Surveilling the Masses with Wi-Fi Positioning Systems

Erik Rye
University of Maryland

vitæ

Erik Rye

- rye (*noun)* a cereal plant that tolerates poor soils and low temperatures

- University of Maryland Comp Sci PhD Student 🐢
  - Advised by Dave Levin 👨‍🎓

- Research interests
  - Security 🔒 privacy 🤫 networks 🛜

- Other interests
  - Dogs 🐕
  - Fonts, kerning ✍️
  - Telling infants 👶 about Arch 💻

UNIVERSITY OF MARYLAND

Wi-Fi Positioning Systems (WPSes)

How mobile devices use Wi-Fi routers as landmarks

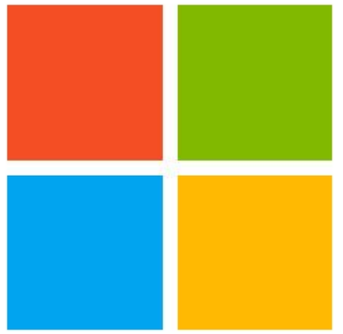
Wi-Fi Positioning Systems (WPSes)

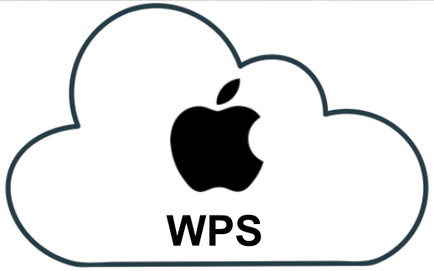
Operated by mobile OS vendors, others

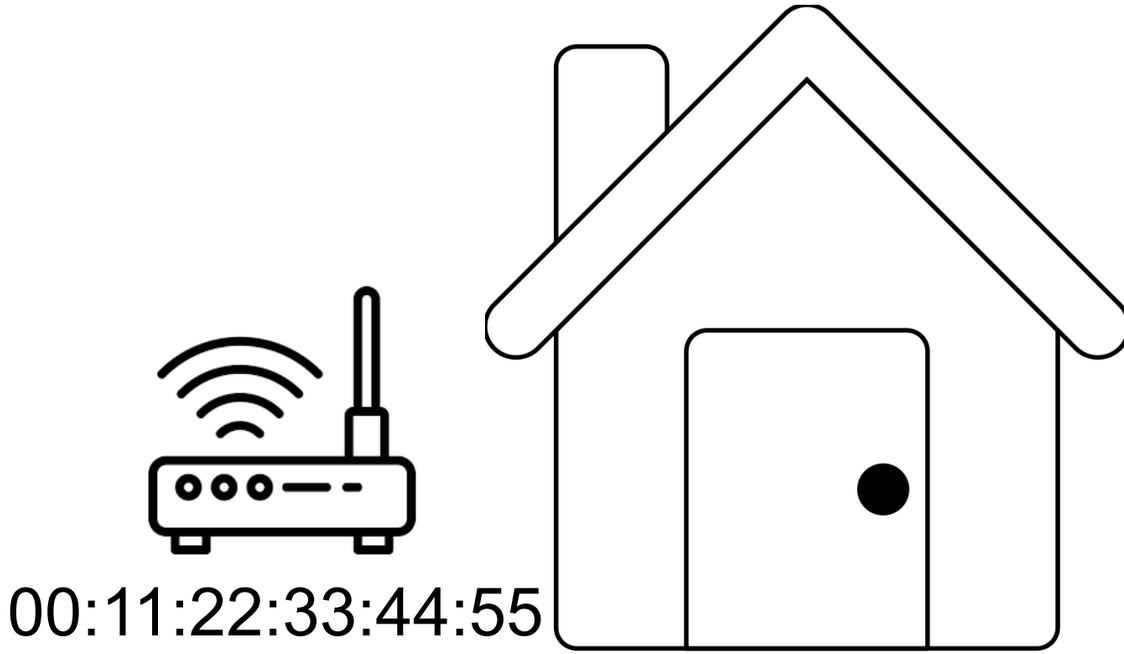
- Apple
- Google
- Microsoft
- Skyhook
- Mozilla Location Service 🪦

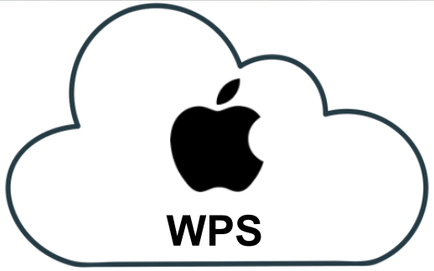
Apple's implementation is uniquely vulnerable to certain attacks

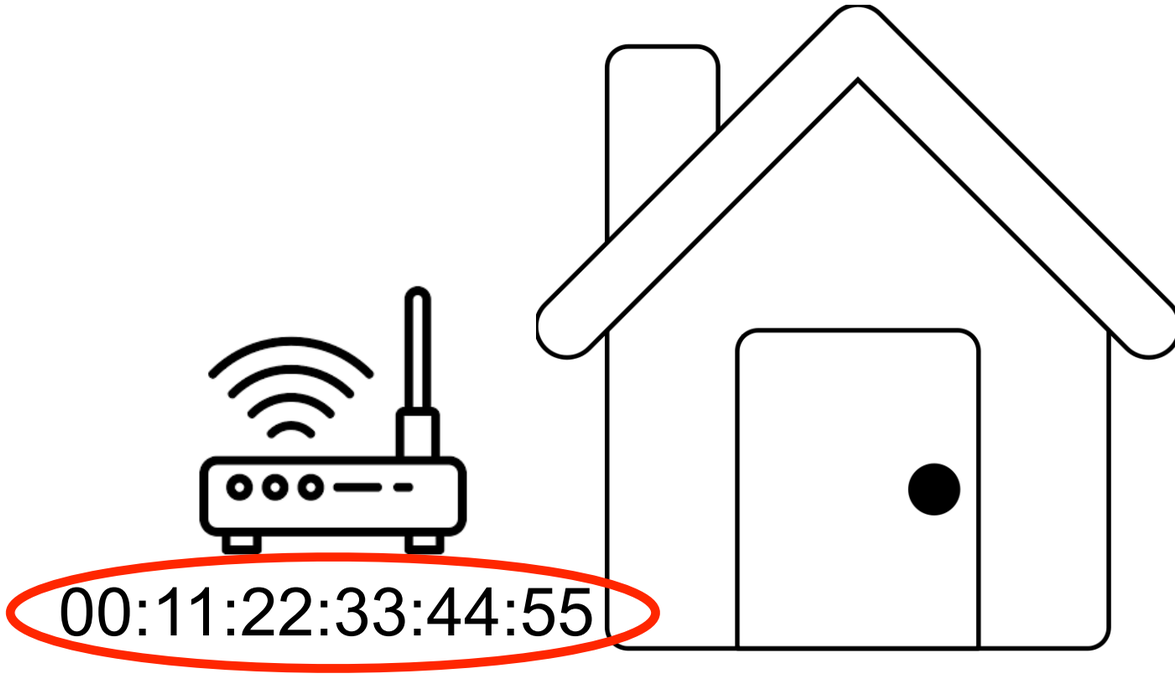
SKYHOOK®



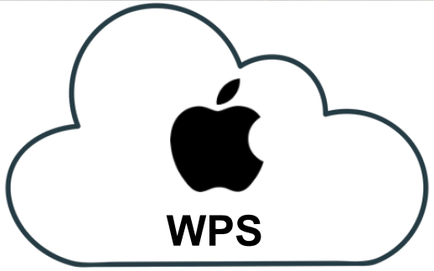

WPS

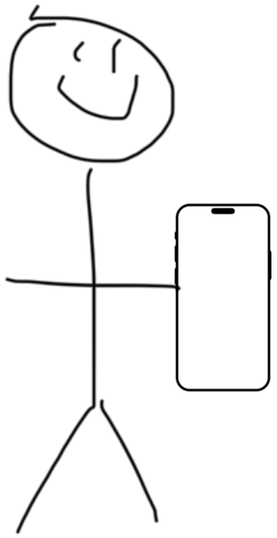

00:11:22:33:44:55

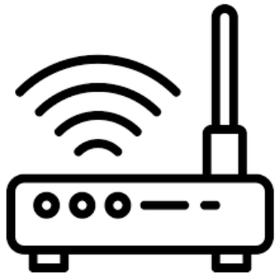




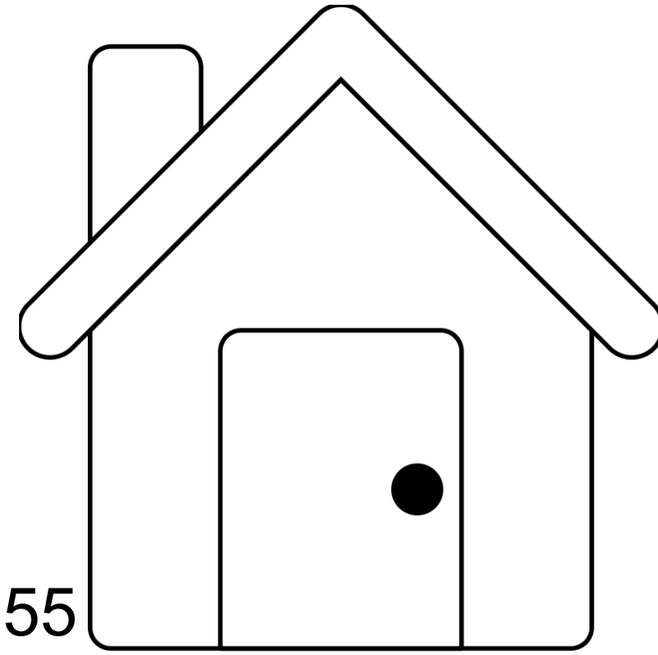
Basic Service Set Identifier (BSSID)

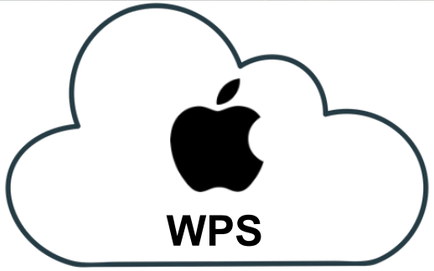


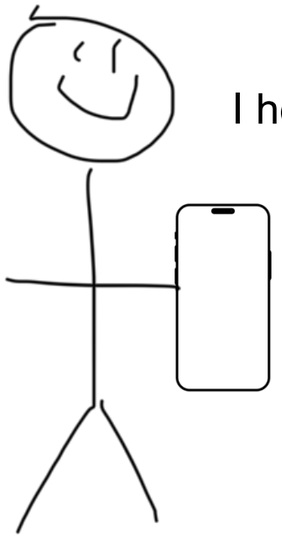




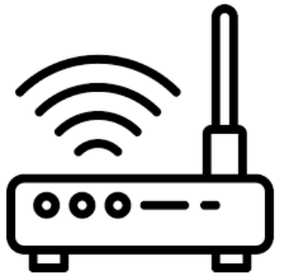
00:11:22:33:44:55



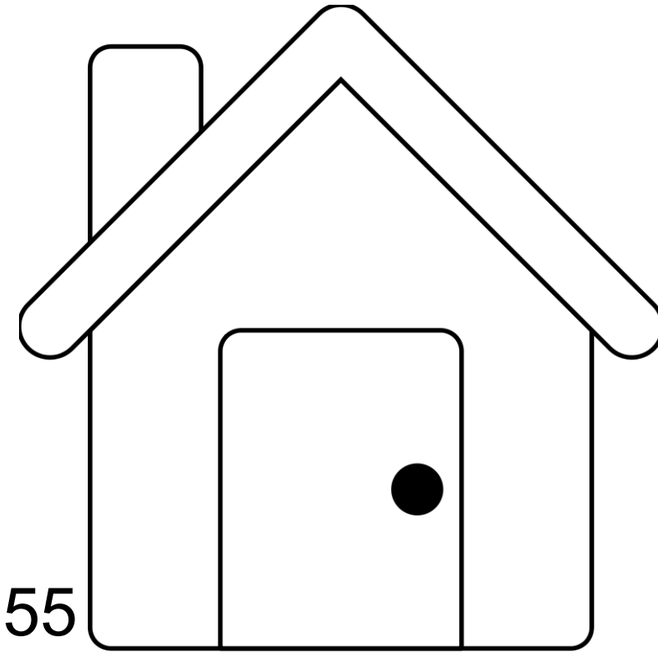


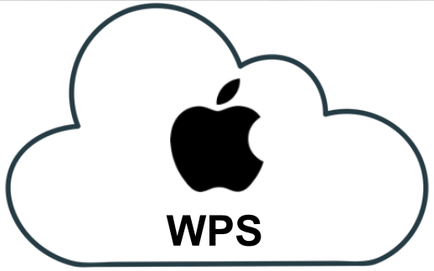


I hear 00:11:22:33:44:55
I'm at 12.34,56.78

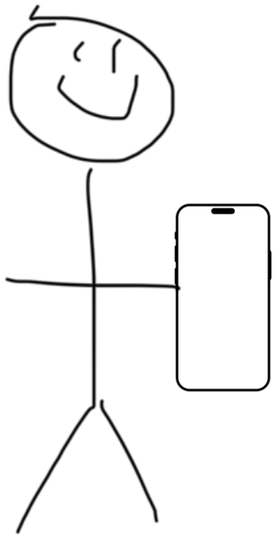


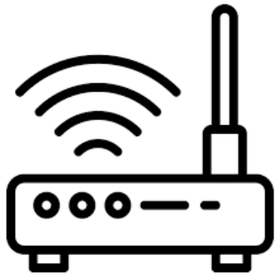
00:11:22:33:44:55



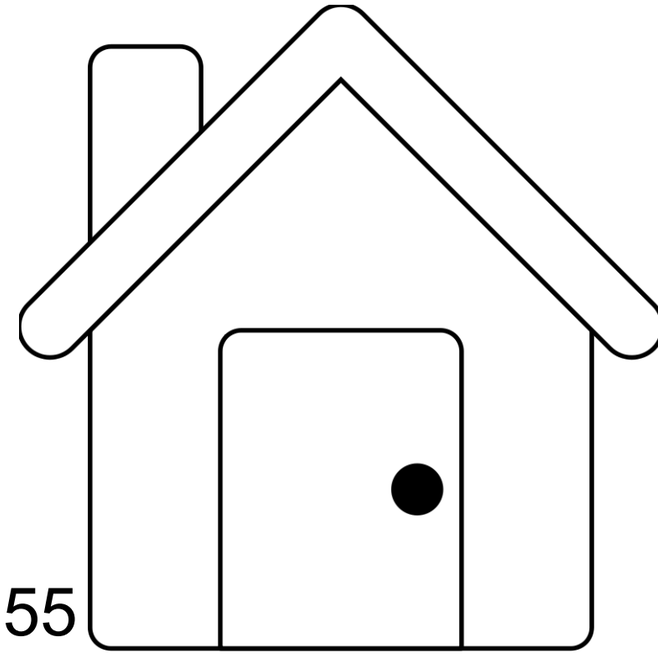


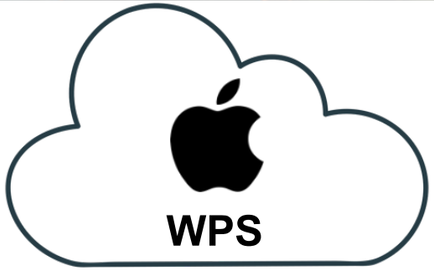
I hear 00:11:22:33:44:55
I'm at 12.34,56.78

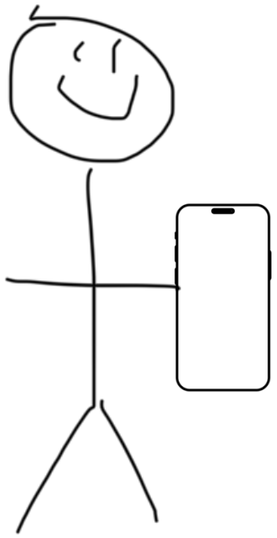


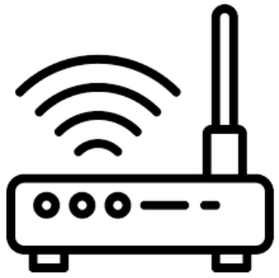


00:11:22:33:44:55

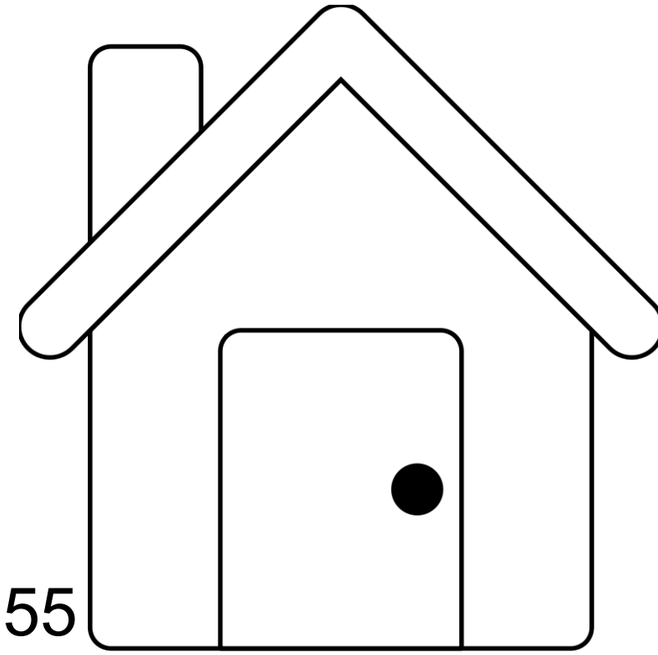


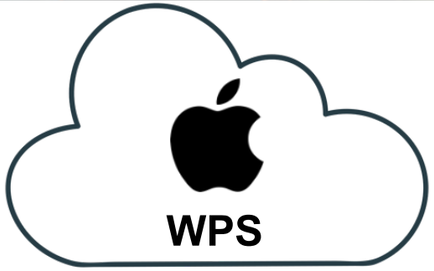


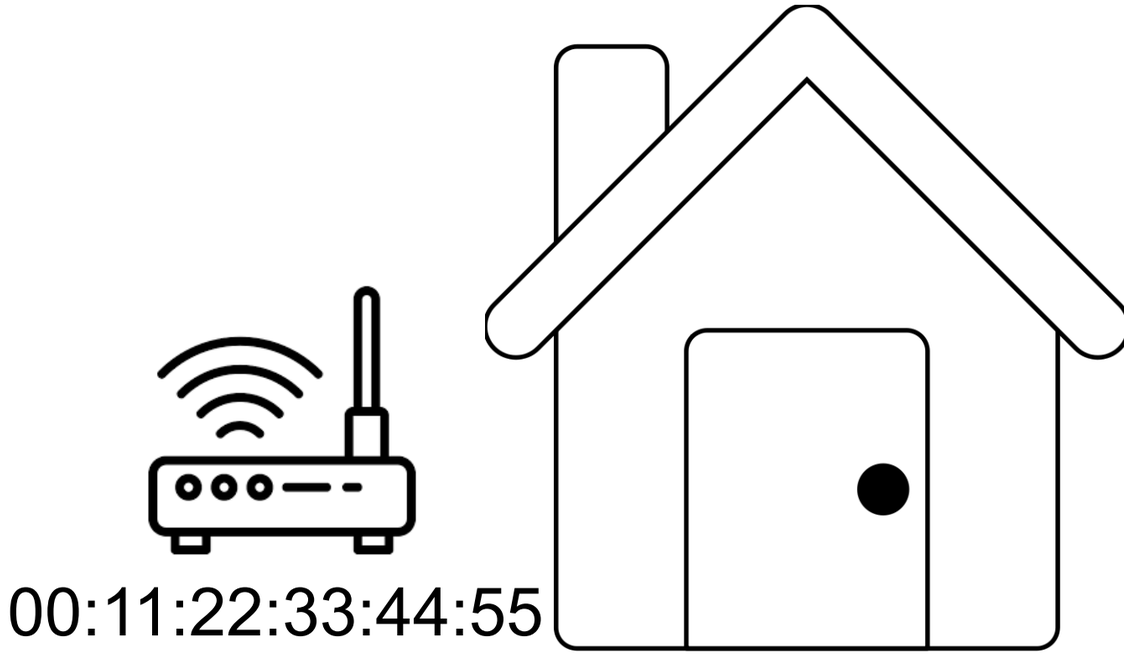


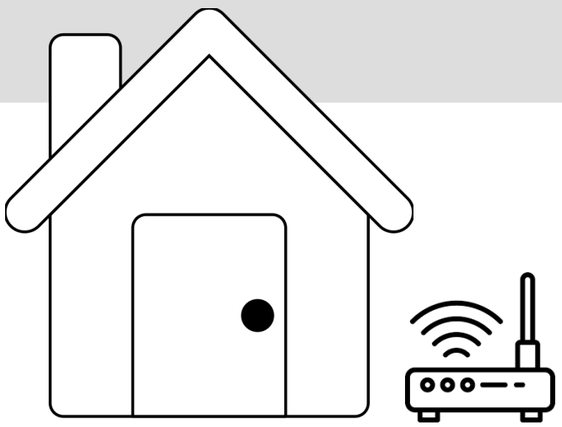


00:11:22:33:44:55

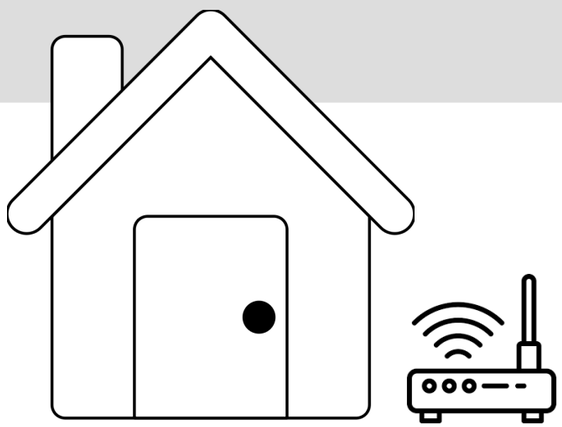



WPS

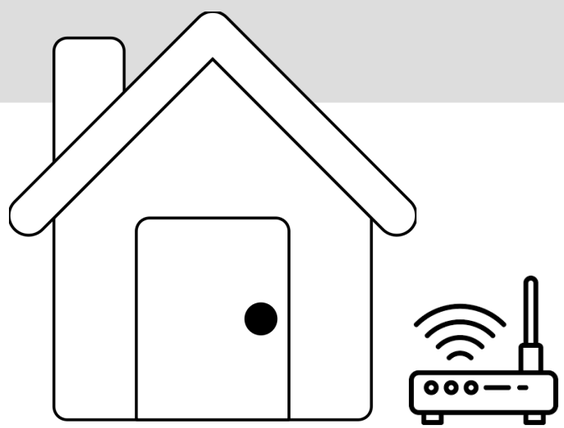

00:11:22:33:44:55



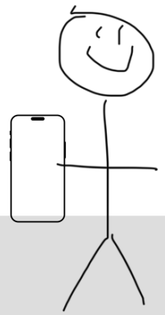
66:77:88:99:aa:bb

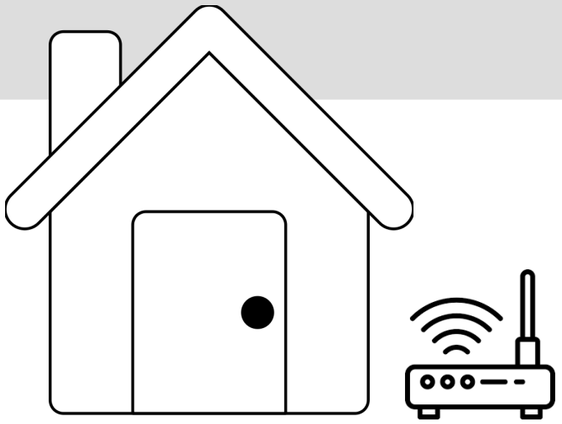


44:55:66:77:88:99

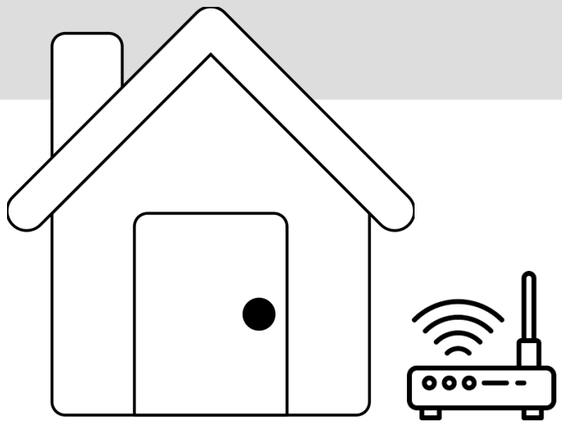


22:33:44:55:66:77

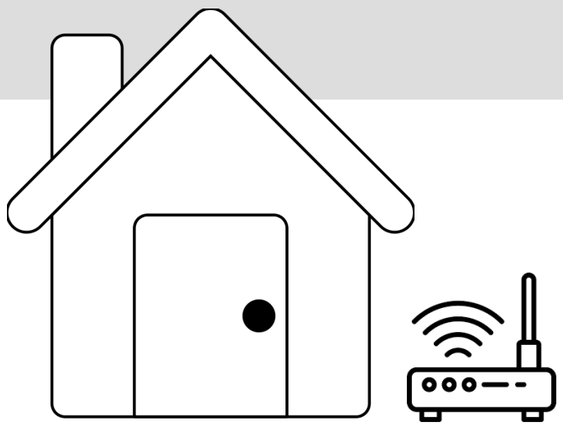




66:77:88:99:aa:bb

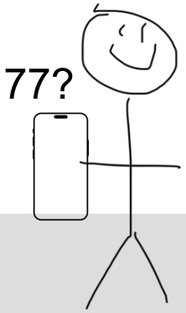


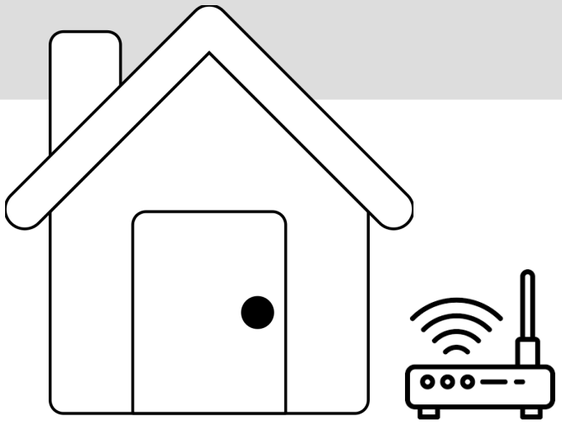
44:55:66:77:88:99



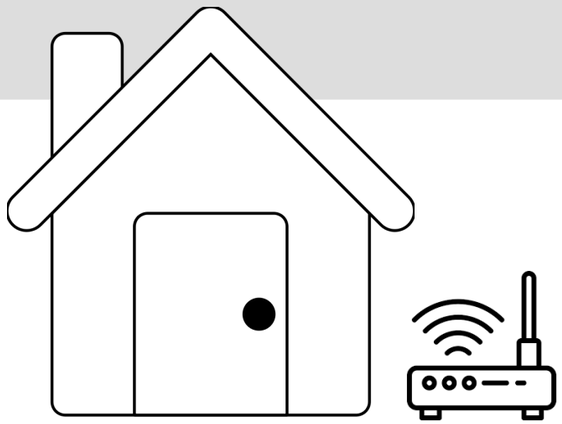
22:33:44:55:66:77

Where is 22:33:44:55:66:77?

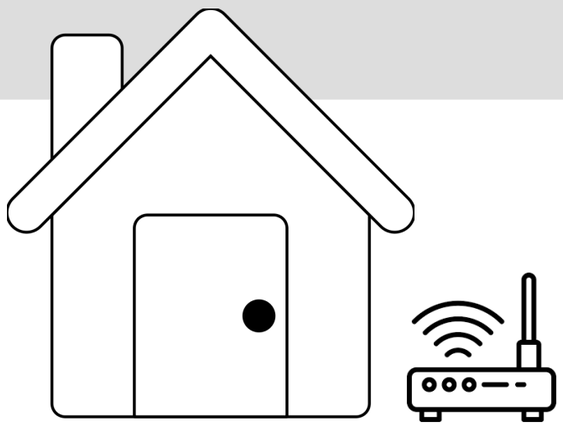




66:77:88:99:aa:bb

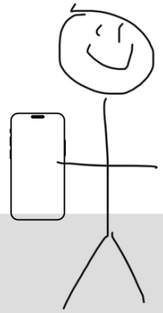


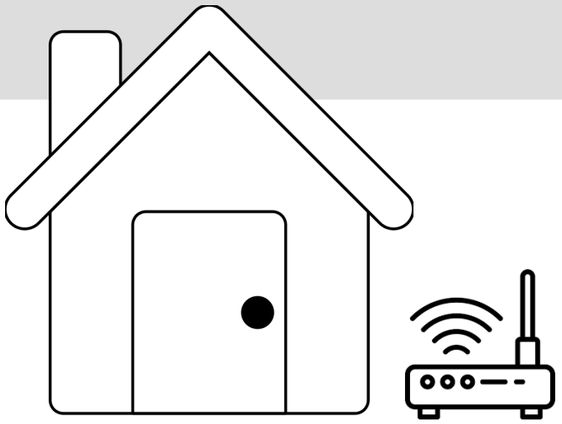
44:55:66:77:88:99



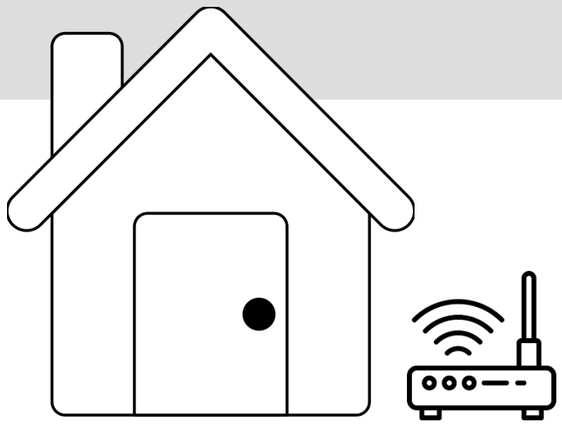
22:33:44:55:66:77

Where is 22:33:44:55:66:77?

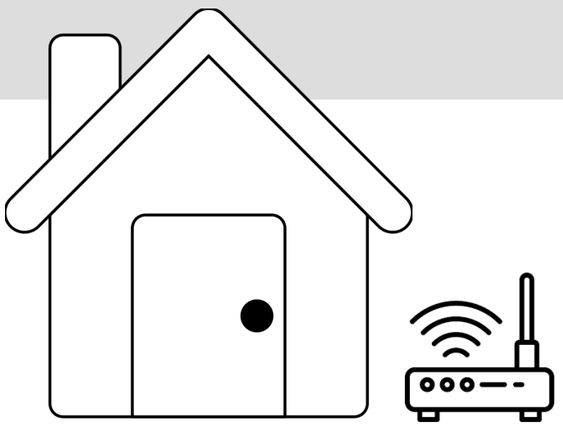




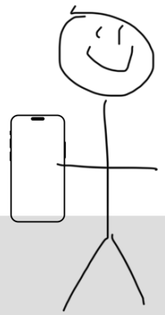
66:77:88:99:aa:bb

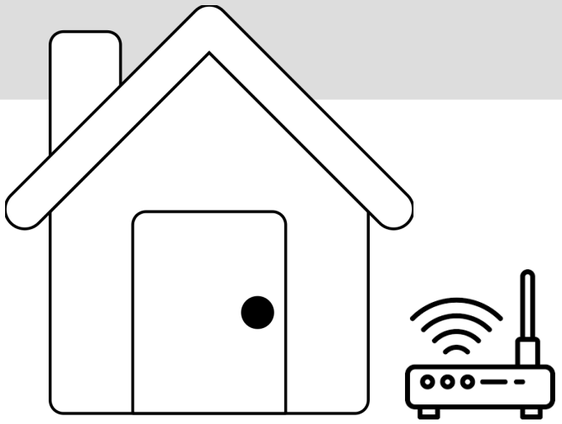


44:55:66:77:88:99

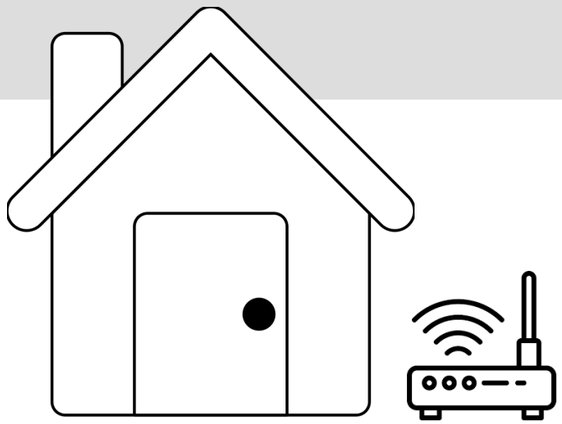


22:33:44:55:66:77

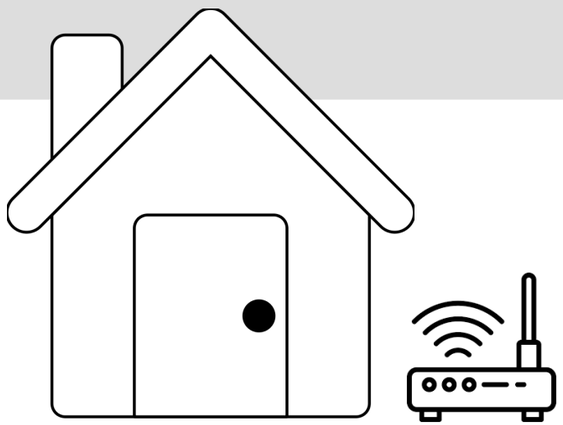




66:77:88:99:aa:bb

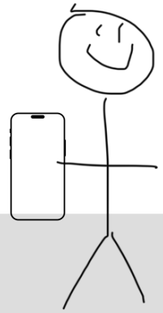


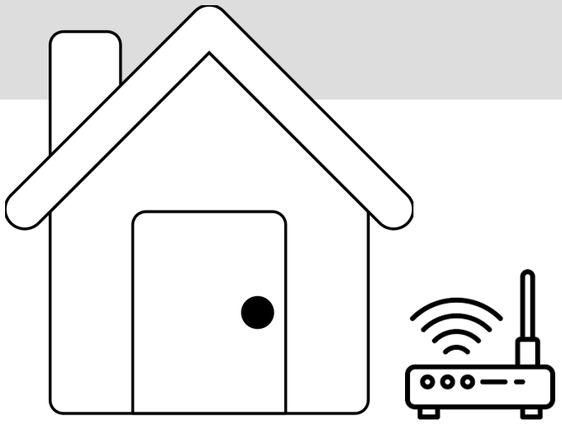
44:55:66:77:88:99



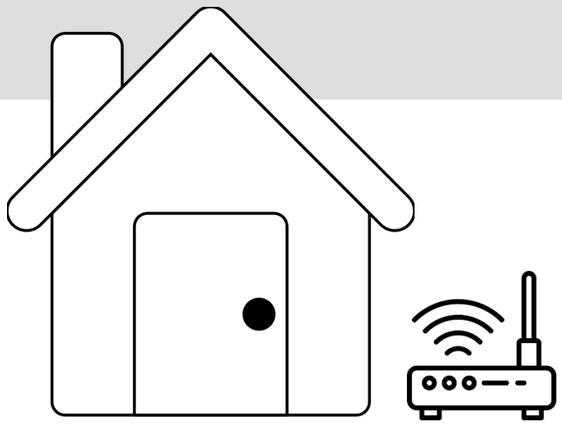
22:33:44:55:66:77

22:33:44:55:66:77 is at 12.34,56.67
44:55:66:77:88:99 is at 12.33,56.66
66:77:88:99:aa:bb is at 12.32,56.68
…

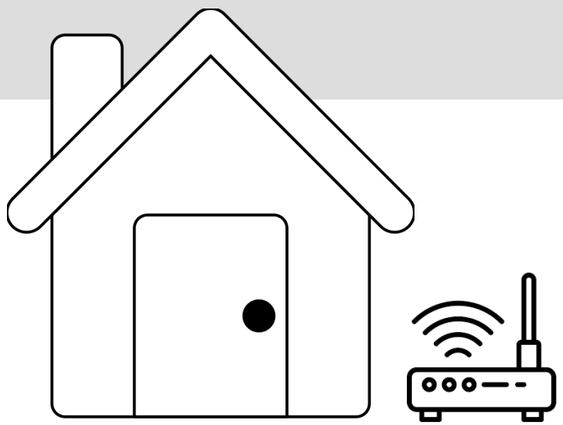




66:77:88:99:aa:bb

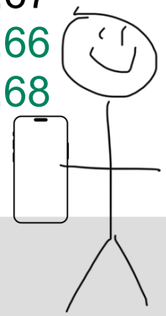


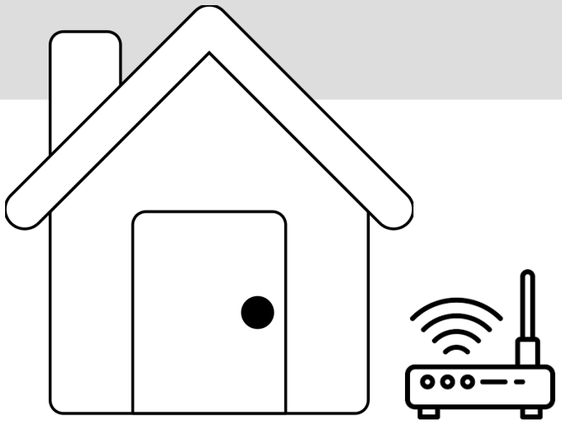
44:55:66:77:88:99



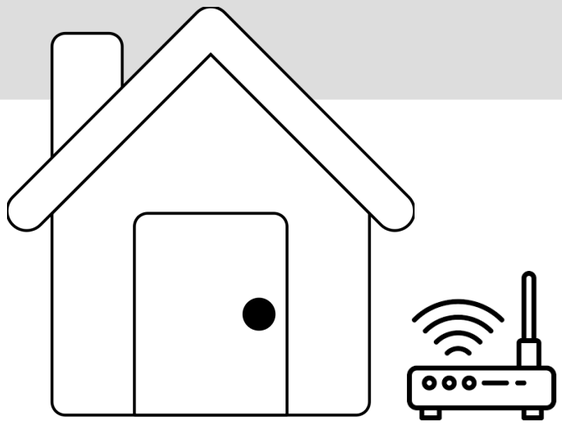
22:33:44:55:66:77

22:33:44:55:66:77 is at 12.34,56.67
44:55:66:77:88:99 is at 12.33,56.66
66:77:88:99:aa:bb is at 12.32,56.68
…

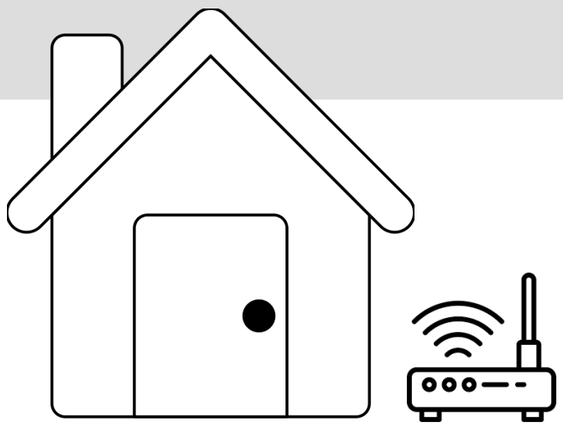




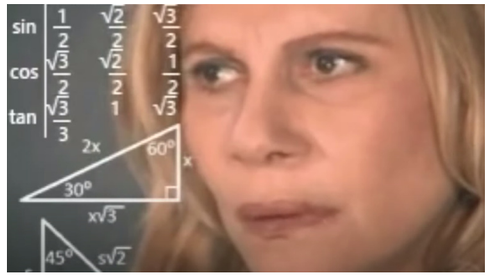
66:77:88:99:aa:bb



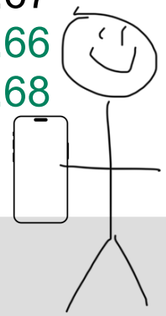
44:55:66:77:88:99

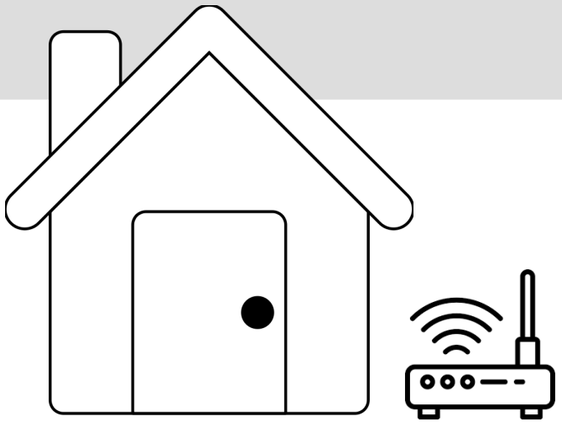


22:33:44:55:66:77

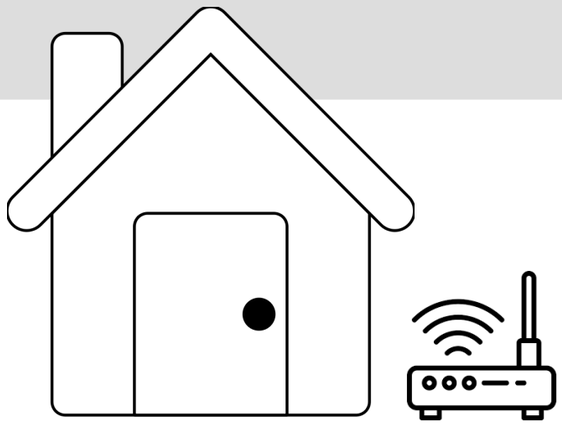


22:33:44:55:66:77 is at 12.34,56.67
44:55:66:77:88:99 is at 12.33,56.66
66:77:88:99:aa:bb is at 12.32,56.68
…

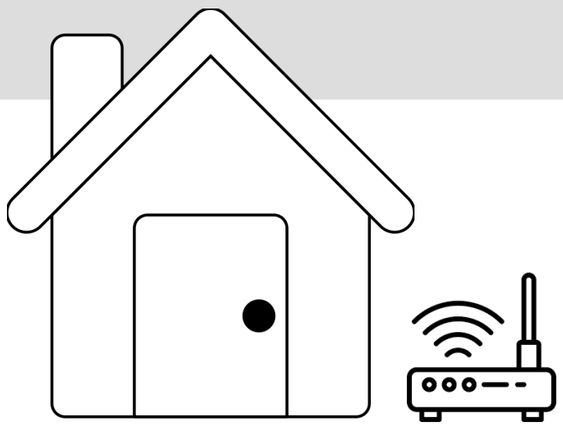




66:77:88:99:aa:bb

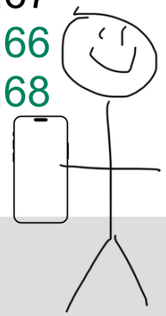


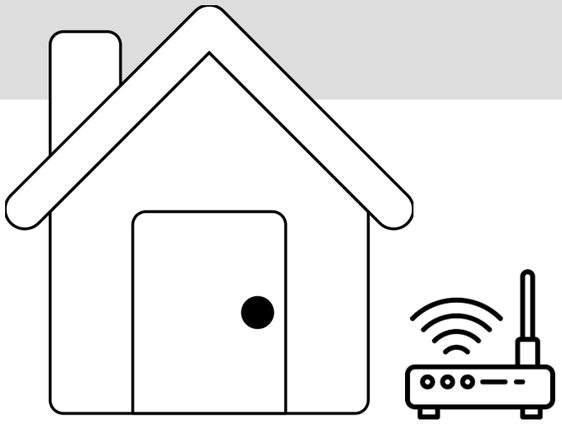
44:55:66:77:88:99



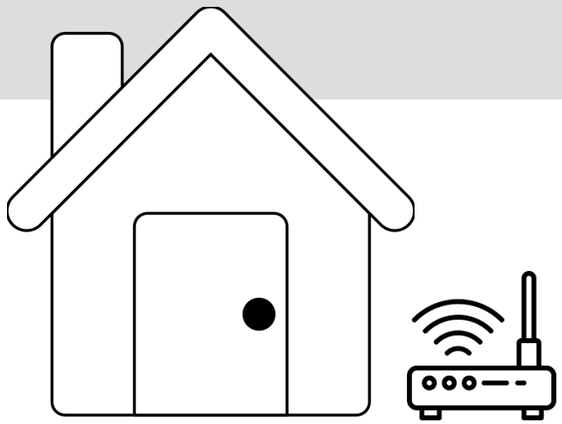
22:33:44:55:66:77

22:33:44:55:66:77 is at 12.34,56.67
44:55:66:77:88:99 is at 12.33,56.66
66:77:88:99:aa:bb is at 12.32,56.68
…

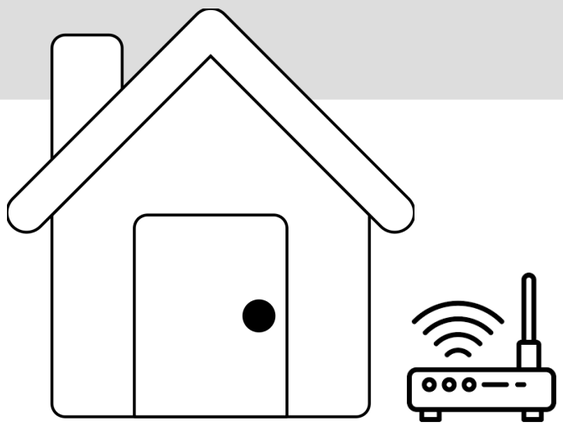




66:77:88:99:aa:bb



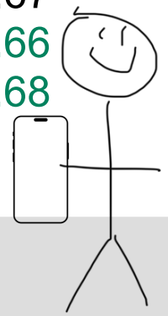
44:55:66:77:88:99

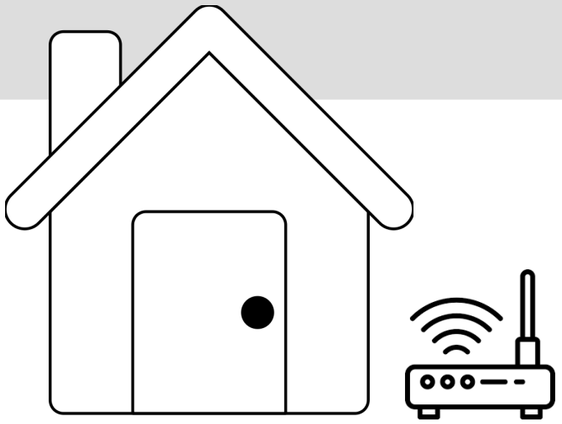


22:33:44:55:66:77

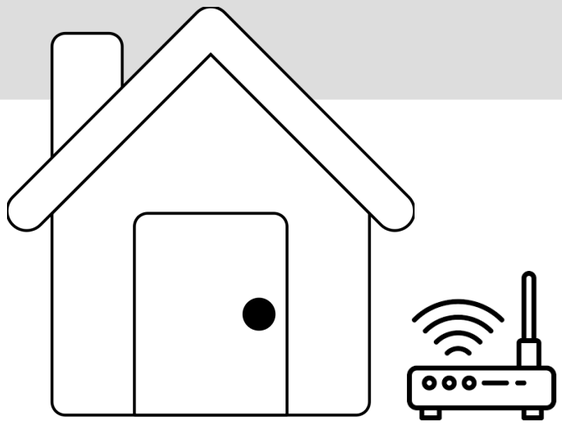
I’m at 12.335,56.665!

22:33:44:55:66:77 is at 12.34,56.67
44:55:66:77:88:99 is at 12.33,56.66
66:77:88:99:aa:bb is at 12.32,56.68
…

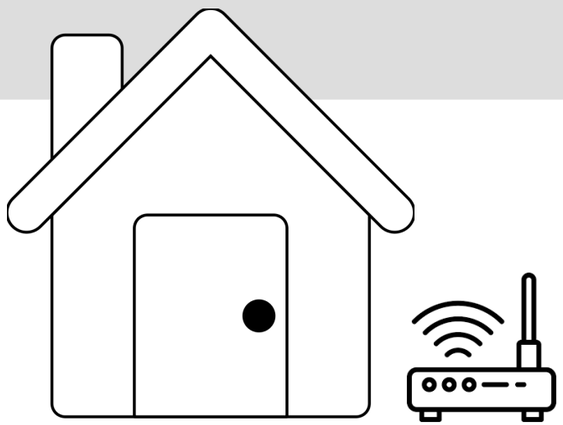




66:77:88:99:aa:bb

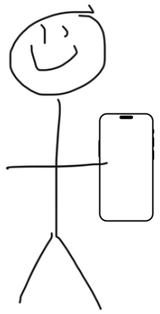


44:55:66:77:88:99



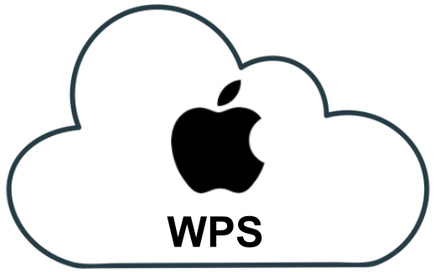
22:33:44:55:66:77

Apple's Wi-Fi Positioning System (WPS)

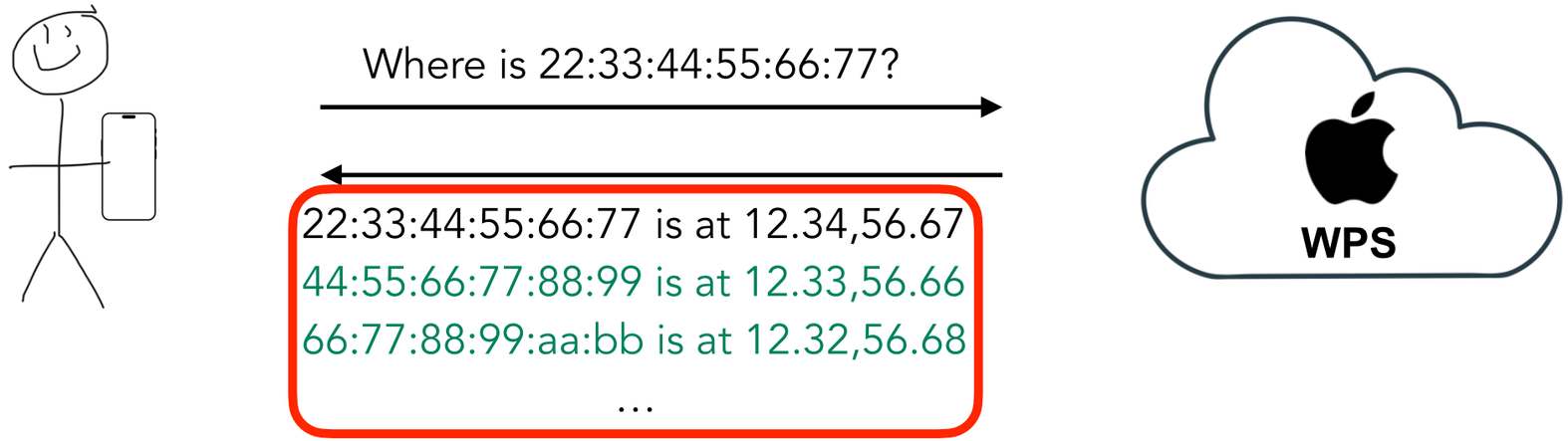


Where is 22:33:44:55:66:77?

22:33:44:55:66:77 is at 12.34,56.67
44:55:66:77:88:99 is at 12.33,56.66
66:77:88:99:aa:bb is at 12.32,56.68
…

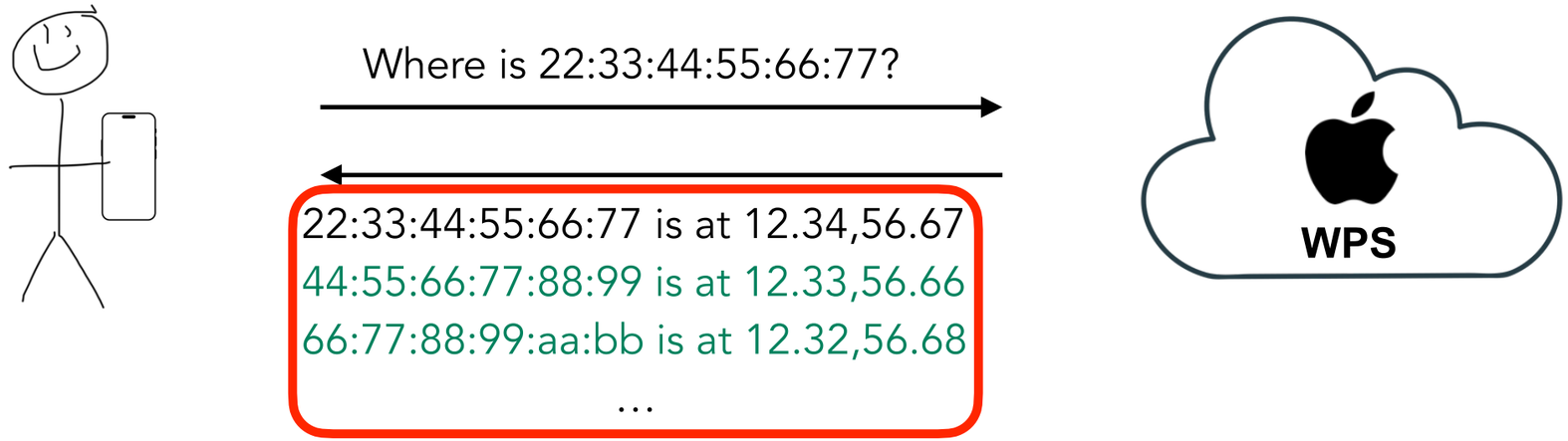


Apple's Wi-Fi Positioning System (WPS)



Returns up to 400 **additional unrequested** BSSID locations per query

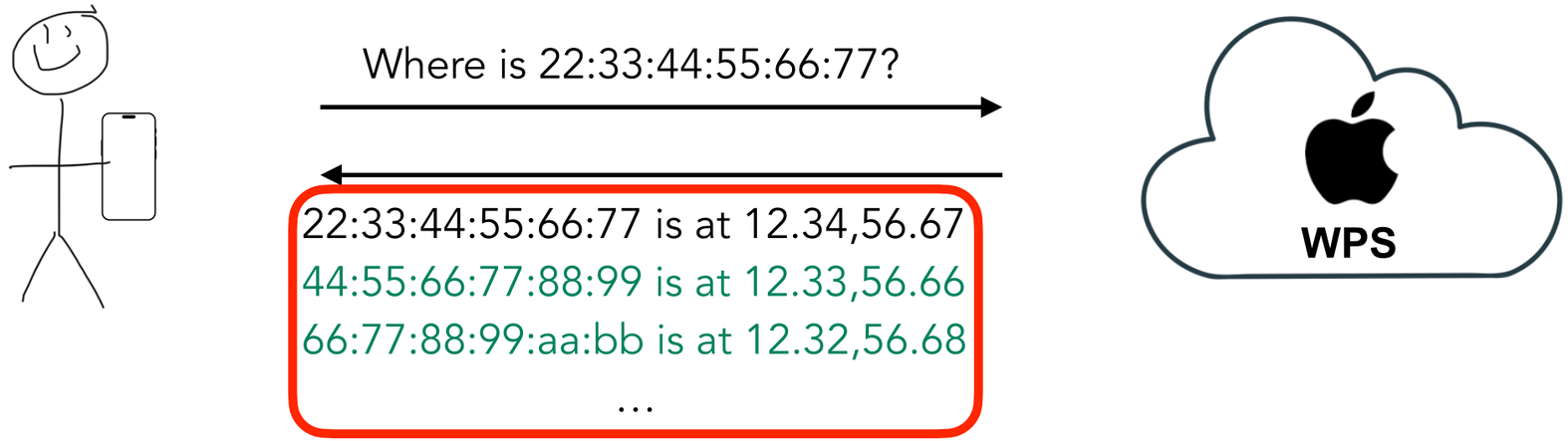
Apple's Wi-Fi Positioning System (WPS)



Returns up to 400 **additional unrequested** BSSID locations per query

Tracks the location of *ALL* APs — (was) no way to opt-out

Apple's Wi-Fi Positioning System (WPS)

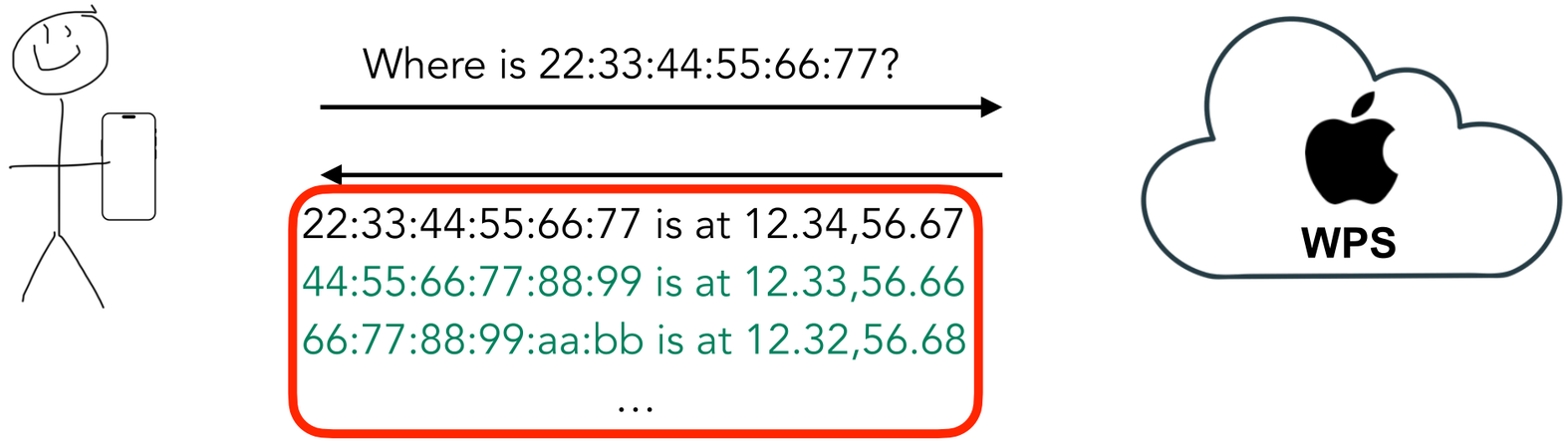


Returns up to 400 **additional unrequested** BSSID locations per query

Tracks the location of *ALL* APs — (was) no way to opt-out

Exposed via an unauthenticated, publicly-accessible API with no rate limit

Apple's Wi-Fi Positioning System (WPS)



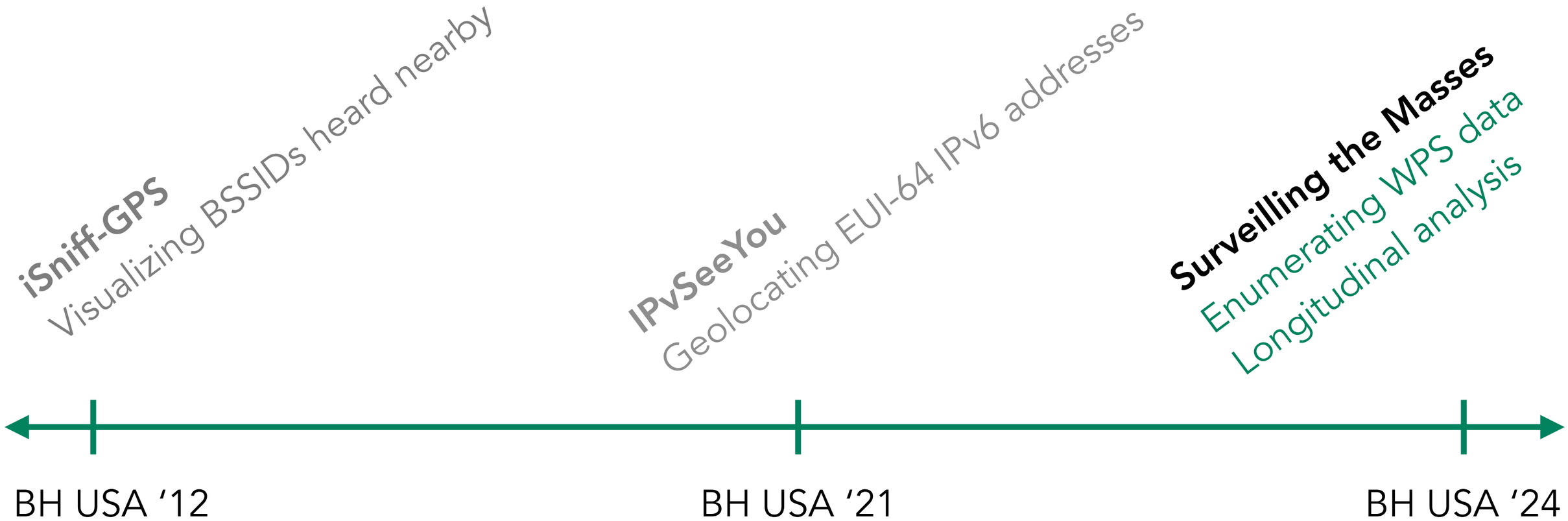
Returns up to 400 **additional unrequested** BSSID locations per query

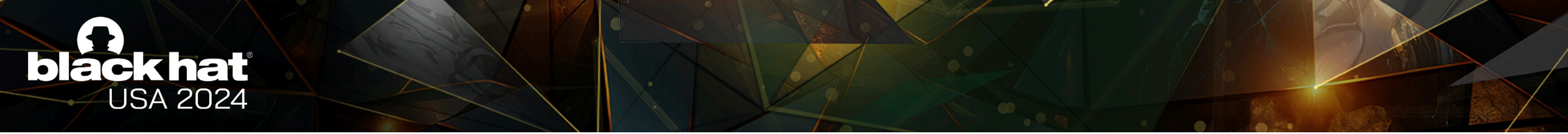
Tracks the location of *ALL* APs — (was) no way to opt-out

Exposed via an unauthenticated, publicly-accessible API with no rate limit

Permits several attacks by a low-power attacker

Apple's WPS & Black Hat





Querying Apple's WPS for fun and profit

How much can we learn about the world's Wi-Fi?

MAC Address Review

48-bit/6-byte hardware identifiers

MAC address(es) of Wi-Fi APs —
Basic Service Set Identifier (BSSID)

20:cc:27:a8:92:01

Upper three bytes IEEE-assigned to manufacturers
Organizationally-Unique Identifier (OUI)

MAC Address Review

48-bit/6-byte hardware identifiers

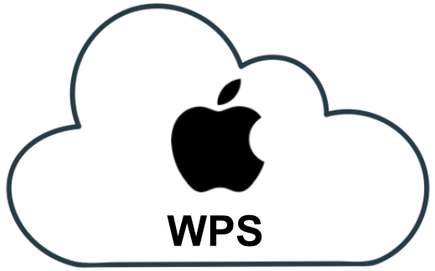
MAC address(es) of Wi-Fi APs —
Basic Service Set Identifier (BSSID)

20:cc:27:a8:92:01

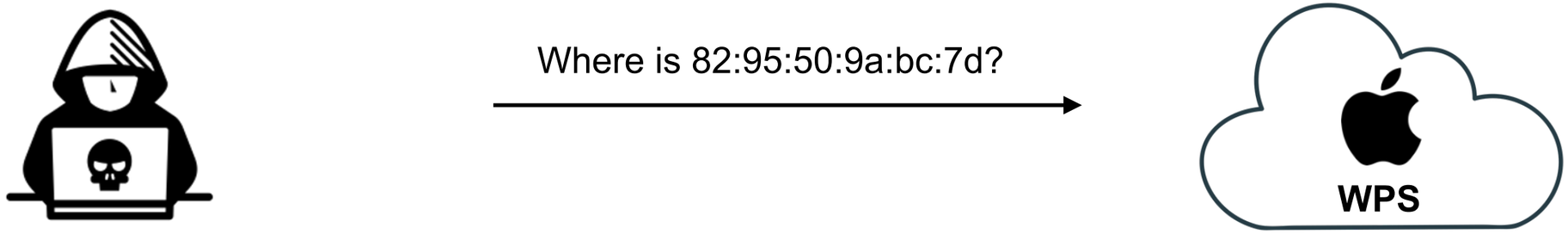
Cisco Systems

Upper three bytes IEEE-assigned to manufacturers
Organizationally-Unique Identifier (OUI)

Naïve Attack — Random BSSID Guessing

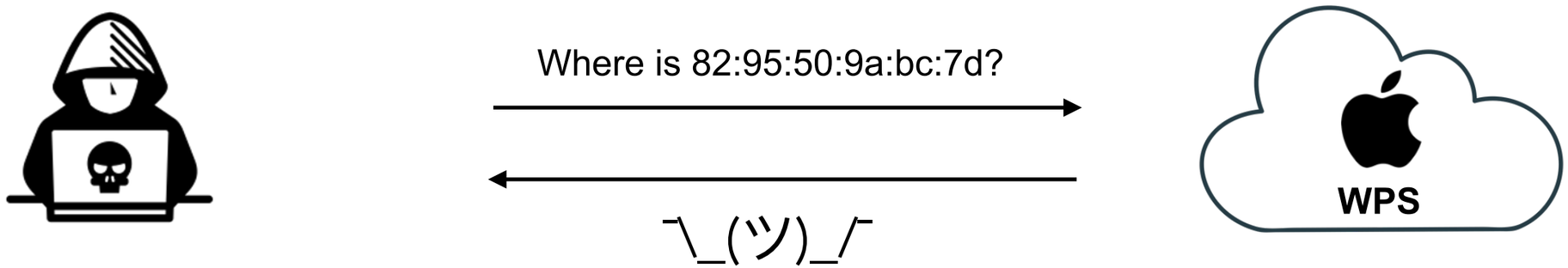


Naïve Attack — Random BSSID Guessing



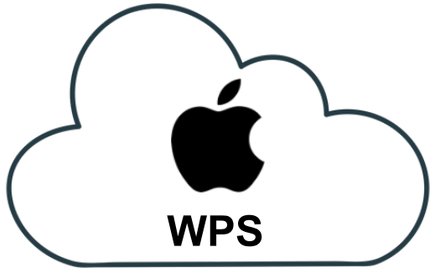
BSSIDs are 48 bits — guess random 48-bit numbers

Naïve Attack — Random BSSID Guessing



BSSIDs are 48 bits — guess random 48-bit numbers

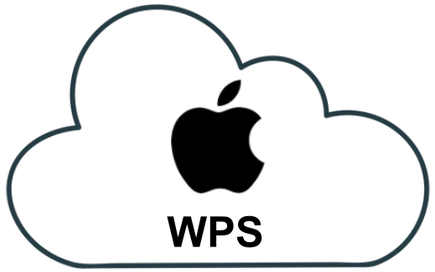
Naïve Attack — Random BSSID Guessing



BSSIDs are 48 bits — guess random 48-bit numbers

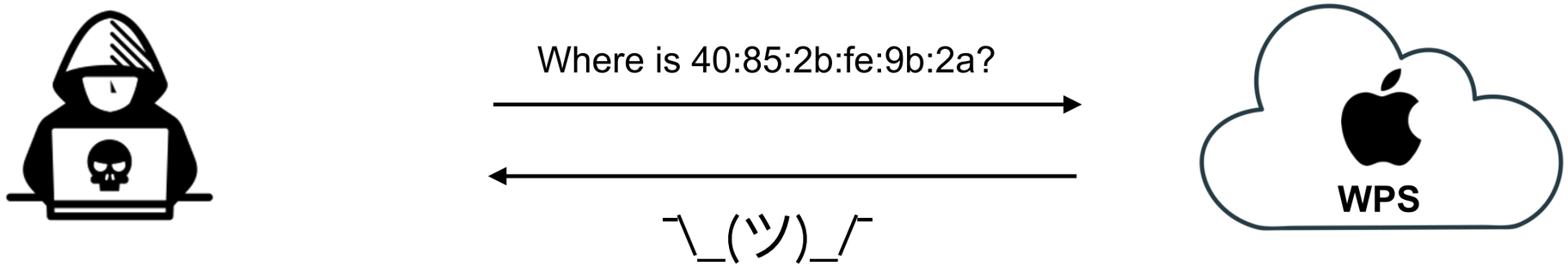
Naïve Attack — Random BSSID Guessing

Where is 40:85:2b:fe:9b:2a?



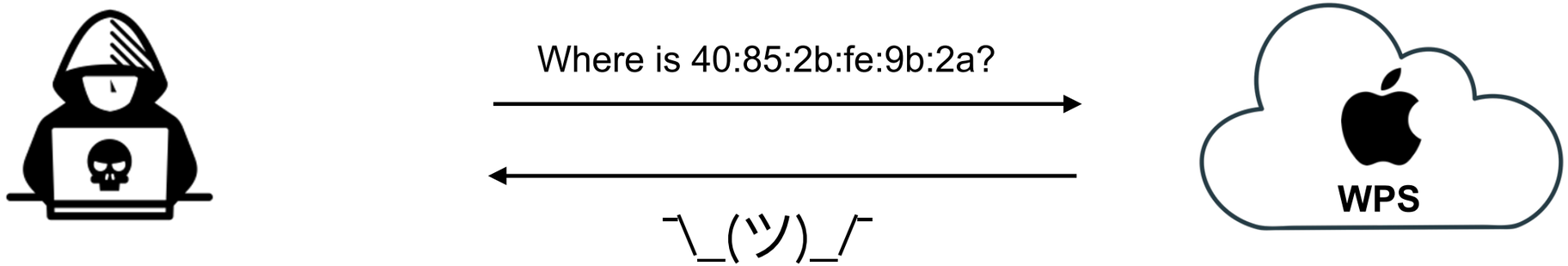
BSSIDs are 48 bits — guess random 48-bit numbers

Naïve Attack — Random BSSID Guessing



BSSIDs are 48 bits — guess random 48-bit numbers

Naïve Attack — Random BSSID Guessing



BSSIDs are 48 bits — guess random 48-bit numbers

281,474,976,710,656 possible BSSIDs — unlikely to guess an active BSSID

Improving the Odds

24 bits in OUI; 2^{24} ~ 16M possible OUIs

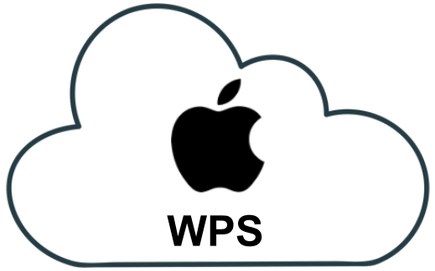
But **only 36k OUIs assigned by IEEE**

20:cc:27:a8:92:01

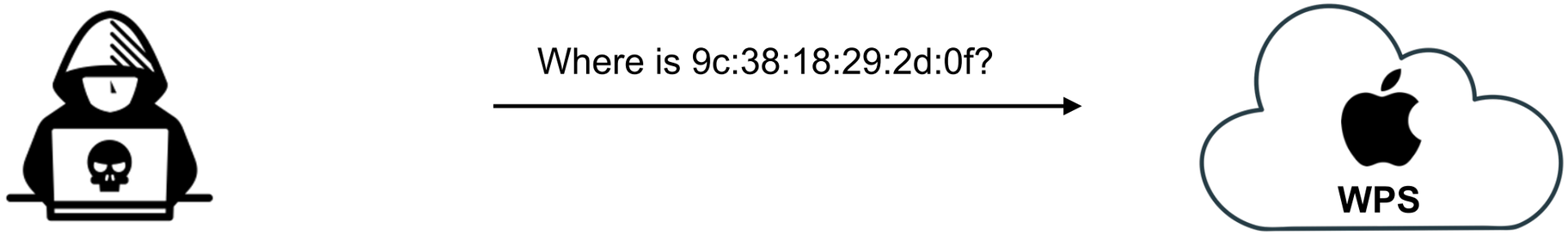
Solution: Guess random BSSIDs from allocated OUIs

>99% reduction in search space

OUI-Based, Intelligent BSSID Guessing

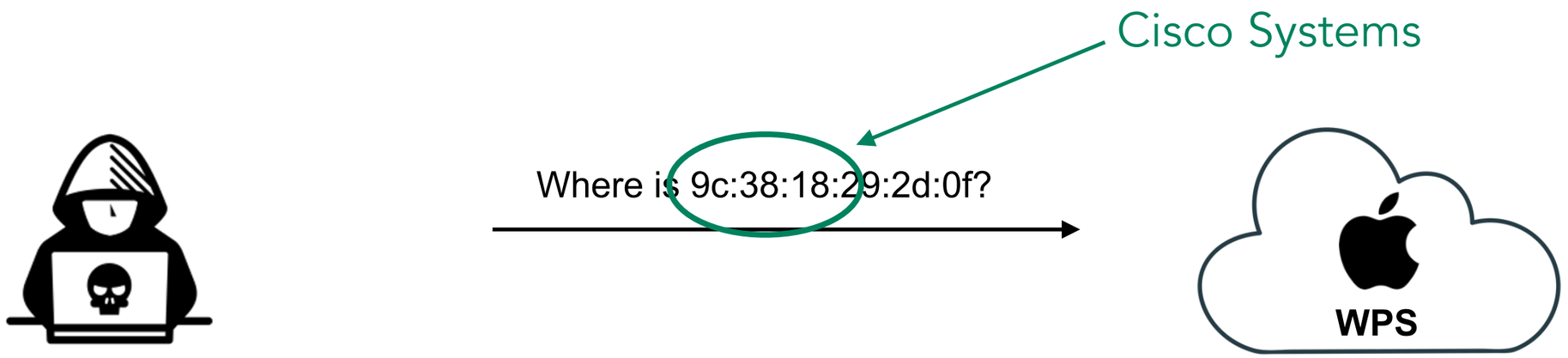


OUI-Based, Intelligent BSSID Guessing



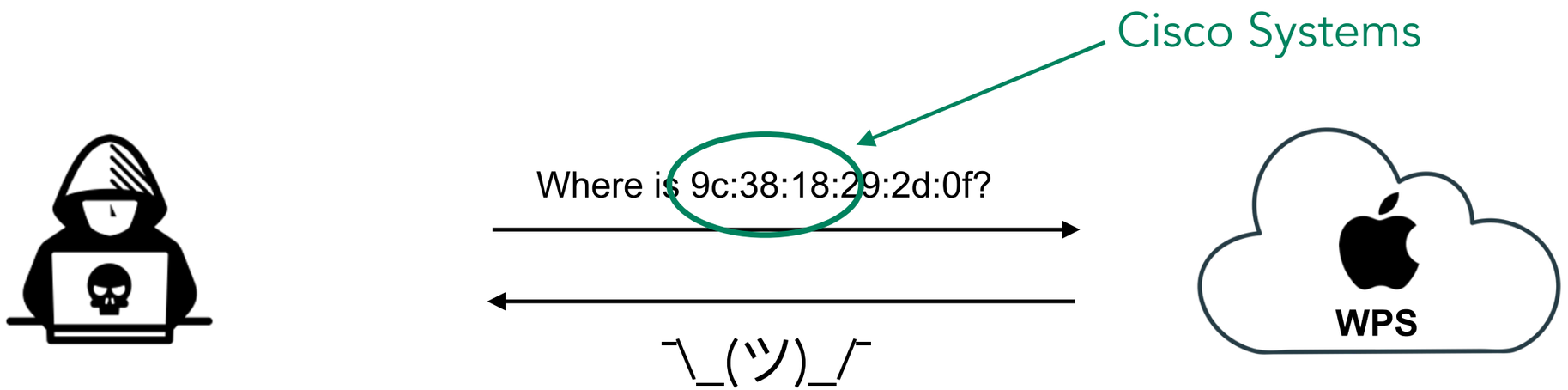
Still many “incorrect” BSSID guesses

OUI-Based, Intelligent BSSID Guessing



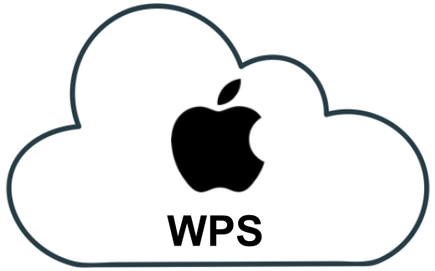
Still many “incorrect” BSSID guesses

OUI-Based, Intelligent BSSID Guessing



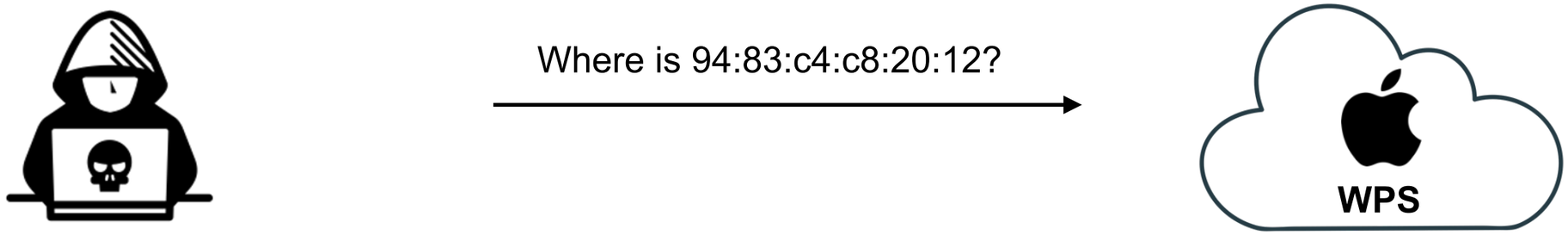
Still many “incorrect” BSSID guesses

OUI-Based, Intelligent BSSID Guessing



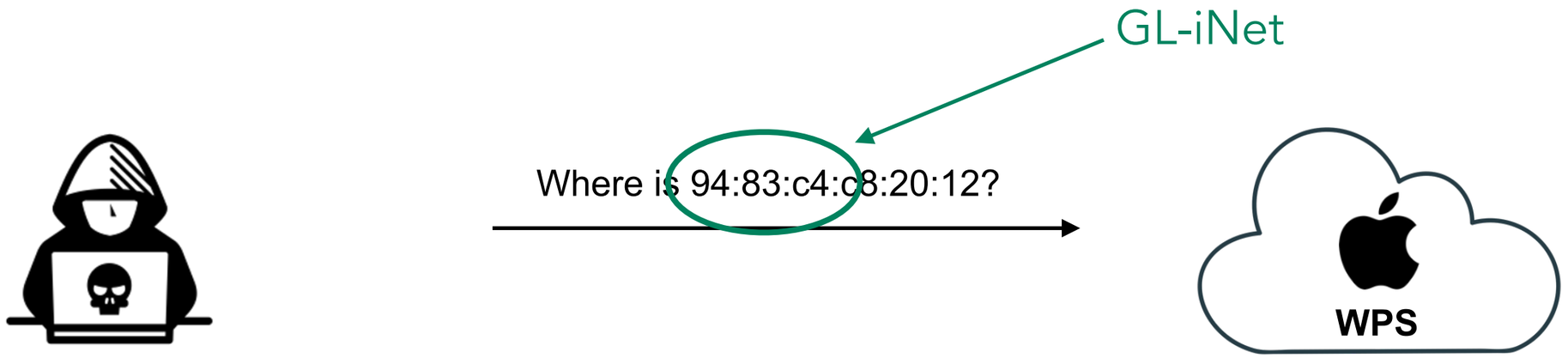
Still many “incorrect” BSSID guesses

OUI-Based, Intelligent BSSID Guessing



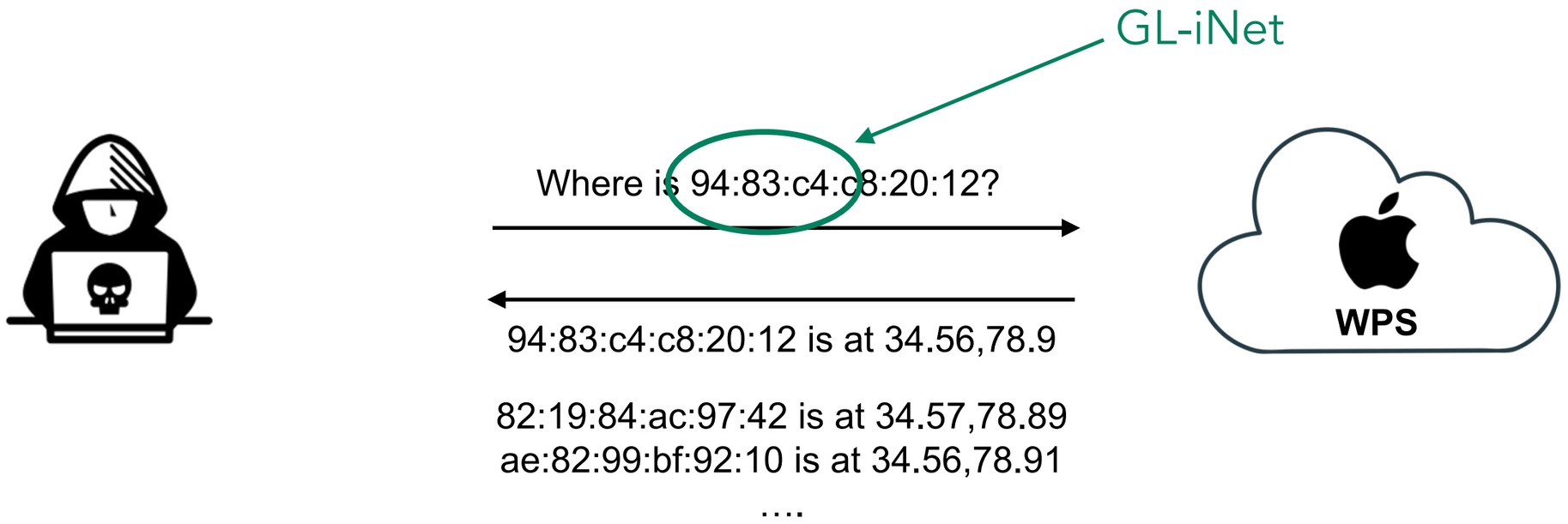
Still many “incorrect” BSSID guesses

OUI-Based, Intelligent BSSID Guessing



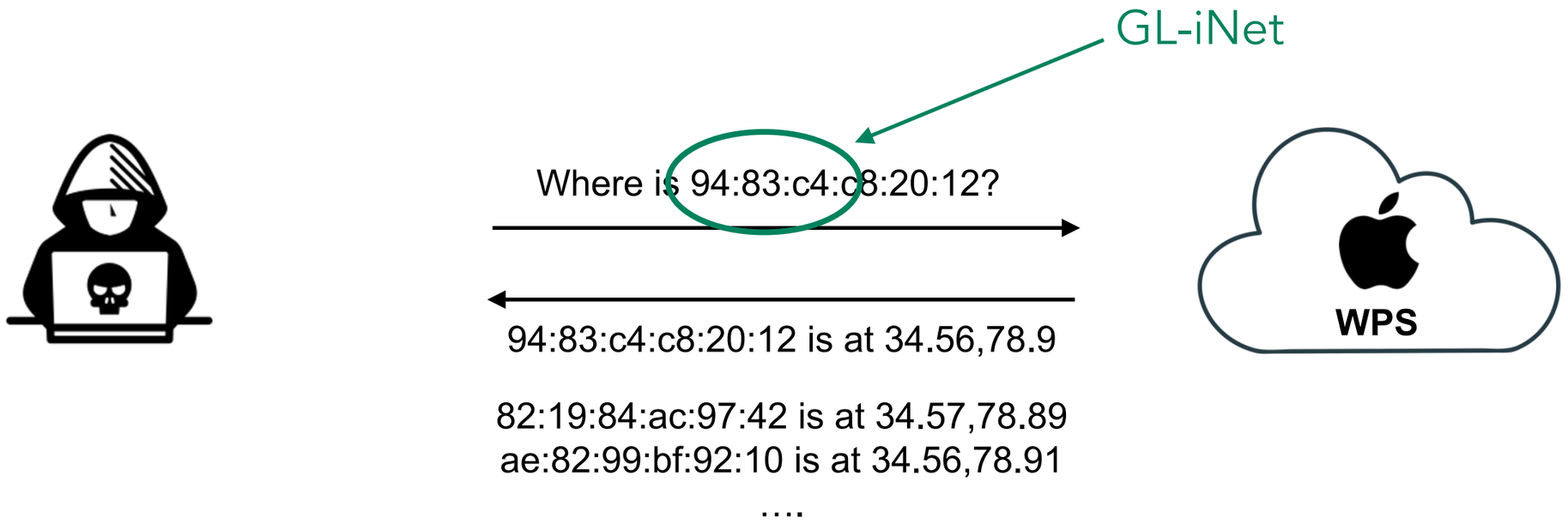
Still many “incorrect” BSSID guesses

OUI-Based, Intelligent BSSID Guessing



Still many “incorrect” BSSID guesses

OUI-Based, Intelligent BSSID Guessing



Still many “incorrect” BSSID guesses

But, odds of correctly guessing an active BSSID **much** higher

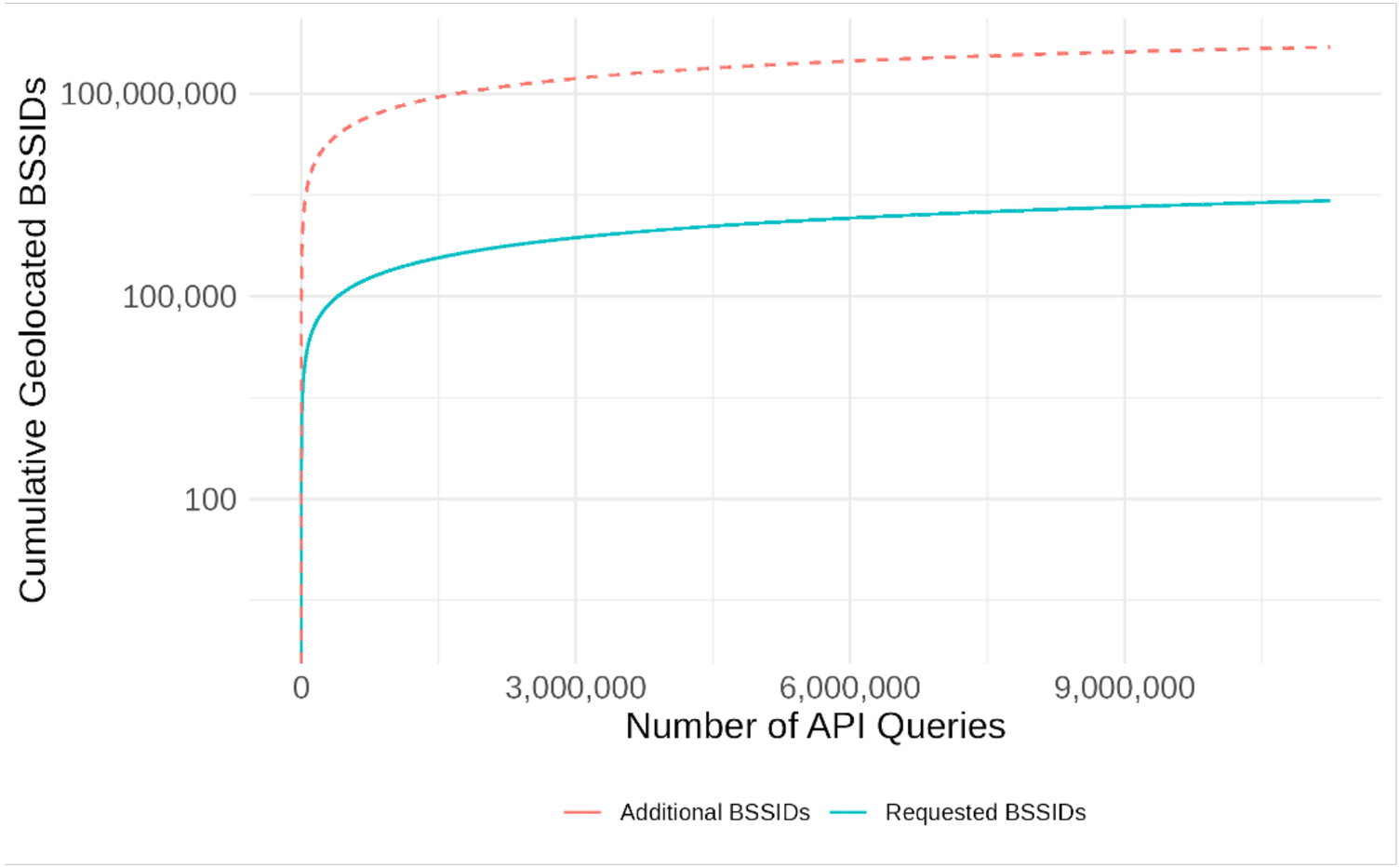
OUI-Based, Intelligent BSSID Guessing

Queried Apple WPS for 2^{14} random BSSIDs/OUI

"Extra" up-to-400 BSSIDs provide incredible ROI

1 day to ~100M BSSIDs

4 days to ~500M BSSIDs



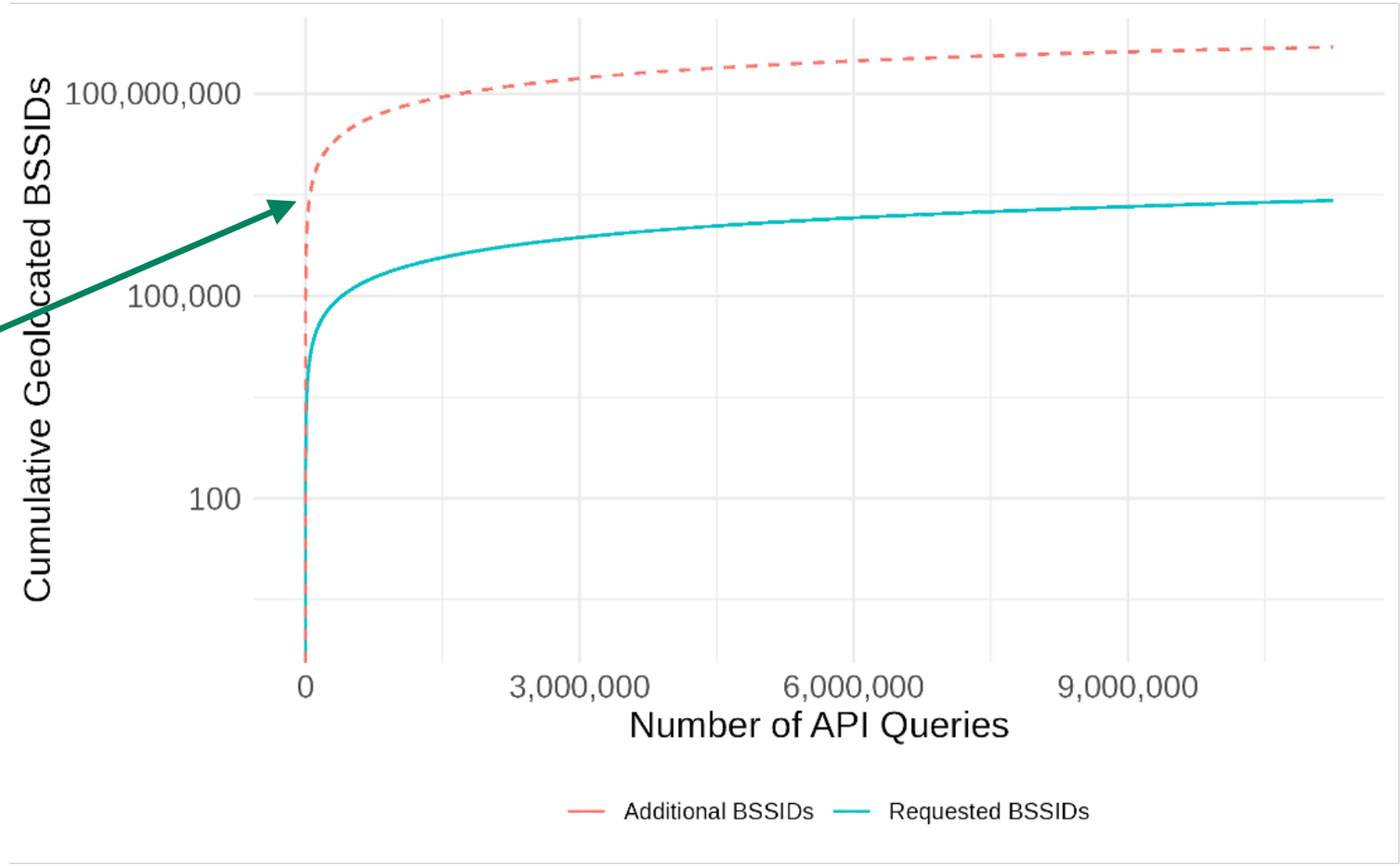
OUI-Based, Intelligent BSSID Guessing

Queried Apple WPS for 2^{14} random BSSIDs/OUI

"Extra" up-to-400 BSSIDs provide incredible ROI

1 day to ~100M BSSIDs

4 days to ~500M BSSIDs



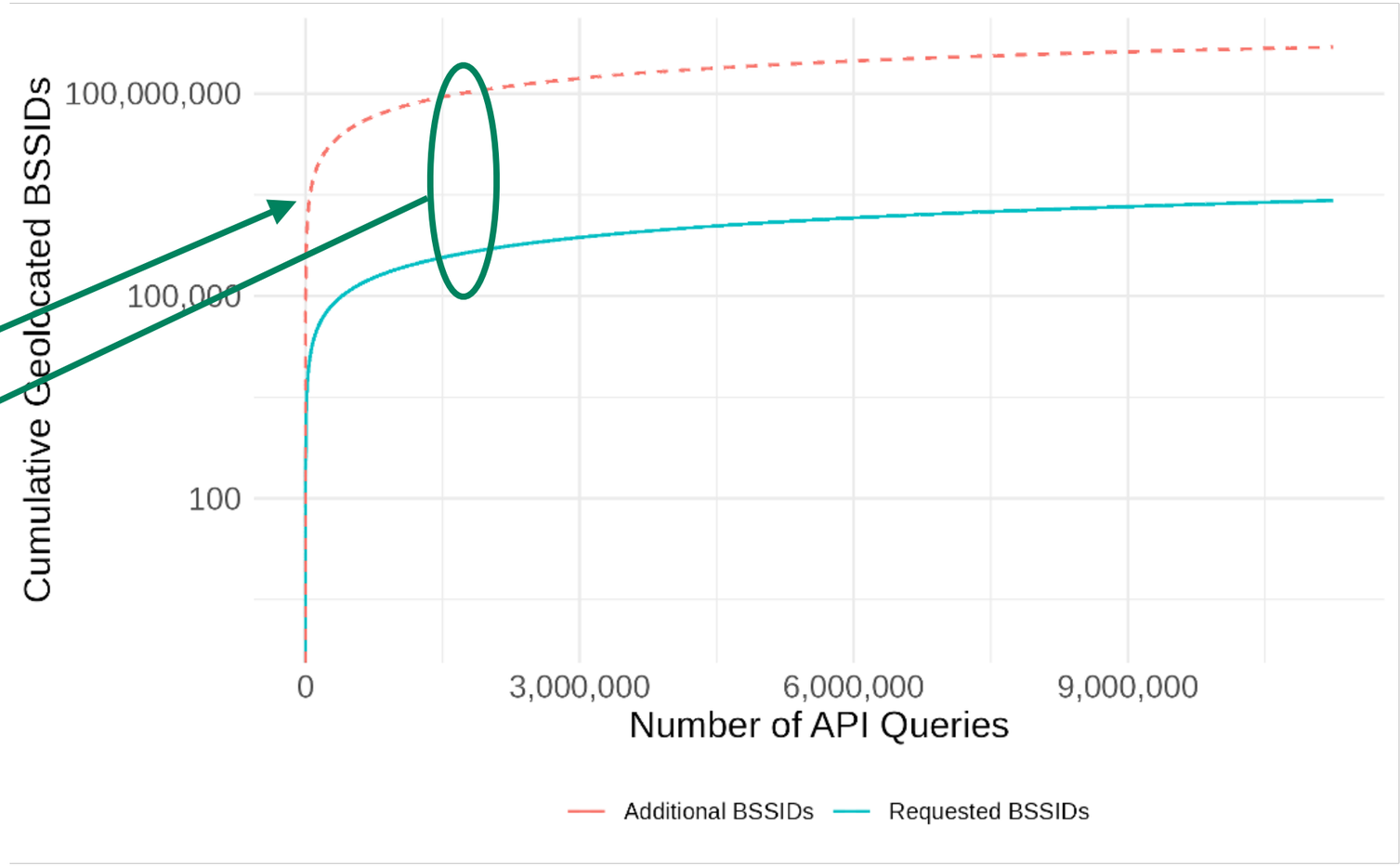
OUI-Based, Intelligent BSSID Guessing

Queried Apple WPS for 2^{14} random BSSIDs/OUI

"Extra" up-to-400 BSSIDs provide incredible ROI

1 day to ~100M BSSIDs

4 days to ~500M BSSIDs



OUI-Based, Intelligent BSSID Guessing

Queried Apple WPS for 2^{14} random BSSIDs/OUI

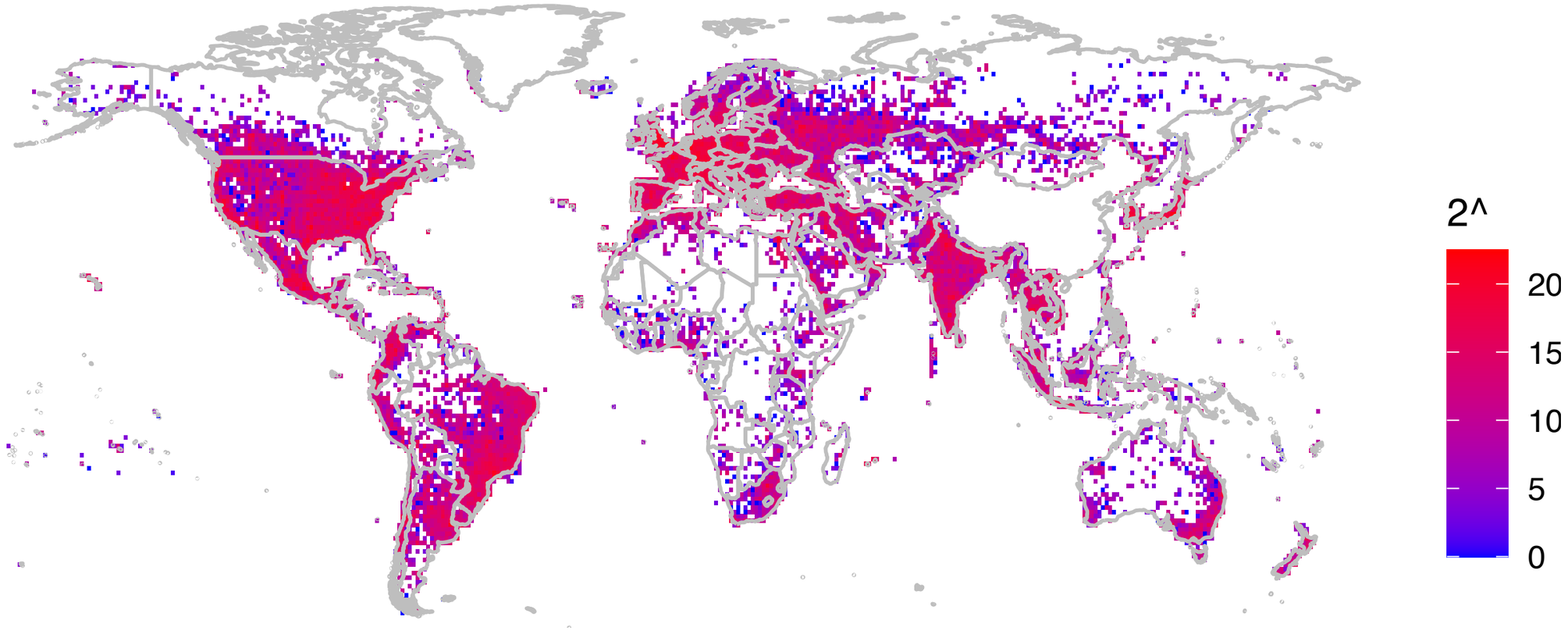
"Extra" up-to-400 BSSIDs provide incredible ROI

1 day to ~100M BSSIDs

4 days to ~500M BSSIDs

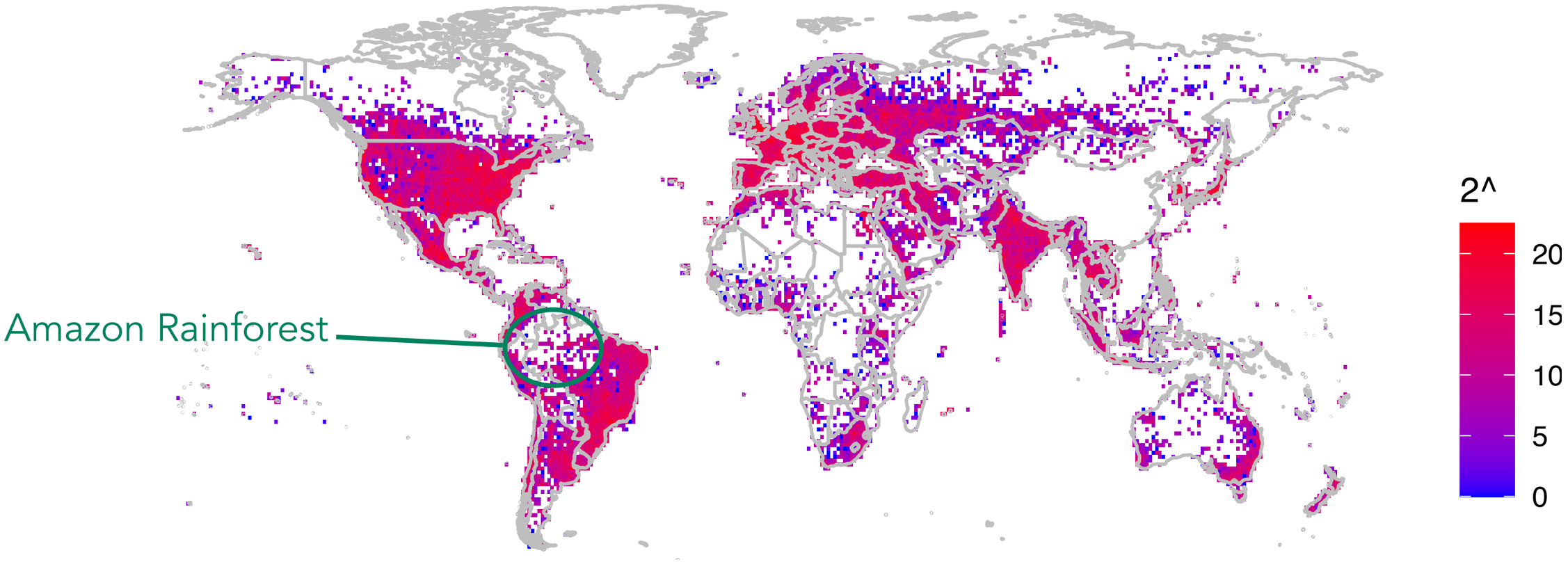
100 BSSIDs per query

Correctly-Guessed BSSID Geolocations (~500M)



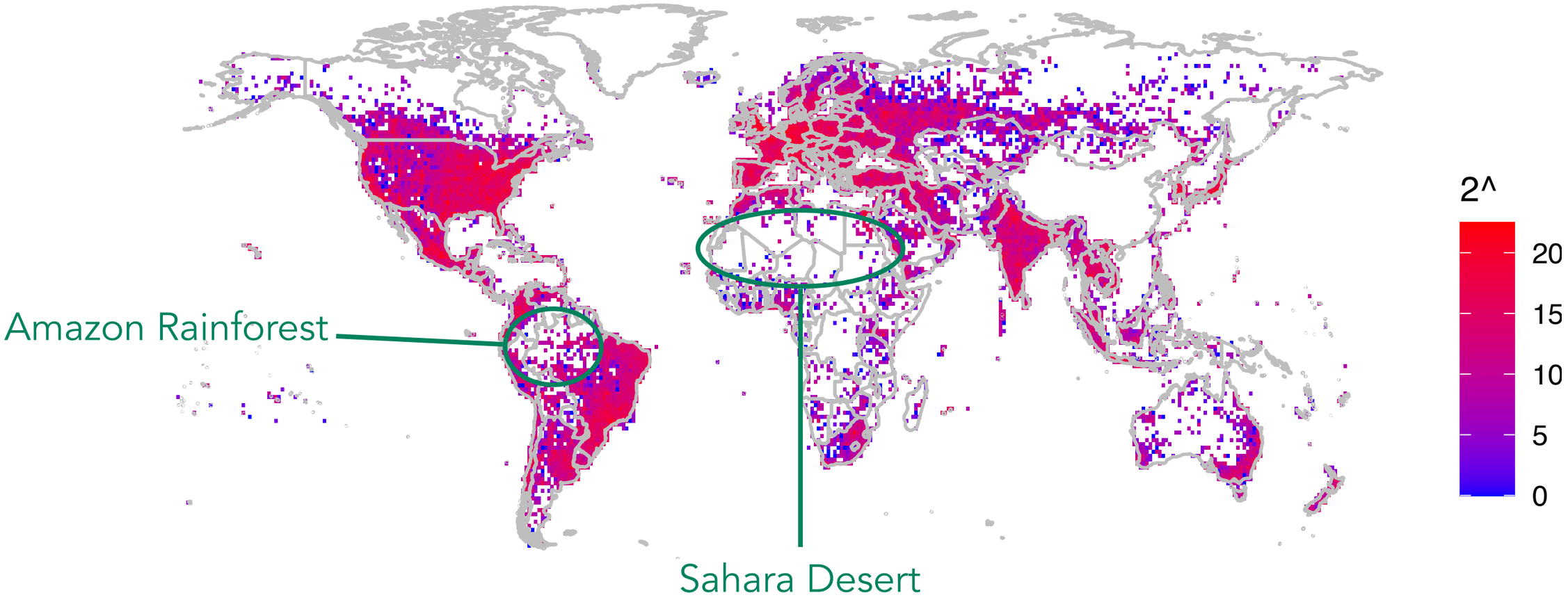
BSSID density (largely) mirrors that of human population density*

Correctly-Guessed BSSID Geolocations (~500M)



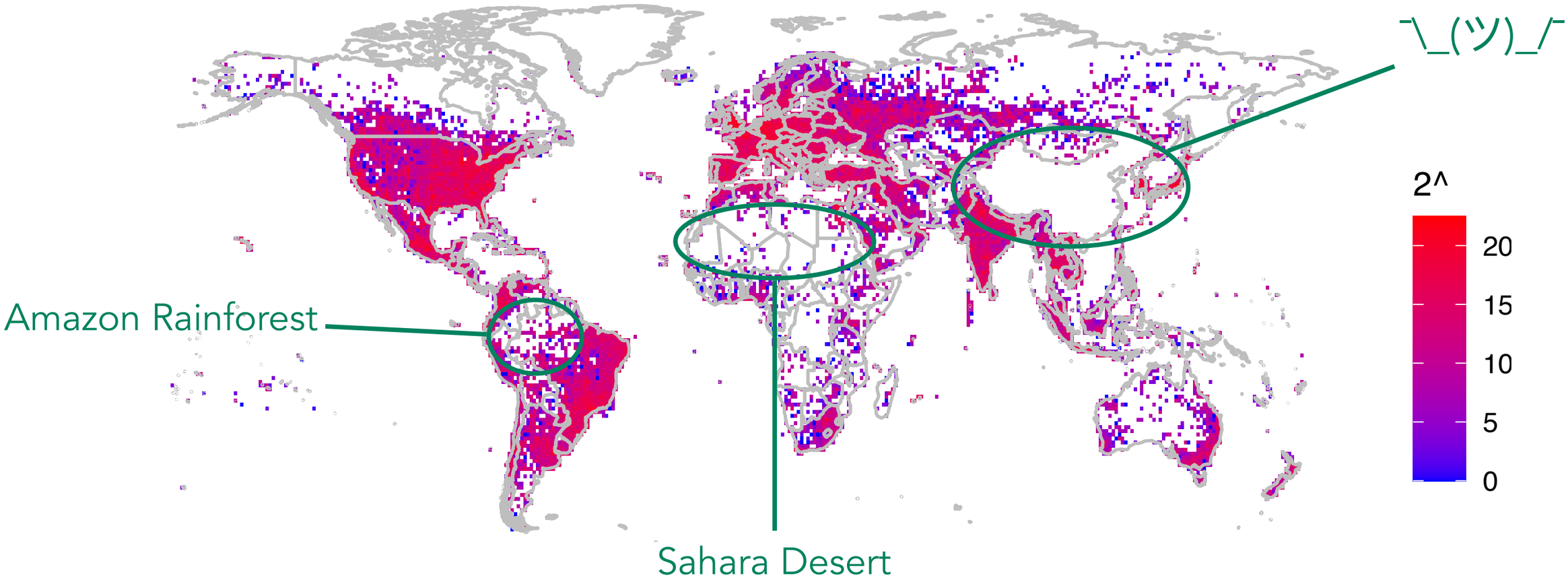
BSSID density (largely) mirrors that of human population density*

Correctly-Guessed BSSID Geolocations (~500M)



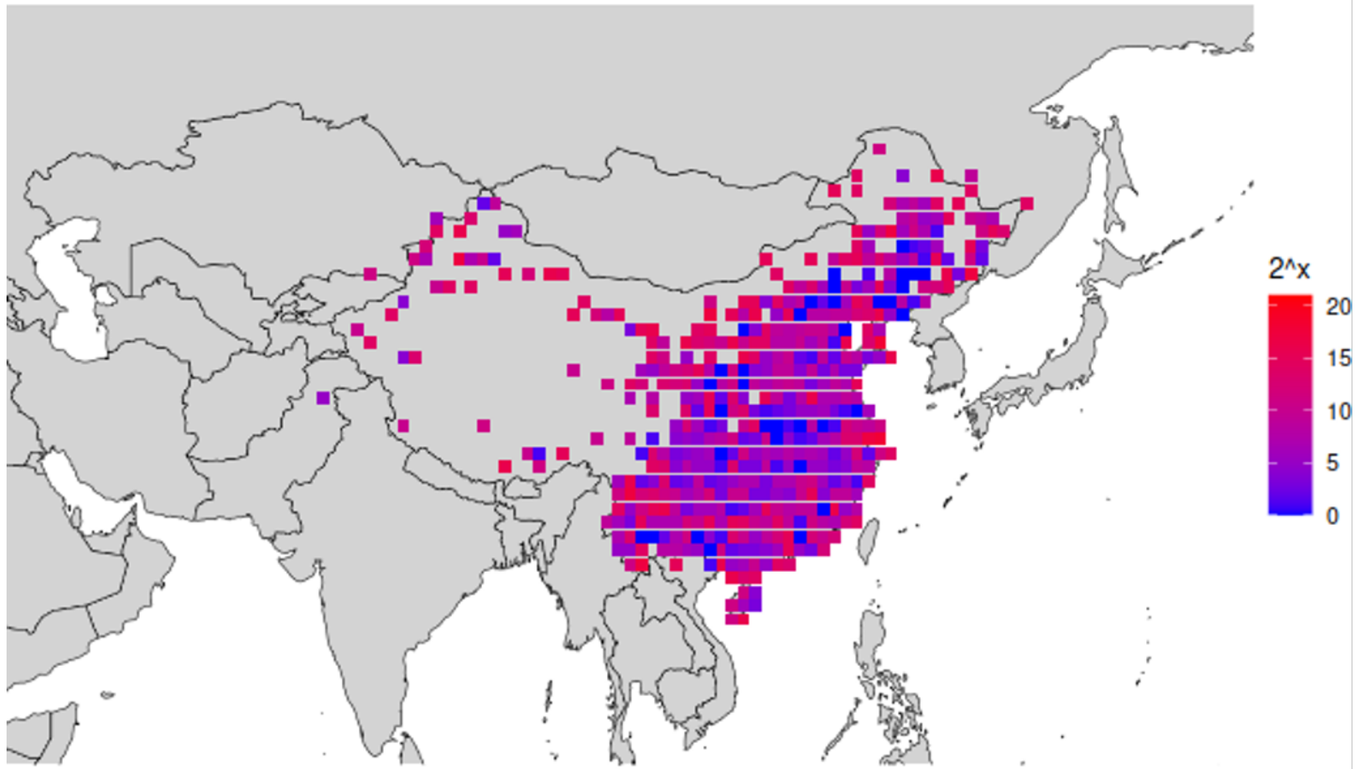
BSSID density (largely) mirrors that of human population density*

Correctly-Guessed BSSID Geolocations (~500M)



BSSID density (largely) mirrors that of human population density*

China-Specific Apple WPS



Credit to JaneCCP/Antonio Cheung (acheong08) for finding China API endpoint

BSSIDs rarely (but not never) appear in non-China Apple WPS

China-specific WPS API exists, perhaps due to data restrictions

China-specific API is **globally-queryable**

Case Study: Remote-est Wi-Fi on Earth

BSSID geolocations on all 7 continents

Wi-Fi present in extremely austere, remote locations

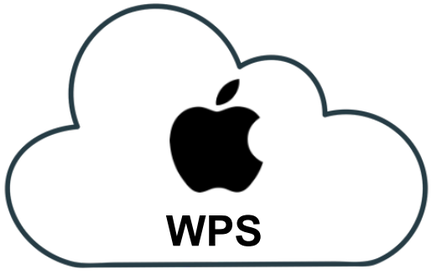
BSSID geolocations among populations of <100 people

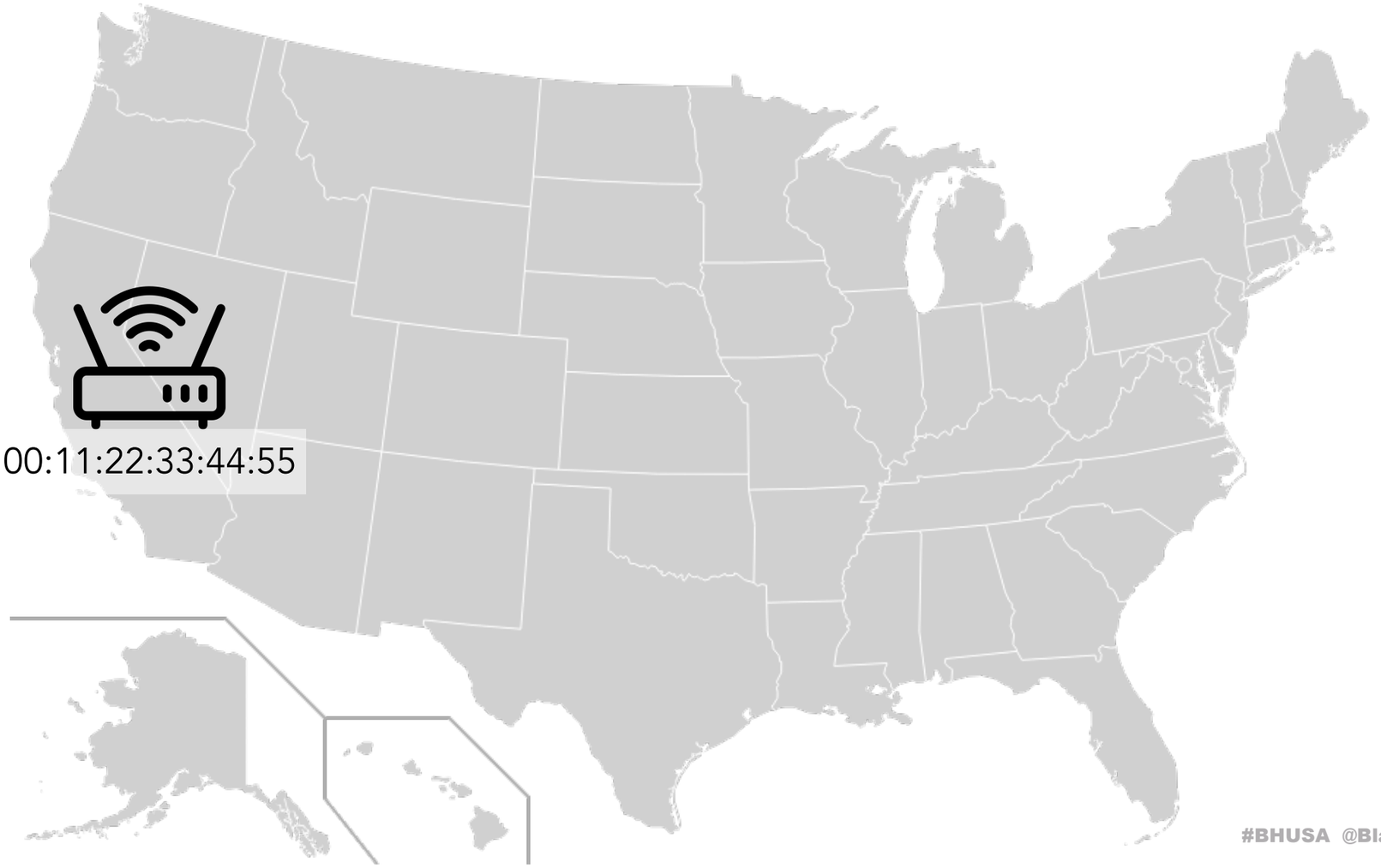
Targeted Surveillance Attack

Stalking via Wi-Fi router

Privacy Threat 1: Targeted Tracking

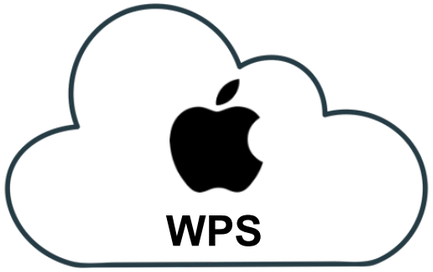
BSSIDs are persistent identifiers

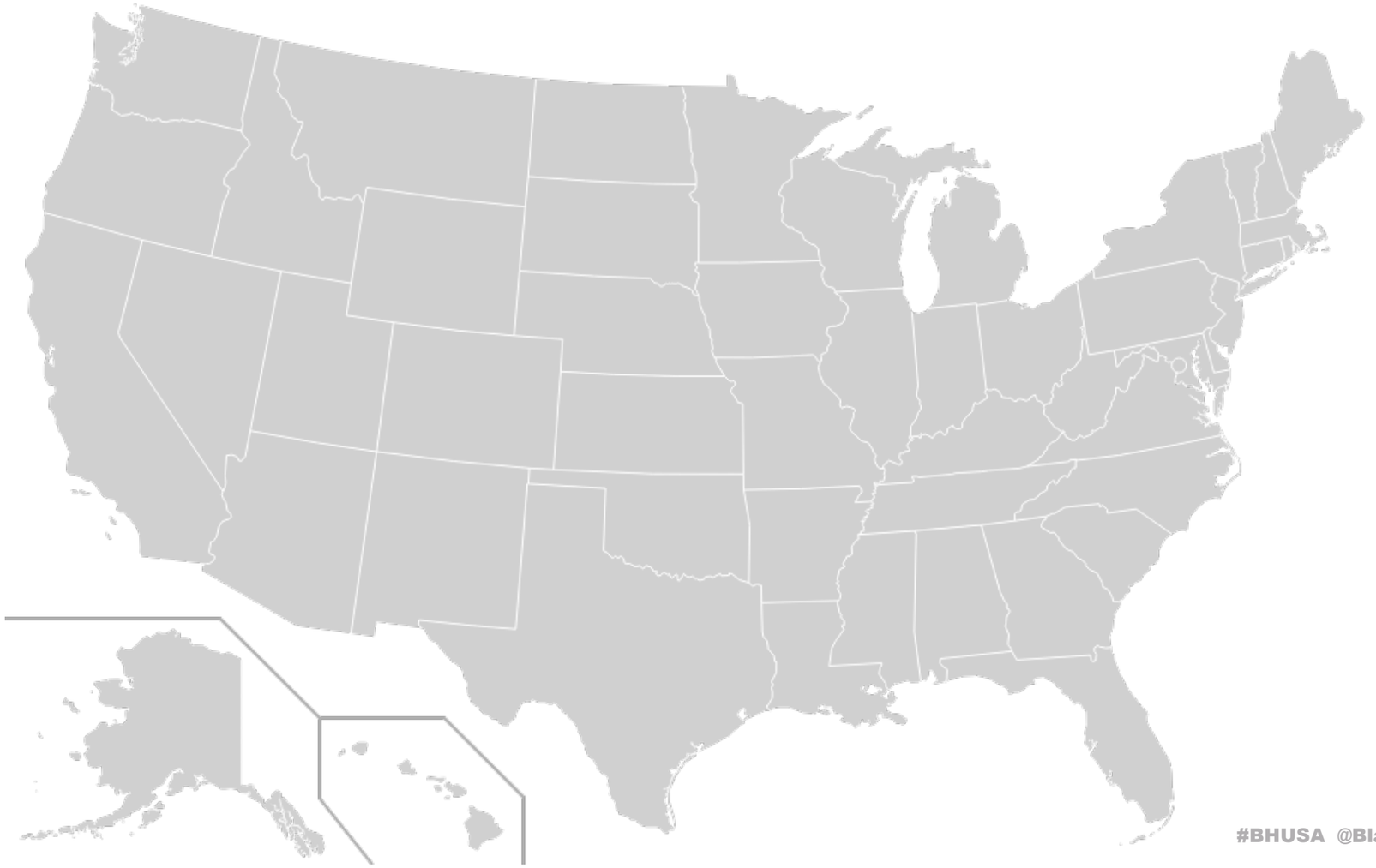




Privacy Threat 1: Targeted Tracking

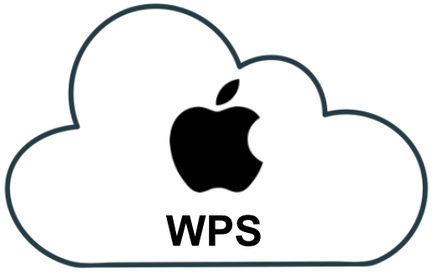
BSSIDs are persistent identifiers

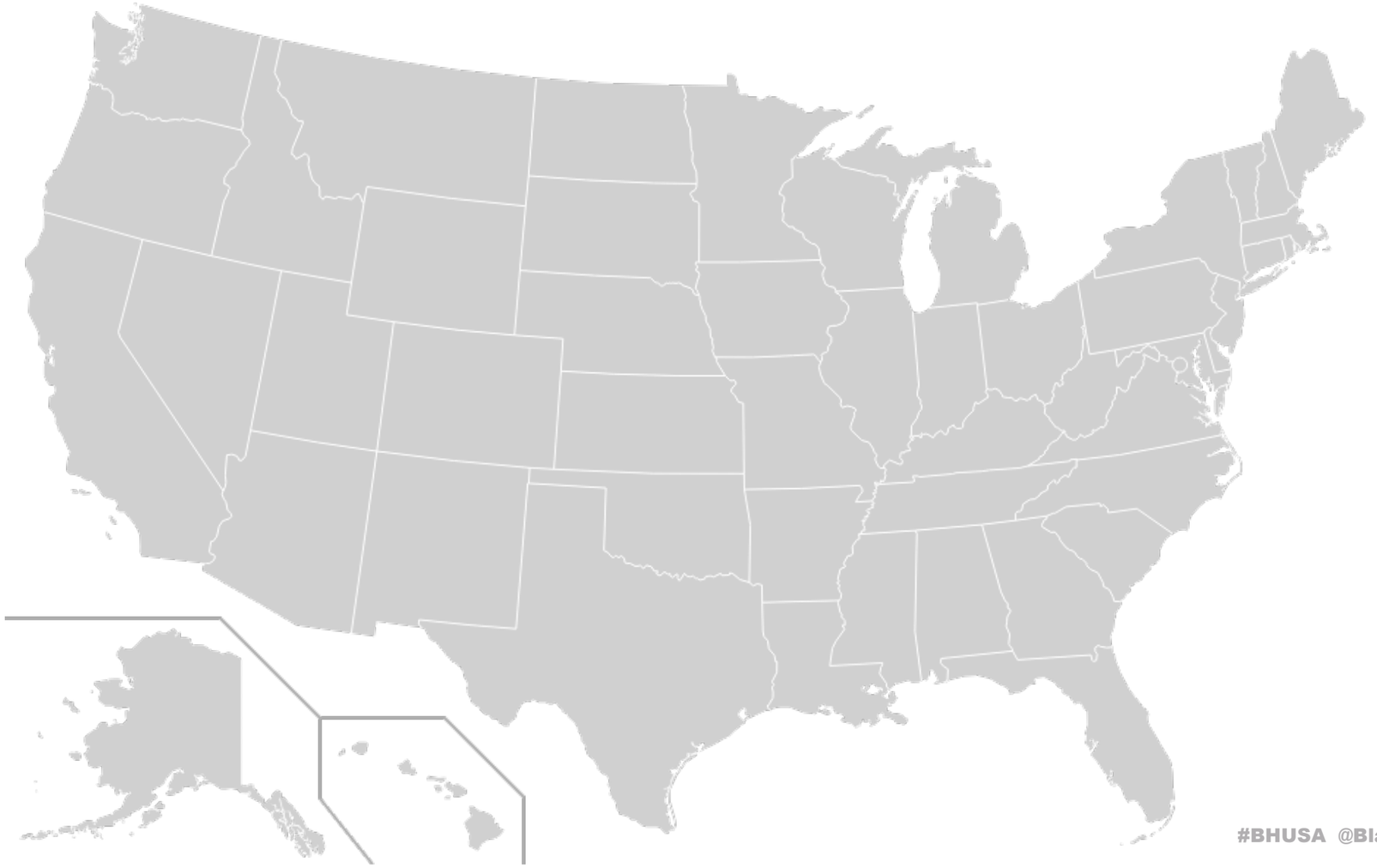




Privacy Threat 1: Targeted Tracking

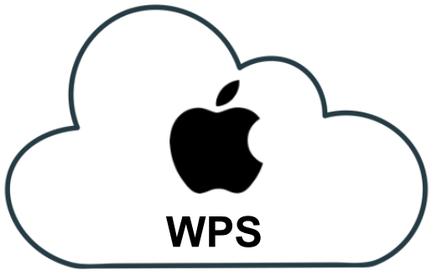
BSSIDs are persistent identifiers





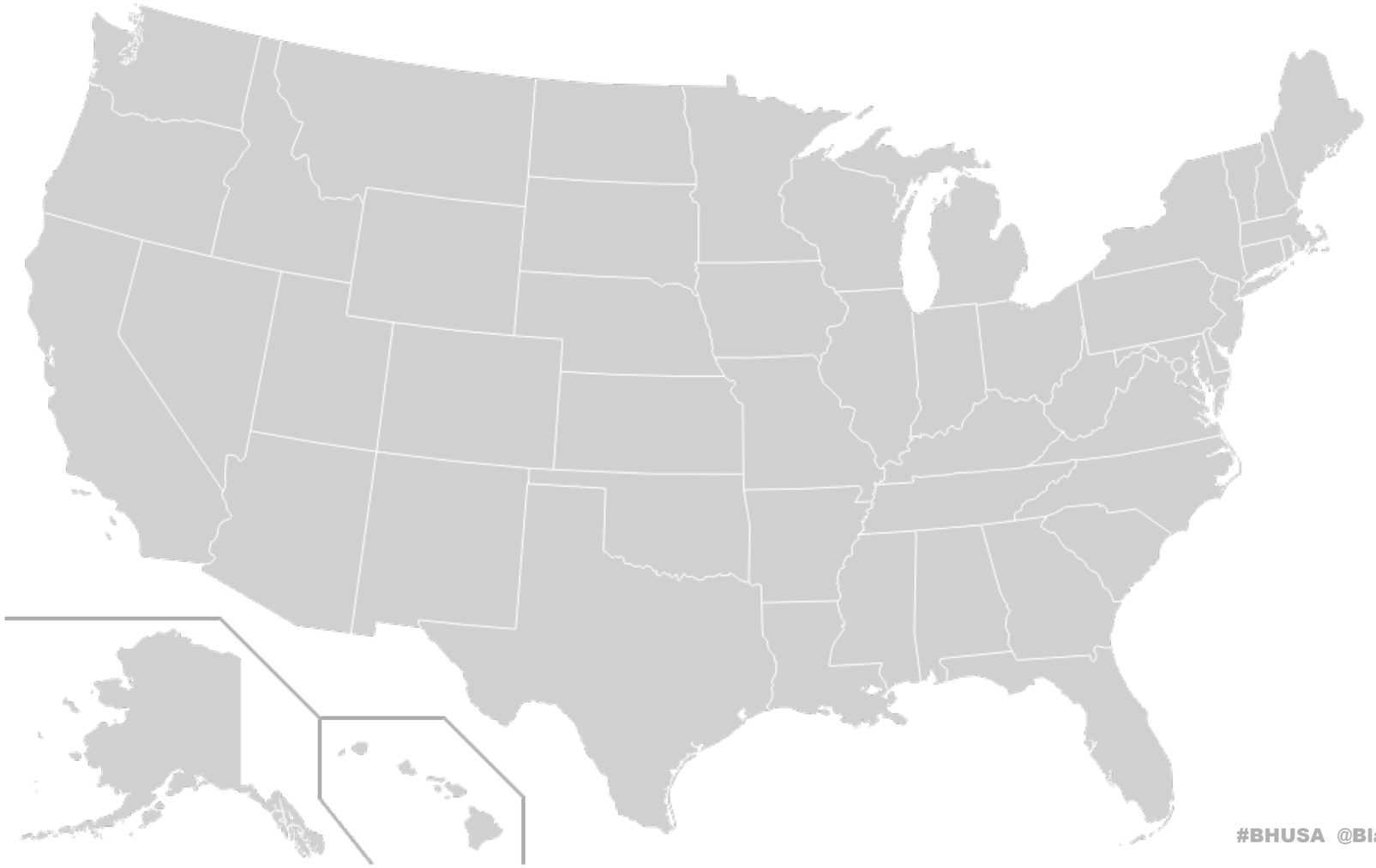
Privacy Threat 1: Targeted Tracking

BSSIDs are persistent identifiers



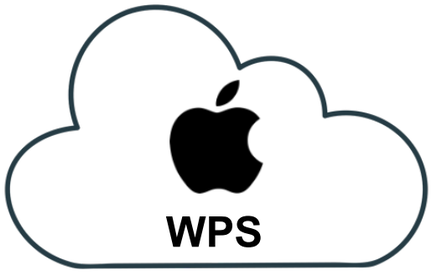
Where is
00:11:22:33:44:55?

?



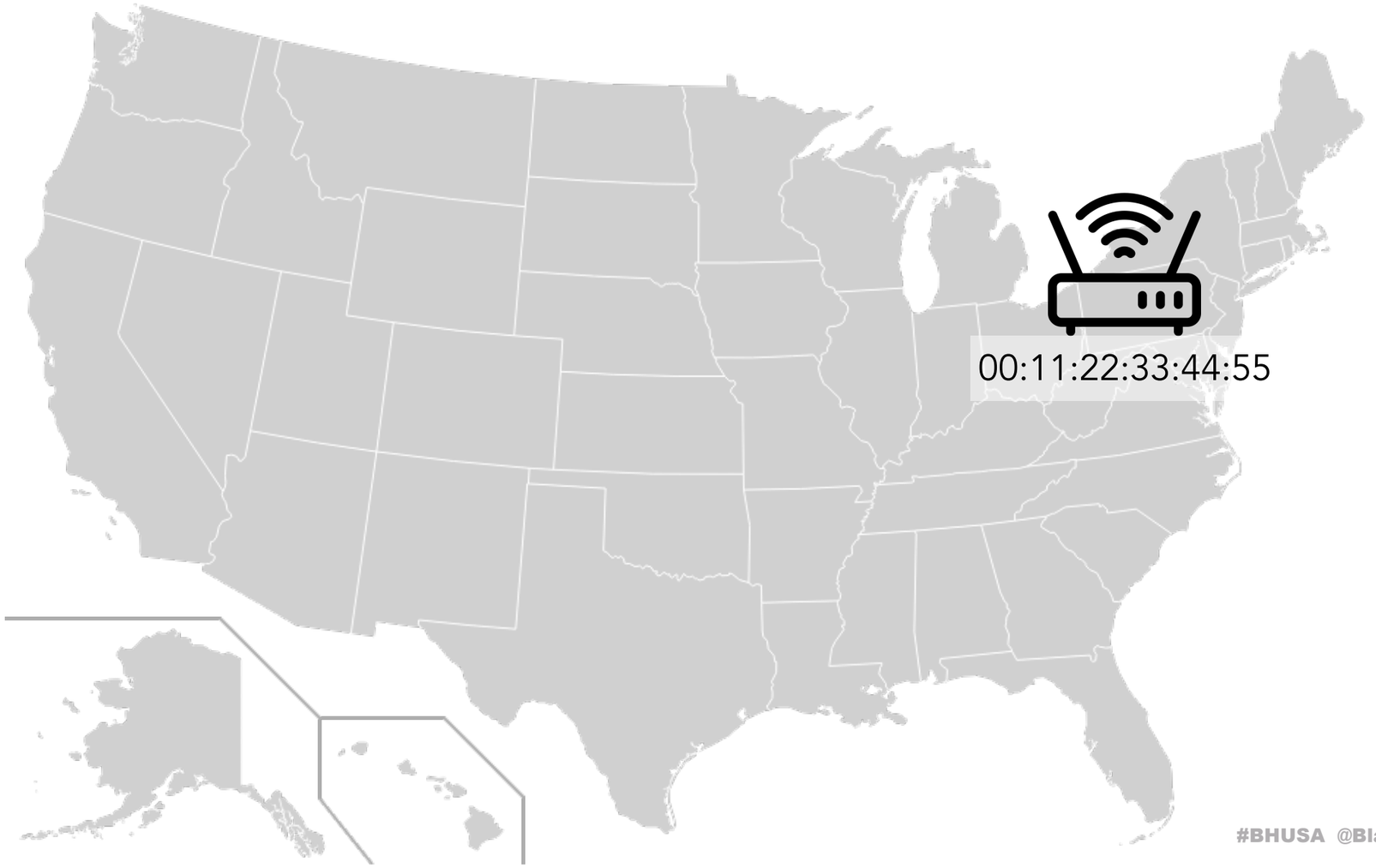
Privacy Threat 1: Targeted Tracking

BSSIDs are persistent identifiers



Where is
00:11:22:33:44:55?

?



Mass Surveillance Attacks

What can you learn from all the Wi-Fi?

Privacy Threat 2: Vendor Enumeration

OUI (typically) identifies the device manufacturer

Possible to enumerate all 16M BSSIDs in an OUI in a matter of hours

Trivial geolocation of privacy-sensitive devices/manufacturers

Privacy Threat 2: Vendor Enumeration

OUI (typically) identifies the device manufacturer

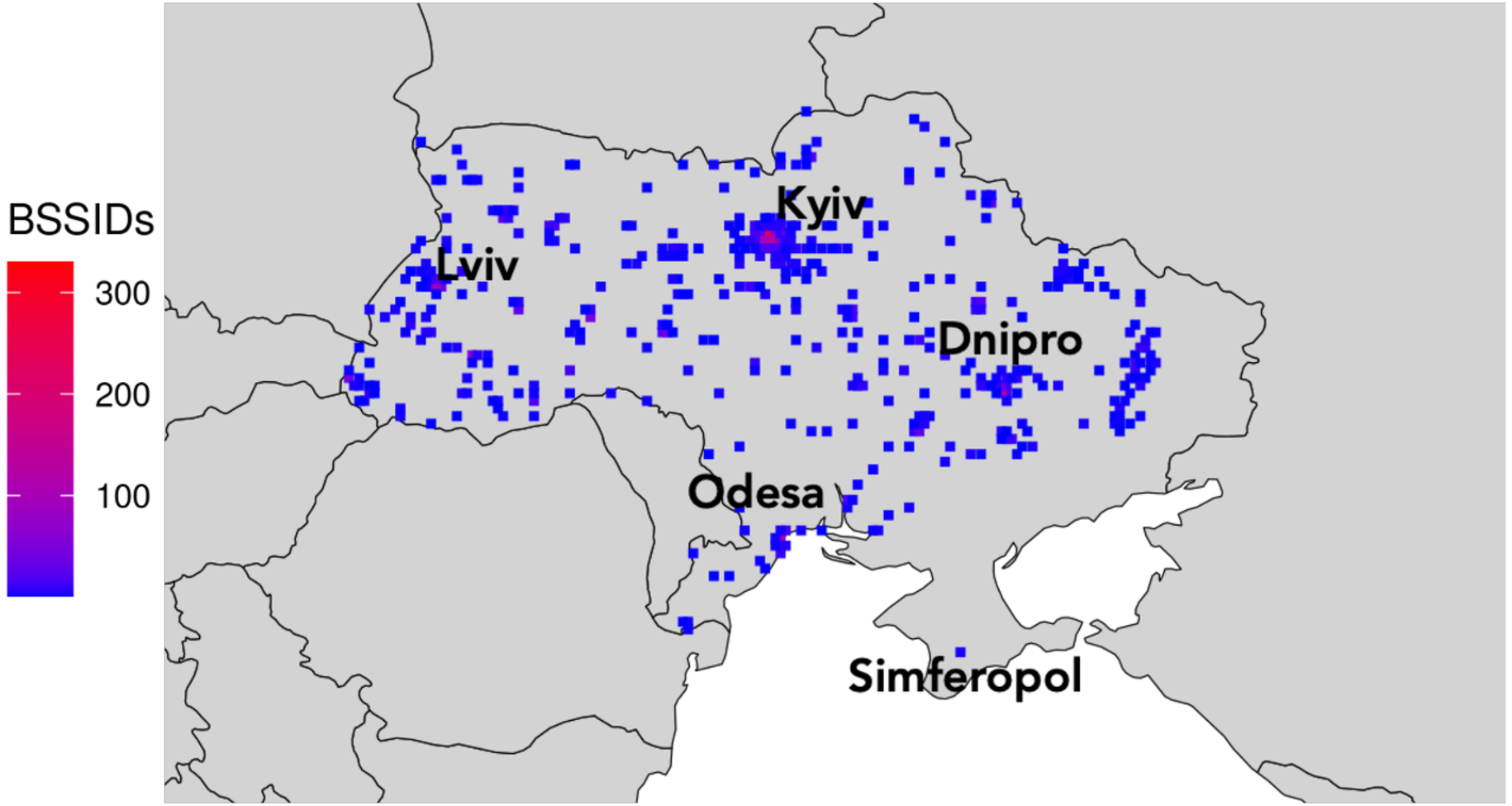
Possible to enumerate all 16M BSSIDs in an OUI in a matter of hours

Trivial geolocation of privacy-sensitive devices/manufacturers

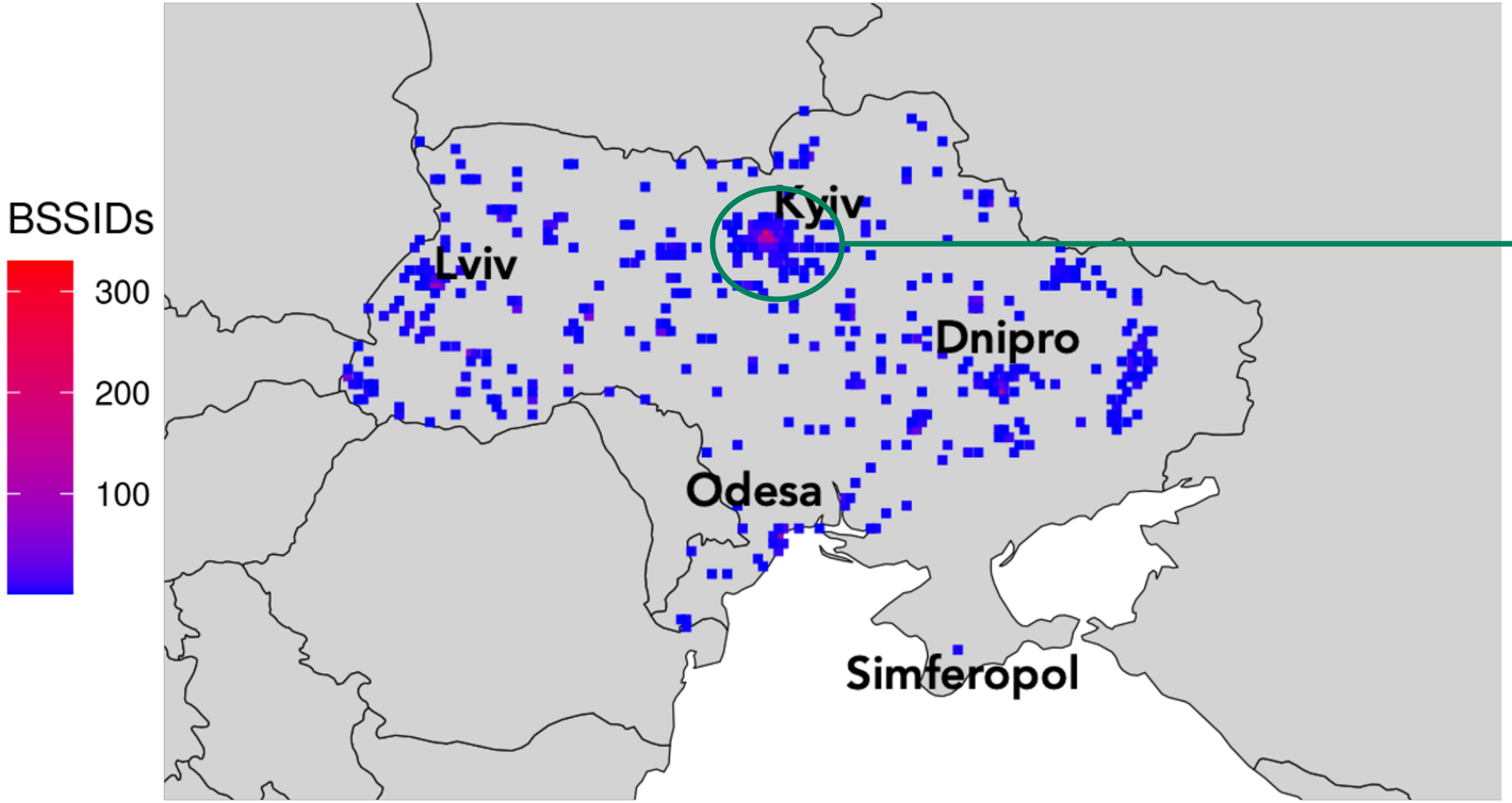
74:24:9f:a8:92:01

Starlink (TIBRO)

Case Study: Russia-Ukraine War

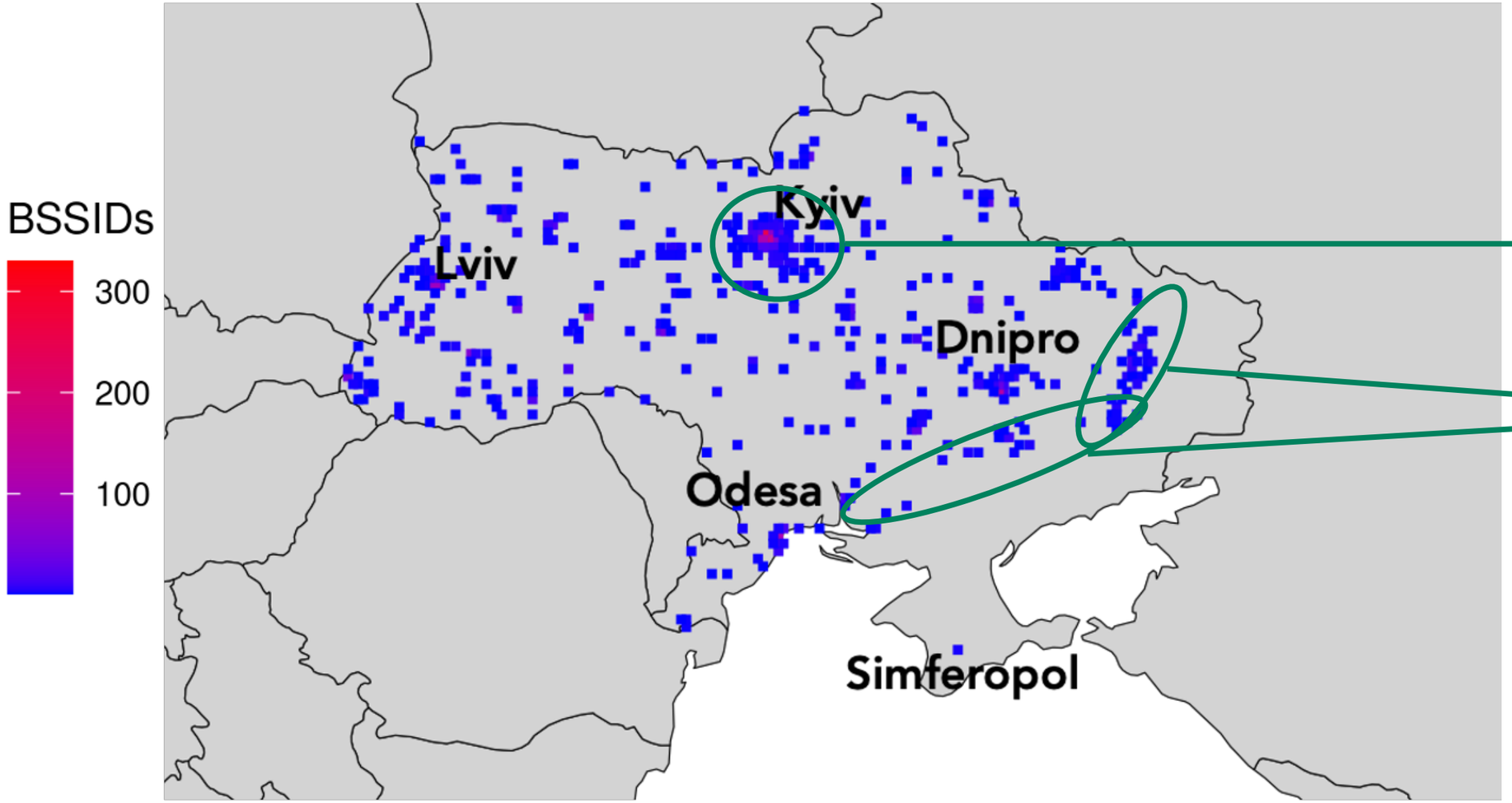


Case Study: Russia-Ukraine War



Hotspots in major cities

Case Study: Russia-Ukraine War

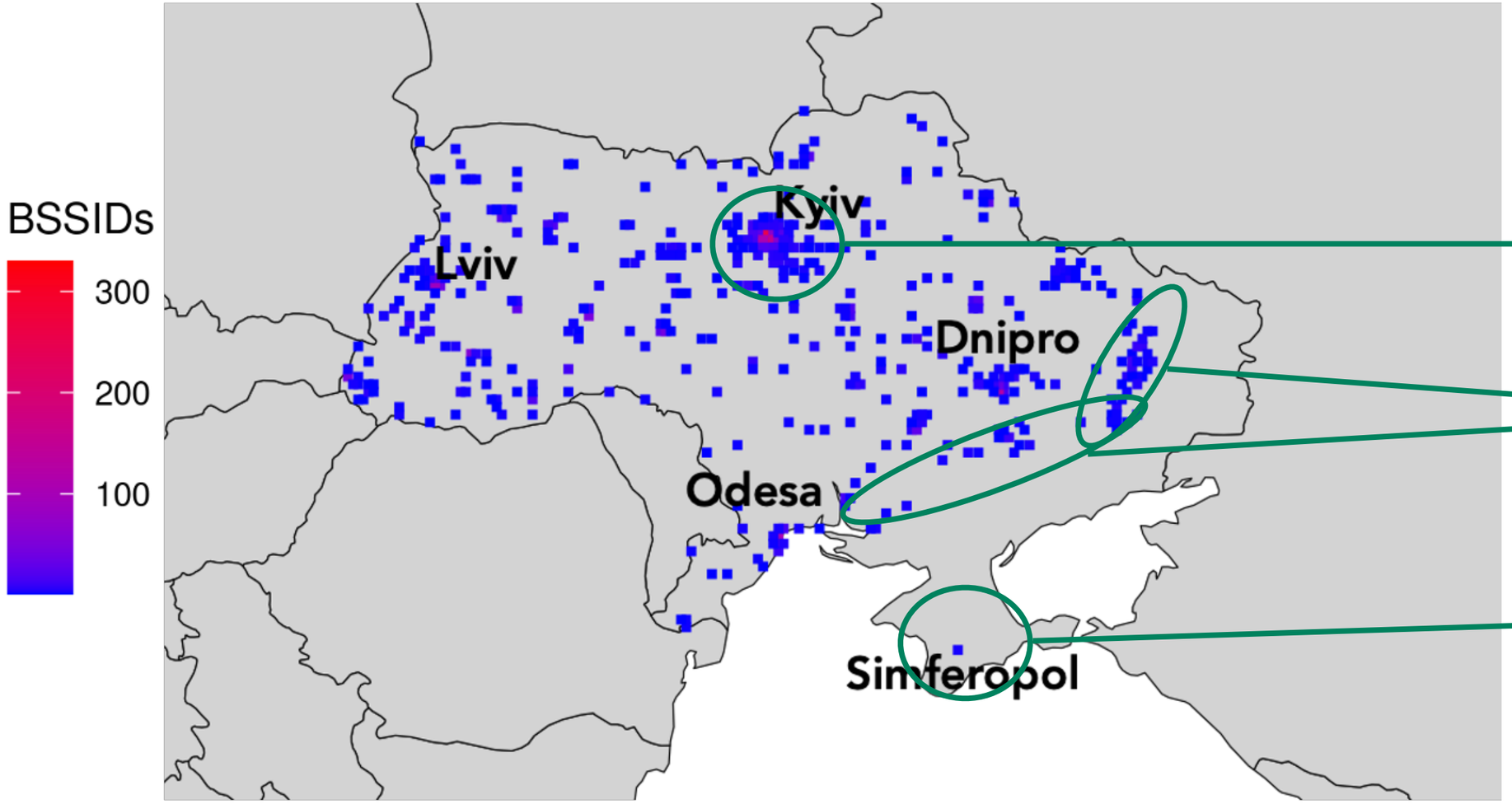


Hotspots in major cities

Presence along frontlines

Case Study: Russia-Ukraine War

Starlink geolocations in Ukraine 2023-2024



Hotspots in major cities

Presence along frontlines

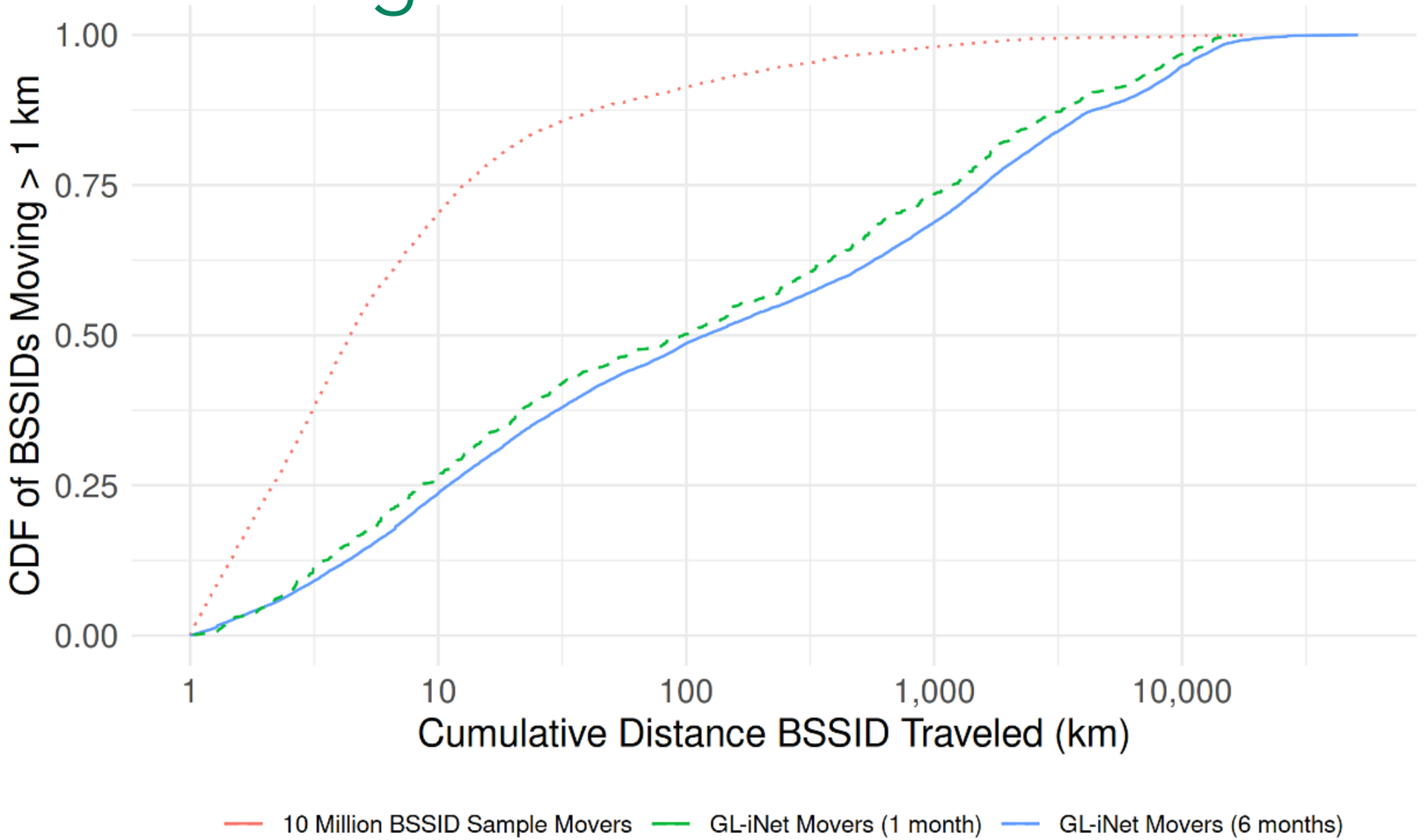
Operation in Russian-occupied territory

Privacy Threat 3: Device Mobility

Privacy Threat 3: Device Mobility

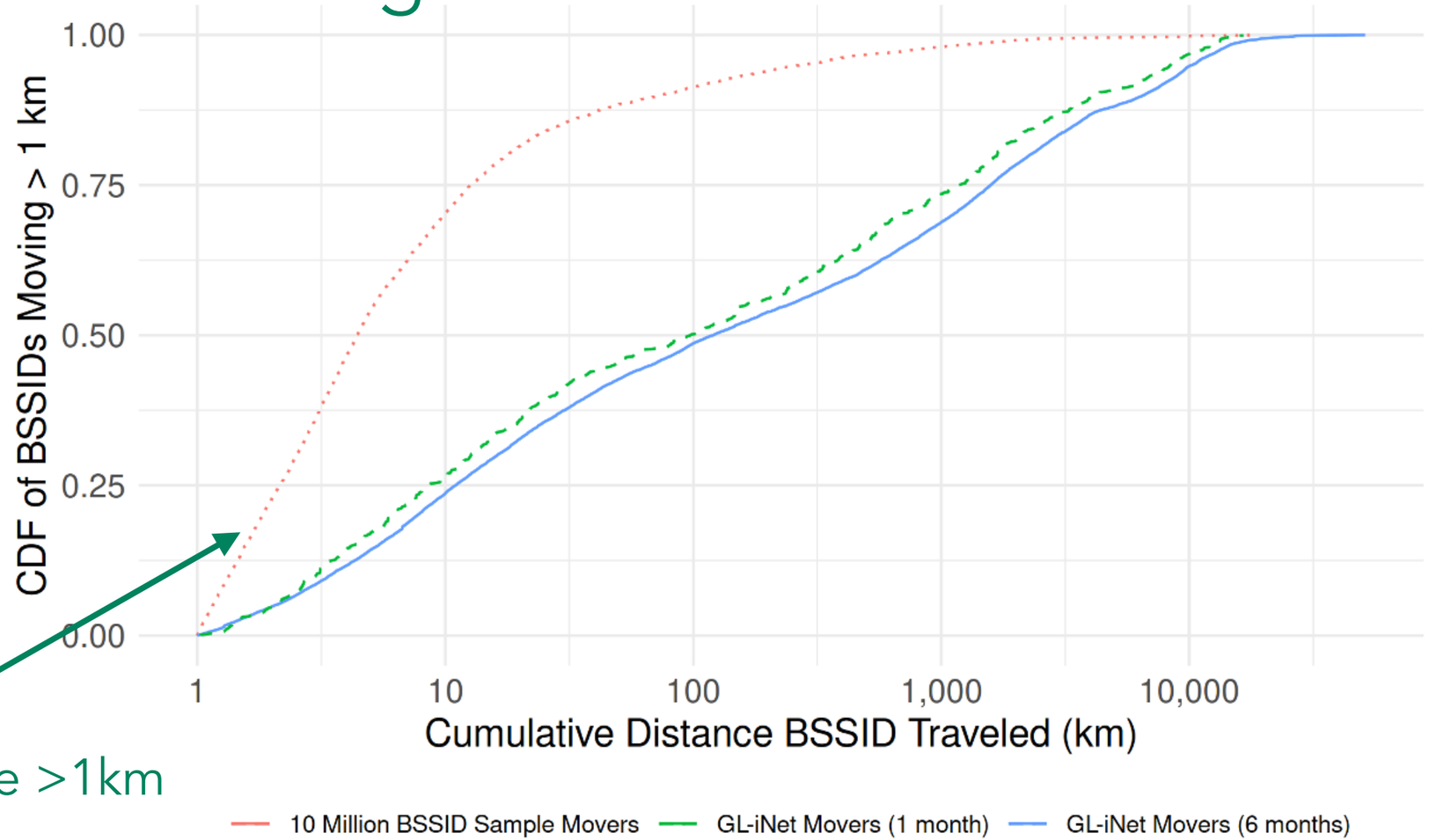
Privacy Threat 3: Device Mobility

Tracking 10M BSSIDs for a Month



Most routers stable for long periods…

Tracking 10M BSSIDs for a Month

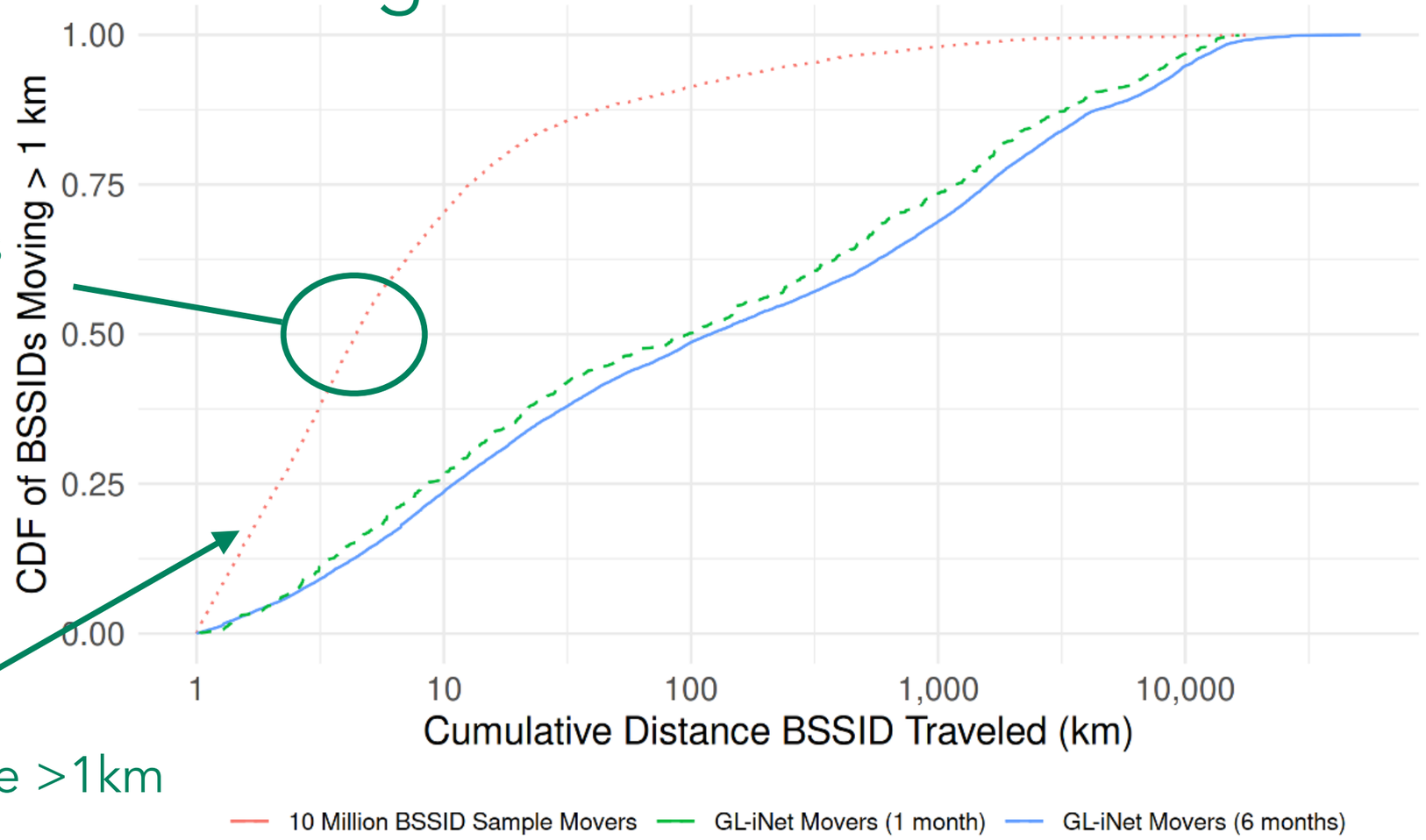


Only 6,002 move >1km

Most routers stable for long periods…

Tracking 10M BSSIDs for a Month

Small movements

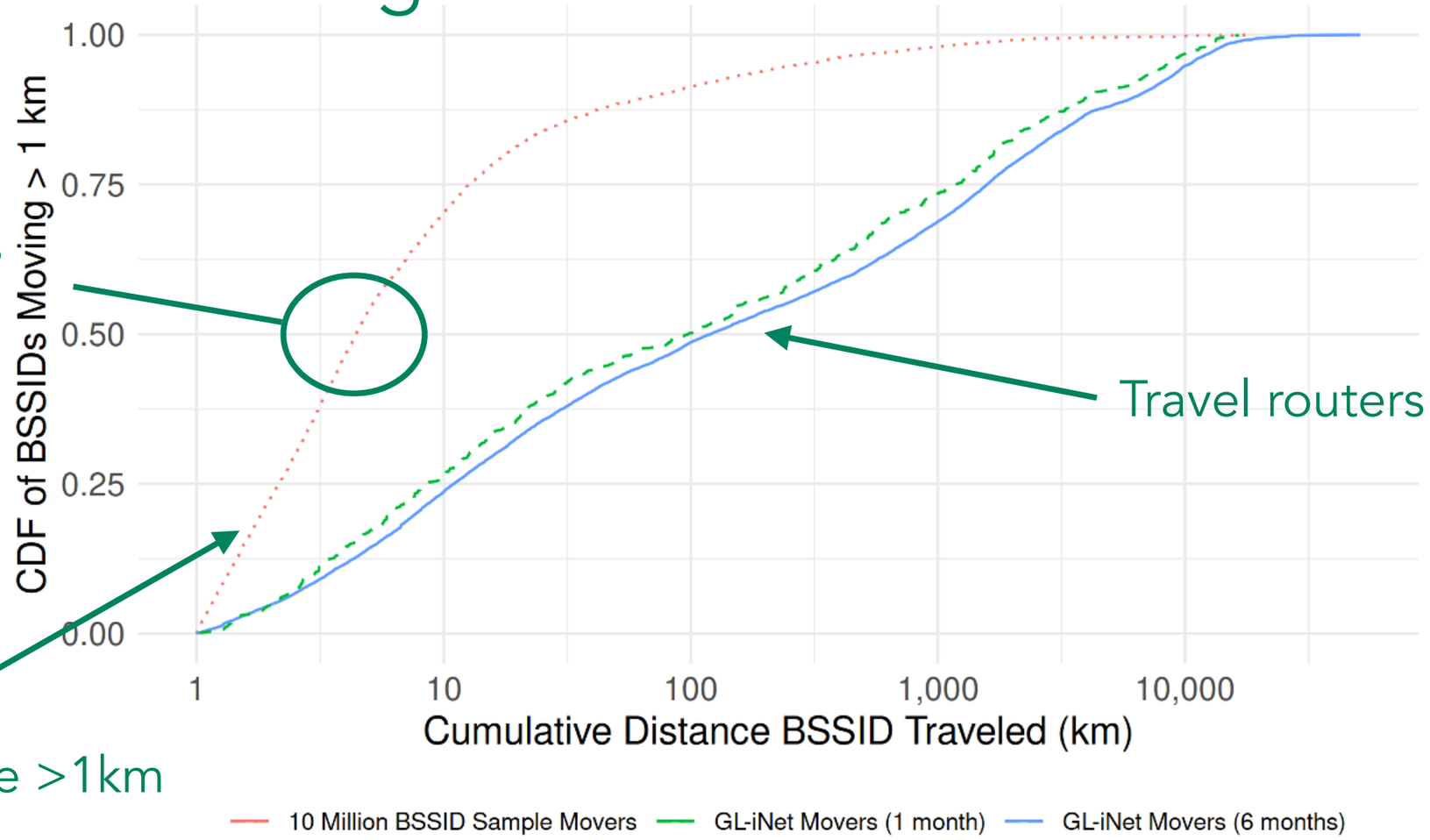


Only 6,002 move >1km

Most routers stable for long periods…

Tracking 10M BSSIDs for a Month

Small movements



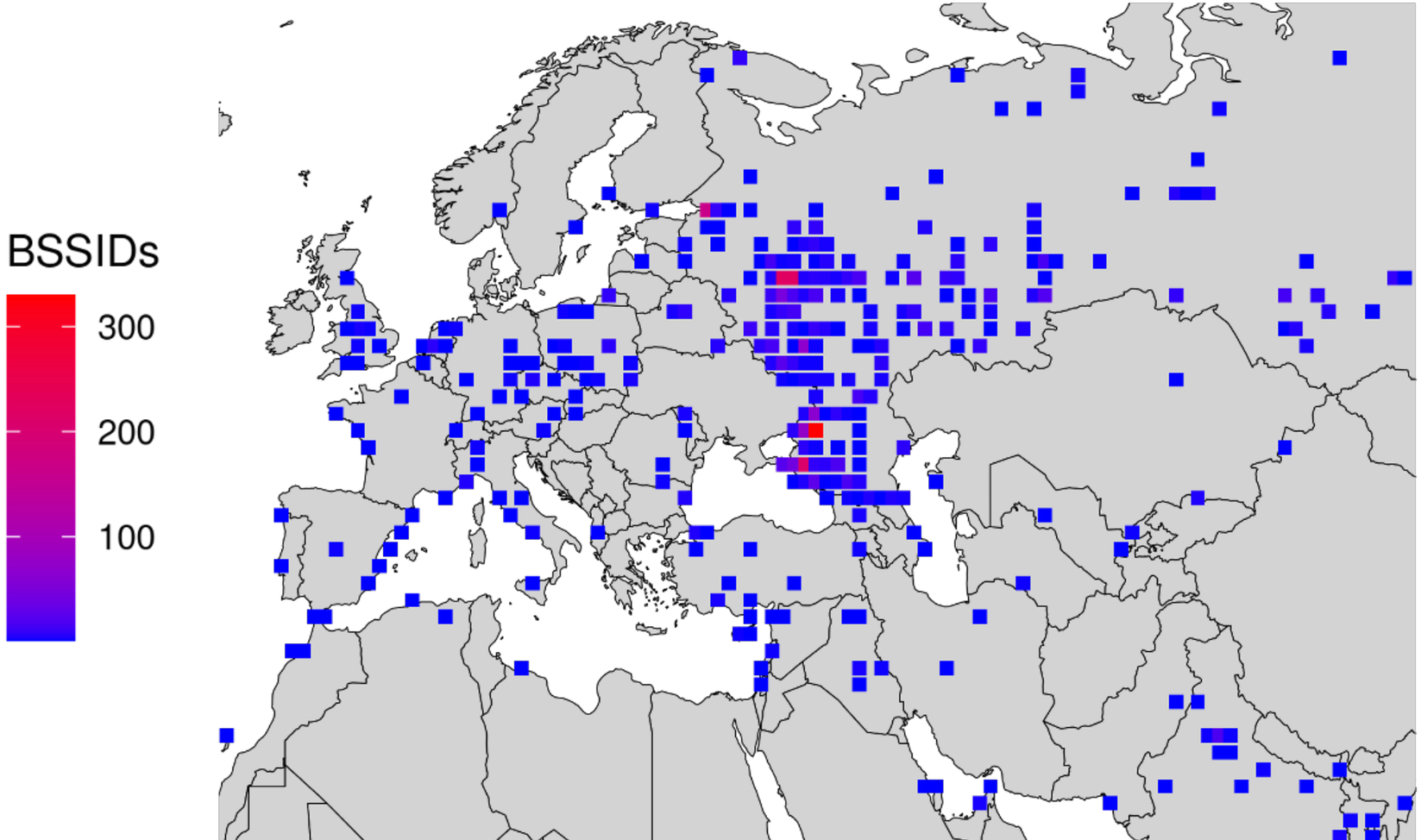
Travel routers

Only 6,002 move >1km

…but some move significant distances

Case Study: Russia-Ukraine War

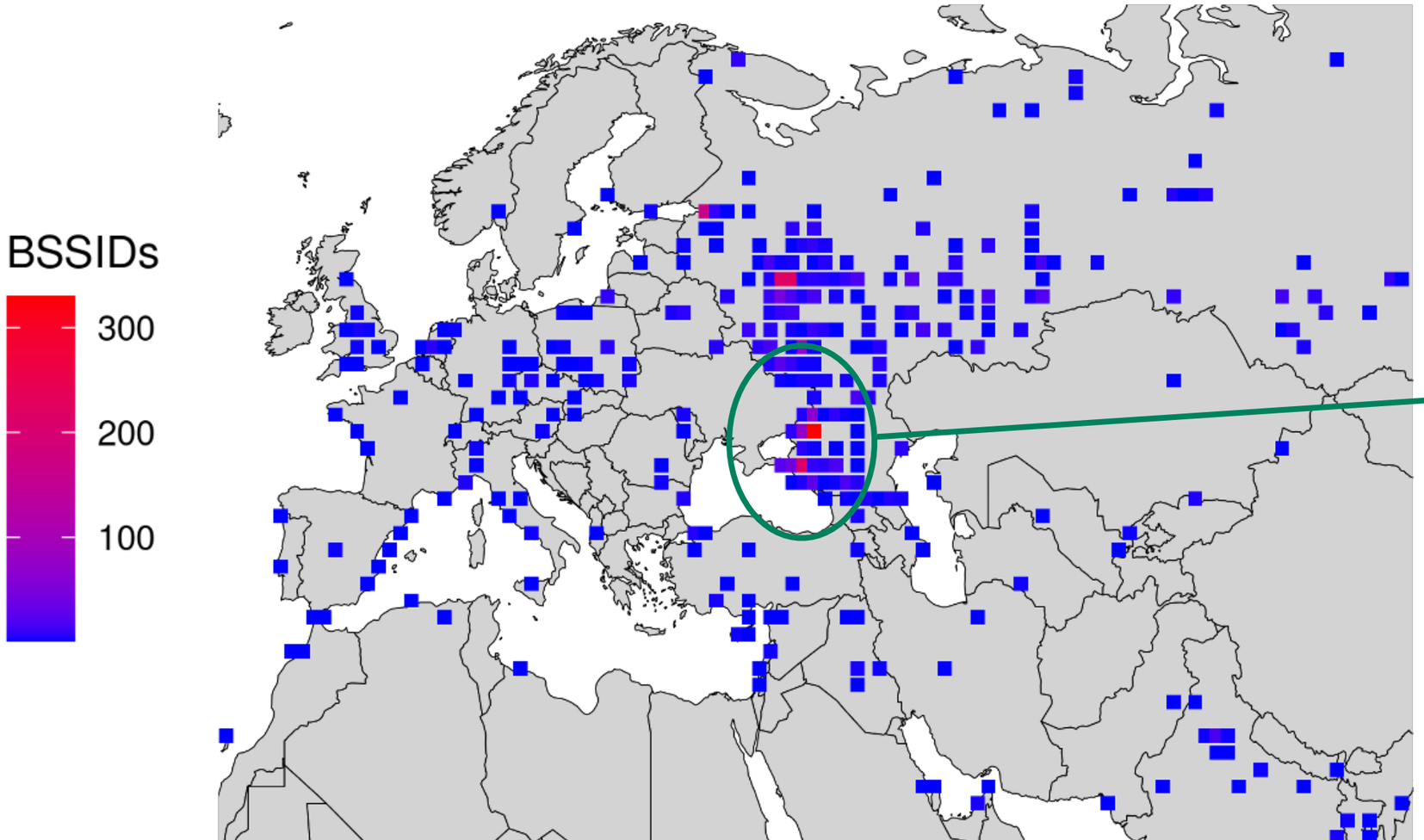
Longitudinal data allows tracking movement into and out of regions



Device locations *before entering Ukraine*

Case Study: Russia-Ukraine War

Longitudinal data allows tracking movement into and out of regions

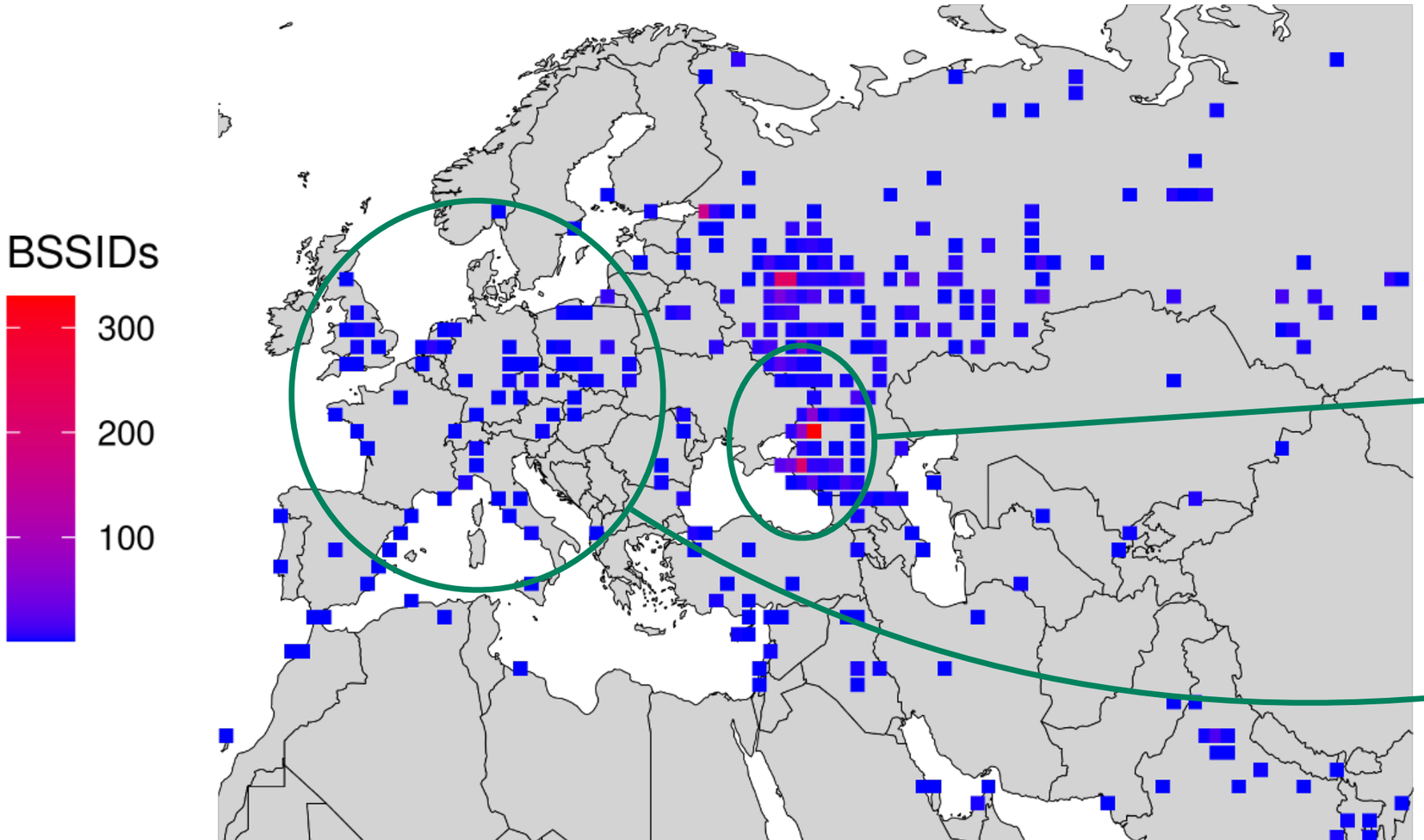


Device locations *before entering Ukraine*

Pre-deployment sites?

Case Study: Russia-Ukraine War

Longitudinal data allows tracking movement into and out of regions



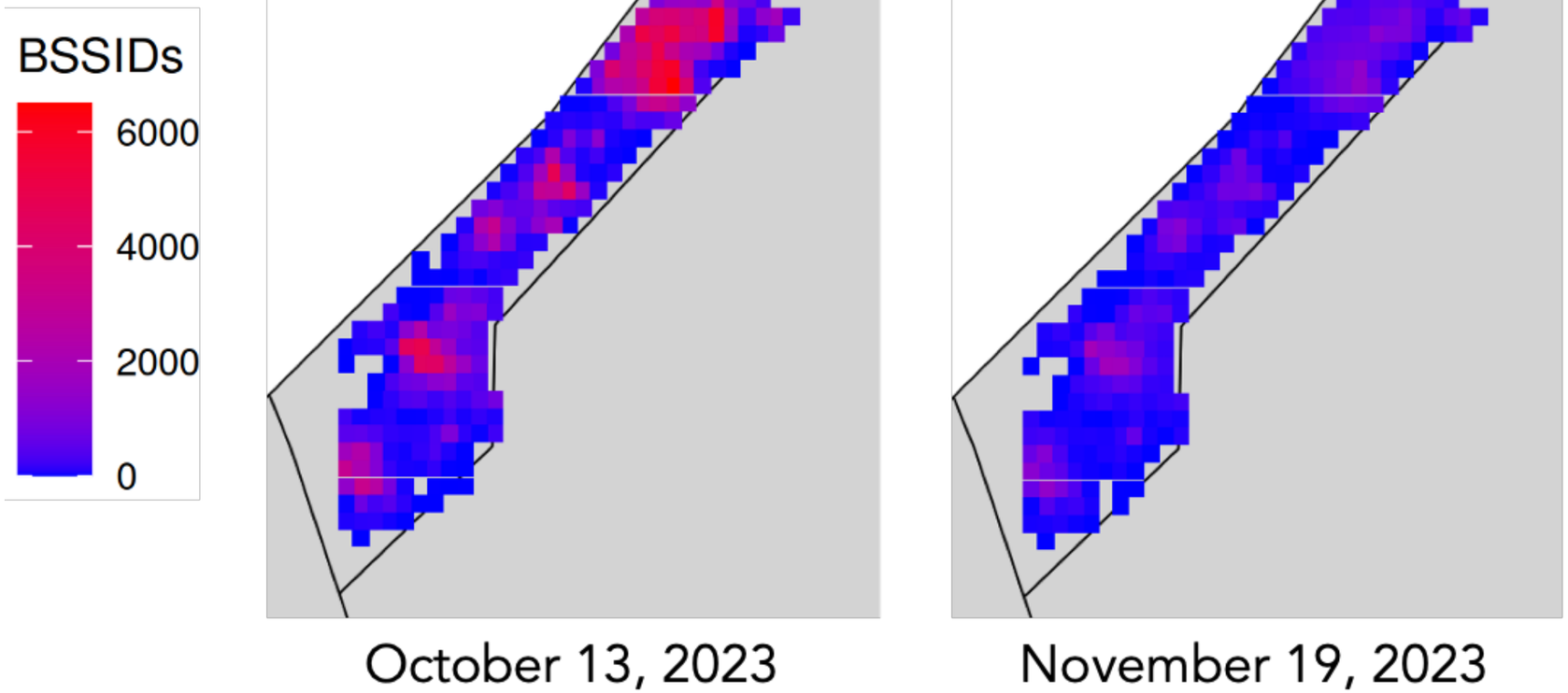
Device locations *before entering Ukraine*

Pre-deployment sites?

NGOs? Foreign legion?

Case Study: Gaza War

Tracking outages and destruction over time



75% decrease in Gaza BSSIDs over 4 weeks

25% decrease in Tel Aviv BSSID control group over same period

Disclosure and Remediation

What can we do about this?

Disclosure

Disclosed Dec 2023

Can now opt-out of Apple's WPS

GL·iNet

SPACEX

Disclosed Mar 2024

Recommend randomizing BSSIDs

Apple Remediation

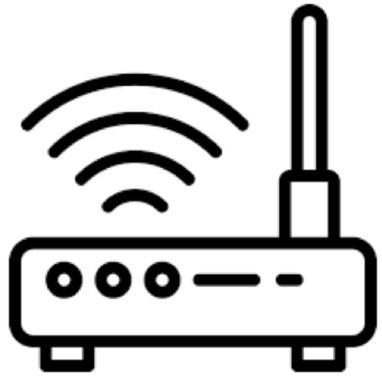
Apple modified privacy page in March 2024 indicating users can opt-out of WPS

Append **_nomap** to SSID to opt-out

What Apple **should** do:

- **Prevent** excessive queries
- **Require** authentication
- **Limit** number of “extra” BSSIDs

SSID: Erik-WiFi



74:09:bc:a0:5e:b8

Apple Remediation

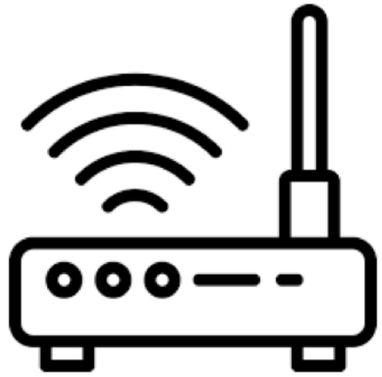
Apple modified privacy page in March 2024 indicating users can opt-out of WPS

Append **_nomap** to SSID to opt-out

What Apple **should** do:

- **Prevent** excessive queries
- **Require** authentication
- **Limit** number of “extra” BSSIDs

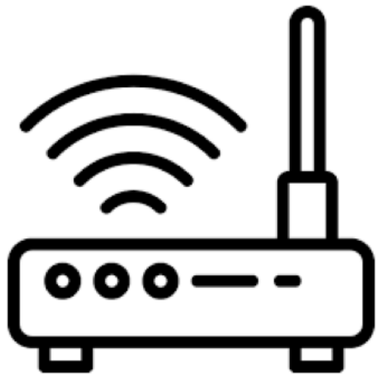
SSID: Erik-WiFi_nomap



74:09:bc:a0:5e:b8

BSSID Randomization

Random BSSIDs prevent device manufacturer identification

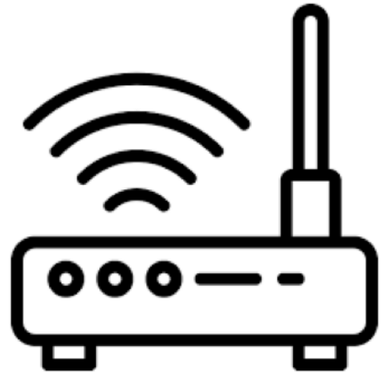


fa:82:d2:ba:04:2d

BSSID Randomization

Random BSSIDs prevent device manufacturer identification

fa:82:d2:ba:04:2d

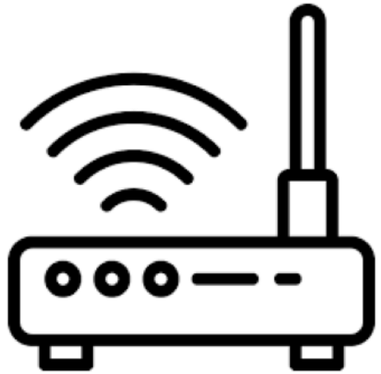


BSSID Randomization

Random BSSIDs prevent device manufacturer identification

fa:82:d2:ba:04:2d

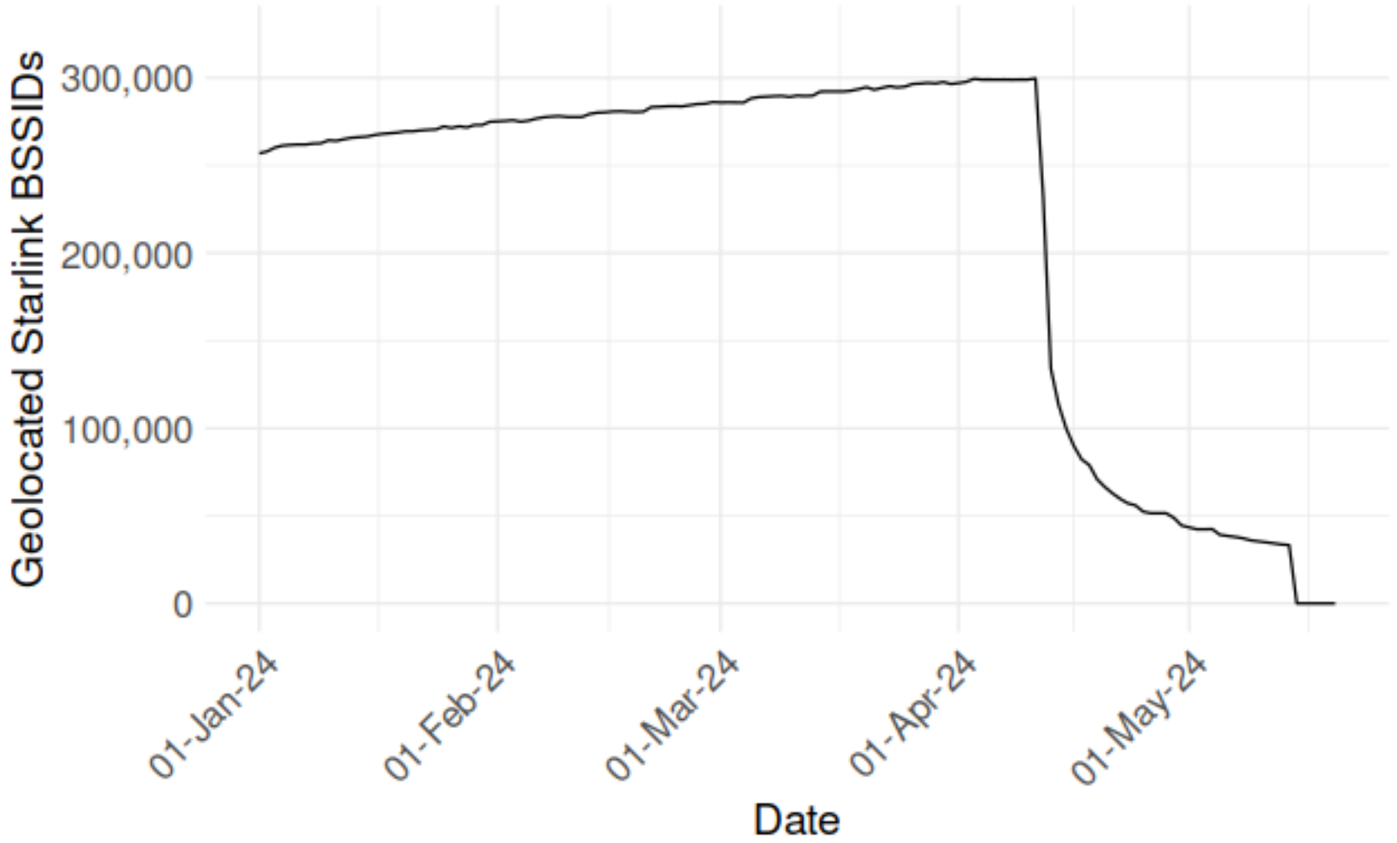
Random BSSIDs prevent device correlation over time and space



2e:29:ba:95:8d:2f

SPACEX Remediation

Starlink routers began randomizing BSSIDs on all products April 2024



GL·iNet Remediation

Initially, no plans to randomize BSSIDs

Reached out in late May 2024 informing us of change of direction

Implemented BSSID randomization in software version v4.6.2+

Surveilling the Masses with Wi-Fi Positioning Systems

Remotely geolocate >2B BSSIDs over course of 2023

Disclosed to Apple December 2023 — Still a threat today

Longitudinally track BSSID movements

Sample Apple WPS query code github.com/gigaryte/bssid-geolocator

UNIVERSITY OF MARYLAND

Surveilling the Masses with Wi-Fi Positioning Systems

Remotely geolocate >2B BSSIDs over course of 2023

Longitudinally track BSSID movements

Thanks!
Erik Rye
rye@umd.edu

UNIVERSITY OF MARYLAND

Disclosed to Apple December 2023 — Still a threat today

Sample Apple WPS query code github.com/gigaryte/bssid-geolocator

Backup Slides

Frequently Asked Questions

FAQ — When Does an AP Become a Landmark?

To be a good landmark, AP must be stable. Apple applies some minimum stability threshold

Black box testing — 3-7 days before new BSSID AP appears

Similarly, 3-7 days for a powered-off AP to disappear

Stability threshold a potential tunable parameter by Apple

FAQ — Mobile Hotspots

Modern Android/iOS use random BSSIDs when in hotspot mode — our best-practice recommendation for mobile APs

Their ephemerality typically precludes them from becoming landmarks — generally only used for several minutes to a few hours

FAQ — Trains, Planes, and Automobiles

Vehicles (typically) don't become WPS landmarks

Intuition: unstable landmarks useless for positioning

Boats are an exception — boats are often stationary for long periods

FAQ — Doesn't WiGLE Do This?

WiGLE is awesome! Several key differences

WPSes use the O(Billions) devices in their ecosystems to do the "wardriving"

WiGLE relies on wardrivers being present in an area and uploading their data to WiGLE

WiGLE captures some additional data the WPS does not — e.g., SSID