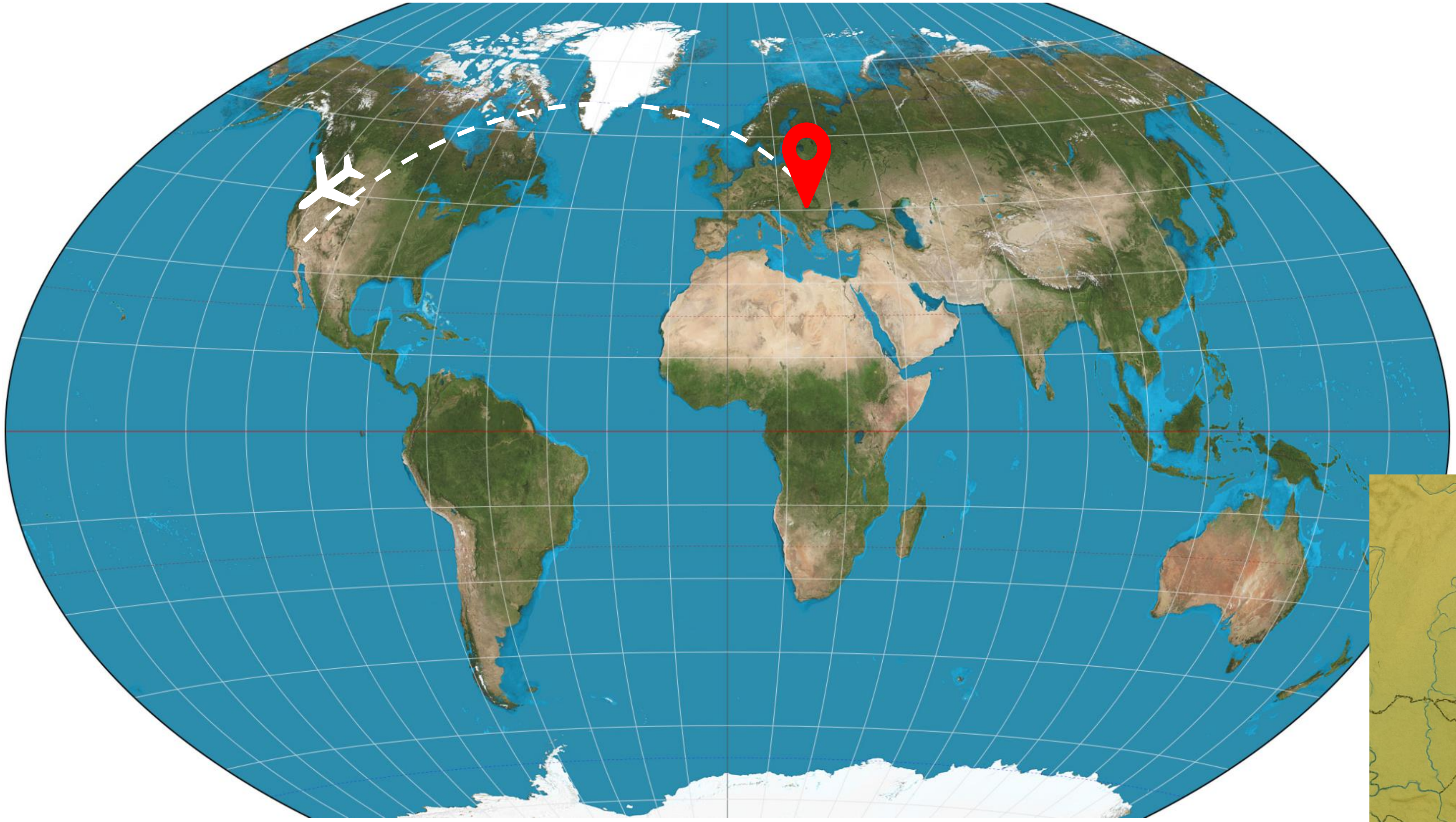
Dan MACOVEI

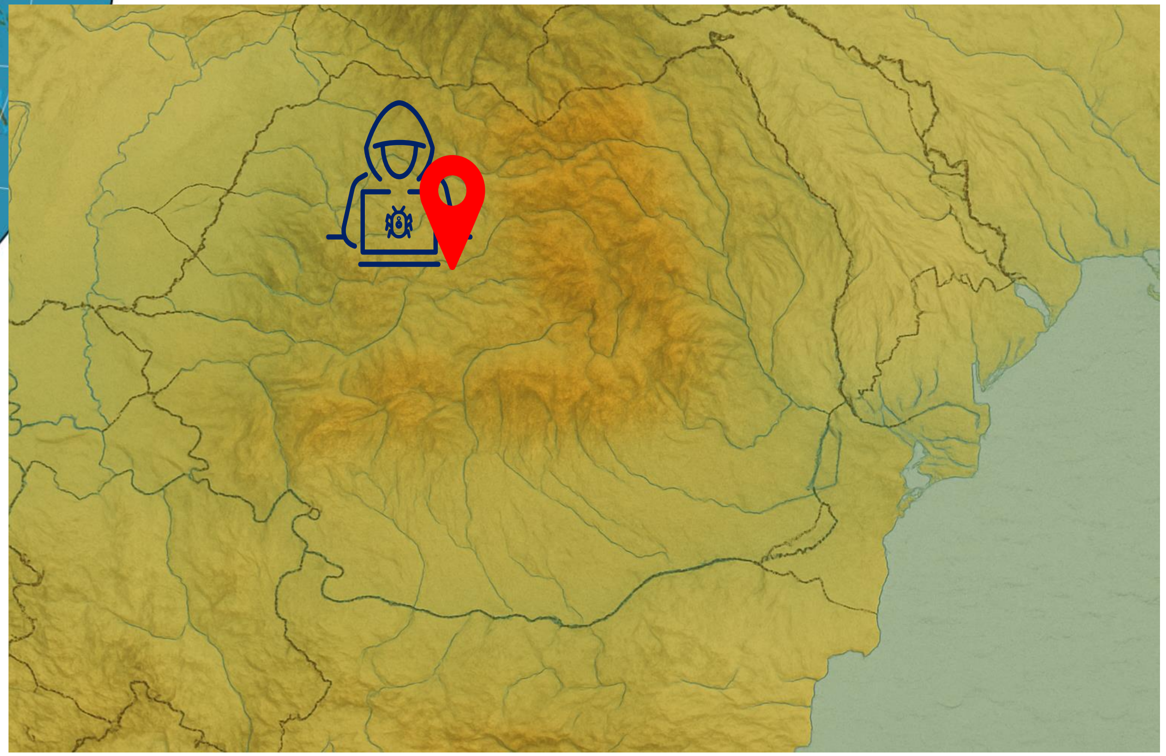
Director of Product Management

Security Product Strategy

Bitdefender

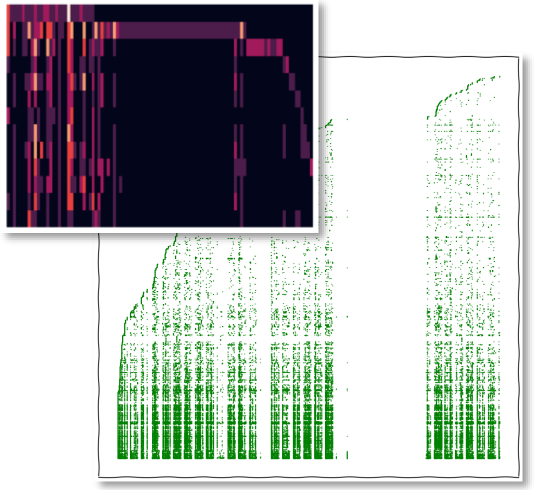
The Transylvanian researchers





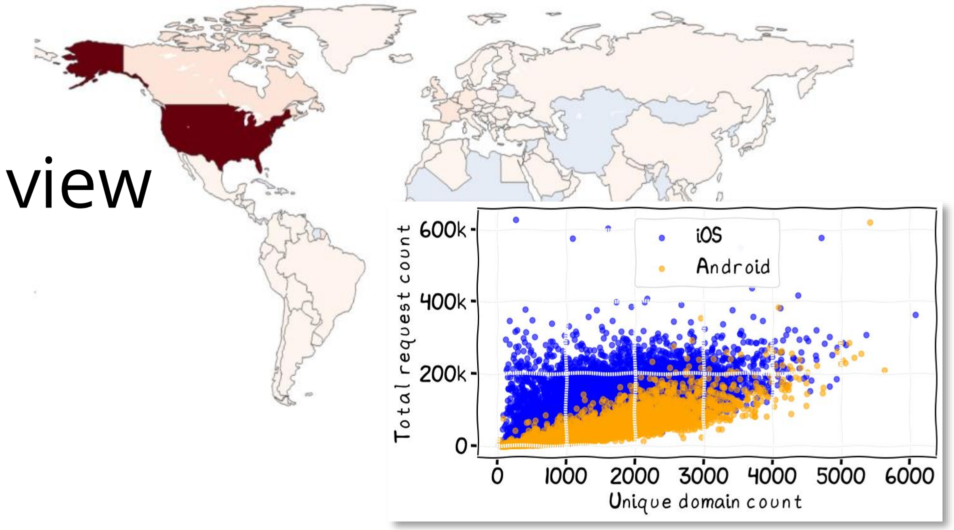
https://en.wikipedia.org/wiki/World_map

Agenda



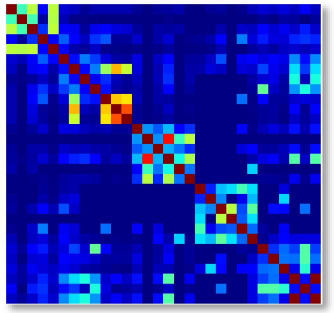
1 Introduction & the why?

2 A bird's eye view



3 DNS request patterns & transformations

4 User tracking: approach and results

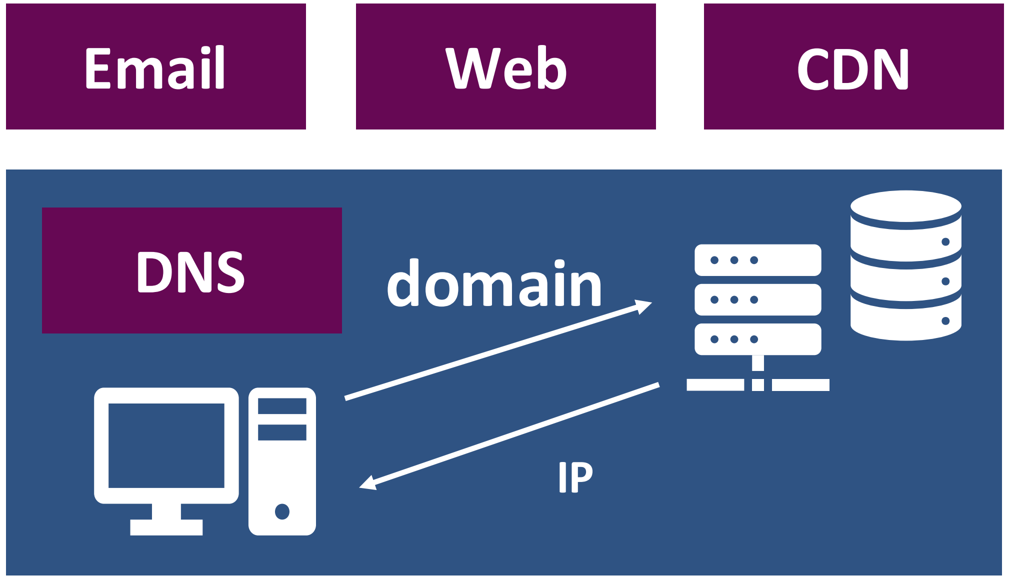


5 Conclusions & key takeaways

Introduction & motivation

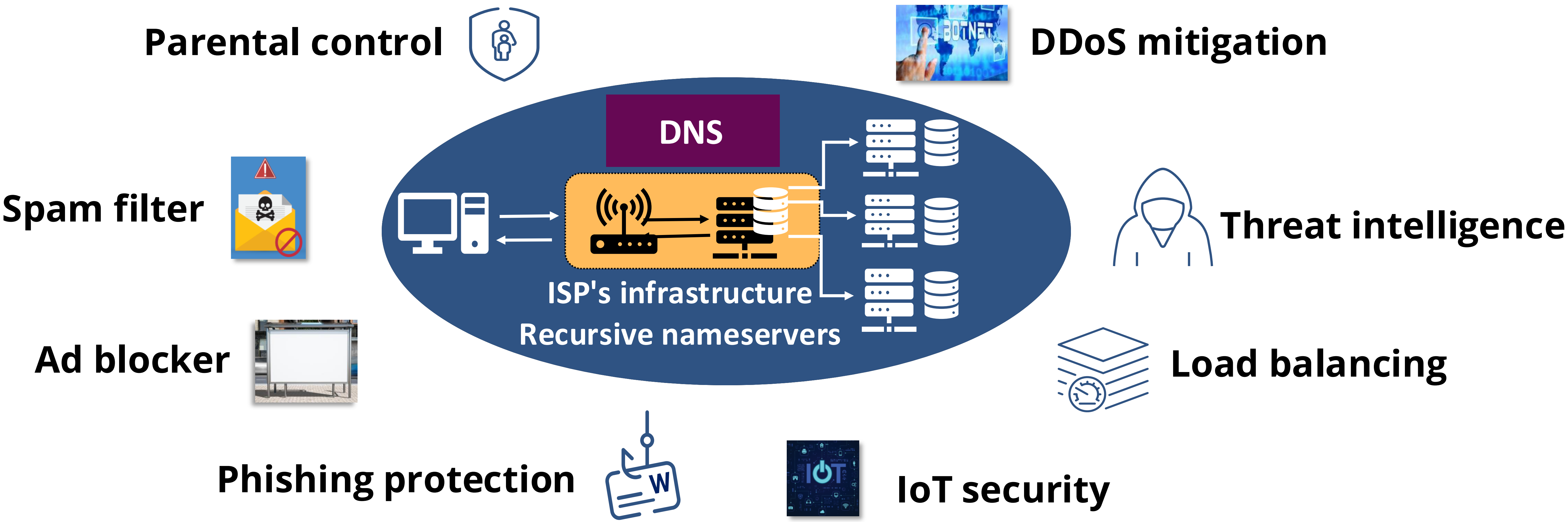
The Domain Name System (DNS)

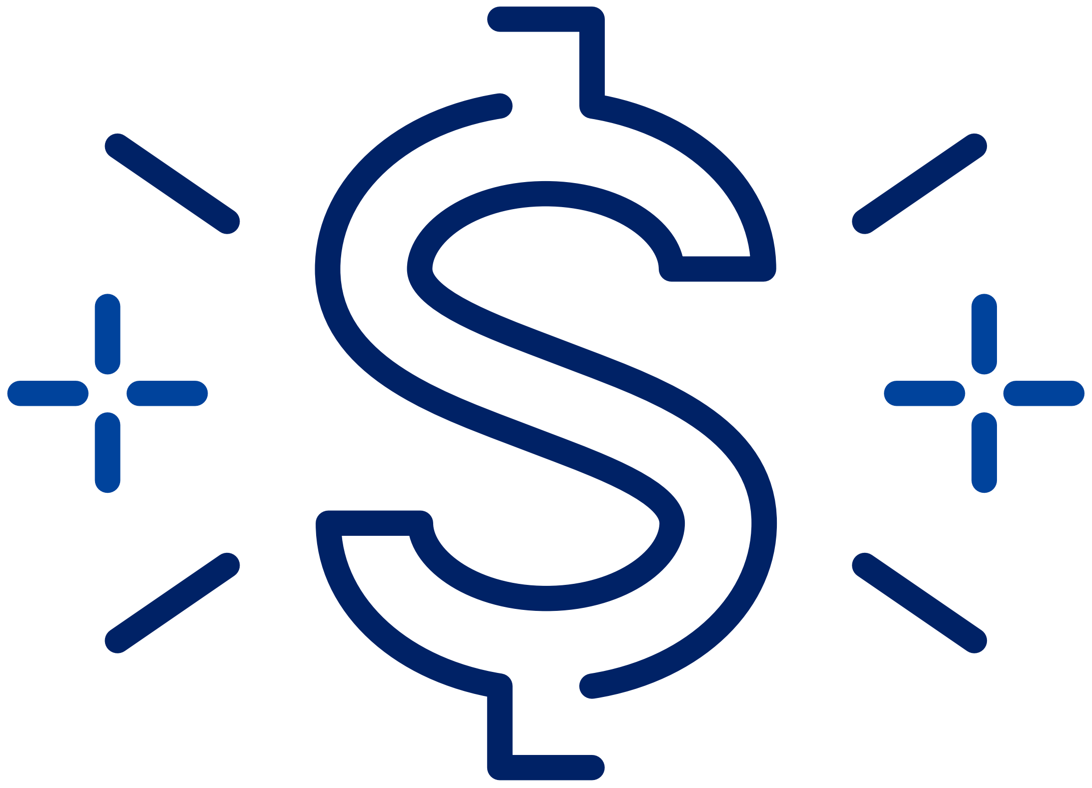
- The "phonebook of the internet"
- Translate human-readable domain names into IP addresses
- ALL devices use DNS



DNS and security applications

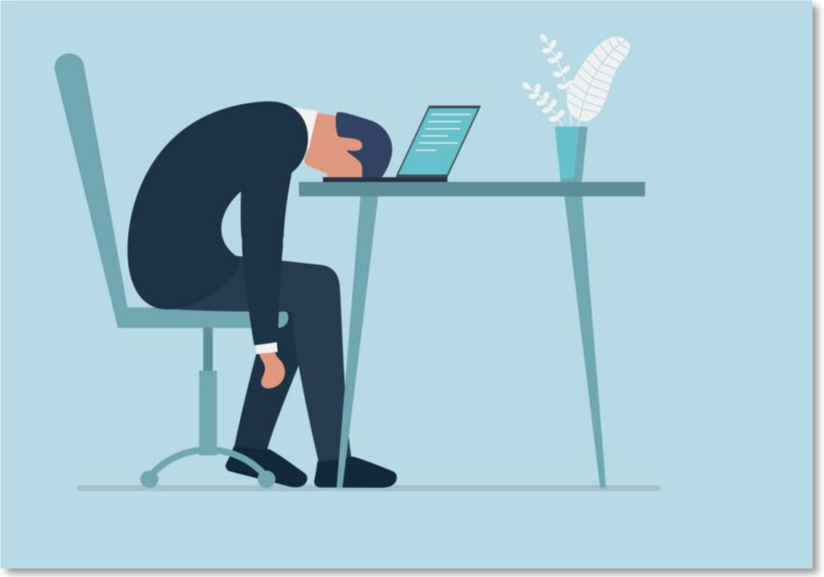
- DNS has a critical role in security applications
- DNS fuels the applications aimed to protect networks and users



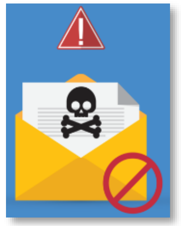


Why this research on DNS?

Looking for ways to improve security solutions



Parental control



Spam filter

Ad blocker

What we observed

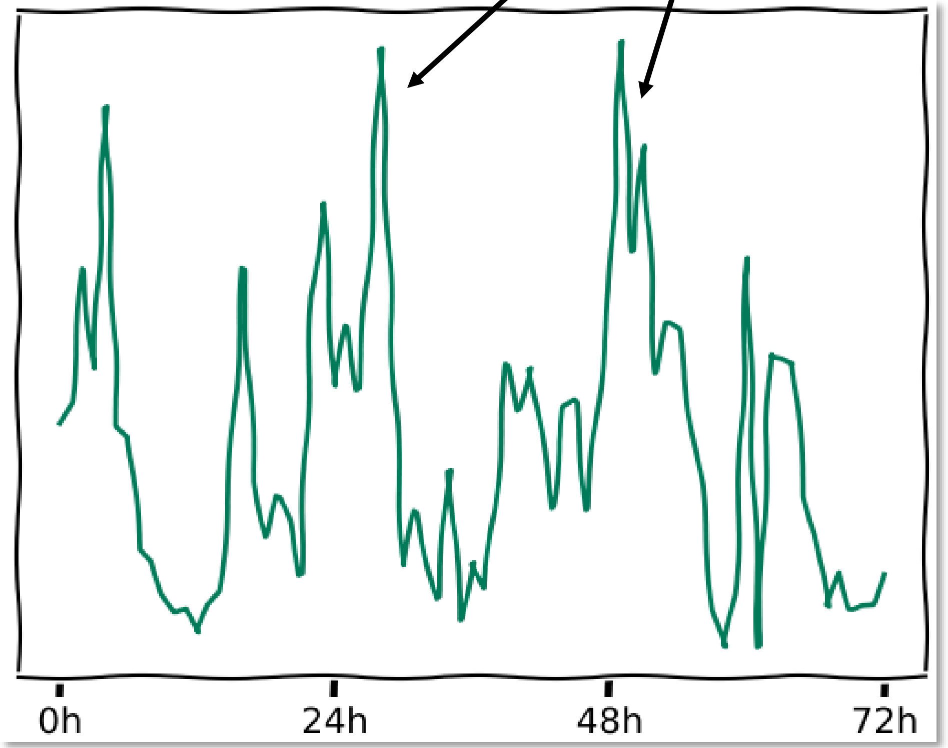
Noticed **interesting** sequences for devices in our testbed @office

iOS

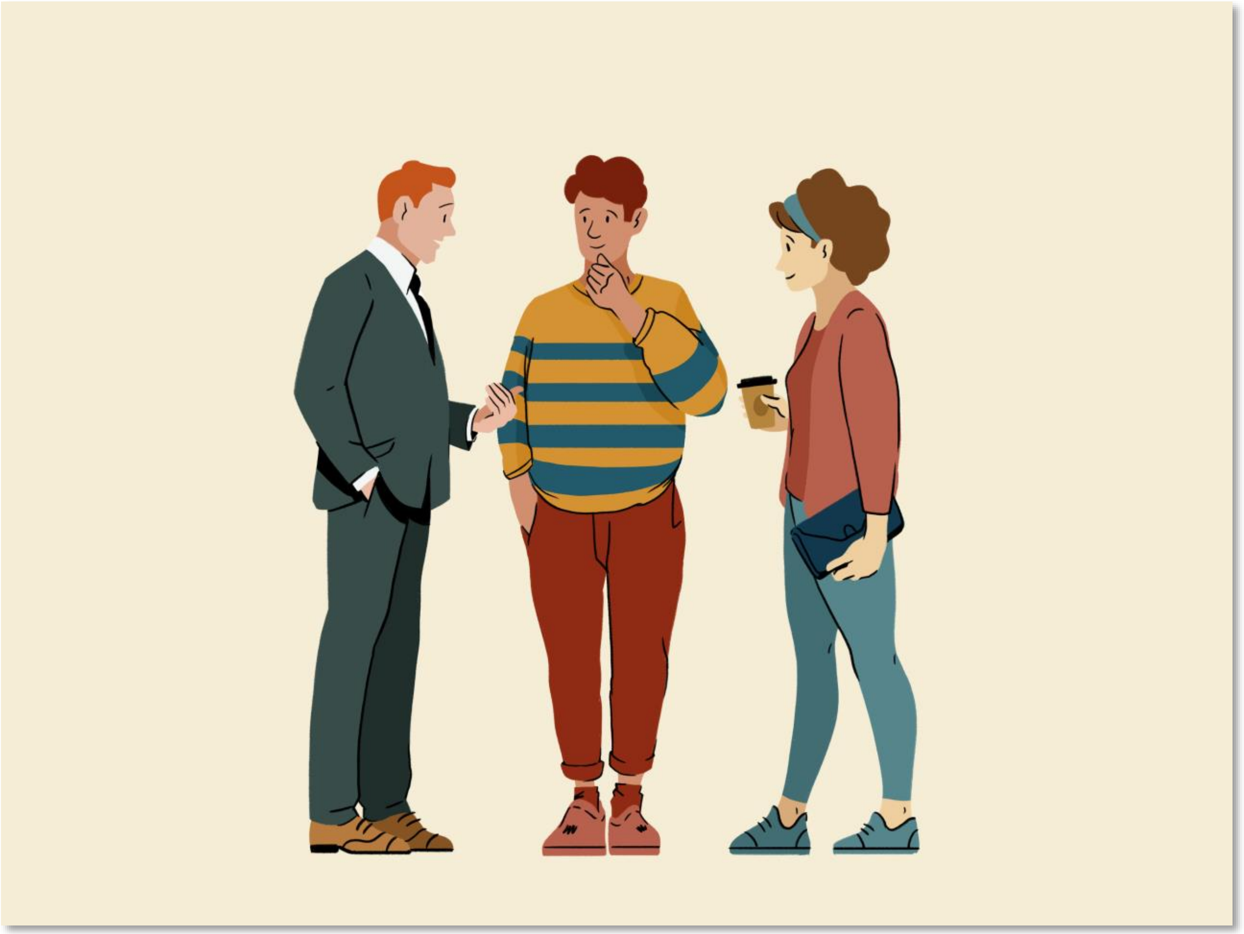
Protocol	Length	Info
DNS	163	Standard query response 0xc9b7 HTTPS mask.apple-dns.net SOA ns-1096.awsdns-09.org
DNS	147	Standard query response 0xf034 A comm-main.ess.apple.com CNAME comm-main.ess-apple.com.akadns.net
DNS	85	Standard query 0x8d80 A comm-cohort.ess.apple.com
DNS	151	Standard query response 0x8d80 A comm-cohort.ess.apple.com CNAME comm-cohort.ess-apple.com.akadns
DNS	69	Standard query 0x7269 HTTPS slack.com
DNS	69	Standard query 0xd4ed A slack.com
DNS	151	Standard query response 0x7269 HTTPS slack.com SOA ns-1493.awsdns-58.org
DNS	165	Standard query response 0xd4ed A slack.com A 52.29.238.212 A 3.68.124.95 A 18.159.197.225 A 3.68.:
DNS	77	Standard query 0x7d2f HTTPS captive.apple.com
DNS	77	Standard query 0xb55b A captive.apple.com

Protocol	Length	Info
DNS	74	Standard query 0x0043 A www.google.com
DNS	89	Standard query 0x13b0 A connectivitycheck.gstatic.com
DNS	90	Standard query response 0x0043 A www.google.com A 142.251.141.36
DNS	105	Standard query response 0x13b0 A connectivitycheck.gstatic.com A 216.58.206.67
DNS	76	Standard query 0x7b07 A mtalk.google.com
DNS	121	Standard query response 0x7b07 A mtalk.google.com CNAME mobile-gtalk.l.google.com
DNS	74	Standard query 0xb028 A g.whatsapp.net
DNS	113	Standard query response 0xb028 A g.whatsapp.net CNAME chat.cdn.whatsapp.net A 185
DNS	78	Standard query 0xf4d1 A graph.facebook.com
DNS	118	Standard query response 0xf4d1 A graph.facebook.com CNAME star.c10r.facebook.com

Repetitive behavior



The question



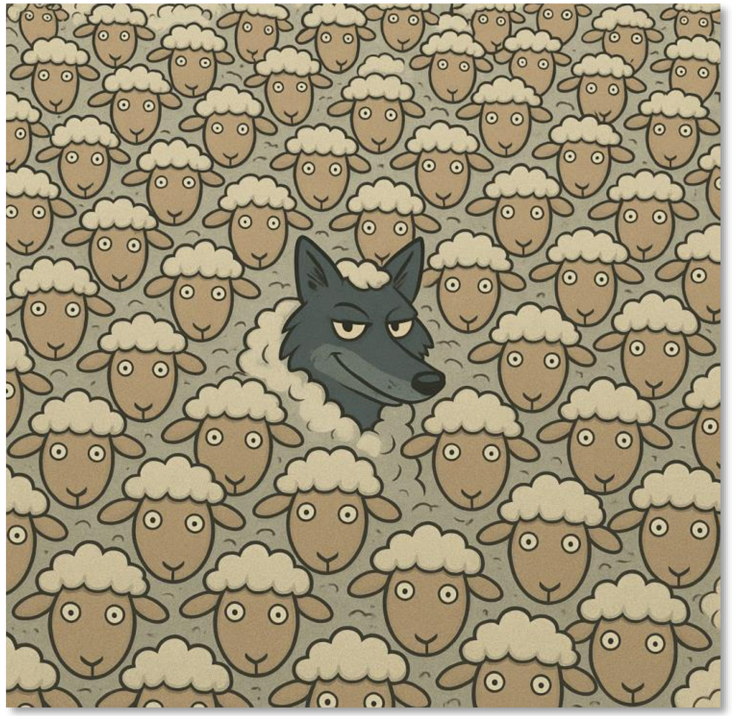
DNS and smartphone activity

User activity from DNS request perspective can be (**IT IS**!) repetitive!

Incentive for user tracking!

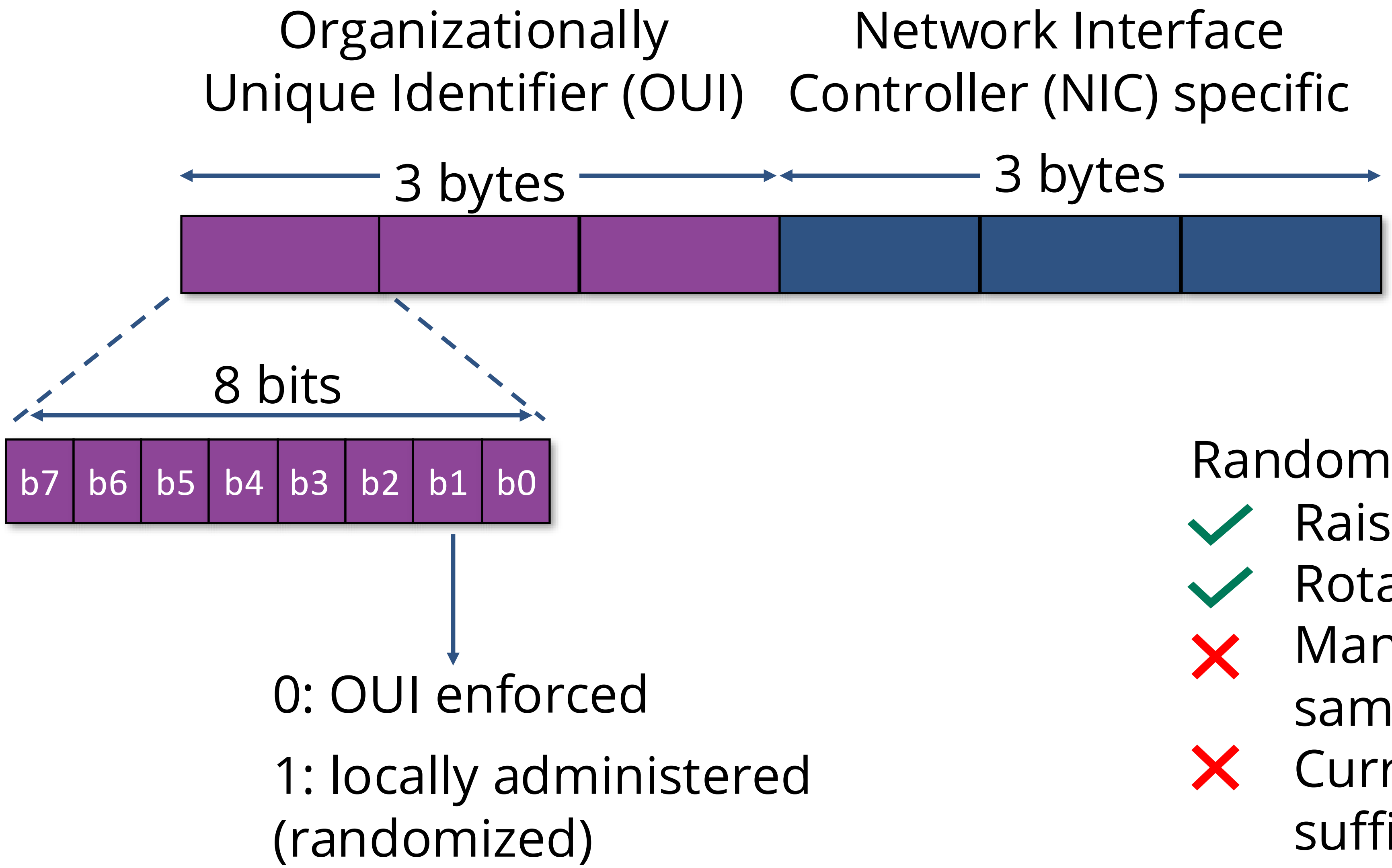
Privacy-related policies

- Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines
- European Union's General Data Protection Regulation (GDPR)
- Country-based (PIPEDA – Canada, HIPAA – US Healthcare, …)
- …



Technical privacy measures: MAC

1 Random MAC address as **privacy feature** to **prevent tracking**



Randomized MAC:

- ✓ Raises the bar for tracking
- ✓ Rotating MAC limits profiling window
- ✗ Many devices use the same MAC for the same network
- ✗ Current time window for rotating MAC is sufficient for tracking

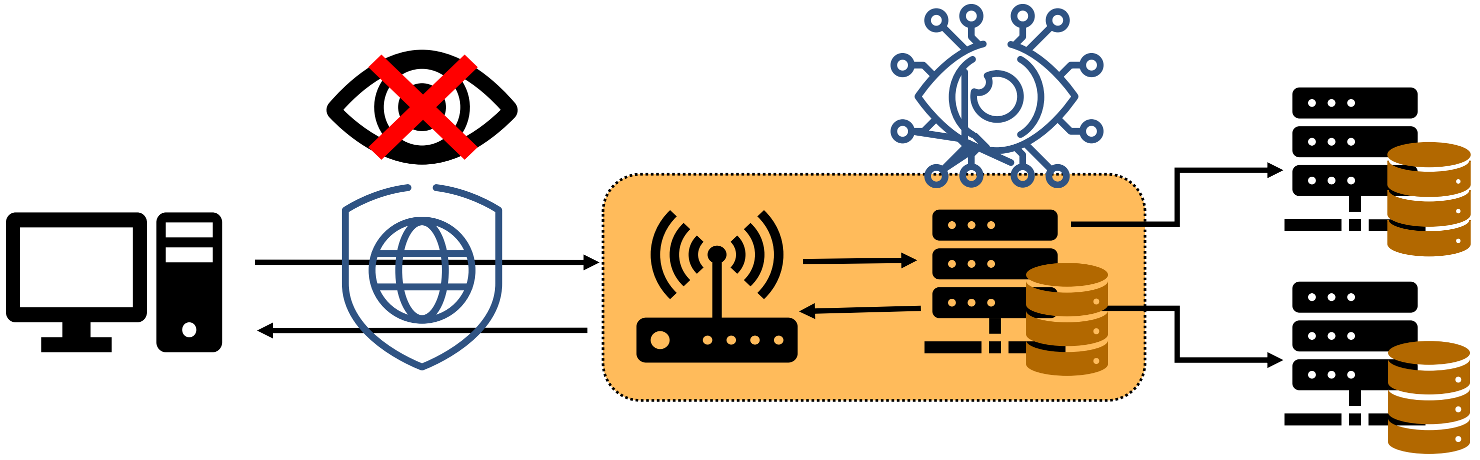
Technical privacy measures: DNS

2 **Secure DNS** (DNS / HTTPS, DNS / TLS):

- ✓ Eliminates **local** snooping
- ✗ Not as wide-spread (yet)
- ✗ Requests still need resolving – the case of the curious DNS resolver

Two flavors:

- DNS / **HTTPS** (DoH) ✓
- DNS / **TLS** (DoT)



How much time do we have?

iOS Wi-Fi settings:

Private Wi-Fi Address	Rotating >
Wi-Fi Address	16:5C:6C:8D:D1:C5

Wi-Fi networks and devices can track other nearby Wi-Fi devices by their Wi-Fi address, even on secure networks.
A rotating priva
periodically ch
this network.

Use private Wi-Fi addresses on Apple devices

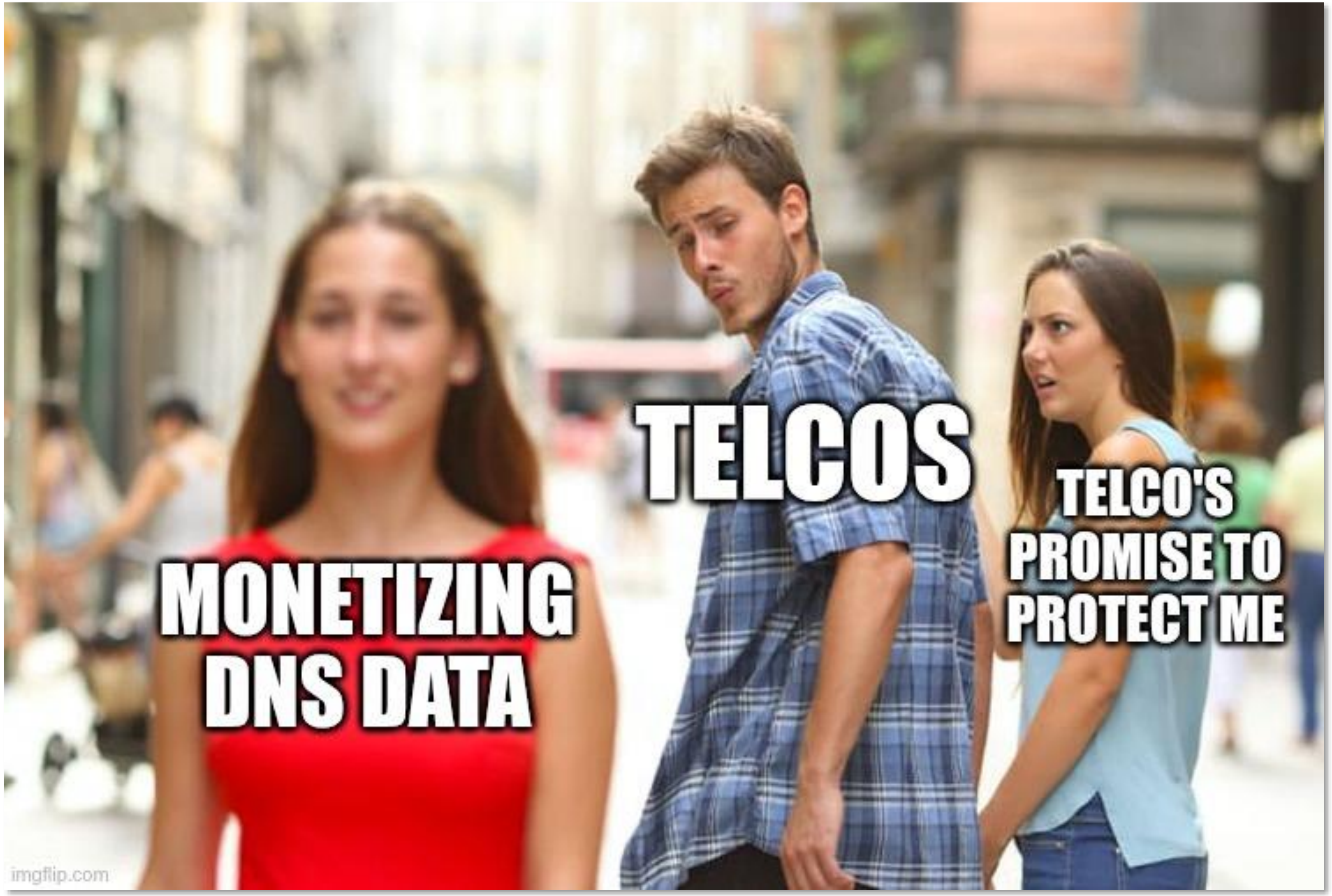
To improve privacy, your iPhone, iPad, iPod touch, Mac, Apple Watch, or Apple Vision Pro identifies itself to each network using a different Wi-Fi address, and might rotate (change) the address periodically.

- The Private Wi-Fi Address feature offers these settings, which you can change at any time:
  - *Rotating*: When set to Rotating, your device uses a private address that rotates to a different private address every 2 weeks. Your device chooses Rotating by default when joining a new network that uses weak security or no security.

https://support.apple.com/en-mt/102509

Tracking deadline

Can we trust telcos?



Looking into the past

2006-2008

secretly tested Phorm's deep packet inspection technology on thousands of broadband users

2013-2014

published a report admitting some governments had **direct access to customer data and networks**

2018

shared access to consumers' location data without obtaining proper user consent

2020

fined for **unauthorized use of personal and location data** for advertising and profiling

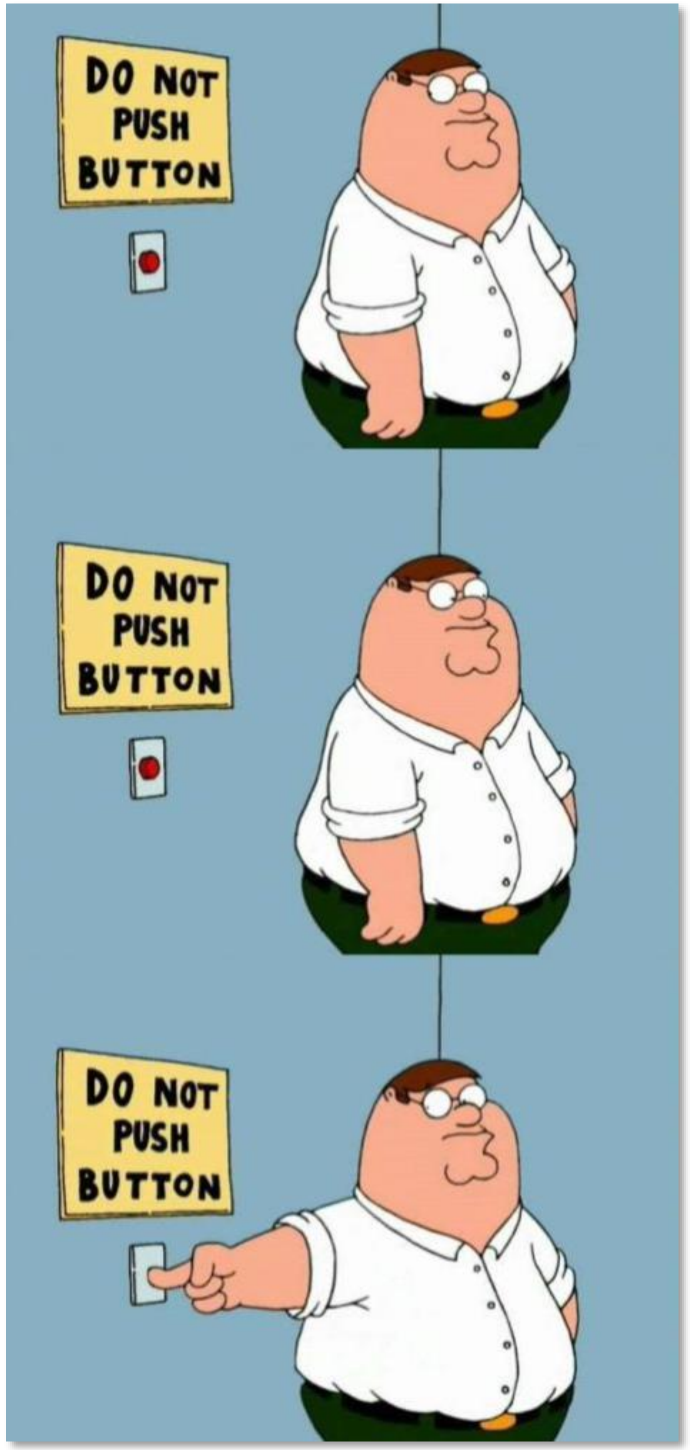
2023

formed a joint venture to **develop a digital advertising platform** that leverages the telcos' extensive customer data for **targeted advertising**

2024

targeted advertisements based on users' inbox activity **without obtaining explicit consent**

The temptation



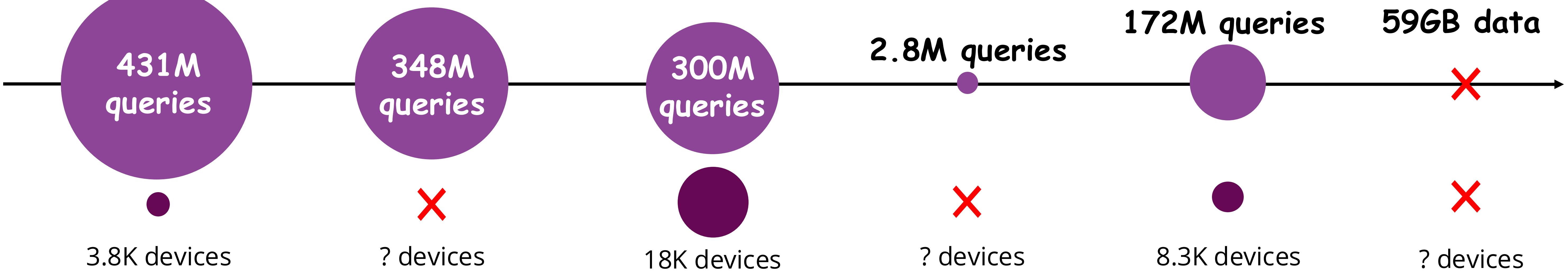
black hat BRIEFINGS

How new is this research?

D. Herrmann, et al.: *Behavior-based tracking: Exploiting characteristic patterns in DNS traffic*, **2013**

K. Schomp, et al.: *Towards a Model of DNS Client Behavior*, **2016**

Jian Qu, et al.: *Who is DNS serving for? A human-software perspective of modeling DNS services*, **2023**



Qingnan Lai, et al. : *Visualizing and characterizing DNS lookup behaviors via log-mining*, **2015**

M. Panza, et al.: *Extracting human behavior patterns from DNS traffic*, **2022**

Zhiyang Sun, et al.: *DNS Request Log Analysis of Universities in Shanghai: A CDN Service Provider's Perspective*, **2024**

Key distinctions

1. First study with exclusive focus on Smart Phones
2. Large pool of devices, 985M requests
3. Key insights specific to popular platforms: **iOS** and **Android**

Communication

Work & productivity

Internet access

Shopping & payments

Multimedia

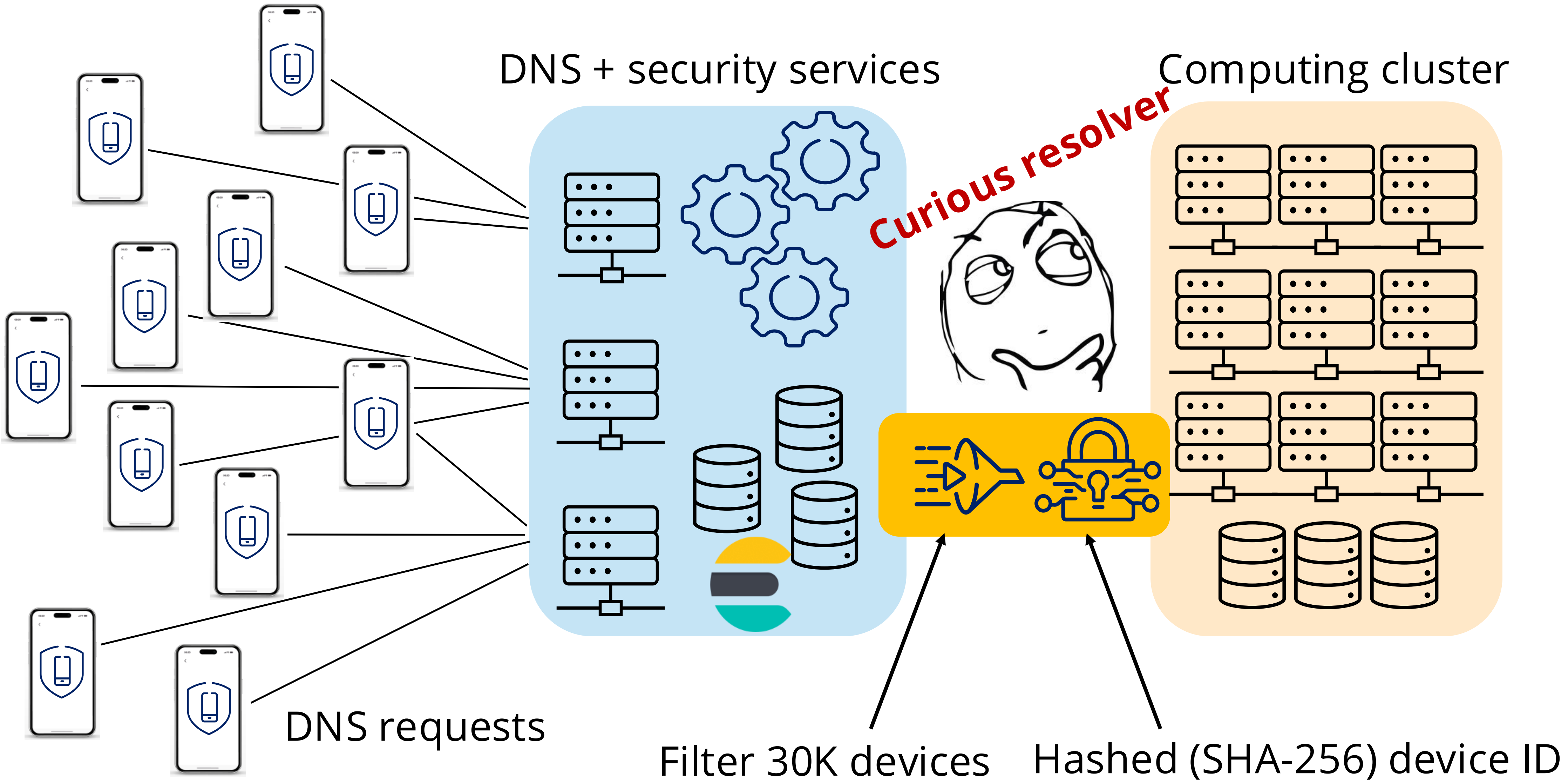
Health & fitness

Entertainment & gaming

Navigation & travel

Down to business: a bird's eye view

The curious DNS resolver

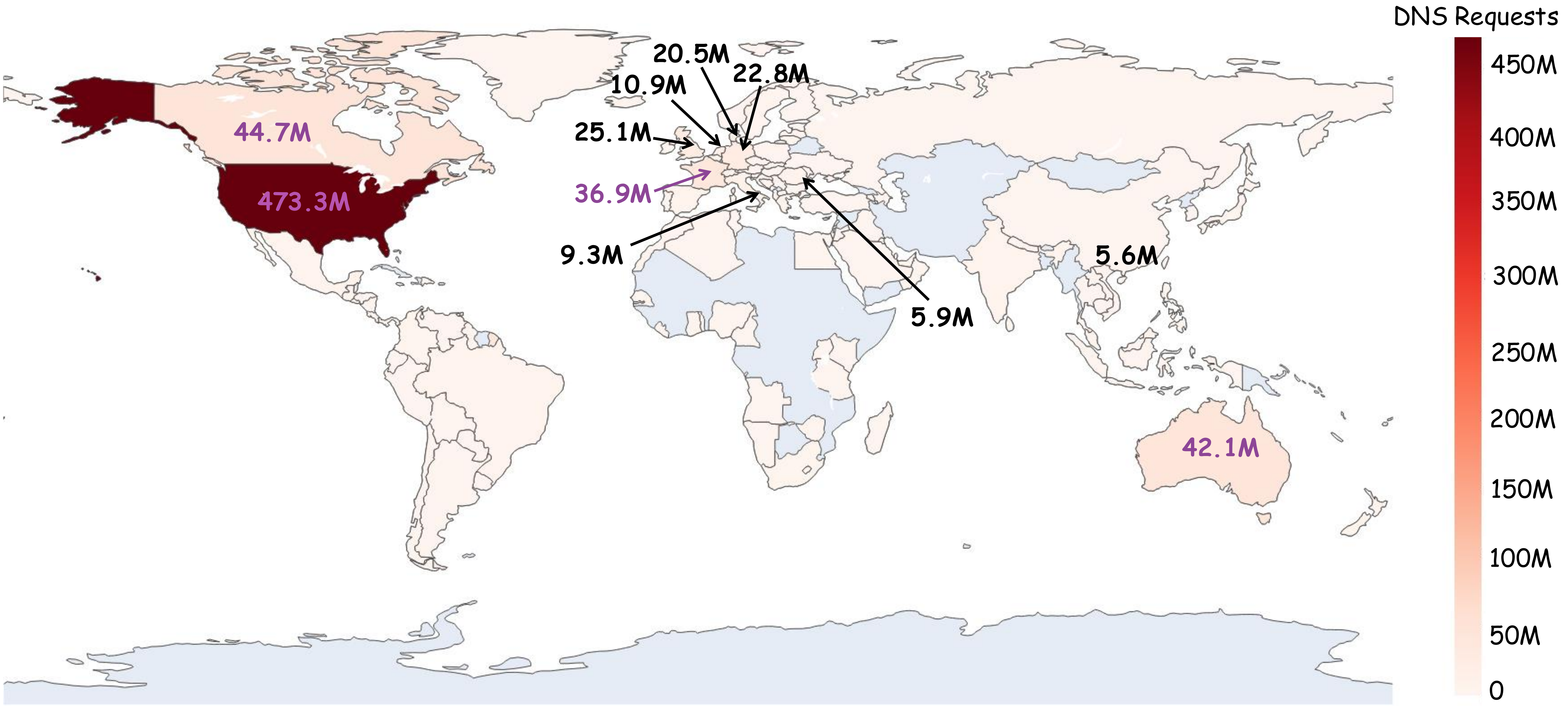


35 days of DNS requests
Request count (after pre-processing): **985M**

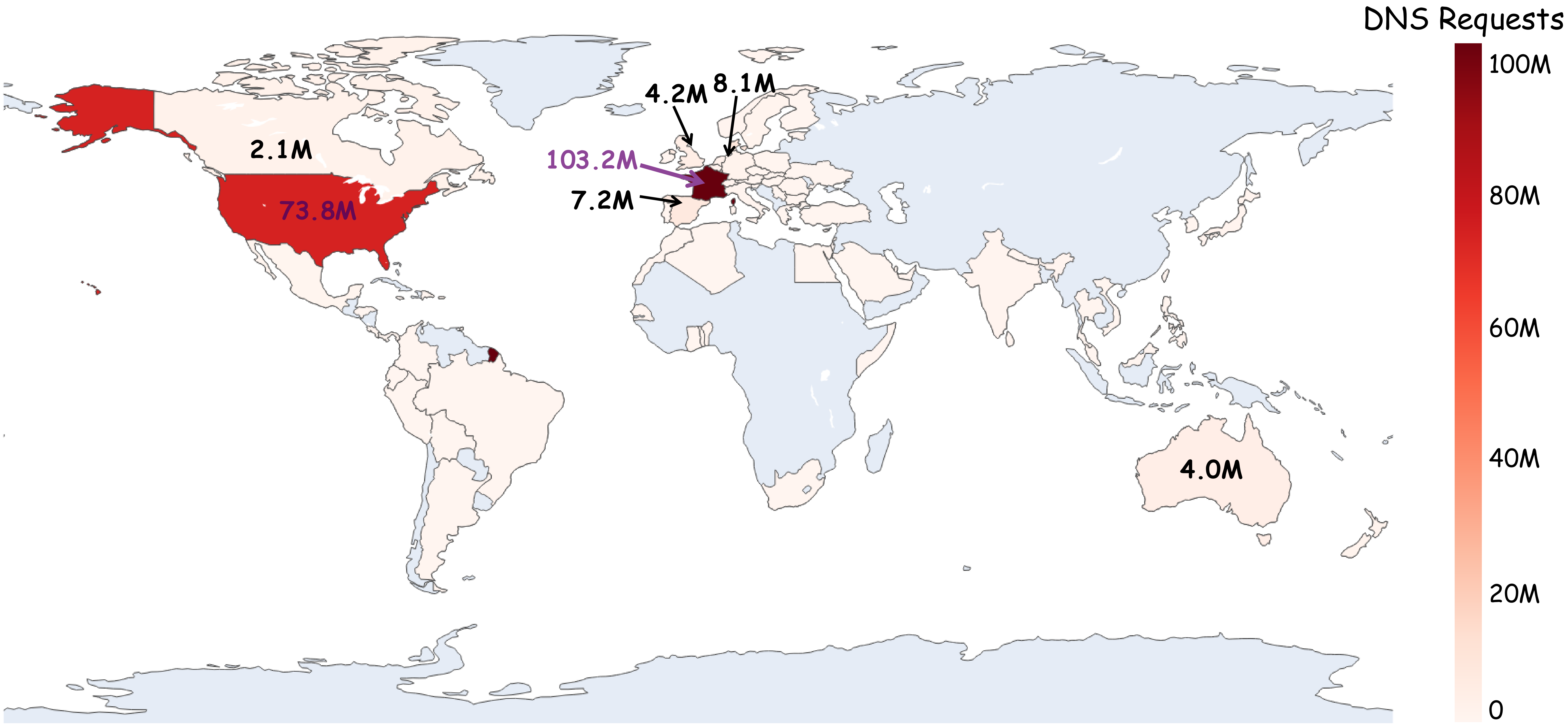
4 computational clusters
Total RAM: **1.5 TB**
Total vCPUs: **80**

~28K phones
(after pre-processing)

DNS requests by country - iOS

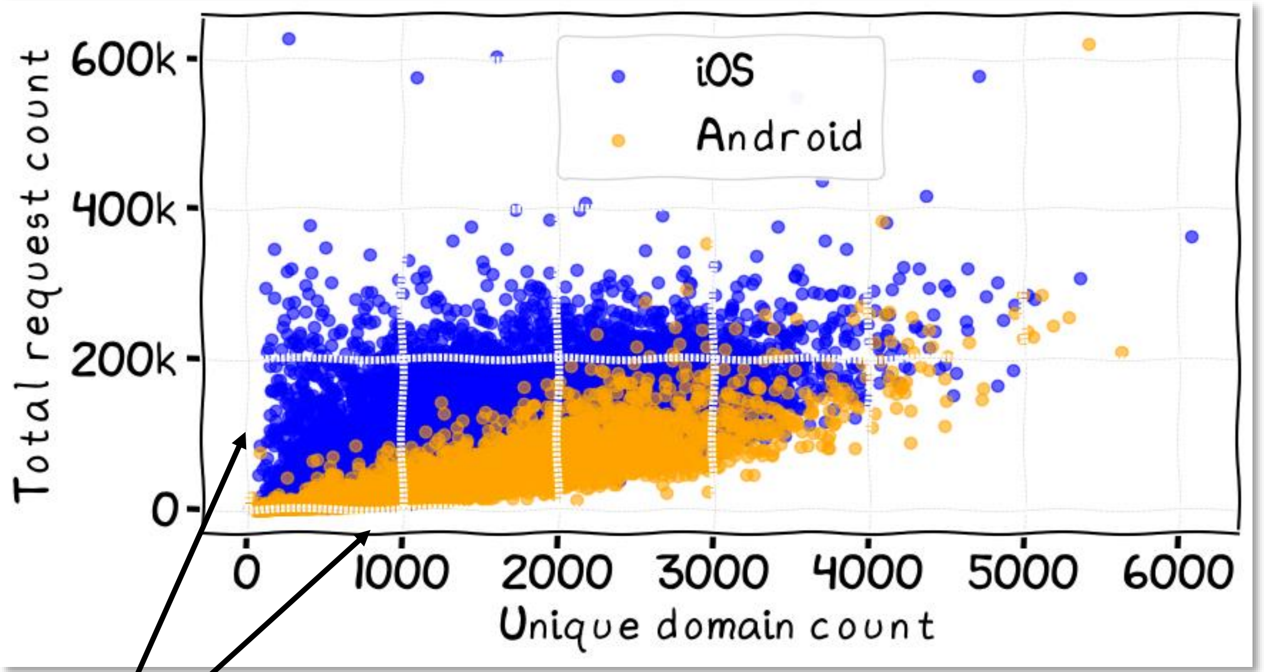


DNS requests by country - Android



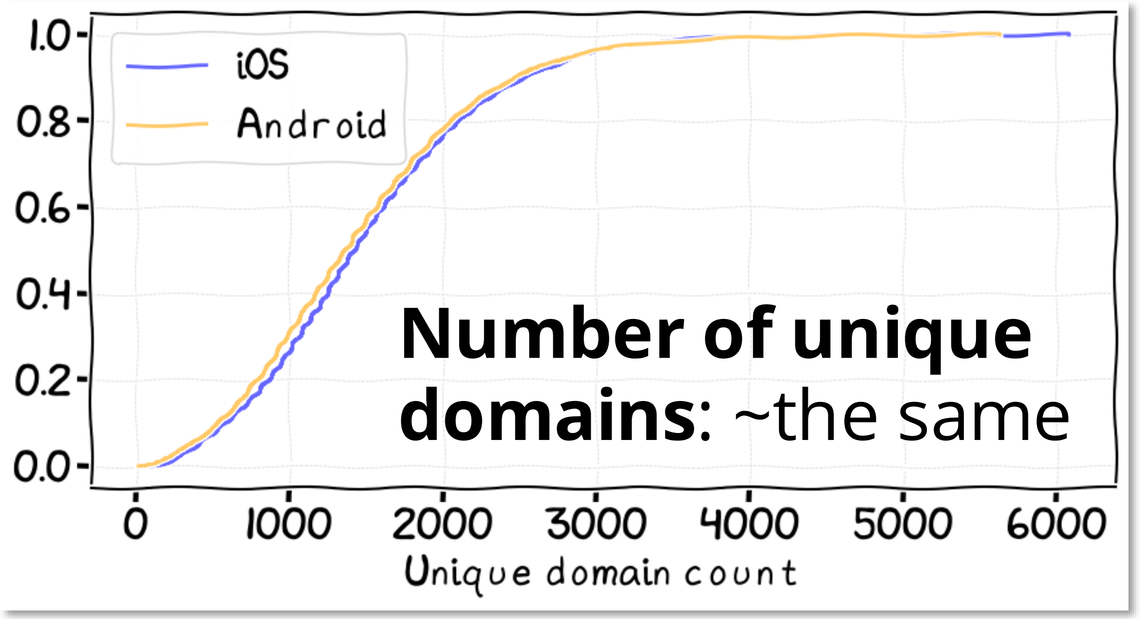
Distribution of domain requests

Unique vs total number of accessed domains

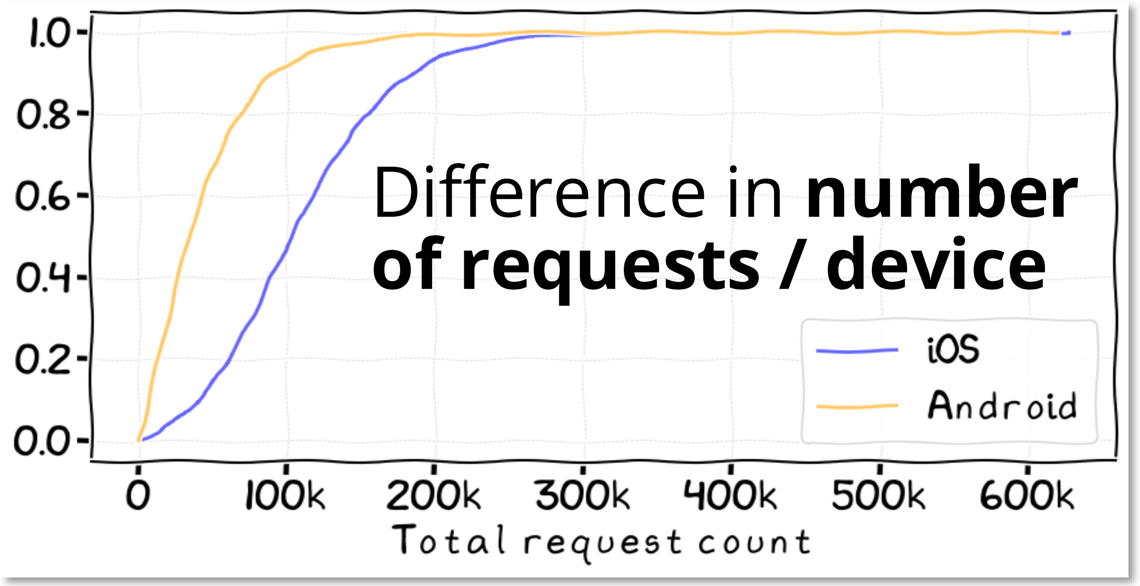


Visible distinction between **iOS** and **Android**

Cumulative Distribution Functions (CDF)



Number of unique domains: ~the same

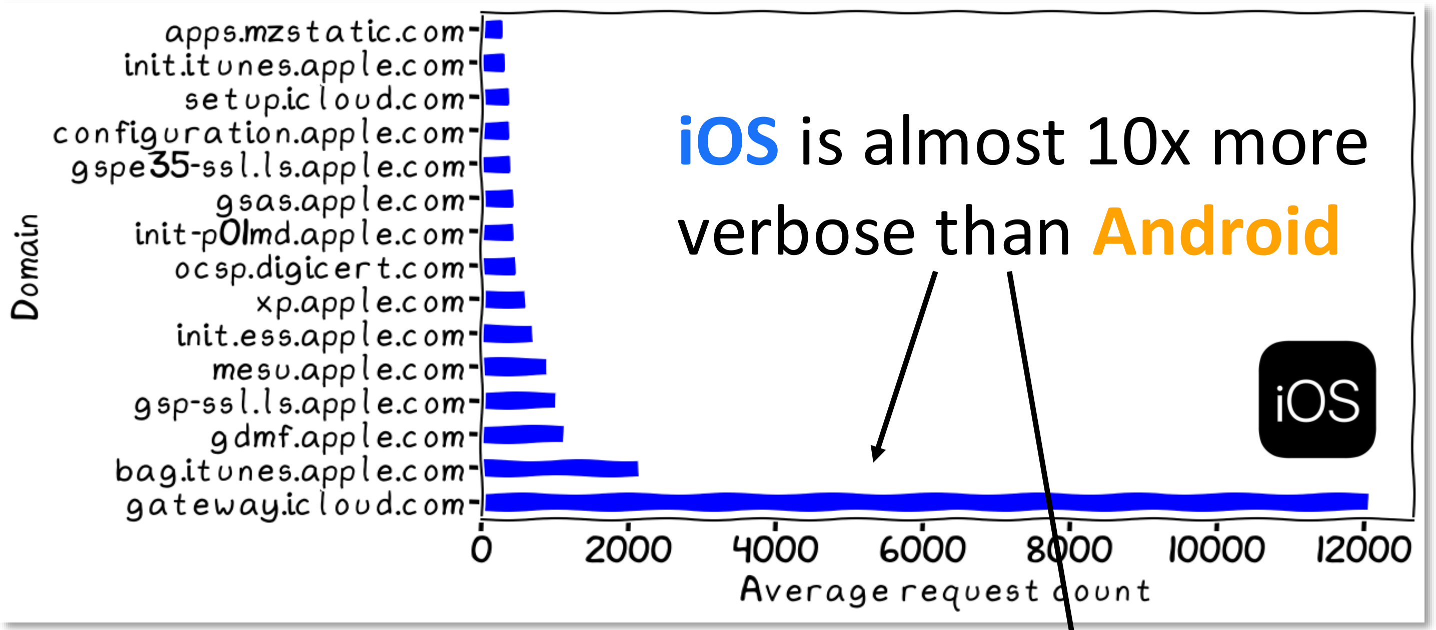


Difference in **number of requests / device**

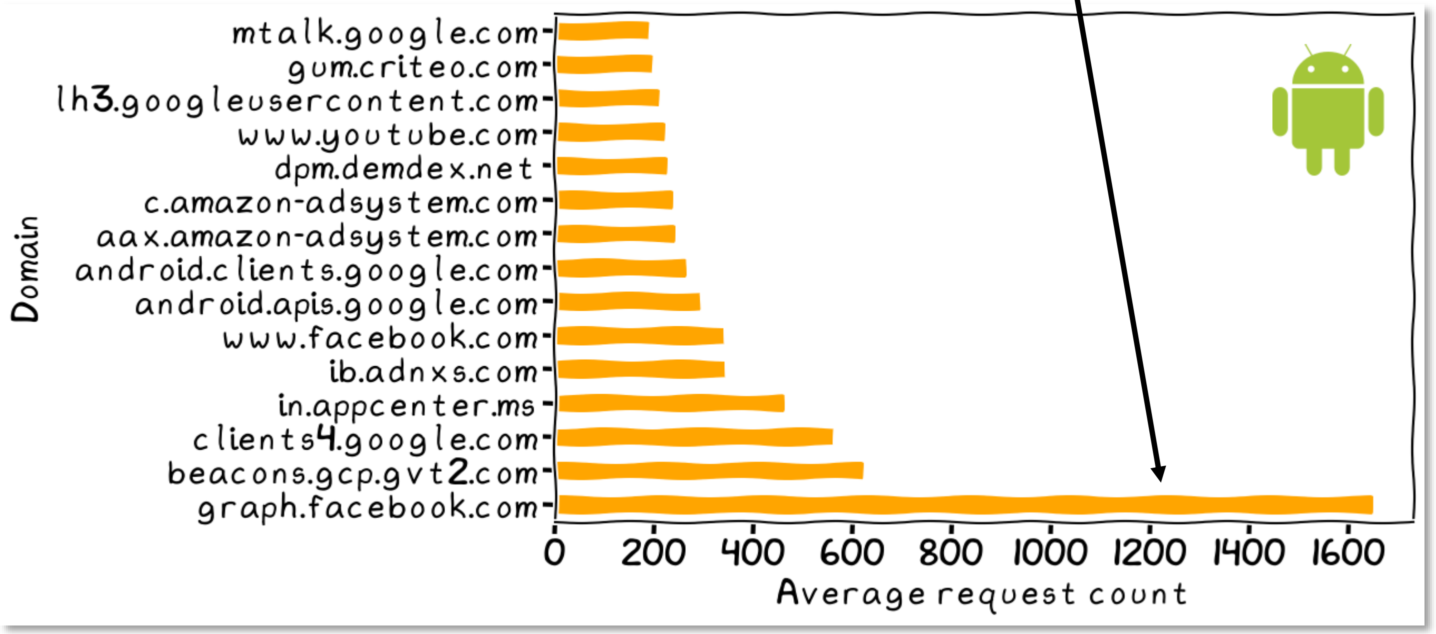
Most frequently accessed domains

- Most common domains: from popular applications
- **iOS**: mostly Apple related
- **Android**: Google and popular platforms

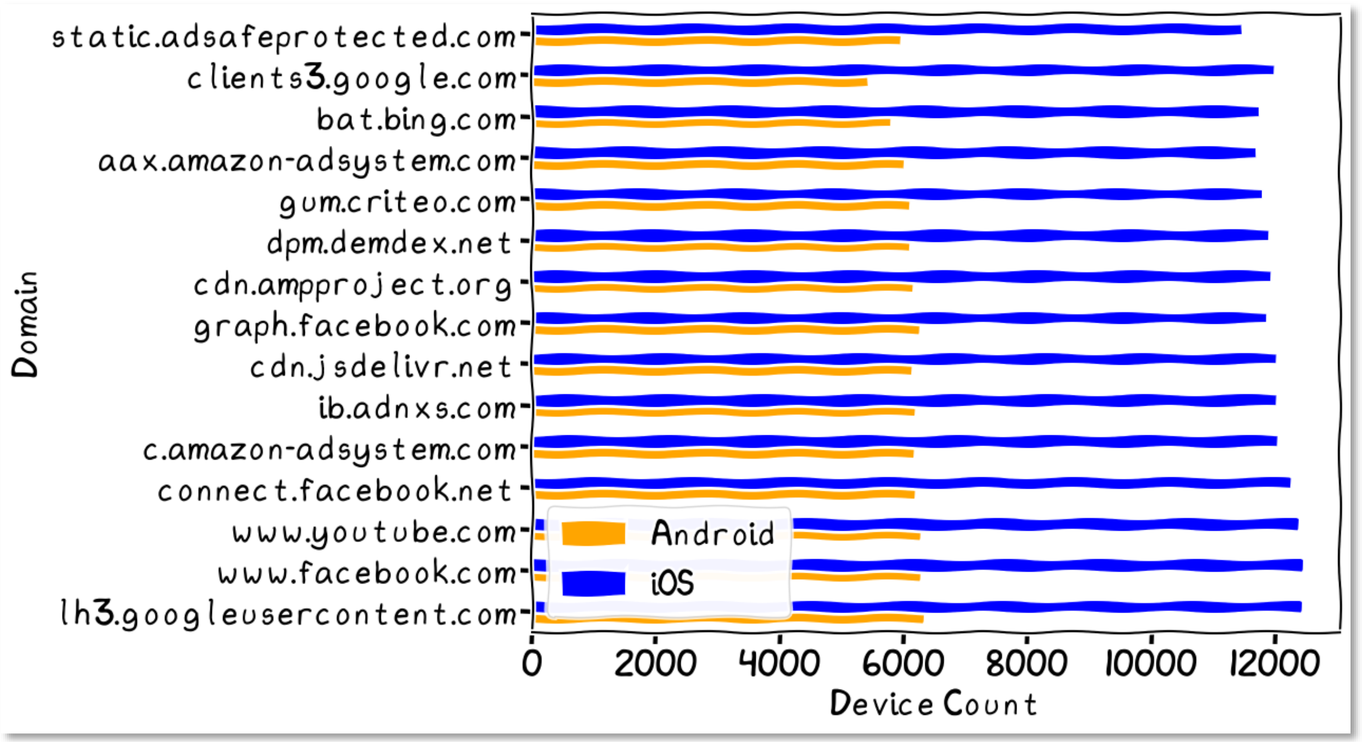
Top 15 domains / OS



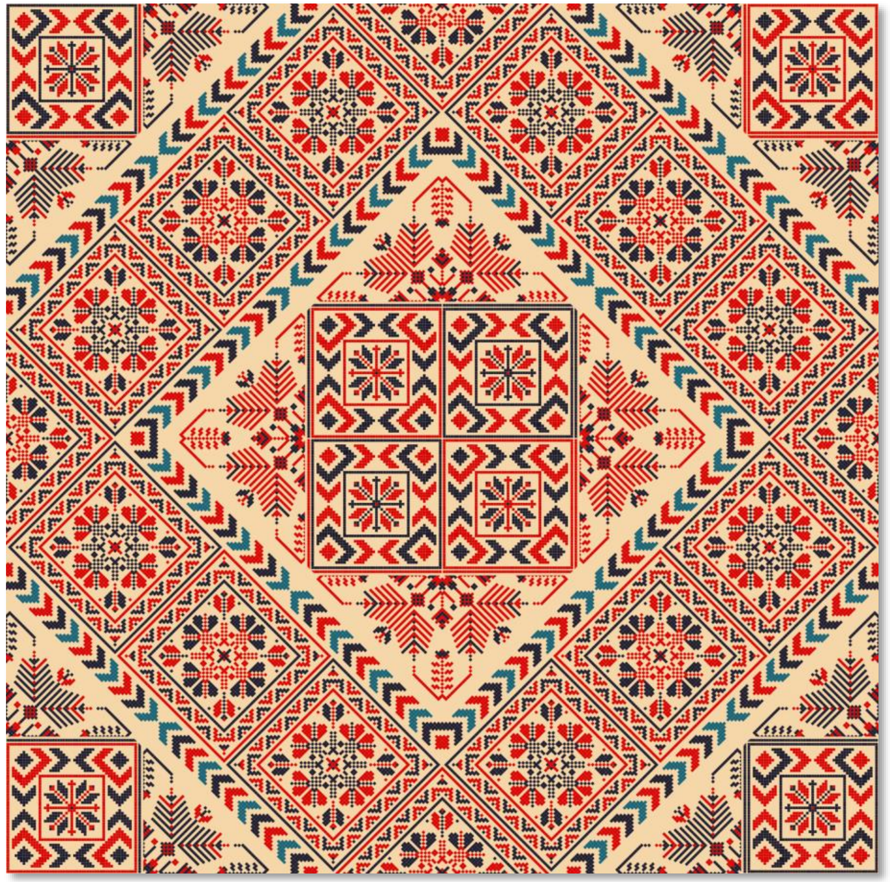
iOS is almost 10x more verbose than Android



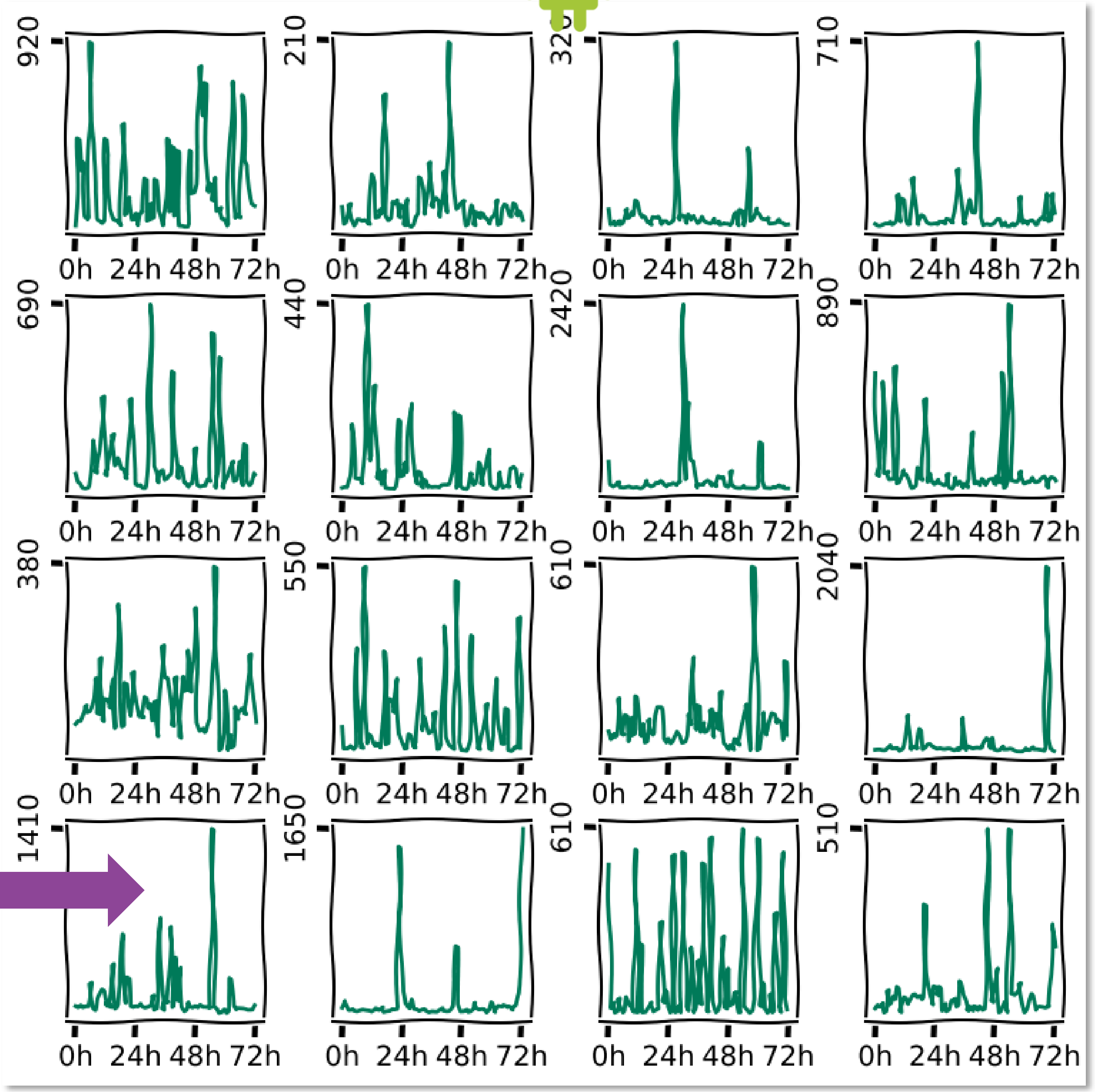
Top 15 common domains



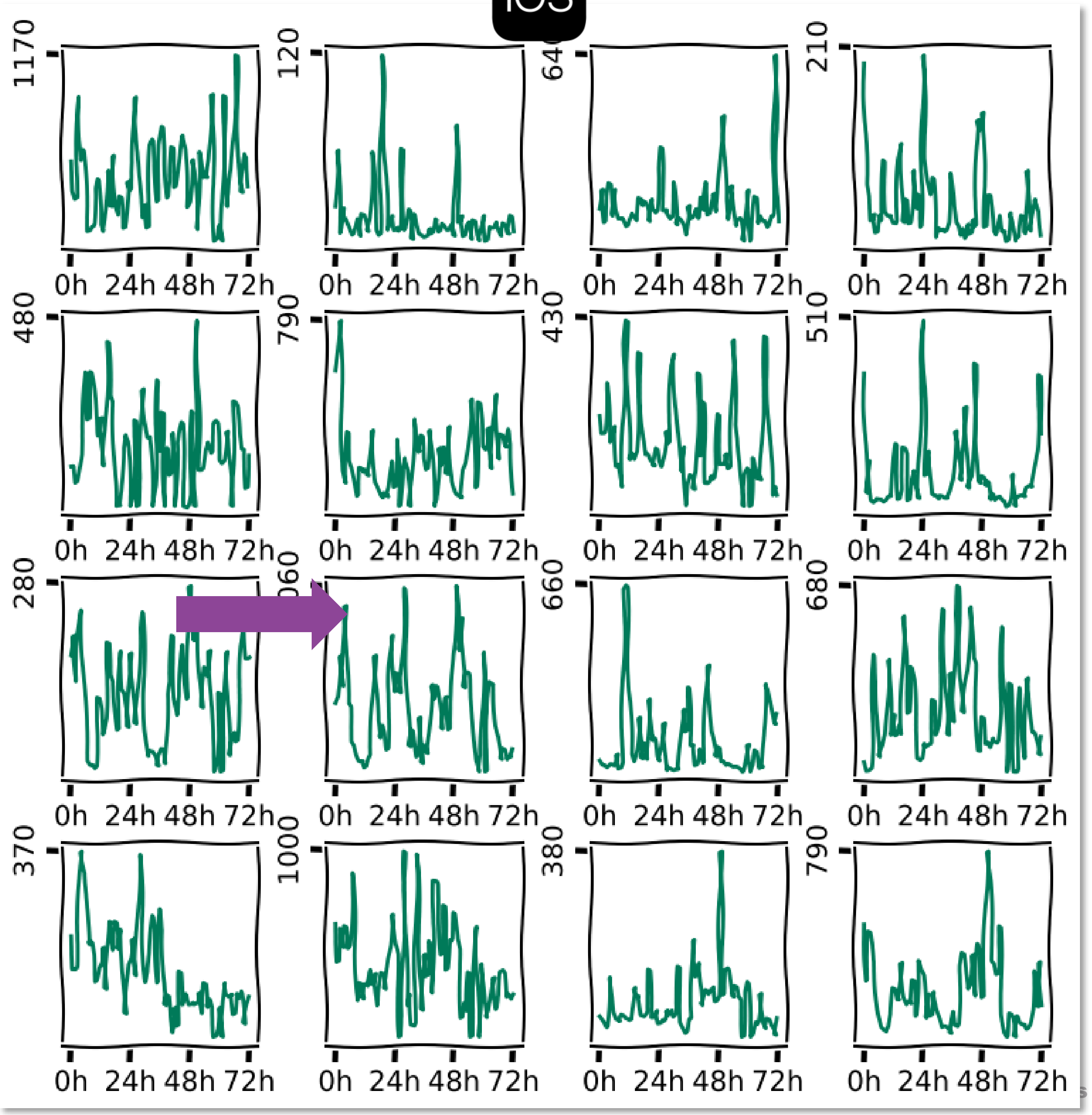
DNS requests as patterns



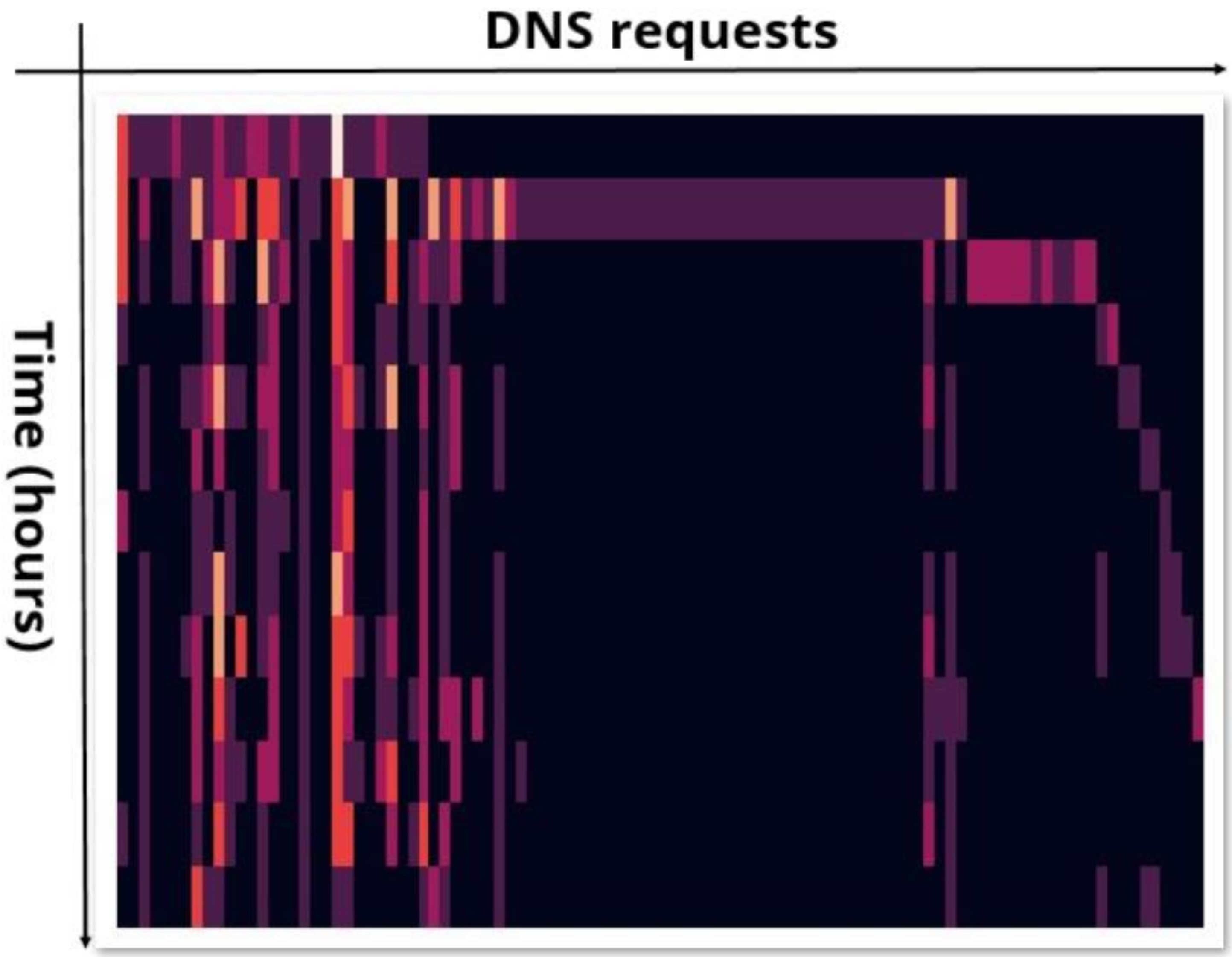
Number of requests



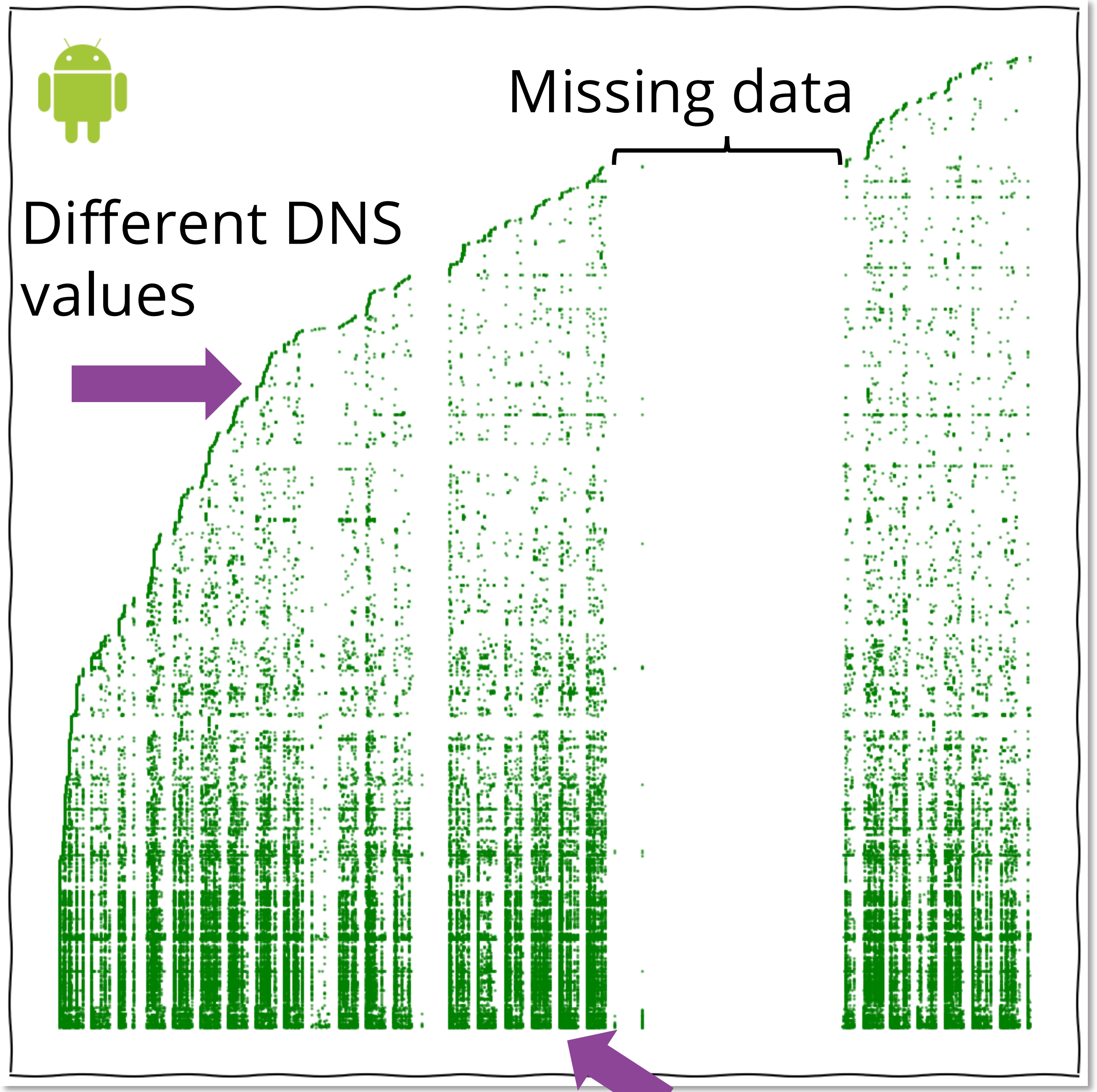
iOS

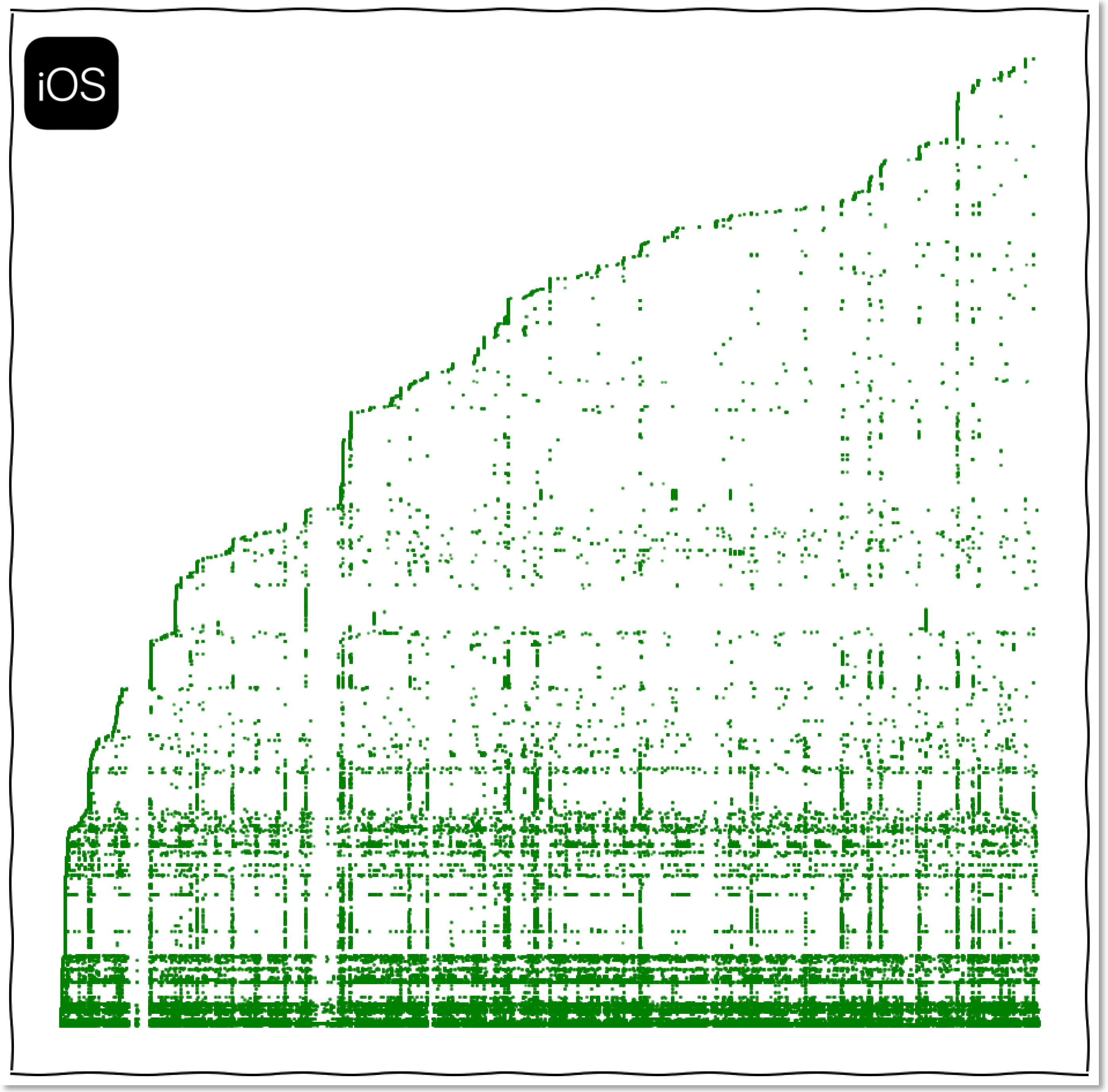


Hourly requests

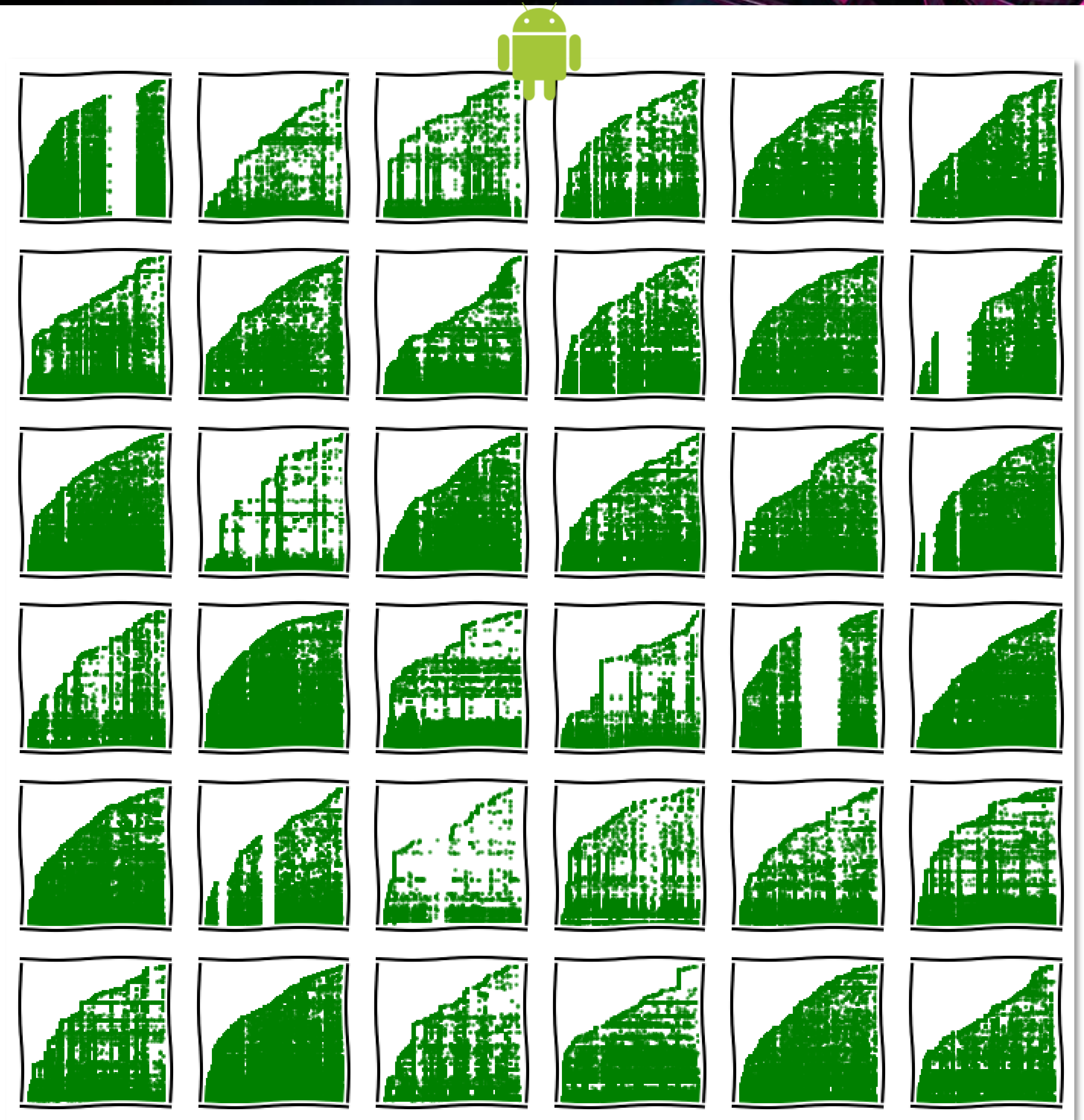


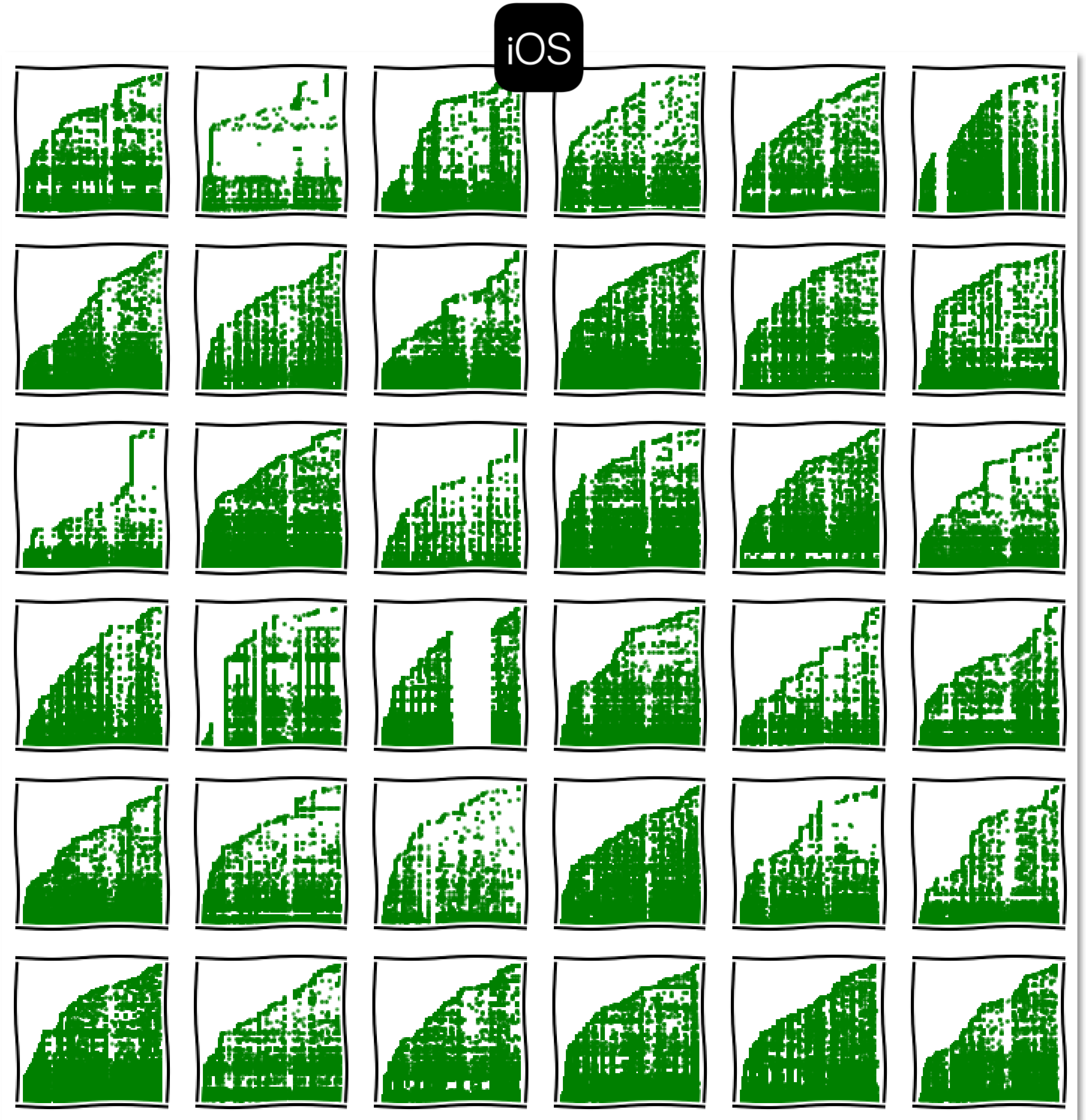
Android vs iOS – requests/domain





Android vs iOS – requests/domains



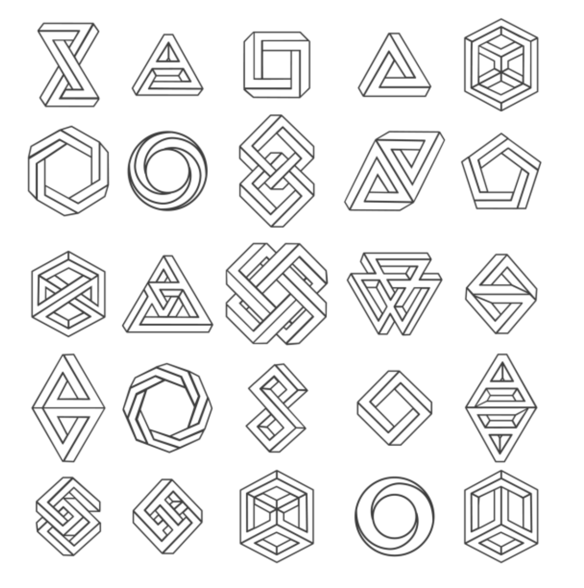


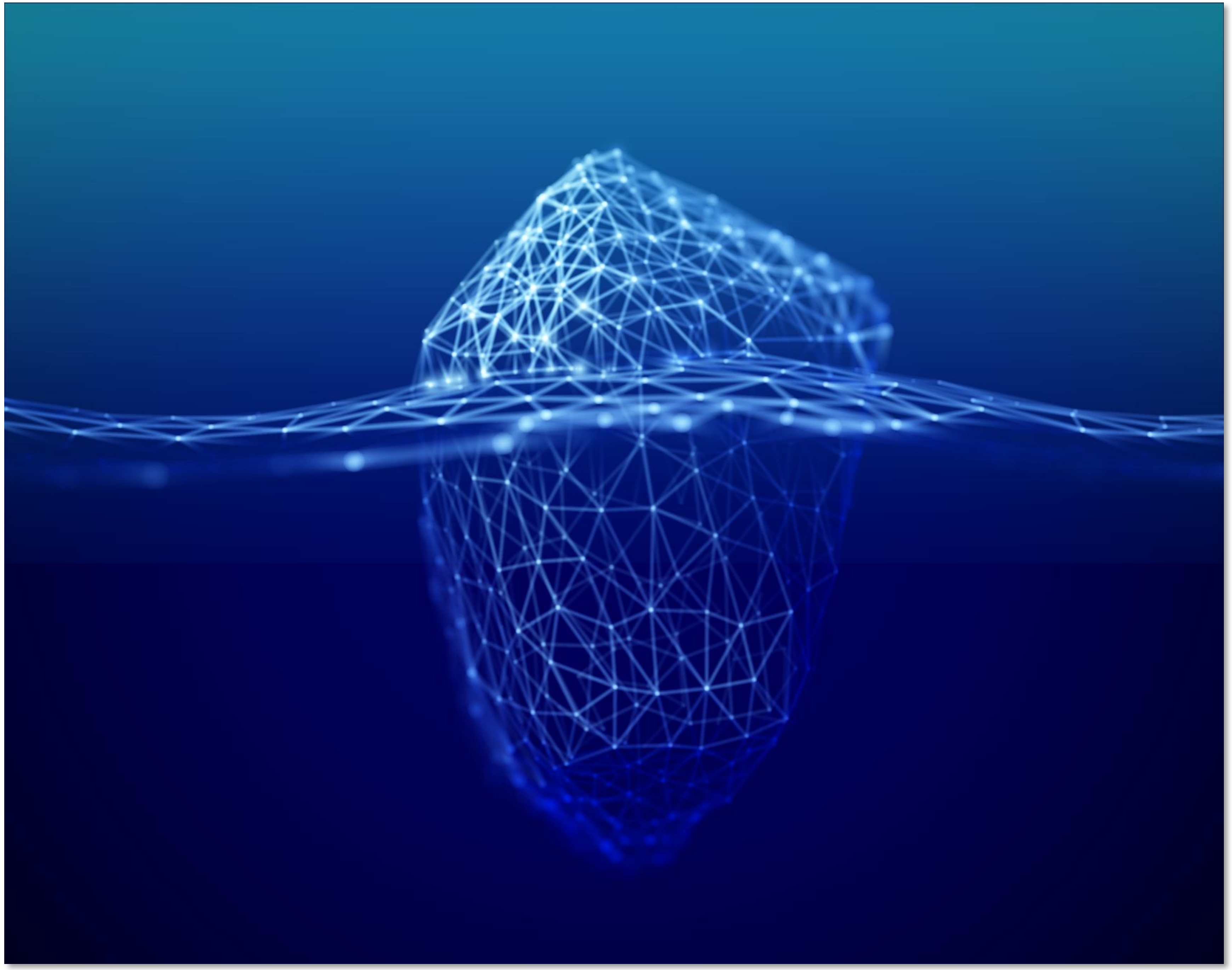
DNS request data processing

Technical challenges

1

Categorical values





2

Large number of requests

Challenge 1: Encoding

- In general, algorithms are good with numbers, bad with strings
- We need to transform strings to numbers

Domain
play.googleapis.com
itunes.apple.com
captive.apple.com
youtube.com
facebook.com

One-hot encoding

play.googleapis .com	itunes.apple .com	captive.apple .com	youtube.com	facebook.com
1	0	0	0	0
0	1	0	0	0
0	0	1	0	0
0	0	0	1	0
0	0	0	0	1

Label encoding

2	1	0	3	4

Feature hashing

288	12	98	45	187

Traditional encoding - drawbacks

One-hot encoding ✗

play.googleapis.com	itunes.apple.com	captive.apple.com	youtube.com	facebook.com
1	0	0	0	0
0	1	0	0	0
0	0	1	0	0
0	0	0	1	0
0	0	0	0	1

- High dimensionality
- Sparsity
- Lack of ordinal relationship
- Scalability issues
- Potential overfitting

Label encoding ✗

2	1	0	3	4

- Imposes ordinal relationship
- Unsuitable for algorithms relying on distance (e.g., linear regression)
- Risk of unintended bias

Feature hashing ✗

288	12	98	45	187

- Hash collision
- Irreversible mapping
- Difficult to find optimal hash function

Eureka! Word encoding

- View DNS requests as word sequences in a ***document/trace***
- Inspiration from the field of Natural Language Processing (NLP)
- Compute the ***Term Frequency-Inverse Document Frequency***

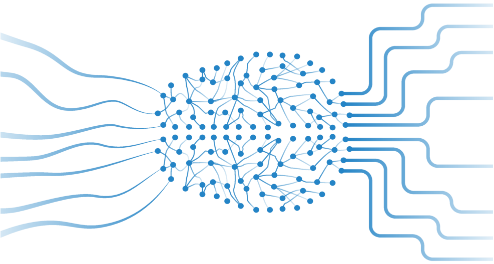
Term frequency (TF): how often a term appears in a trace
Inverse document frequency (IDF): how rare the term is across traces

Android

```
cl4.apple.com cl4.apple.com gspe19-
ssl.ls.apple.com gspe19-ssl.ls.apple.com
ocsp.digicert.com ocsp.digicert.com 36-
courier.push.apple.com web.facebook.com
web.facebook.com 11-courier.push.apple.com
gateway.facebook.com chat-e2ee.facebook.com
itunes.apple.com itunes.apple.com
mask.icloud.com mask.icloud.com
```

Repetitive requests

vs.



iOS

```
amazon.com kinapp-notifications-
na.amazon.com fls-na.amazon.com
unagi.amazon.com m.media-amazon.com
api.weather.com api.account.samsung.com
kinapp-notifications-na.amazon.com
amazon.com api.audible.com m.media-
amazon.com fls-na.amazon.com...
api.weather.com auth.simplisafe.com
cdn.contentful.com sdk.iad-06.braze.com
```

Repetitive requests

Adopted encoding

Term Frequency-Inverse Document Frequency: **TF-IDF**

- ☑ Suitable for string-based processing
- ☑ Quantifies term (word) frequency
- ☑ Highlights terms that are not common across all traces
- ☑ Scales well
- ☑ Low risk for bias

TF-IDF value

- The term **is common** across documents or **is less frequent** in the document
- The term **is less useful** to distinguish this document from others

- The term **appears frequently** in a document, but is not that frequent in other documents
- The term **is important / unique** to that document

TF-IDF: example

Example traces
1 The **Black Hat** conference always **rocks** with exciting talks
2 My friend thinks **Black Hat rocks**
3 **Black Hat rocks** the tech world with new talks

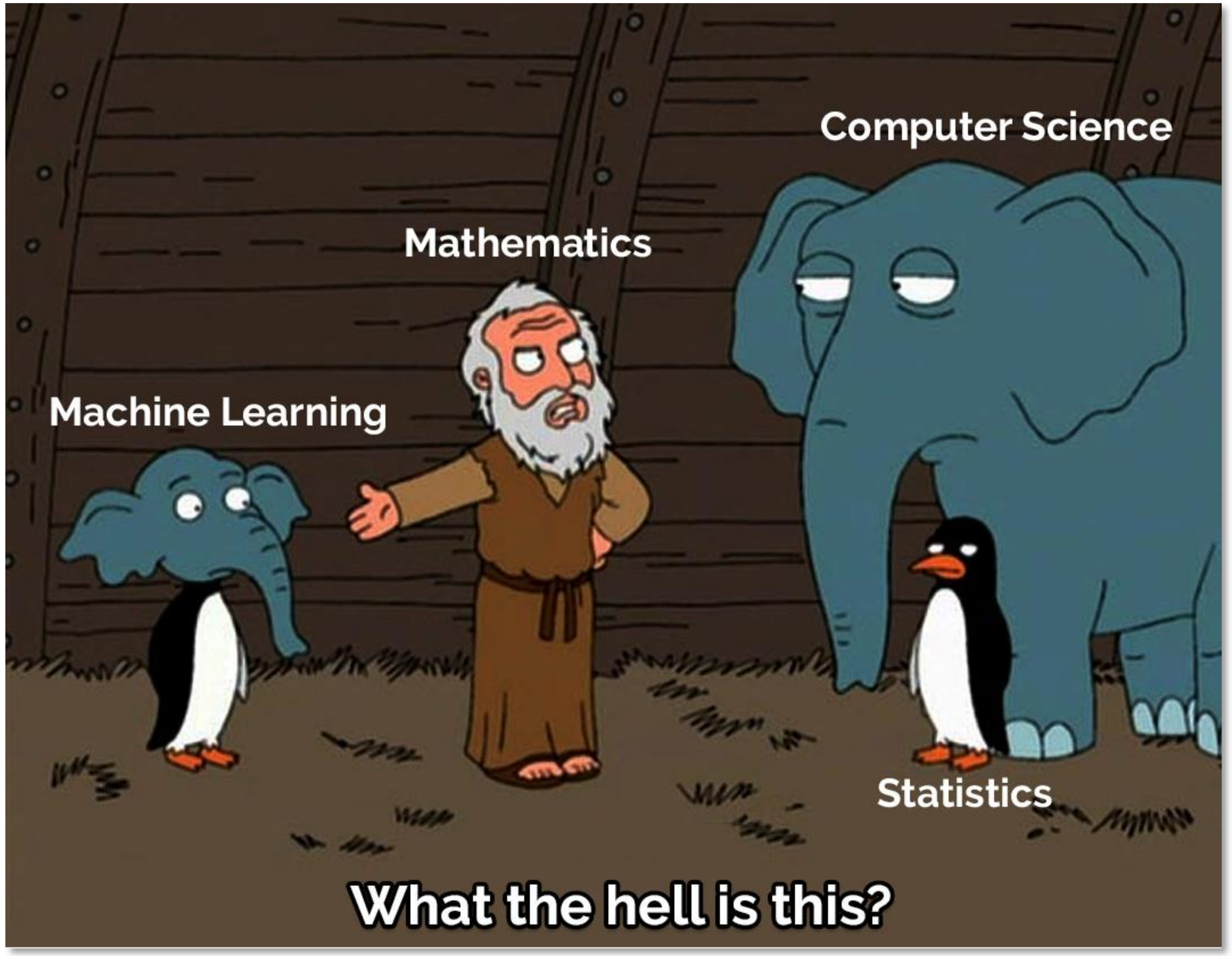
Inverse document frequency: idf

the	black	hat	conference	always	rocks	with	exciting	talks	my	friend	thinks	tech	world	new
1.0	0.7123	0.7123	1.4055	1.4055	0.7123	1.0	1.4055	1.0	1.4055	1.4055	1.4055	1.4055	1.4055	1.4055

tf-idf

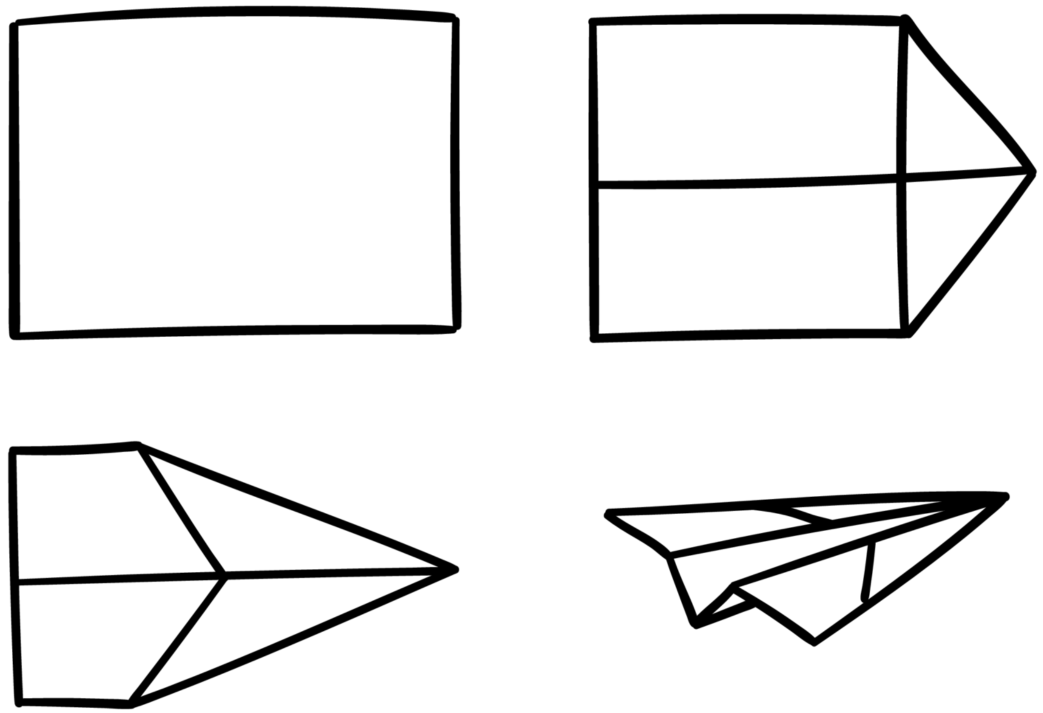
	the	black	hat	conference	always	rocks	with	exciting	talks	my	friend	thinks	tech	world	new
1	0.1111	0.0791	0.0791	0.1562	0.1562	0.0791	0.1111	0.1562	0.1111	0	0	0	0	0	0
2	0	0.1187	0.1187	0	0	0.1187	0	0	0	0.2342	0.2342	0.2342	0	0	0
3	0.1111	0.0791	0.0791	0	0	0.0791	0.1111	0	0.1111	0	0	0	0.1562	0.1562	0.1562

To AI or not to AI?



weights-initialization
hidden-layers
adam
nr-neurons
sgd
metrics
activation-function
learning-rate
adamw
randomness
optimizers

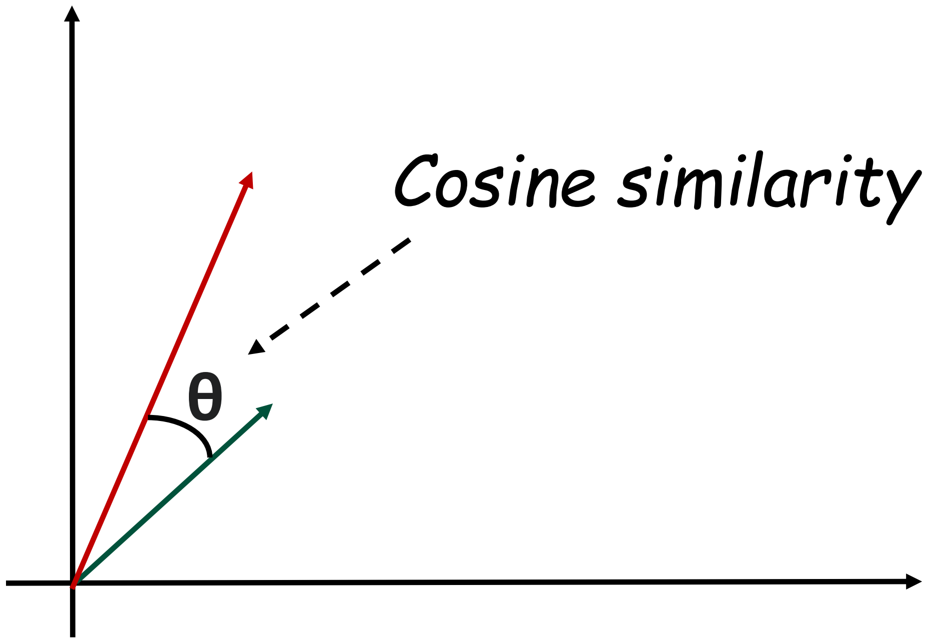
We kept it simple



Compare traces: Cosine similarity

- Preferred approach for measuring similarity between traces
- Handles well high-dimensional, sparse data
- Compares angles, instead of magnitude (i.e., vector length)

Cosine similarity: $$\frac{\vec{A} \cdot \vec{B}}{||\vec{A}|| \times ||\vec{B}||}$$



$\vec{A} \cdot \vec{B}$ Dot product: captures direction and magnitude

$||\vec{A}|| \; ||\vec{B}||$ Denominator: normalize computations

We end up with **direction** (compare ratio of values)

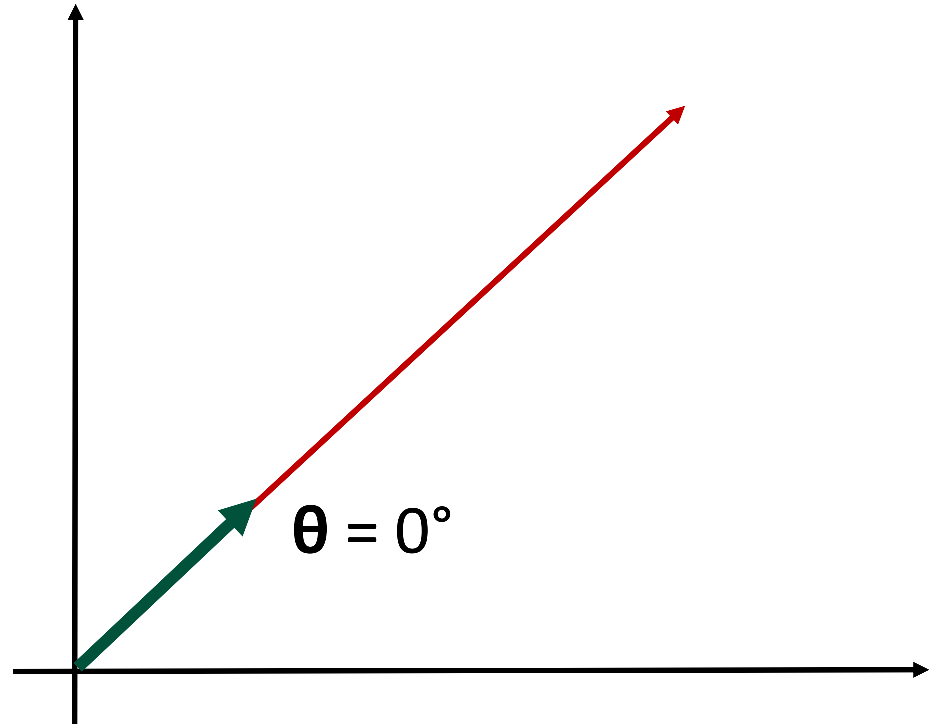
Cosine similarity: Example

Trace 1 *Black Hat*

Trace 2 *Black Hat Black Hat Black Hat*

Vector representation (using raw term counts)

Term	Trace 1: Black Hat	Trace 2: Black Hat Black Hat Black Hat
Black	1	3
Hat	1	3



Vectors: A: [1, 1] B: [3, 3]

Cosine similarity: 1.0 → Vectors point in the same direction
Same words, just repeated – so **they're basically the same**

Euclidean distance: 2.83 → The vectors are far apart in absolute space
They're far apart numerically – so **they're different**

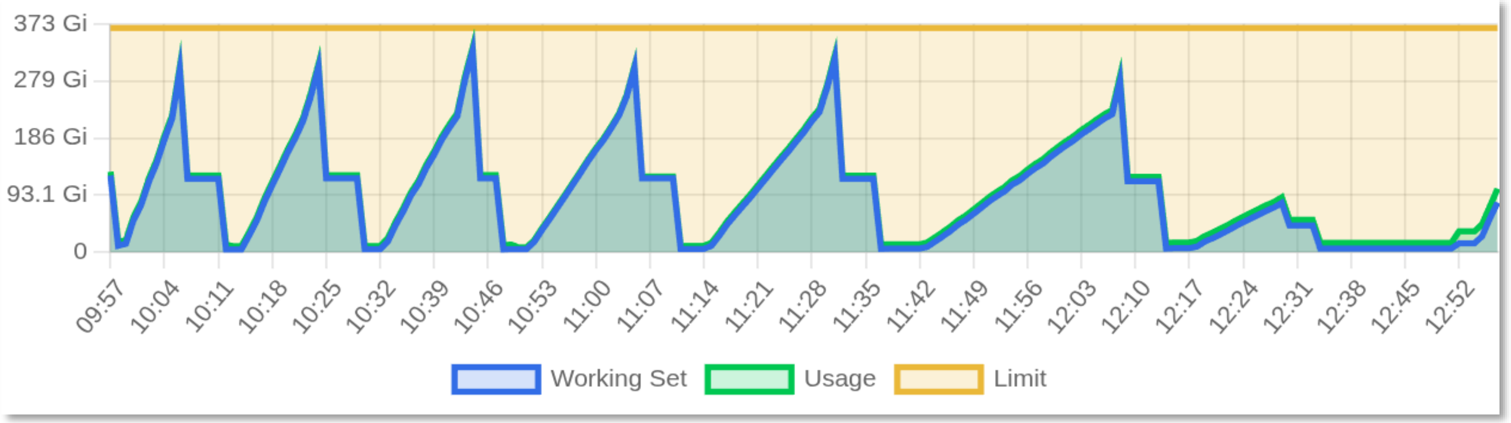
Challenge 2: Data size

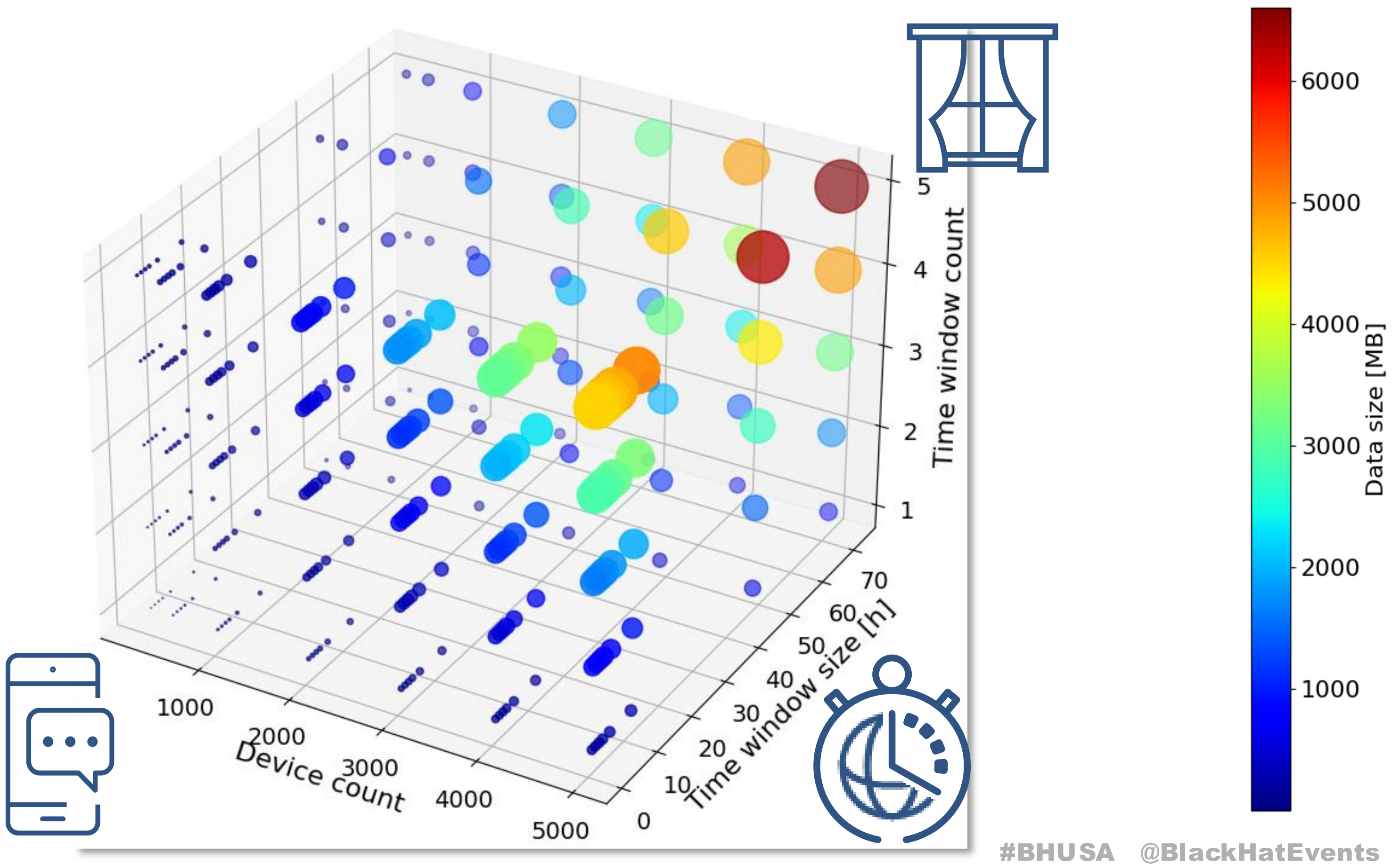
- Cannot fit all data in memory!

- Three key parameters:
  - Number of devices
  - Number of time windows
  - The size of each time window

- Process **device batches** (**200 … 5000**)

Memory usage: 5k devices x 24 time windows (1 hour each)



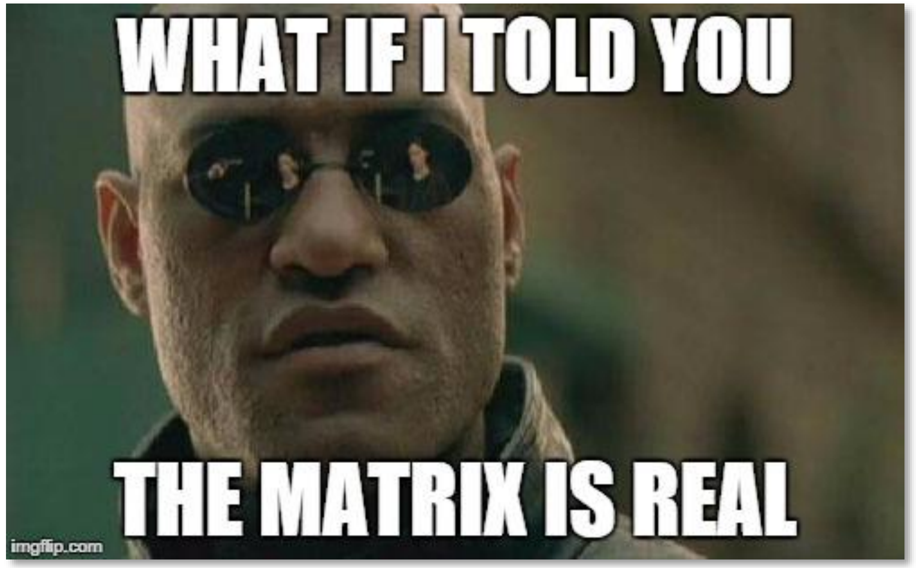


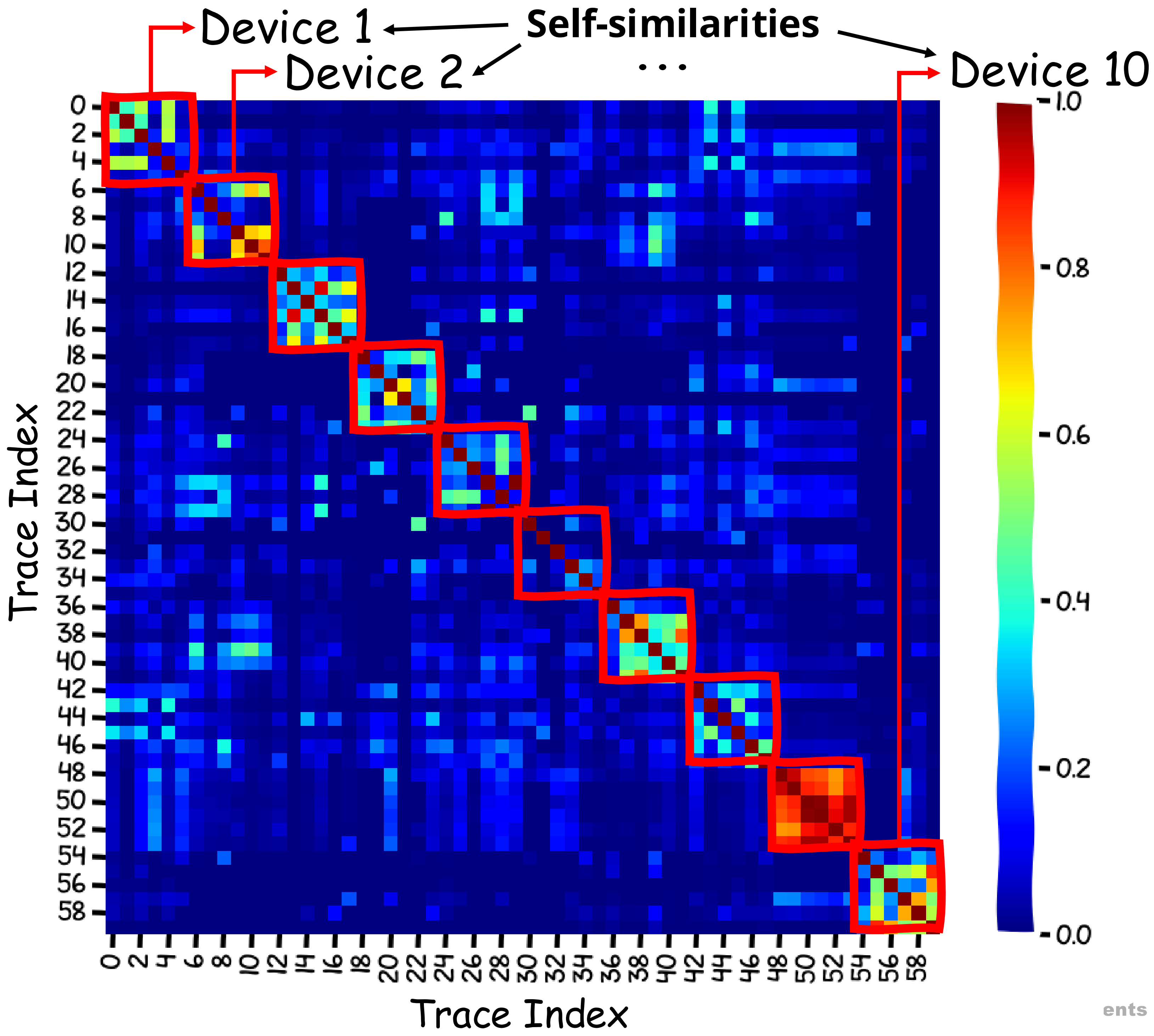
User (device) tracking

Device tracking problem

Analyze the (similarity) matrix

- ☑ Symmetric
- ☑ Each "dot" is a similarity between two traces (i.e., DNS request sequences)
- ☑ Self-similarity is on the diagonal





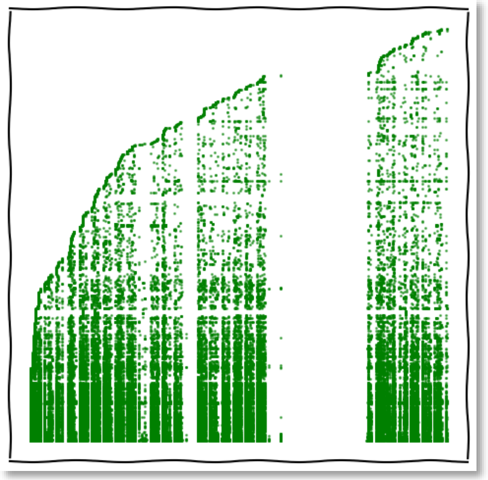
The approach

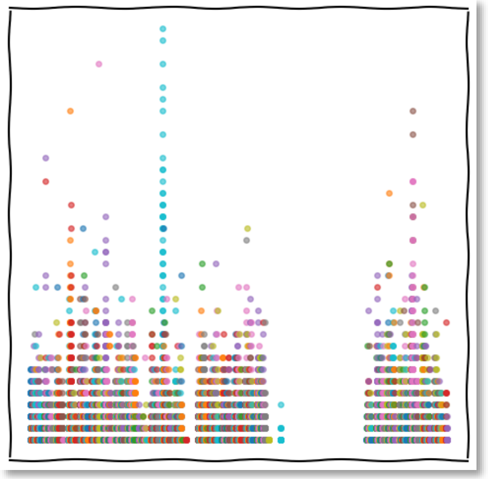
DNS traces

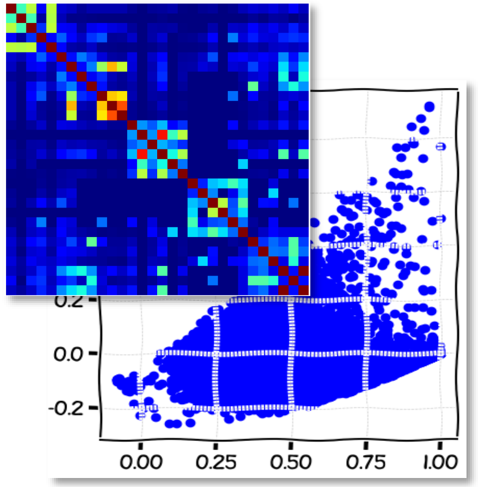
Split in time windows

Compute tf-idf & cosine similarity

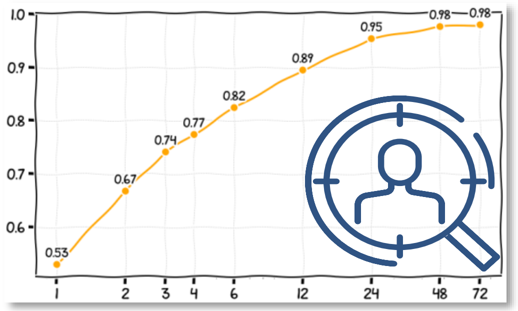
Apply tracking index



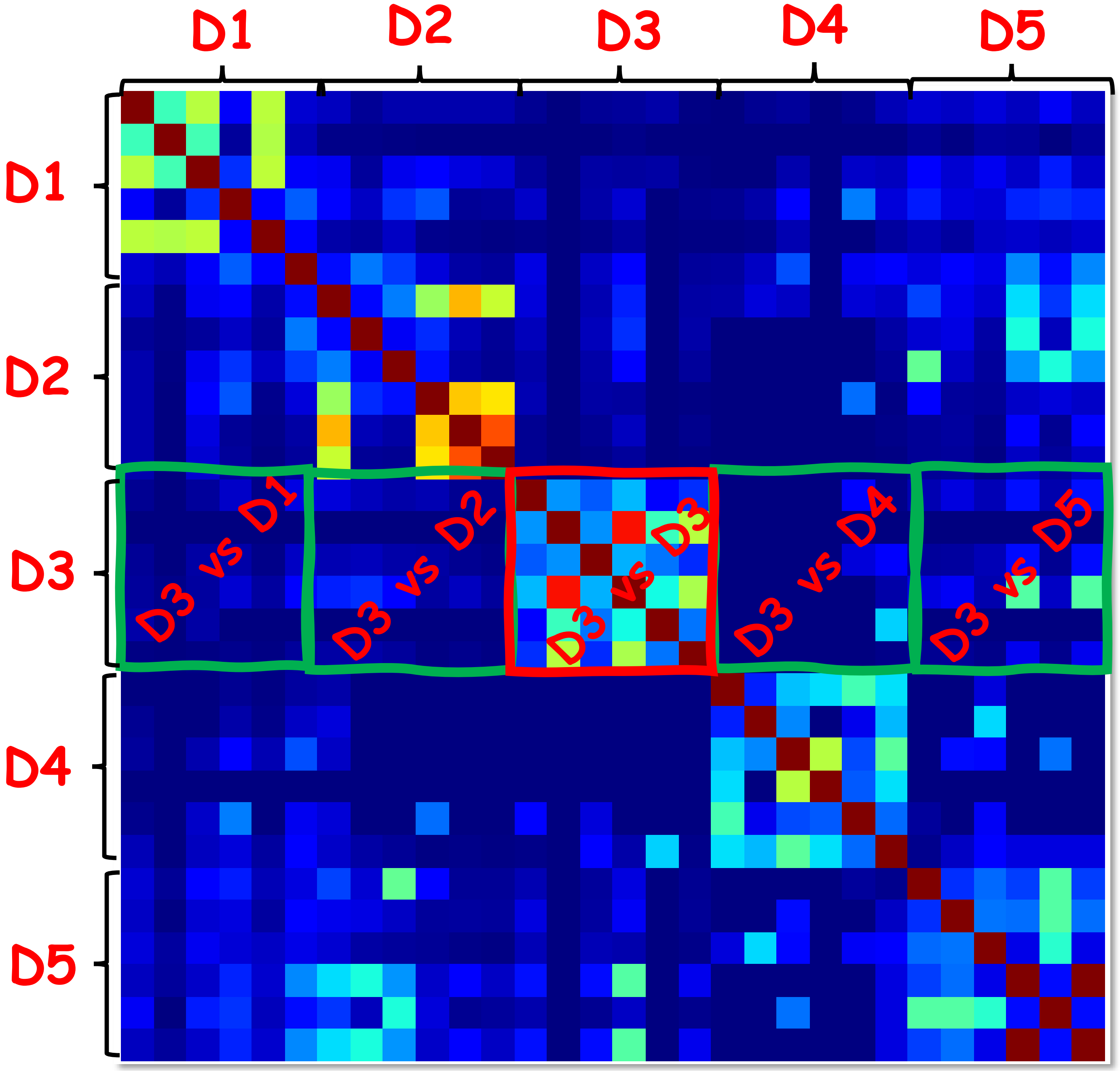




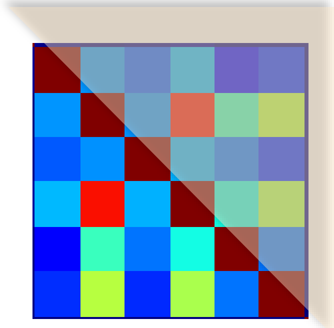
$$T_k = S^s_{kk} - \max_{\forall k,k',k \neq k'} S^c_{kk'}$$



Similarity index computation



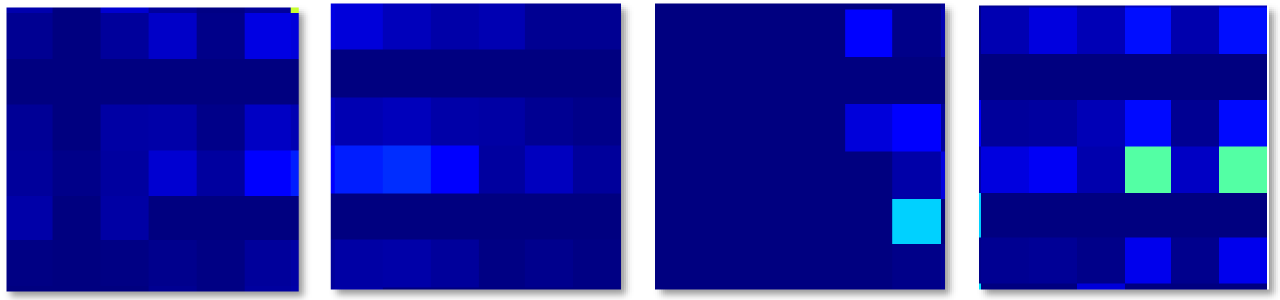
Average self-similarity (*k* = 3)



D3

$$S^{s}_{kk} = \frac{1}{n(n-1)/2} \sum_{i=0}^{n-1} \sum_{j=i+1}^{n-1} M^{kk}_{i,j}$$

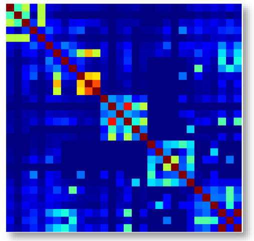
Average cross-similarity (*k* = 3, *k'* = 1, 2, 4, 5)



D1 D2 D4 D5

$$S^{c}_{kk'} = \frac{1}{n^2} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} M^{kk'}_{i,j}$$

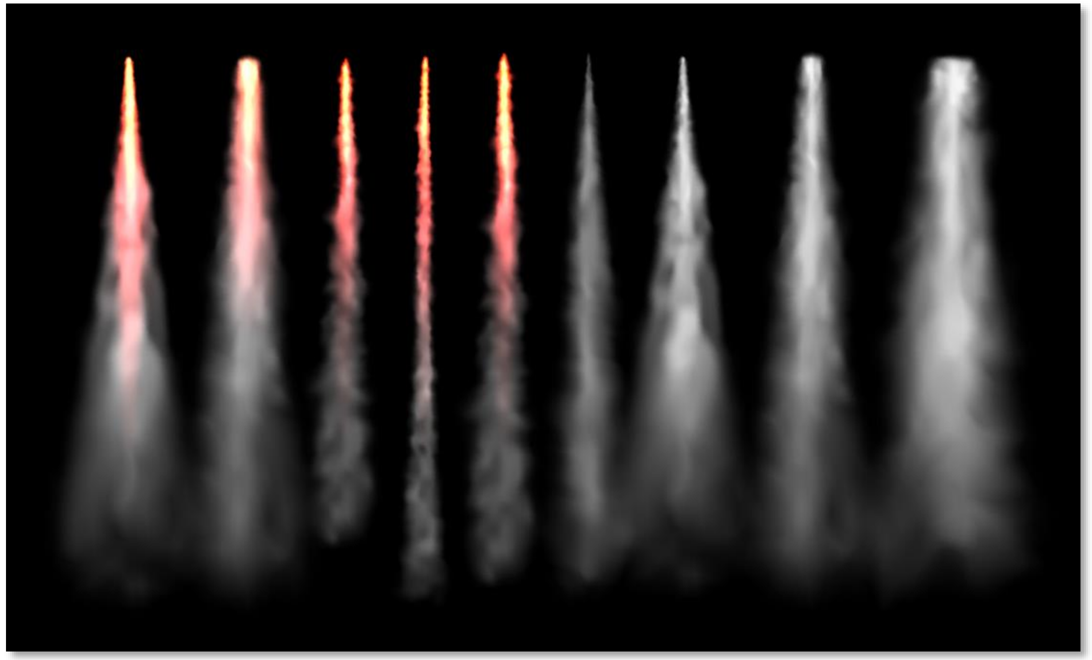
Index for tracking



Tracking index:

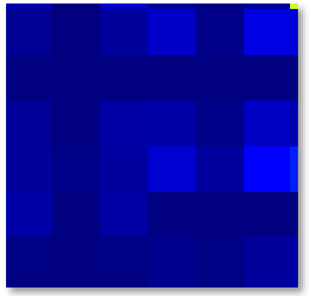
$$T_k = S^s_{kk} - \max_{\forall k,k',k\neq k'} S^c_{kk'}$$

If $T_k > 0$ → Device k is *trackable*

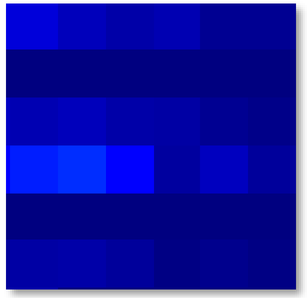


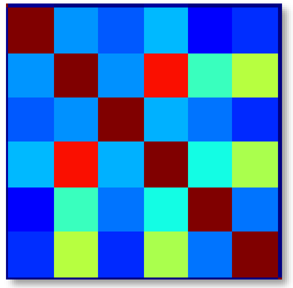
Index for tracking: example

$S^c_{31} = 0.0219$



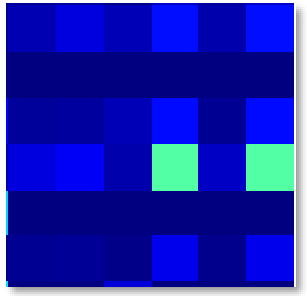
$S^c_{32} = 0.0311$



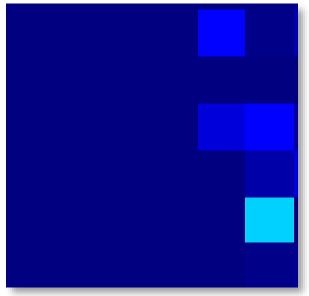


$S^s_{33} = 0.3403$

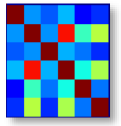
$S^c_{35} = 0.0647$

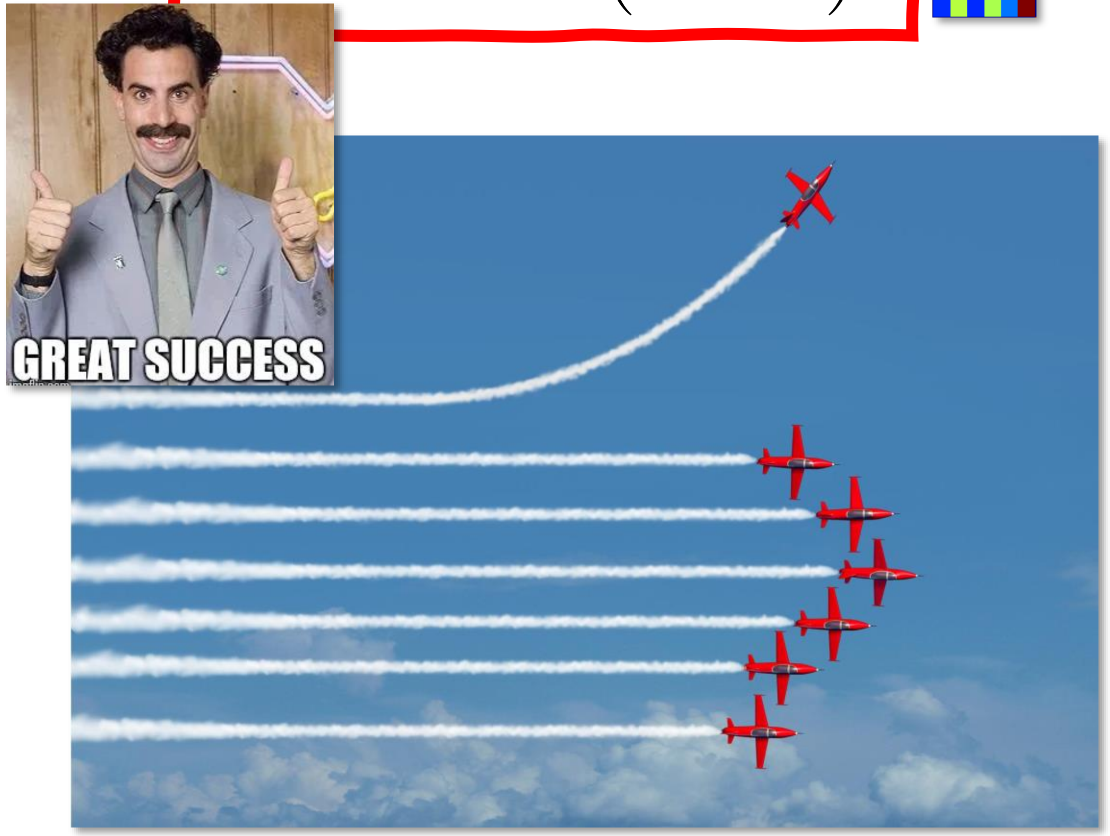


$S^c_{34} = 0.0194$

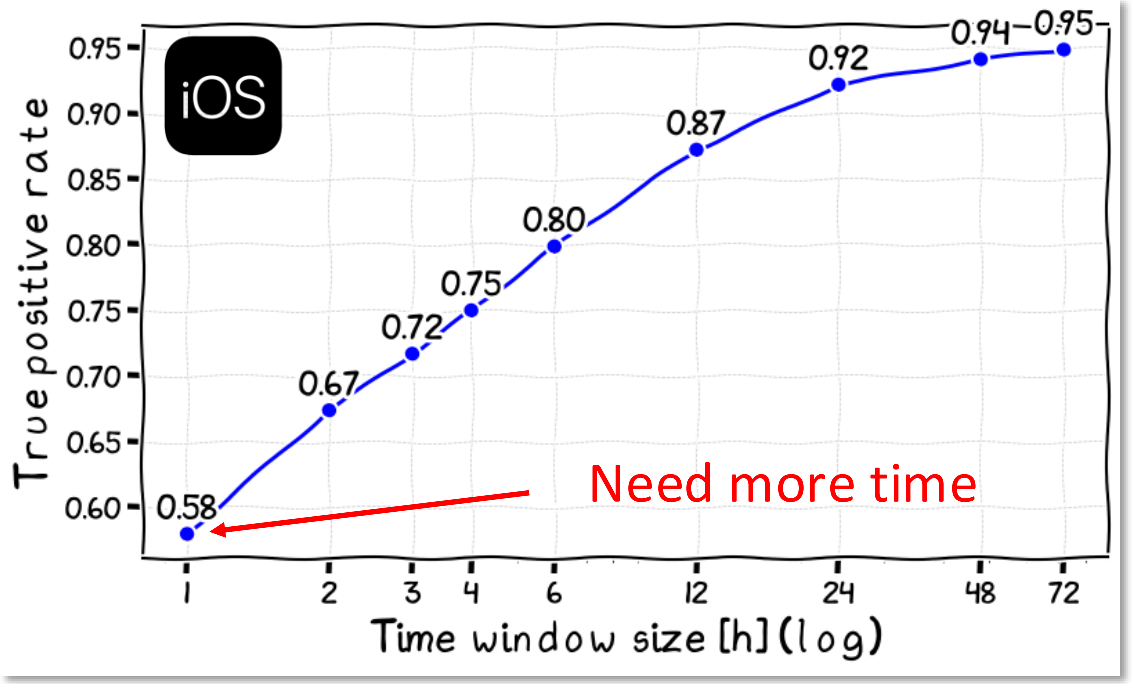


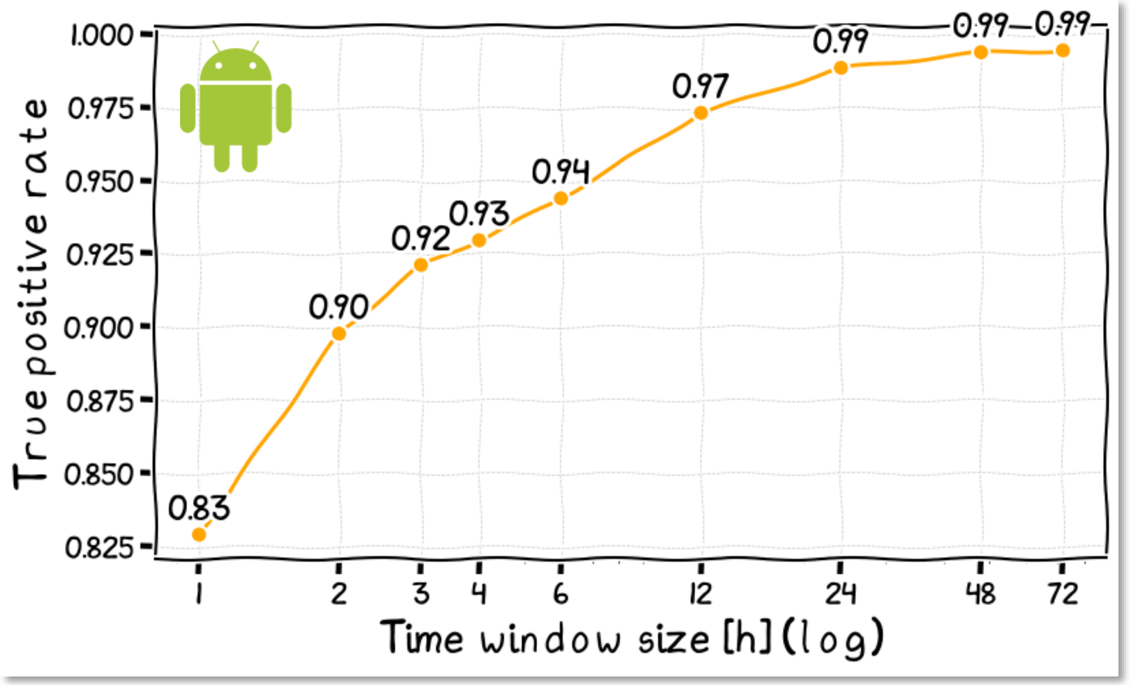
$$
\begin{aligned}
T_3 &= S^s_{33} - S^c_{35} \\
&= 0.3403 - 0.0647 \\
&\boxed{= 0.2756 (> 0!)}
\end{aligned}
$$

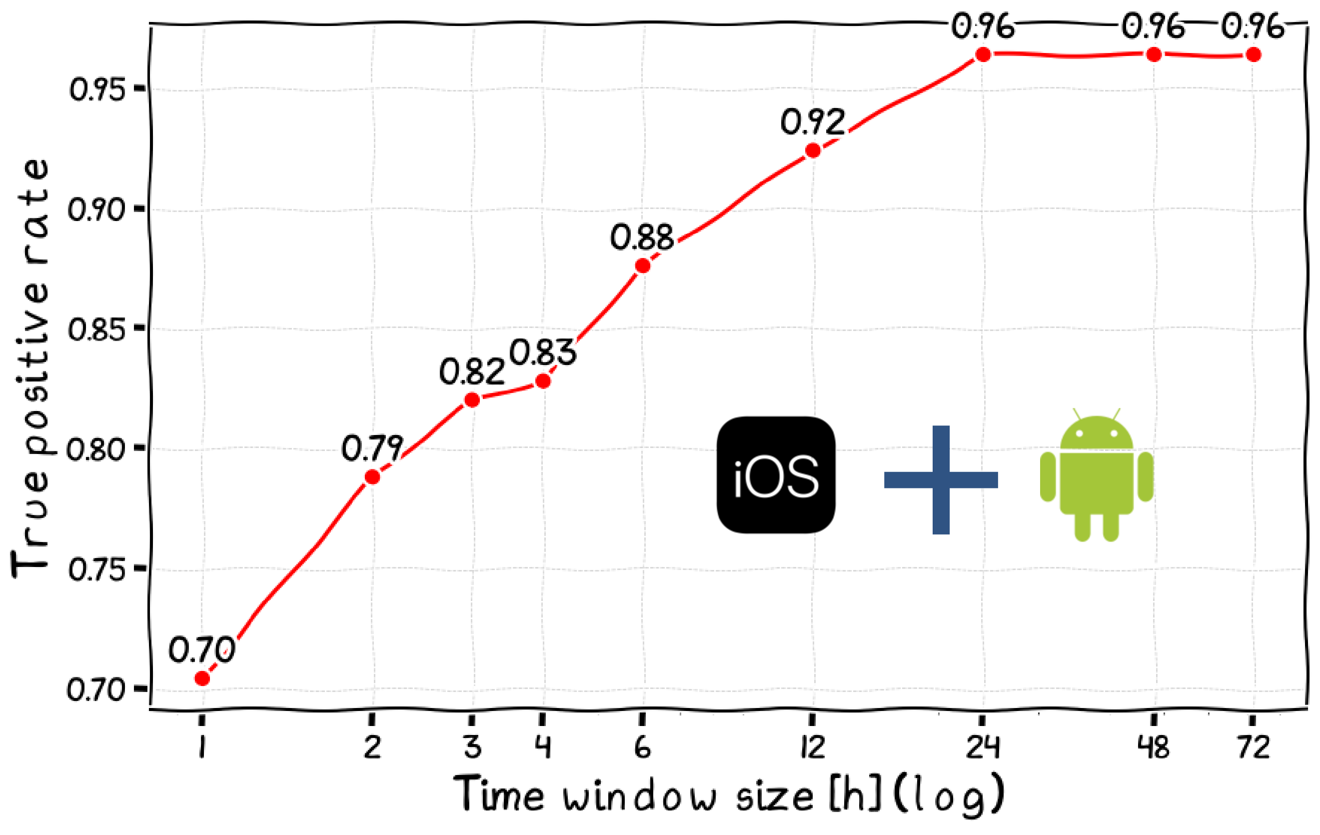




Tracking accuracy: 250 devices





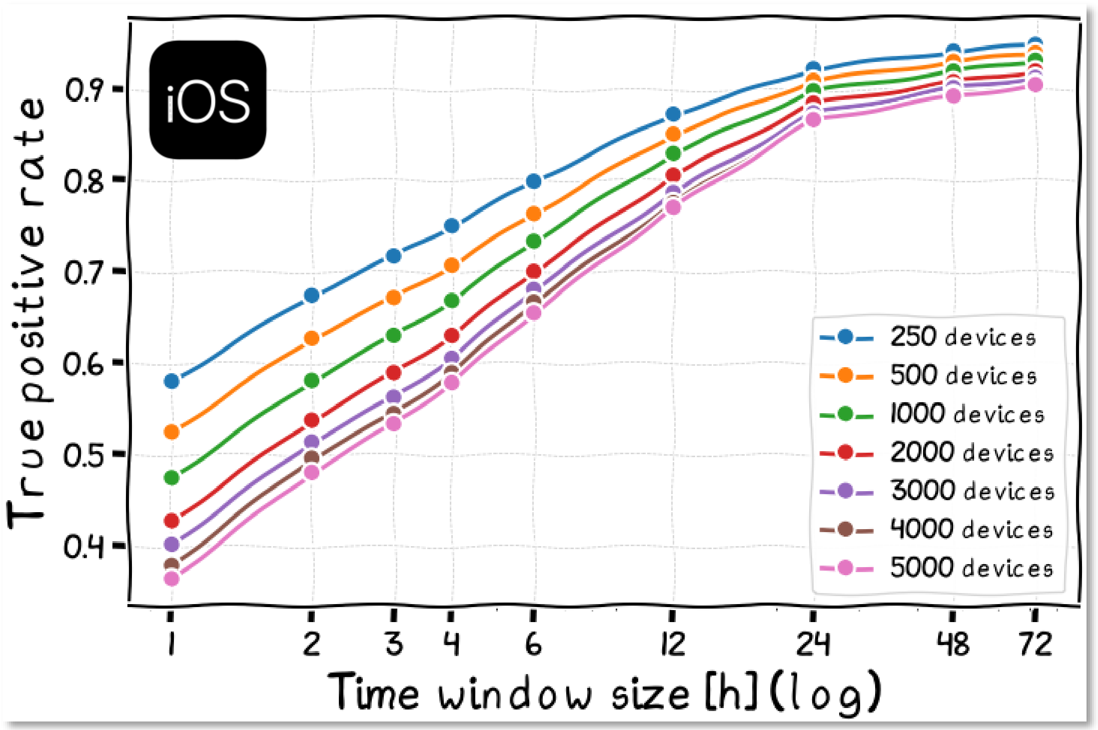


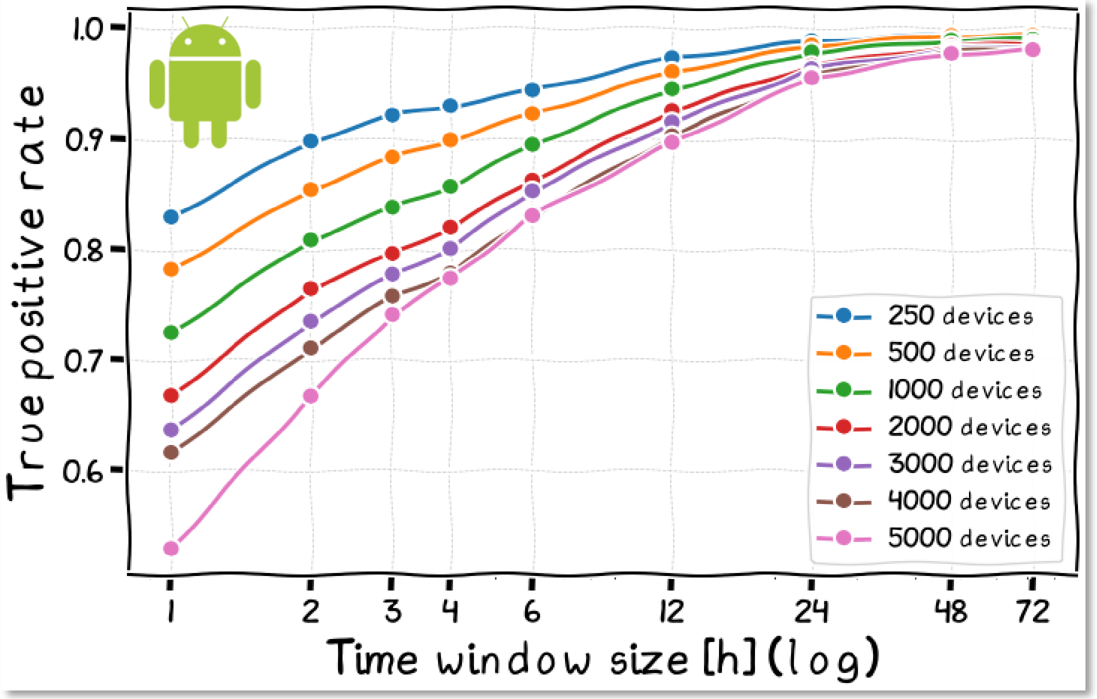
- Larger time windows yield better results
- After 2 hours, **accuracy > 80%**

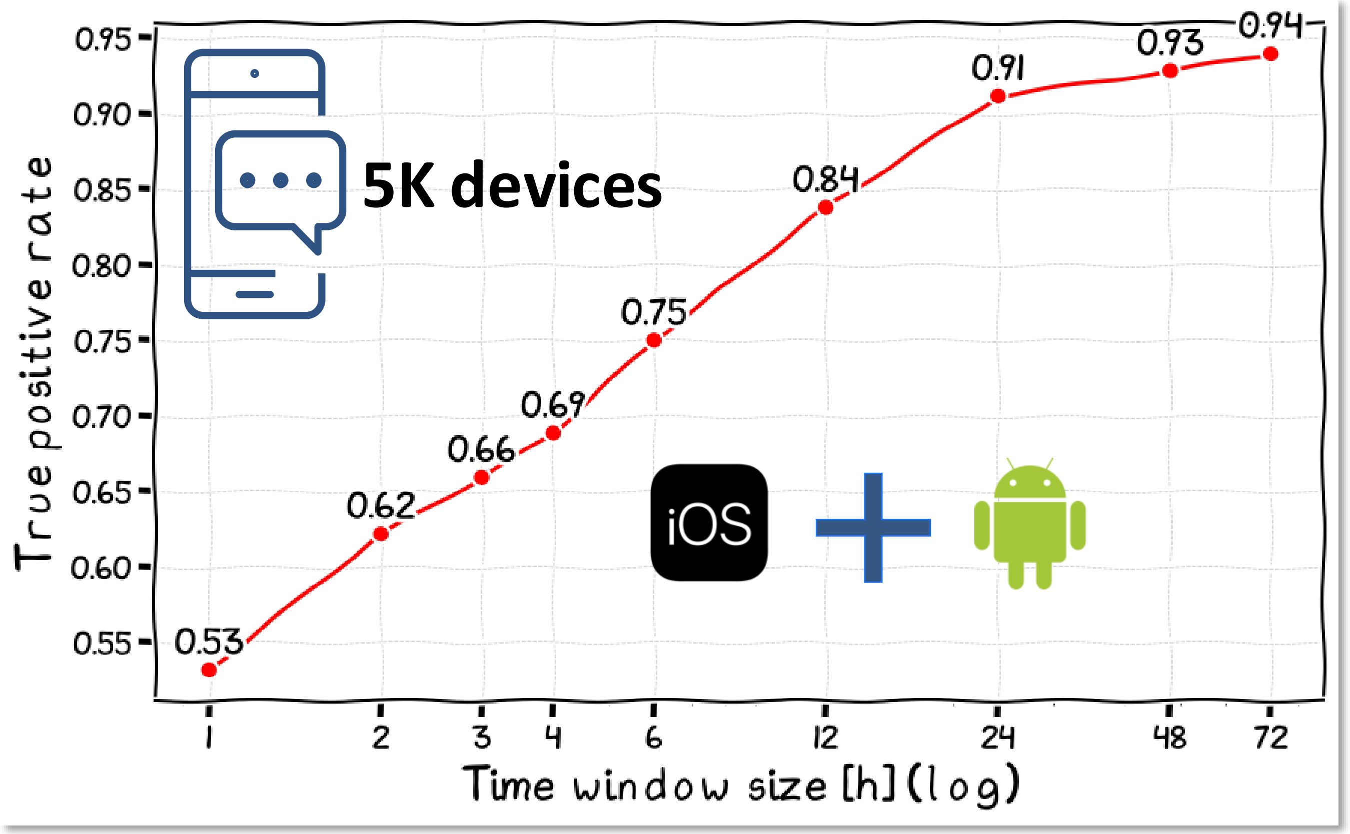
** Used <=12 time windows spread across two weeks*

Lesson 1: change device ID (MAC)

Tracking results: in the crowd



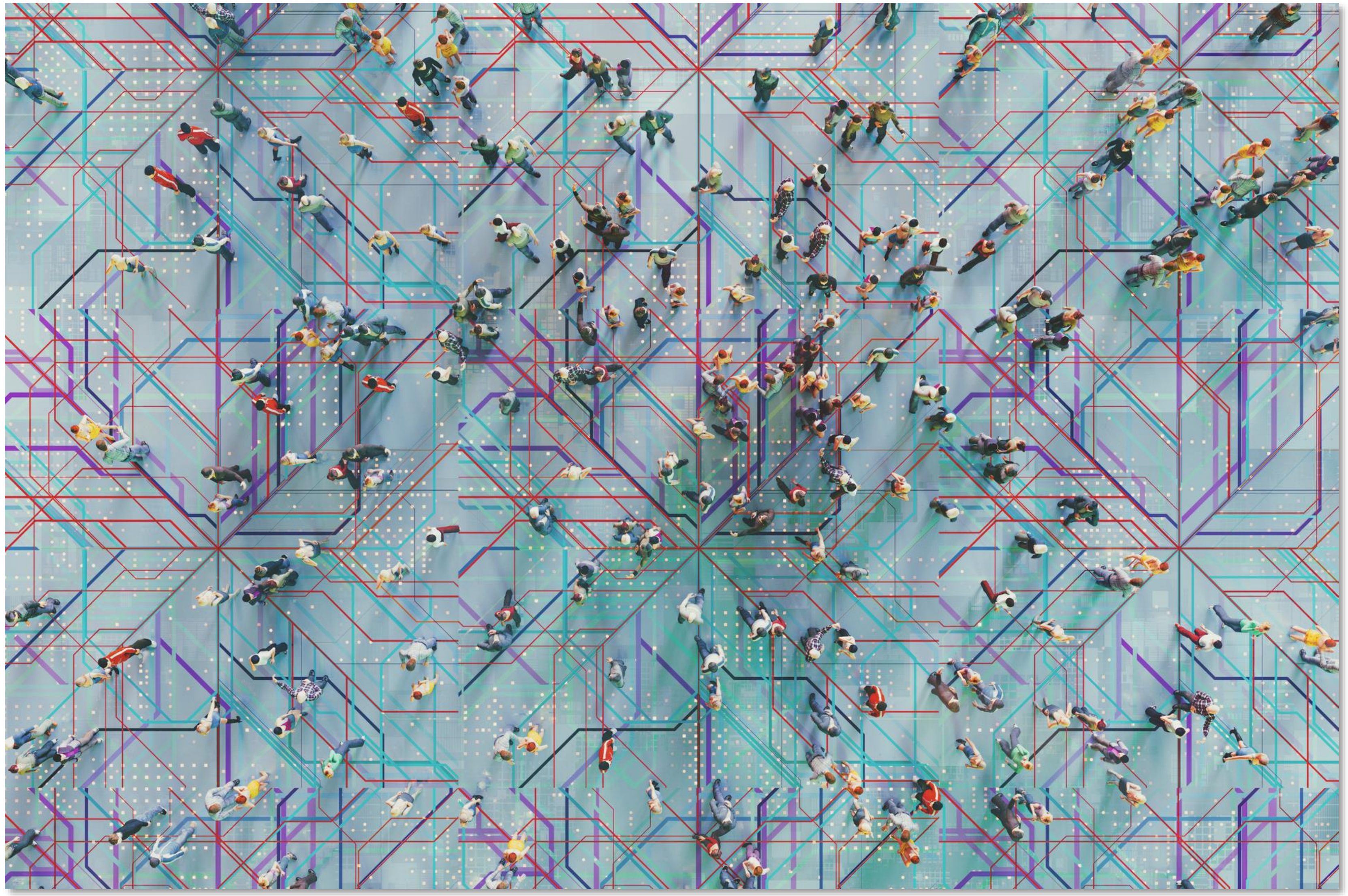




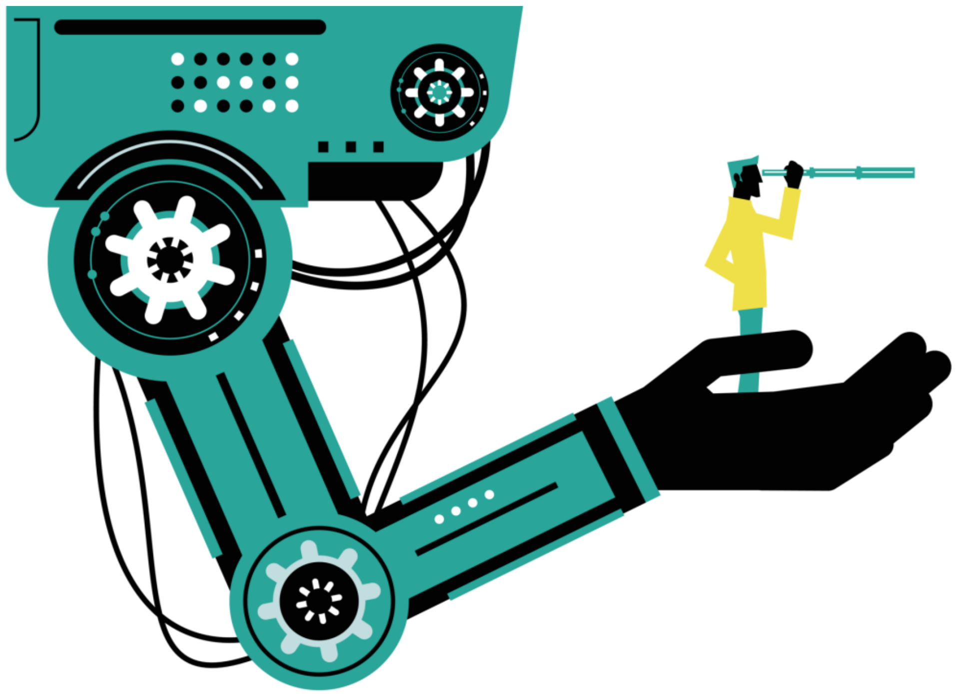
- A larger pool of devices reduce chances of tracking
- 2 hours **accuracy 62%**
- **More time: 90+%**

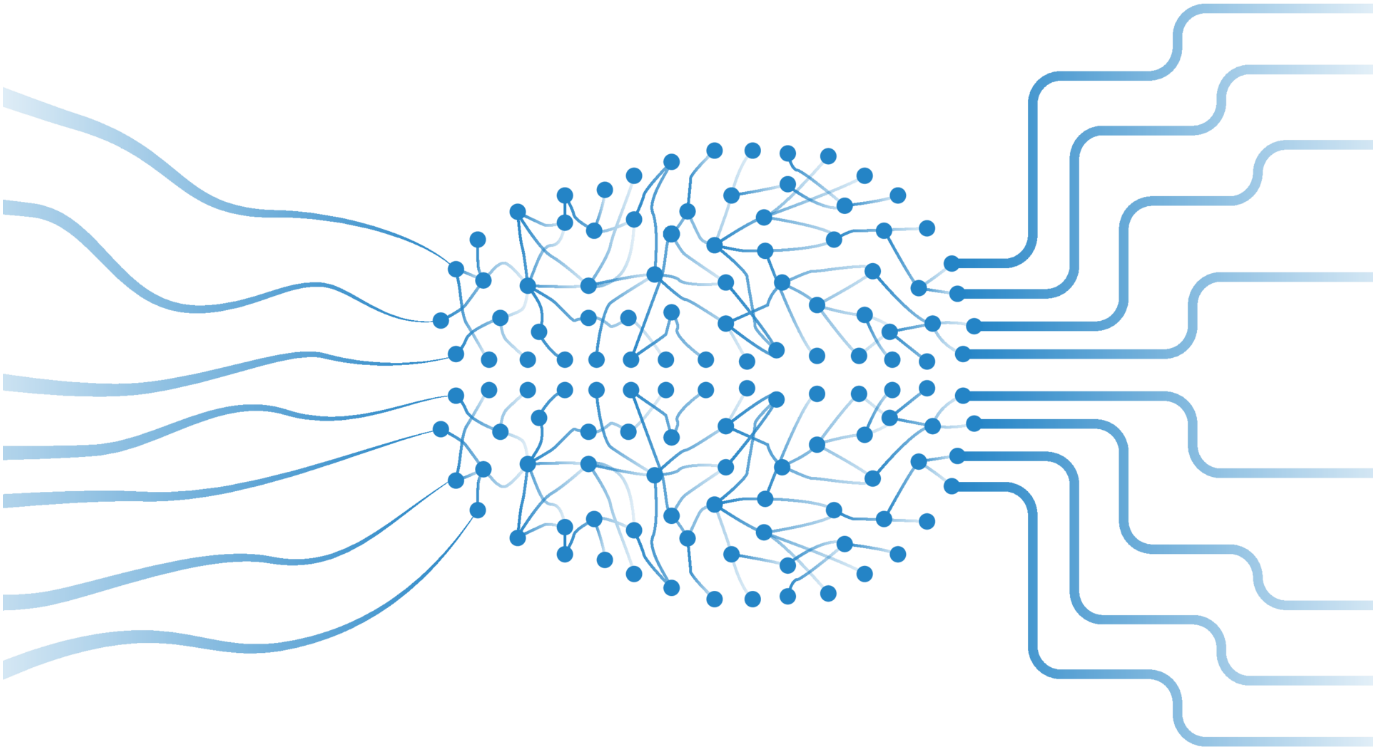
Lesson 2: stay in the crowd

The more crowded, the better (for loosing track)!



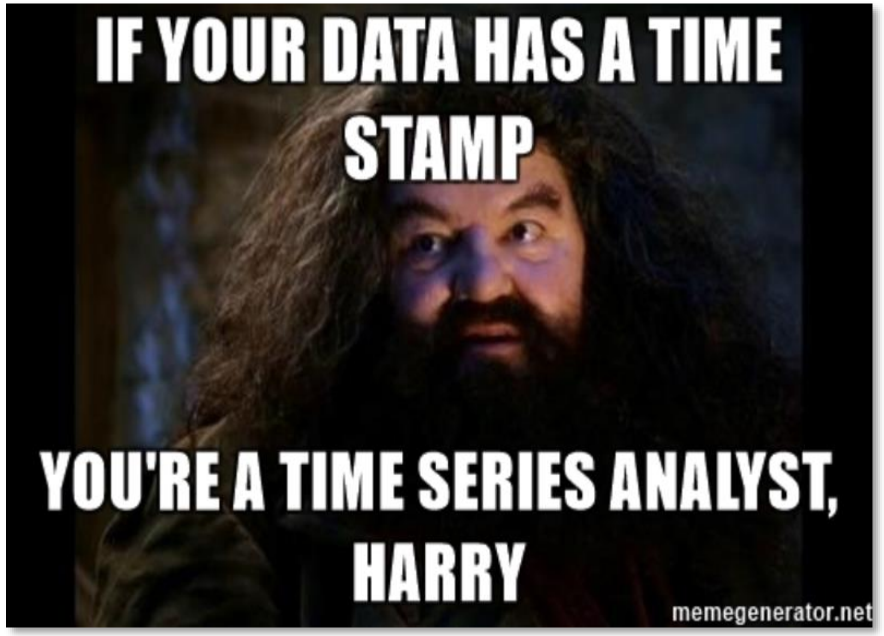
Time for some machine learning

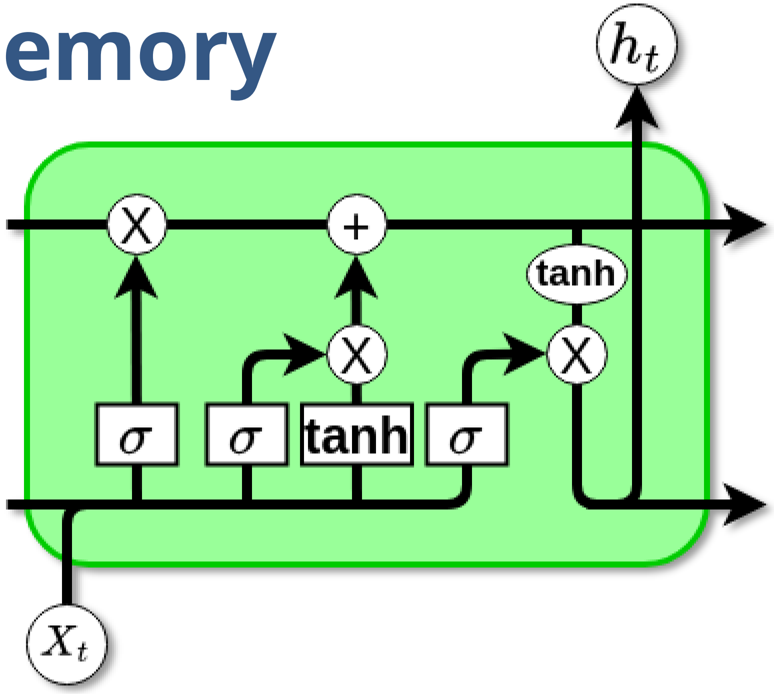


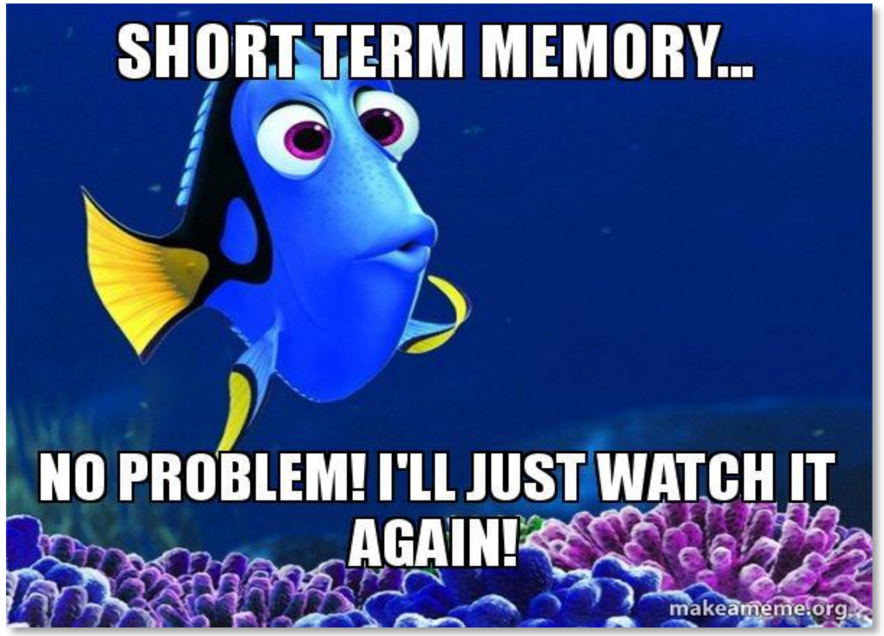


User tracking with memory...

LSTM: Long Short-Term Memory







Use cases:

- Speech recognition
- Time series
- Robot control
- ....

First trials

100 Android

100 iOS

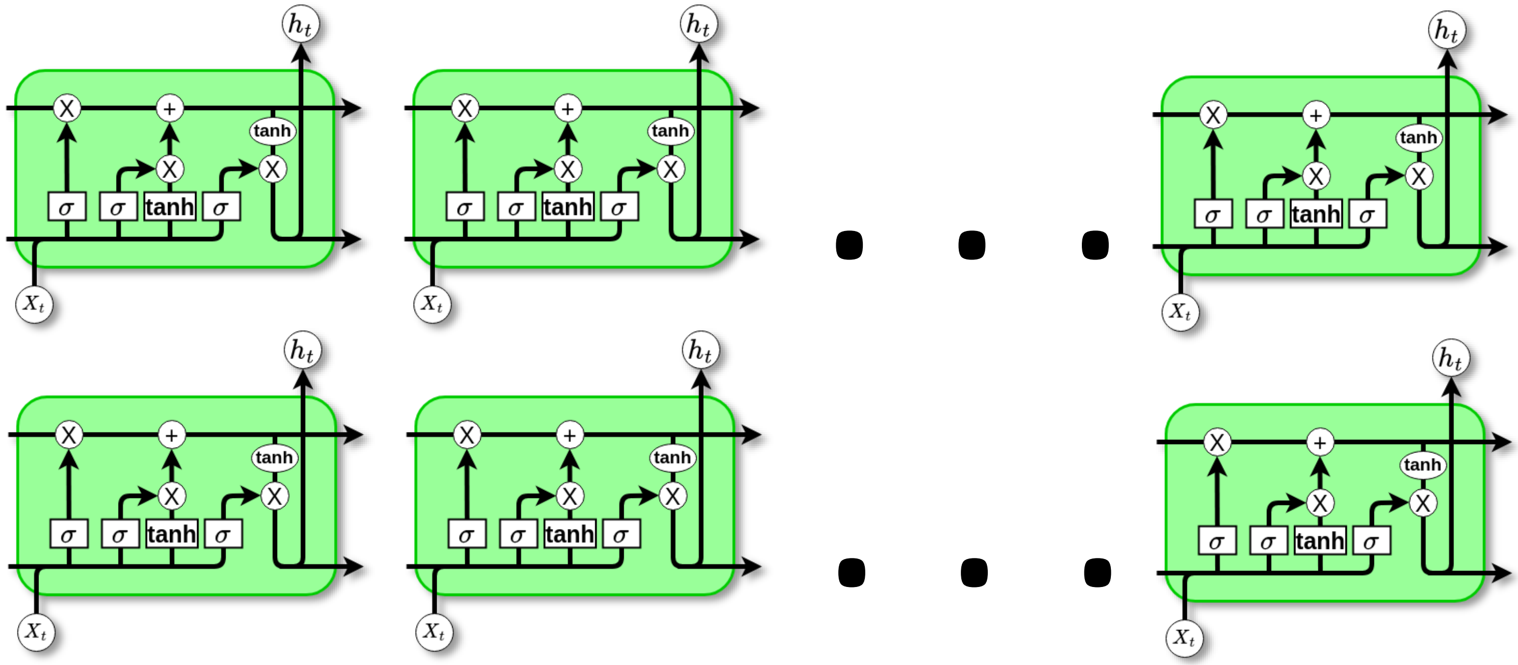
1h

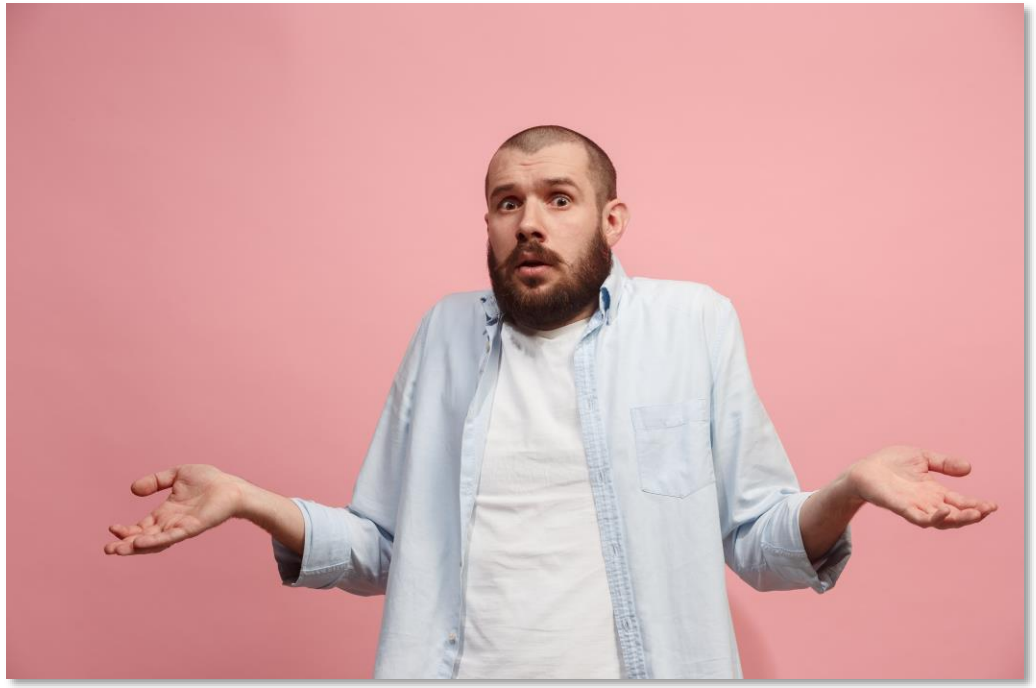
3 weeks

Model	Validation accuracy	Test Accuracy
LSTM - Model 1	83.14%	78.18%
LSTM - Model 2	76.43%	76.43%

Choosing an appropriate model

Adam AdamW SGD



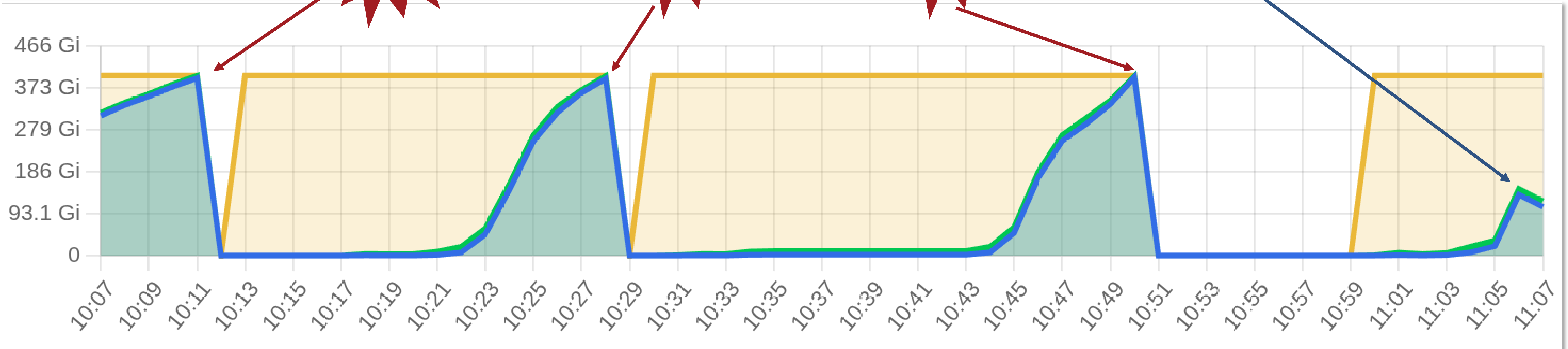


LSTM: hunger for resources

5K phones

Time window

3h	6h	12h	24h
$\begin{pmatrix} 240k & 352k \\ 136k & 352k \\ 171k & 352k \end{pmatrix}$	$\begin{pmatrix} 120k & 348k \\ 69k & 348k \\ 87k & 348k \end{pmatrix}$	$\begin{pmatrix} 64k & 342k \\ 36k & 342k \\ 47k & 342k \end{pmatrix}$	$\begin{pmatrix} 34k & 340k \\ 20k & 340k \\ 26k & 340k \end{pmatrix}$
I'm too big!	Me too...	I was close!	Success!
OOM	OOM	OOM	



*OOM = Out Of Memory

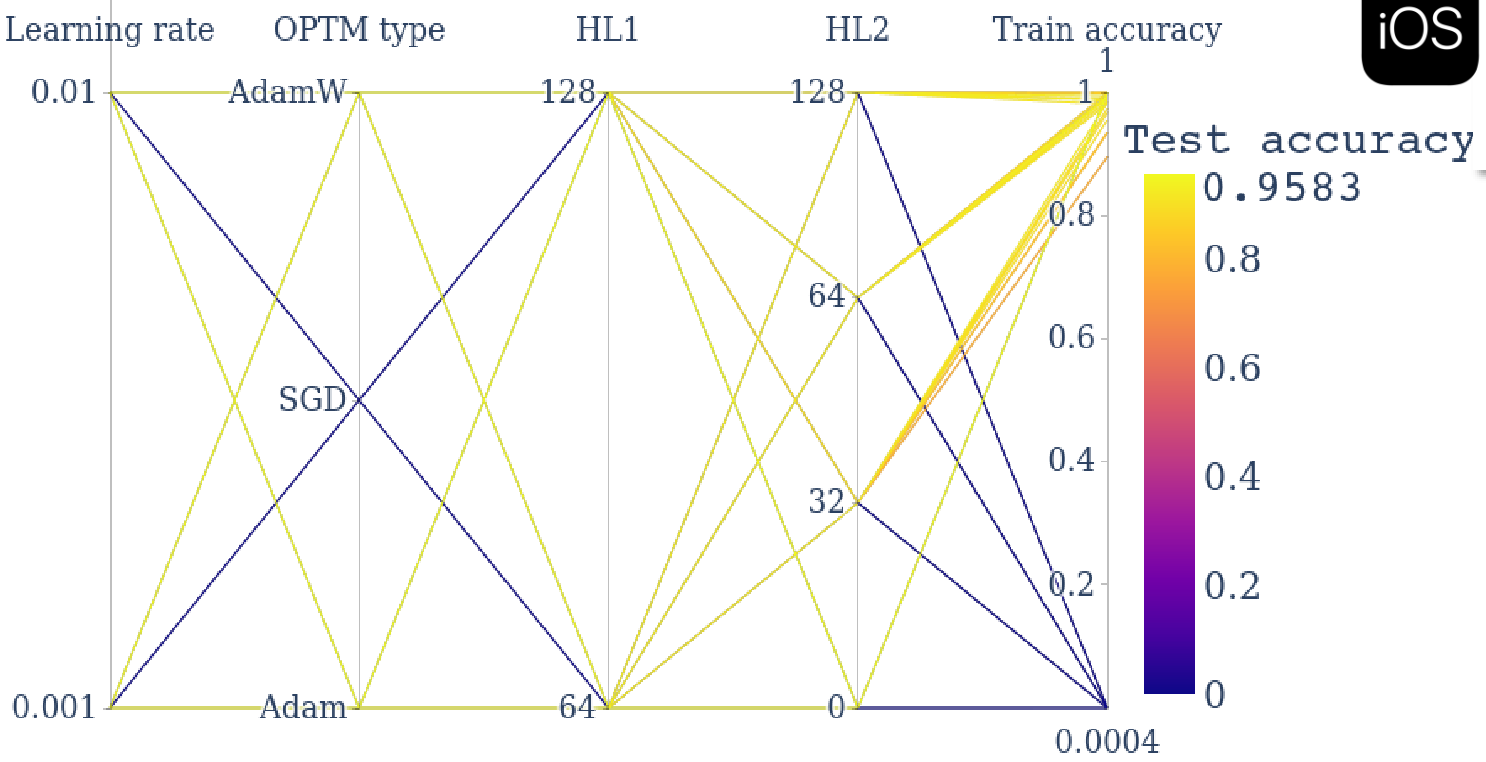
LSTM architecture parameters

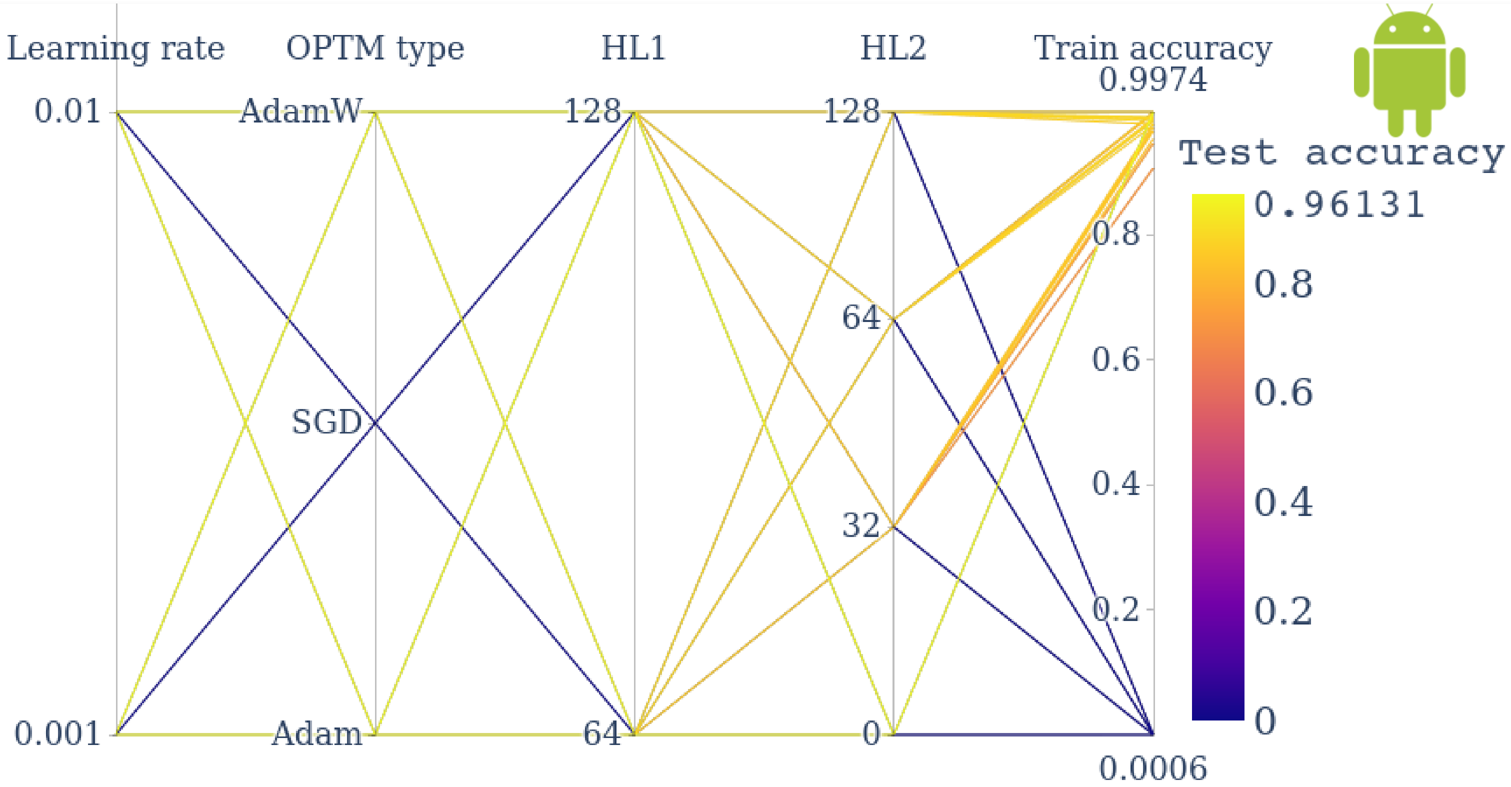
2500 (Android)

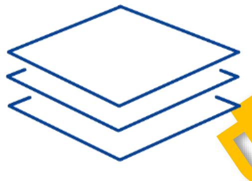
2500 iOS

24h

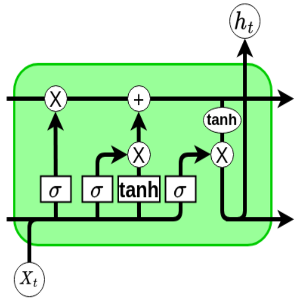
3 weeks







1 LSTM layer



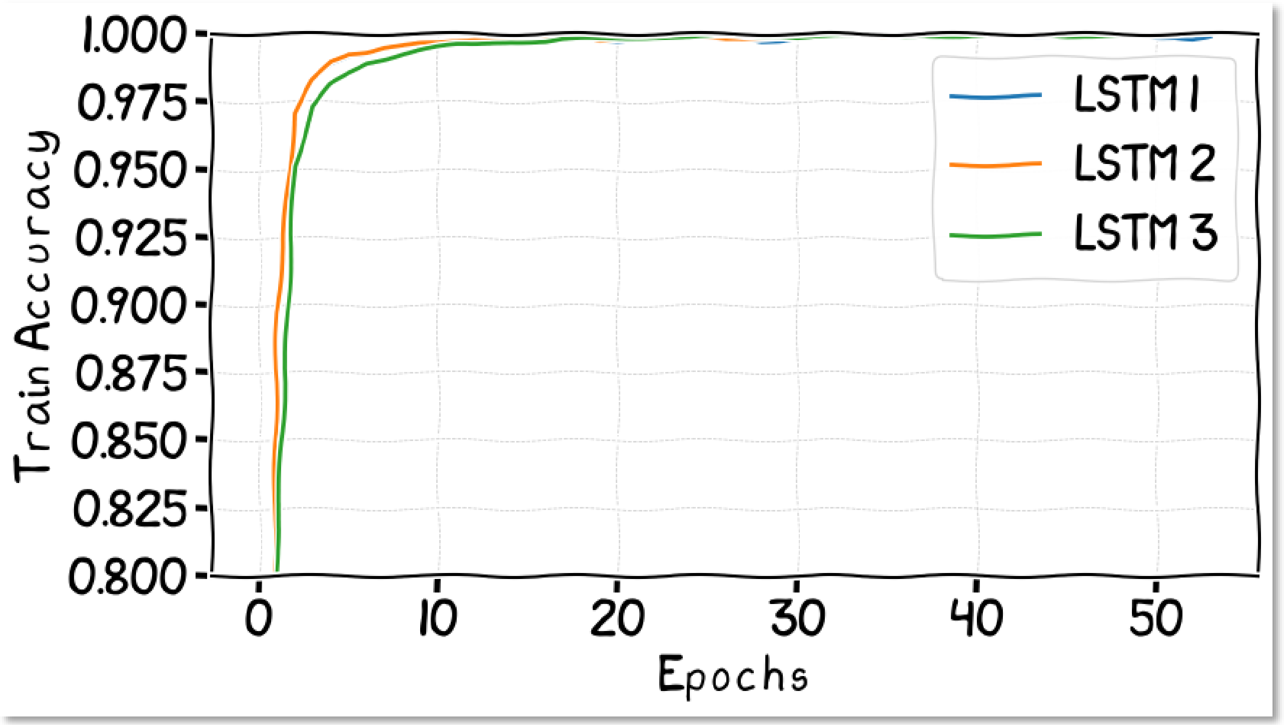
128

LSTM accuracy

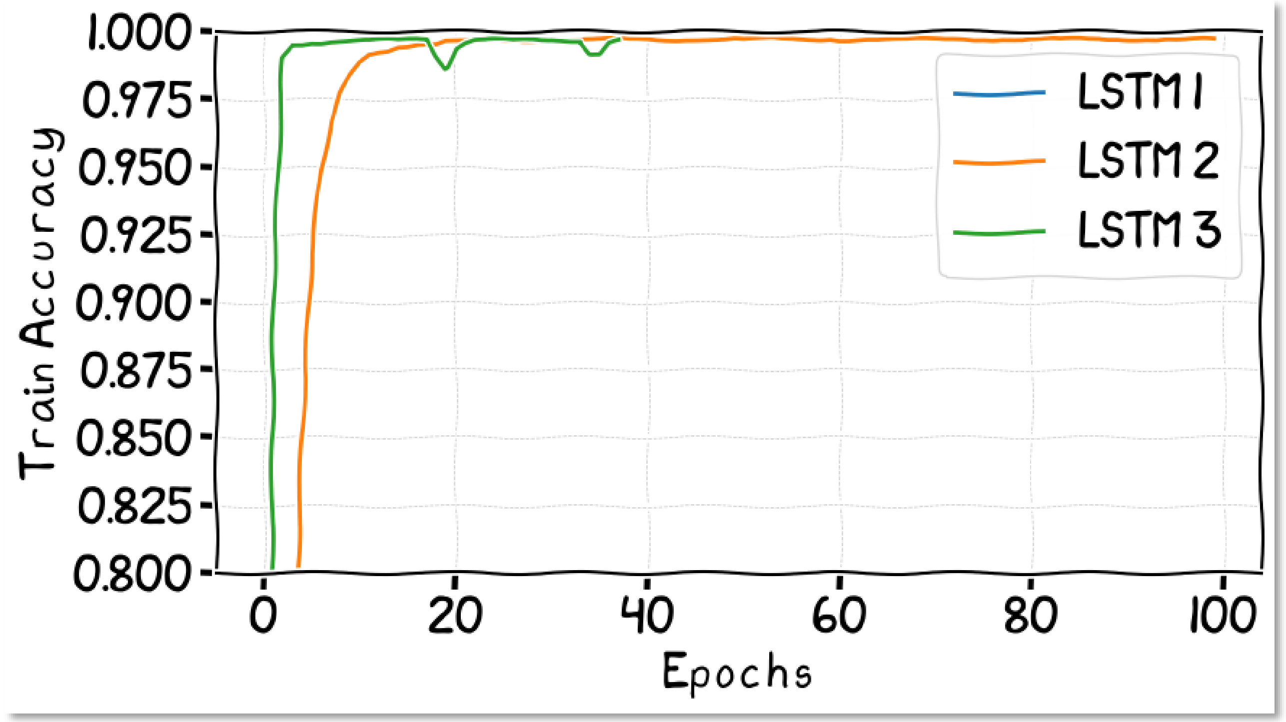
iOS

Model	Train accuracy	Test accuracy	Time
LSTM1	99.97%	95.83%	284 min
LSTM2	99.96%	95.68%	144 min
LSTM3	99.97%	95.25%	116 min

Top 3 iOS LSTM models



Top 3 Android LSTM models



Model	Train accuracy	Test accuracy	Time
LSTM1	99.73%	96.31%	307 min
LSTM2	99.74%	96.28%	235 min
LSTM3	99.70%	95.70%	106 min

LSTM's resource consumption

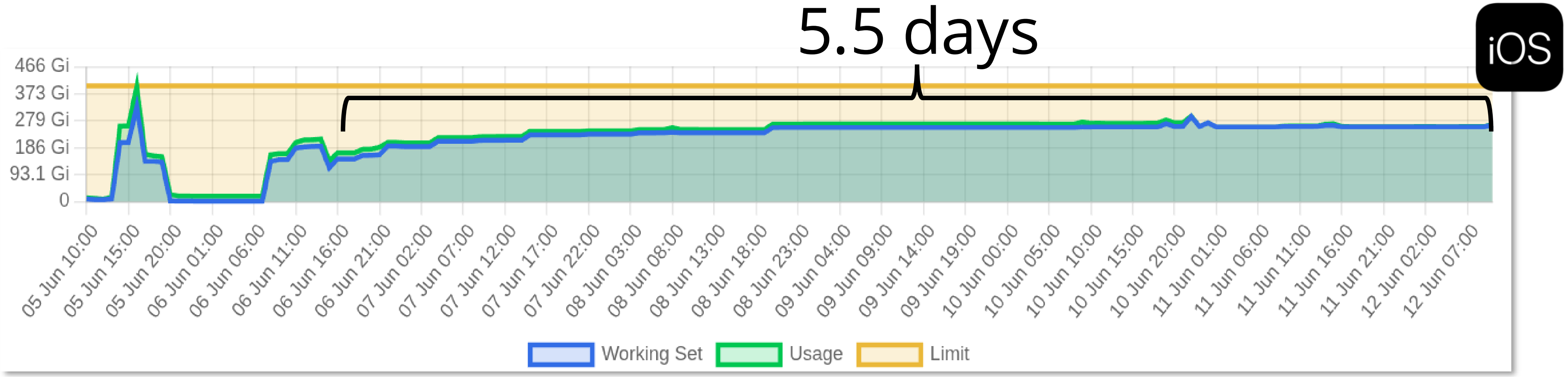
2500

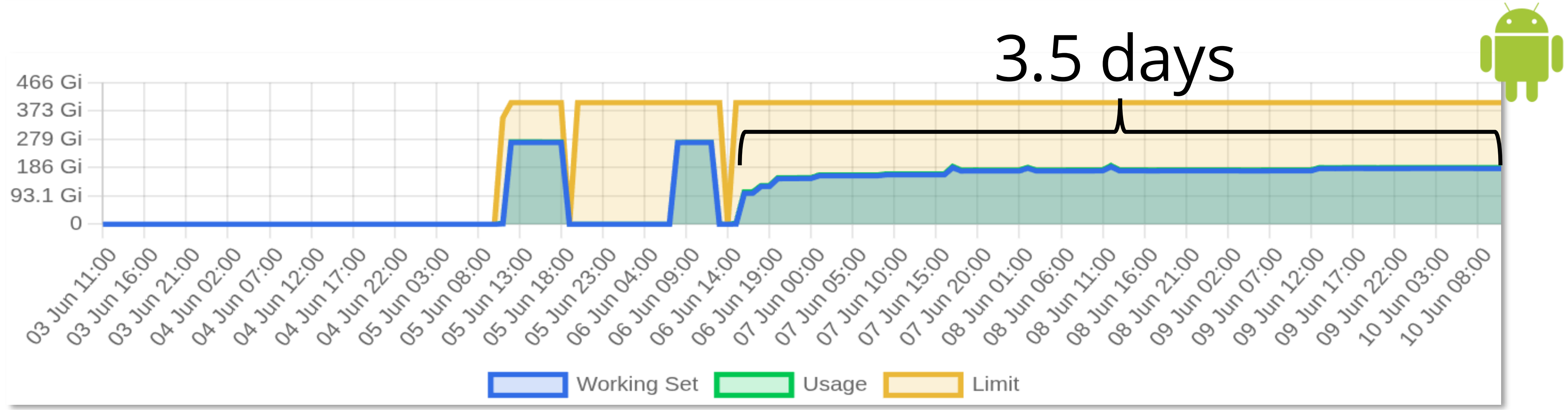
~ 280 / 190 GB RAM

2 clusters (64 vCPUs)

48 models

Memory consumption





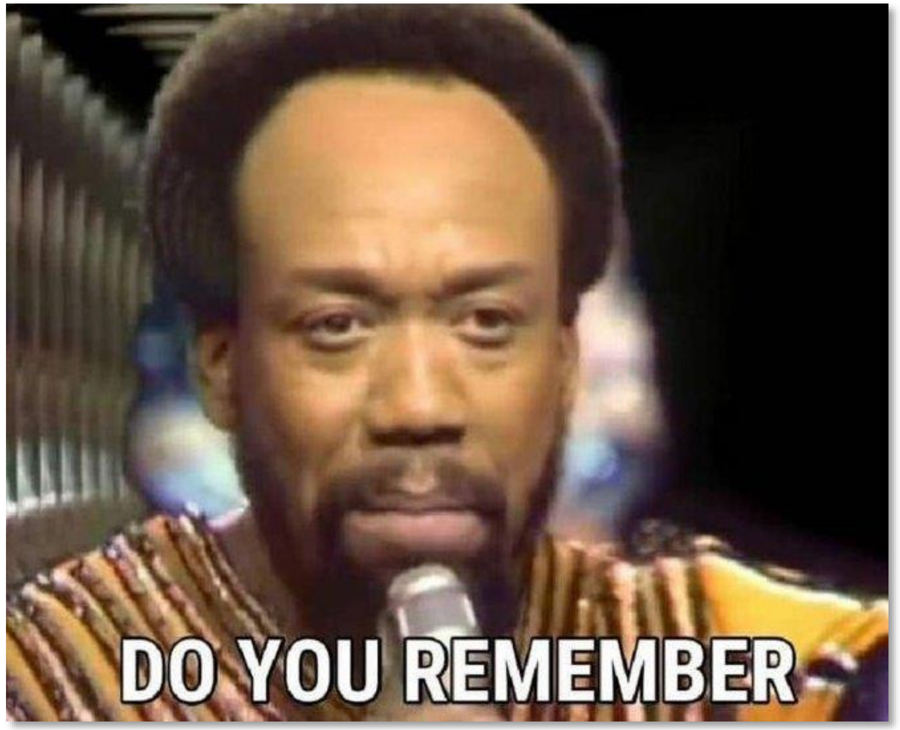
Cosine similarity vs LSTM

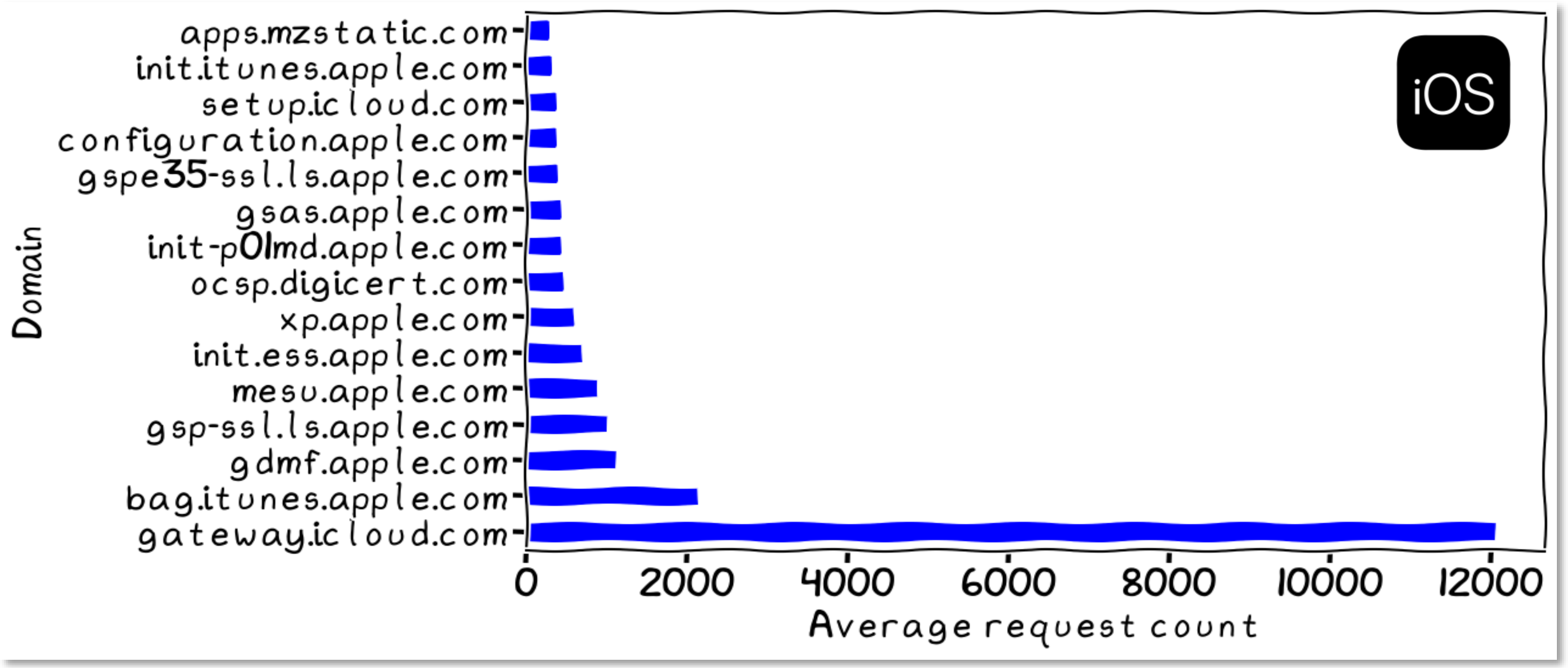
	LSTM	COS similarity
Accuracy score	HIGHER	HIGH
Memory usage	HIGHER	MEDIUM
Number of CPUs	HIGH	LOW
Time consumption	HIGH	LOW

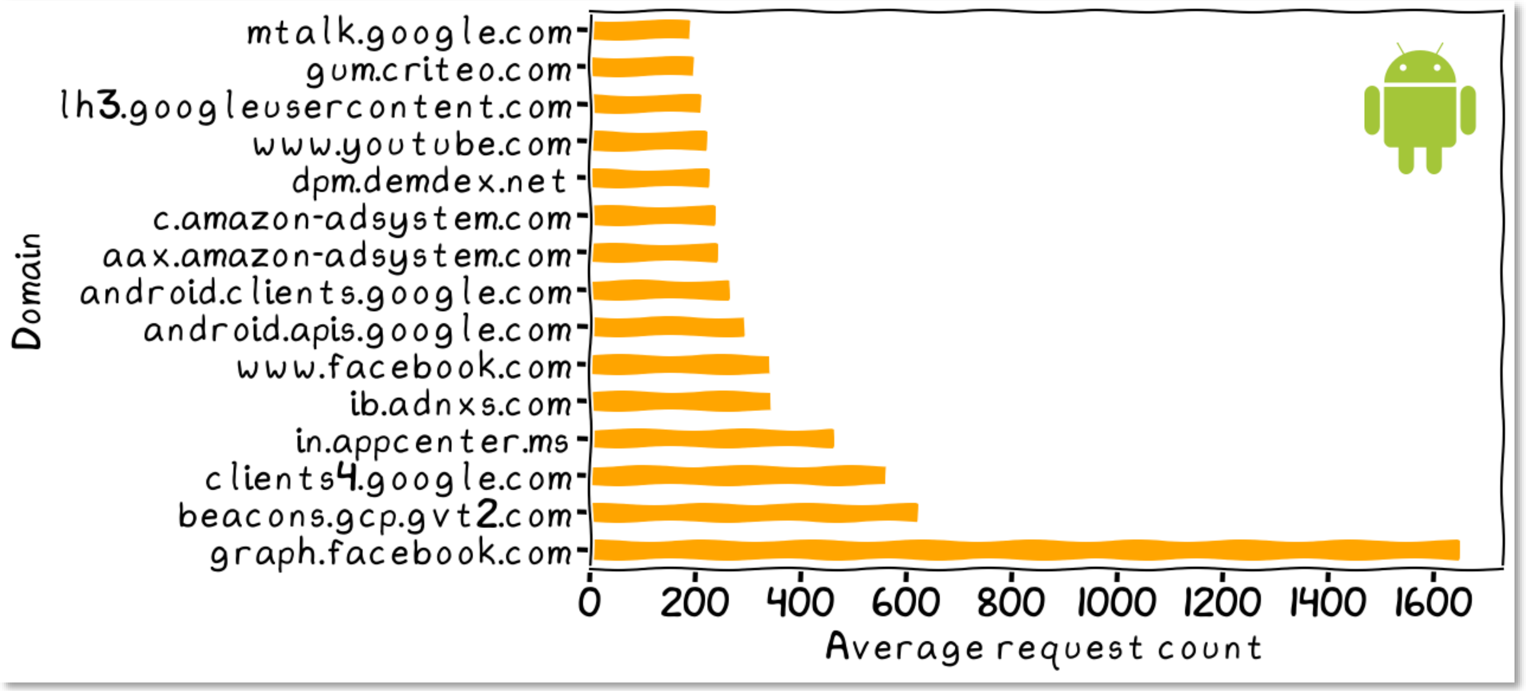
How much does it cost?

Provider	Computation + RAM	Storage (2 TB SSD)	Total/day	Total/month
AWS	$87.28/day	$6.30/day	**$94/day**	**$2,820**
GCP	$101/day	$5.80/day	**$107/day**	**$3,210**
Azure	$129/day	Included	**$129/day**	**$3,870**
Oracle	$116/day	$2.86/day	**$119/day**	**$3,570**
Alibaba	~$96/day	$5.12/day	**$101/day**	**$3,030**

Wait … there is more



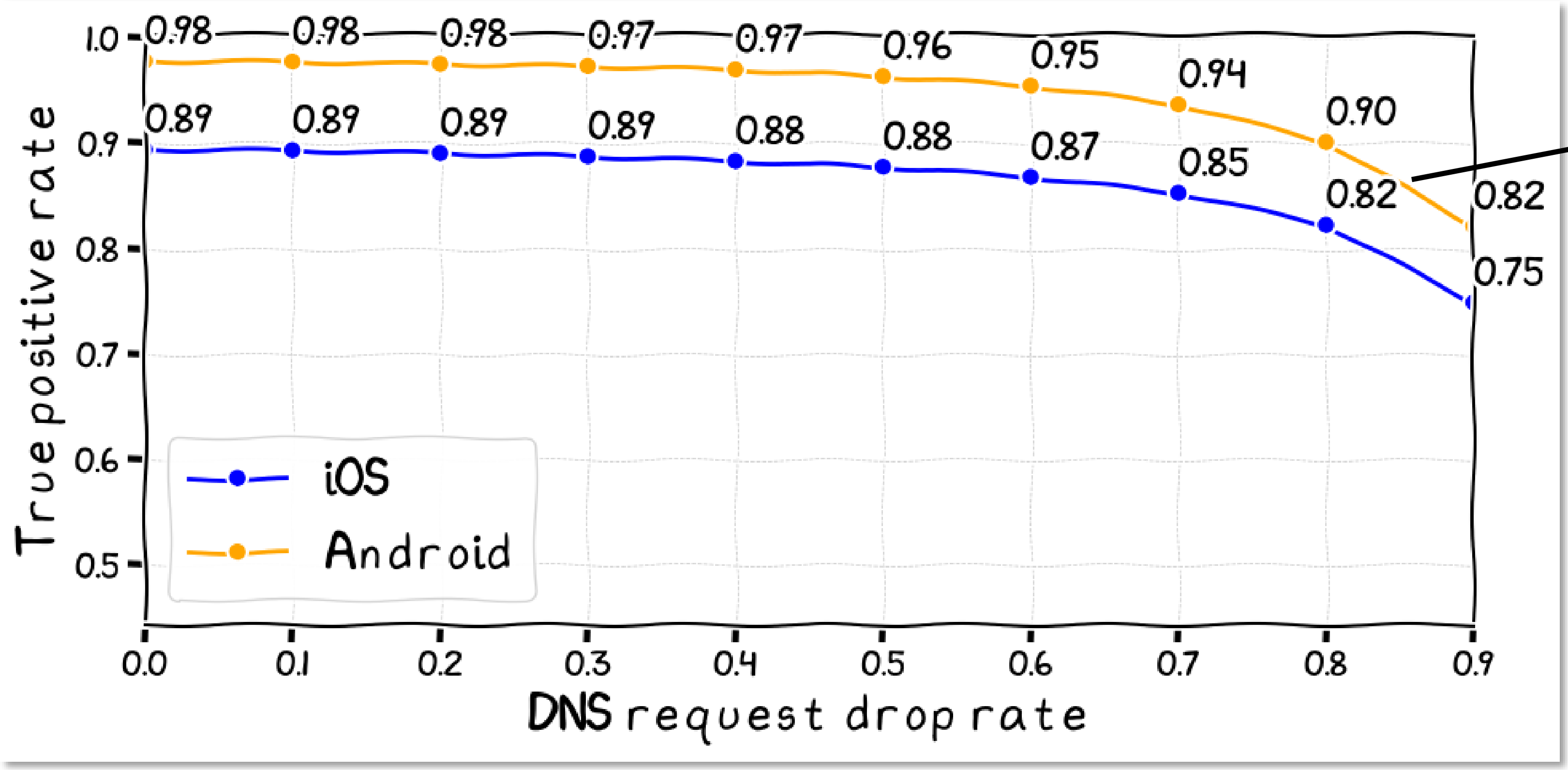




We can do without all that traffic

- Randomly dropping DNS requests preserves statistical distribution
- We can achieve good accuracy with **only 20%**!

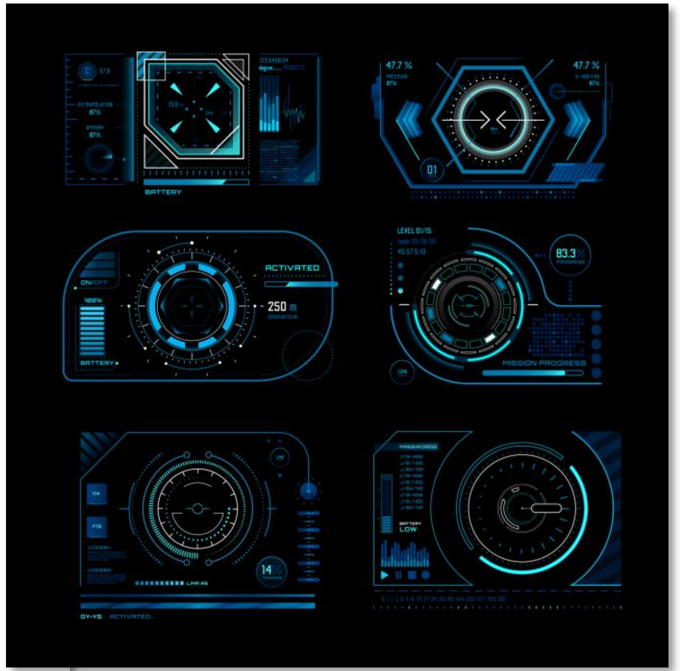
1000 phones
(of each type)



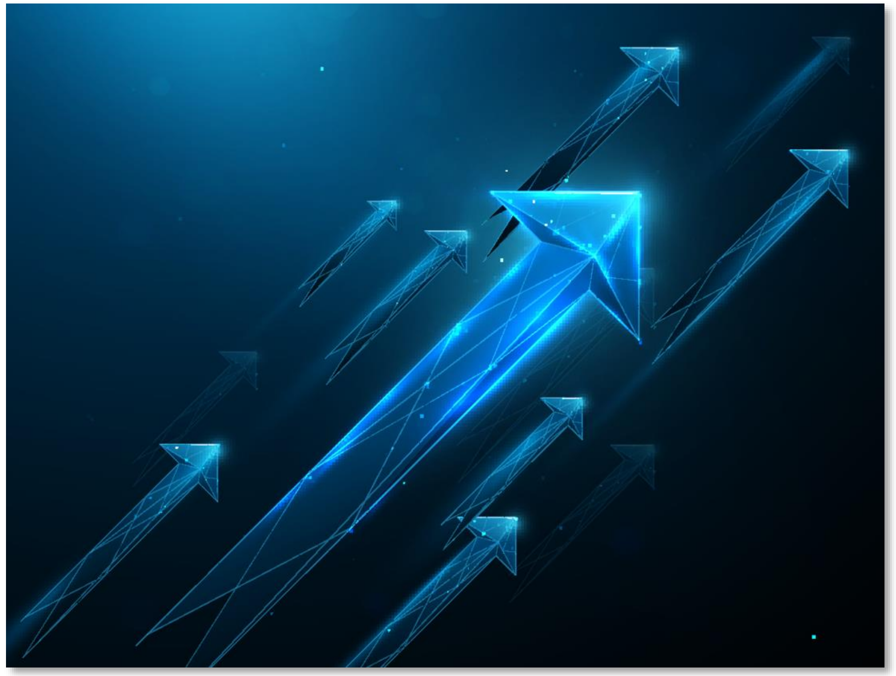
Beyond **0.8**, we start losing statistical significance

If only we had known this earlier…

We would have saved...



Lessons learned & way forward



Lessons learned

- **User Tracking is feasible** with **shocking accuracy** that may increase **above 95%** (subject to various parameters)

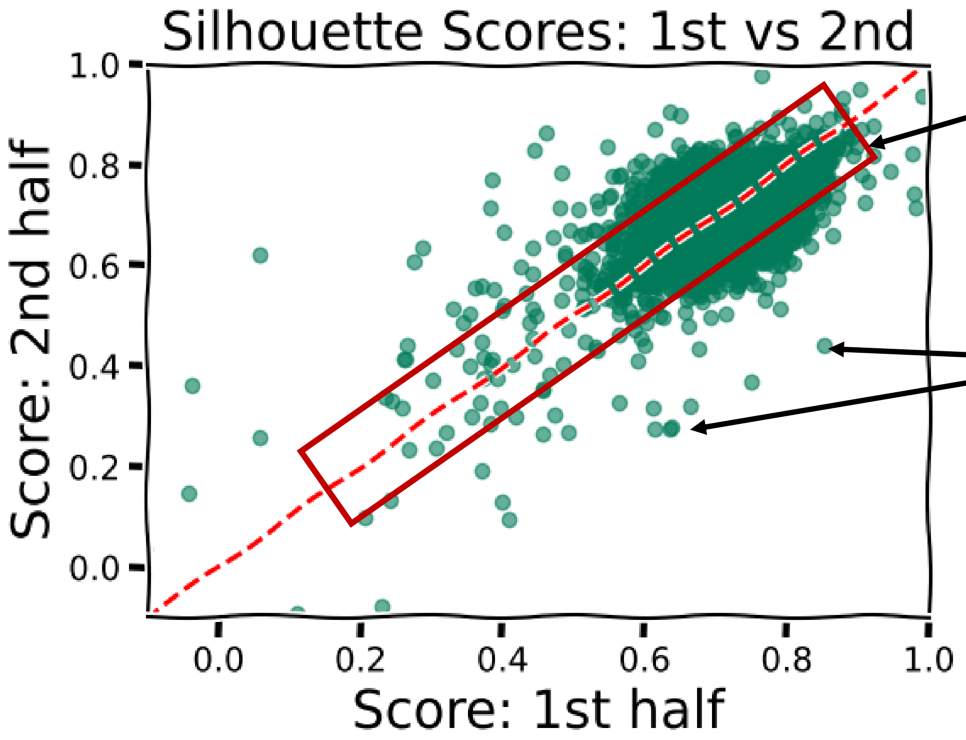
- Simple **statistics can handle larger amounts of data**, with good accuracy

- **AI-based algorithms require more resources** (time, memory, processing power), but can yield **slightly better accuracy** (subject to various parameters)

- **Accurate user-device profiles** expose users to other threats: targeted commercials, placement of products, behavioral analytics

Other applications: user behavior

- Not our main objective, but **behavioral analytics is plausible**
- Analysis of one week vs another, applied clustering + Silhouette score
- **Silhouette**: evaluates clustering quality



Minor
behavior changes

Outliers, **major**
changes

Change in **apps**

Change in **browsing** preferences

Change of **location**

Privacy exposure

Actionable items

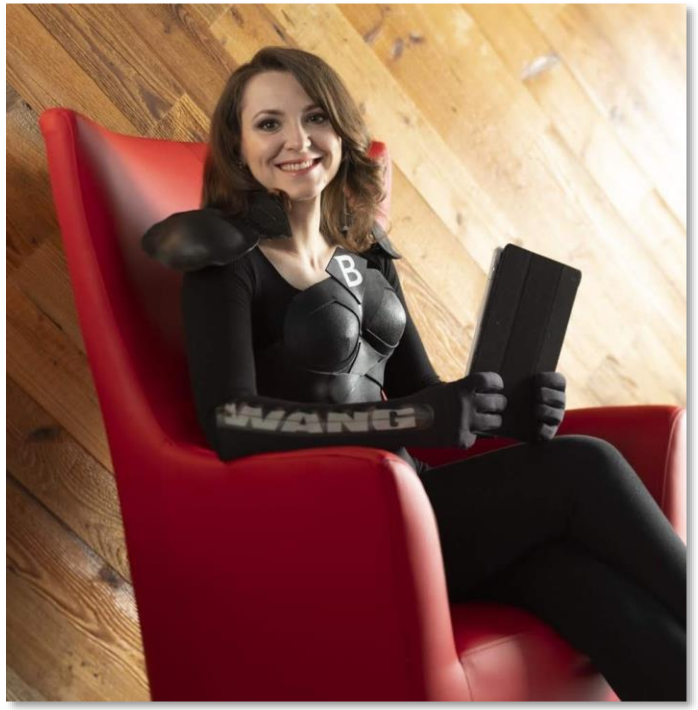
1. Enable **MAC randomization** (with rotating MAC, if option is available), **make it more aggressive** (e.g., change it for each network connection)

2. Use **encrypted DNS**, if available, **enable it by default**

3. Telcos should **inform the user** on the collection of DNS requests an **on their use**

Special thanks

Machine learning team @ Bitdefender



Elena BURCEANU

Dragoș Alexandru BOLDIȘOR

Cristian Daniel PĂDURARU

black hat BRIEFINGS

AUGUST 6-7, 2025
MANDALAY BAY / LAS VEGAS

Thank you!

Béla Genge, Ioan Pădurean, Dan Macovei

{bgenge, ipadurean, dmacovei}@bitdefender.com

Bitdefender