Detecting Fake 4G Base Stations for $20 with Rayhunter

Cooper Quintin - Senior Staff Technologist - EFF
Will Greenberg - Senior Staff Technologist - EFF
oopsbagel - Rayhunter Maintainer
DEF CON 33 - August 2025

Intro

- **Cooper Quintin (he/him)**
  - Senior Staff Technologist
  - At EFF for 10 years
  - Privacy Badger, malware, SLS, Threat Lab, phones

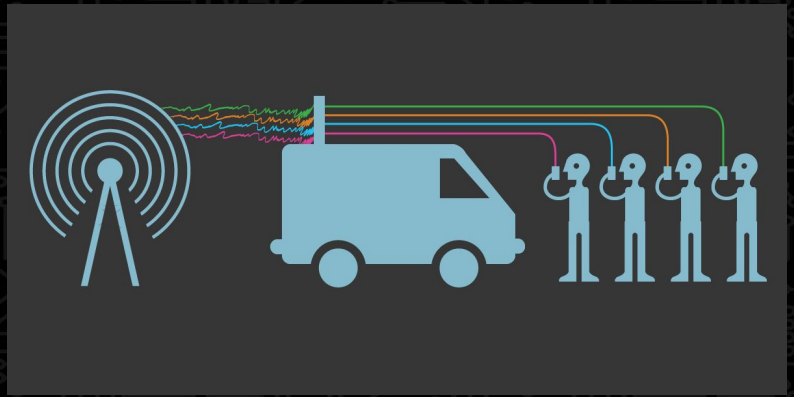
- **oopsbagel (nieźle/toveri)**
  - Rayhunter Maintainer
  - ECE, software development, both kinds of SRE, netsec, cloudsec
  - Does not work for EFF

Shout Out

Will Greenberg

- Co-creator of this research
- Couldn't be here
- Please give him a round of applause

Stingray AKA IMSI Catcher AKA Cell-Site Simulator



Previous Efforts to Detect CSS


I HAVE NO
IDEA WHAT
I'M DOING

Goals

1. Determine how how often CSS are being used.
2. Determine what kind of attacks modern CSS use.
3. Figure out if we can detect modern CSS reliably.

How Often are CSS Being Used

- Foreign Spies
  - IMSI Catchers in DC
- Cyber Mercenaries
  - NSO Group https://www.amnestyusa.org/wp-content/uploads/2020/06/Morocco-NSO-Group-report.pdf

How Often are CSS Being Used

- ICE/DHS - hundreds of times per year
  - https://www.aclu.org/news/immigrants-rights/ice-records-confirm-that-immigration-enforcement-agencies-are-using-invasive-cell-phone-surveillance-devices/
- Local law enforcement
  - Fontana, CA police dept. used theirs > 300 times in 2022-2023
    - Have purchased three cell site simulators
  - Santa Bernardino PD - 231 times in 2017
    - https://www.eff.org/deeplinks/2019/05/eff-asks-san-bernardino-court-review-device-search-and-cell-site-simulator

Law Enforcement with CSS

Atlas of Surveillance

How Often are CSS Being Used

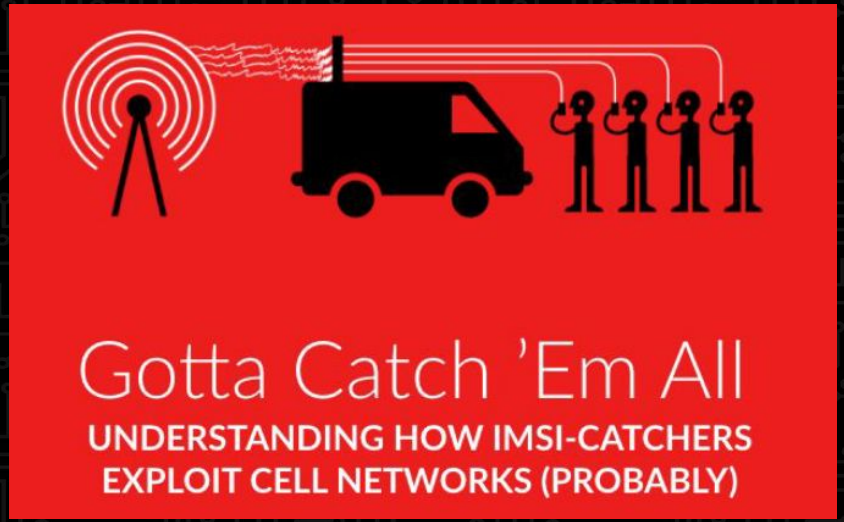
- Crime!
  - https://commsrisk.com/paris-imsi-catcher-mistaken-for-bomb-was-actually-used-for-health-insurance-sms-phishing-scam/

Paris IMSI-Catcher Mistaken for Bomb Was Actually Used for Health Insurance SMS Phishing Scam

By **Eric Priezkalns** 21 Feb 2023 Privacy & Intellectual Property

Regular readers may remember the arrest of a drugged-up driver who carried a mysterious device in the back of her car.

How do 4G CSS Work

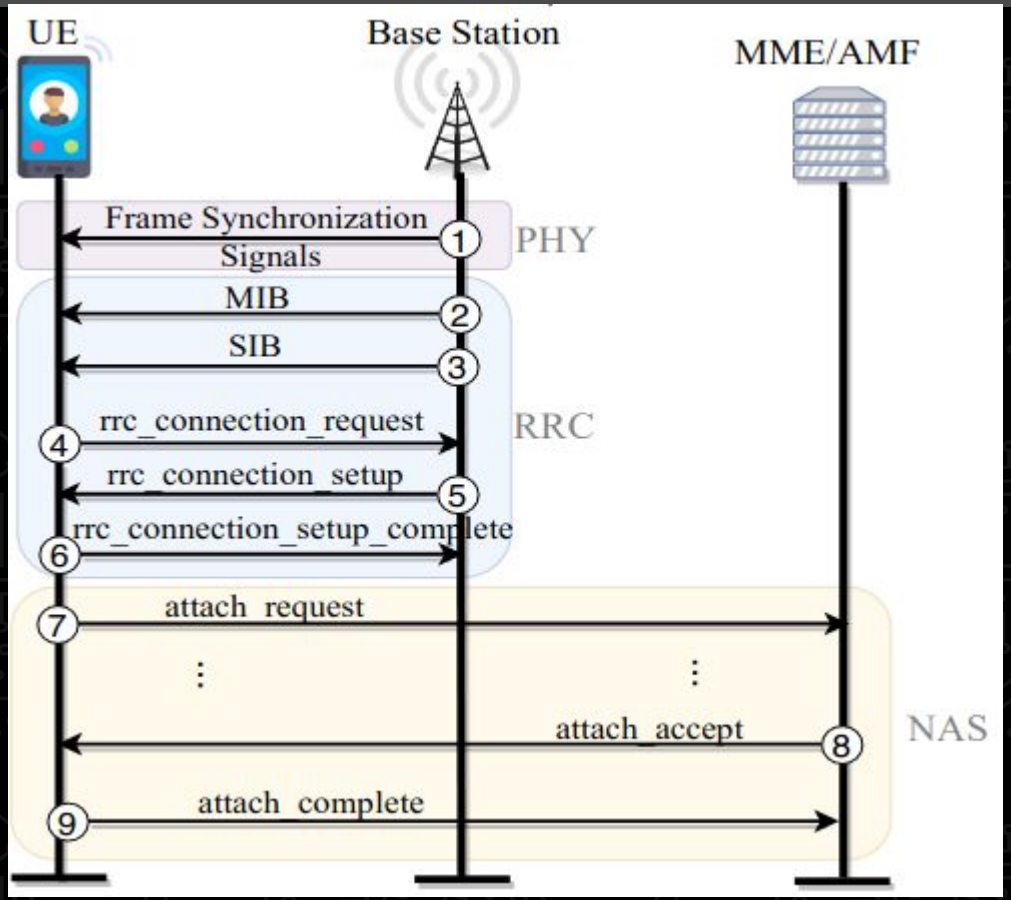


- What are the vulns next gen CSS are taking advantage of?

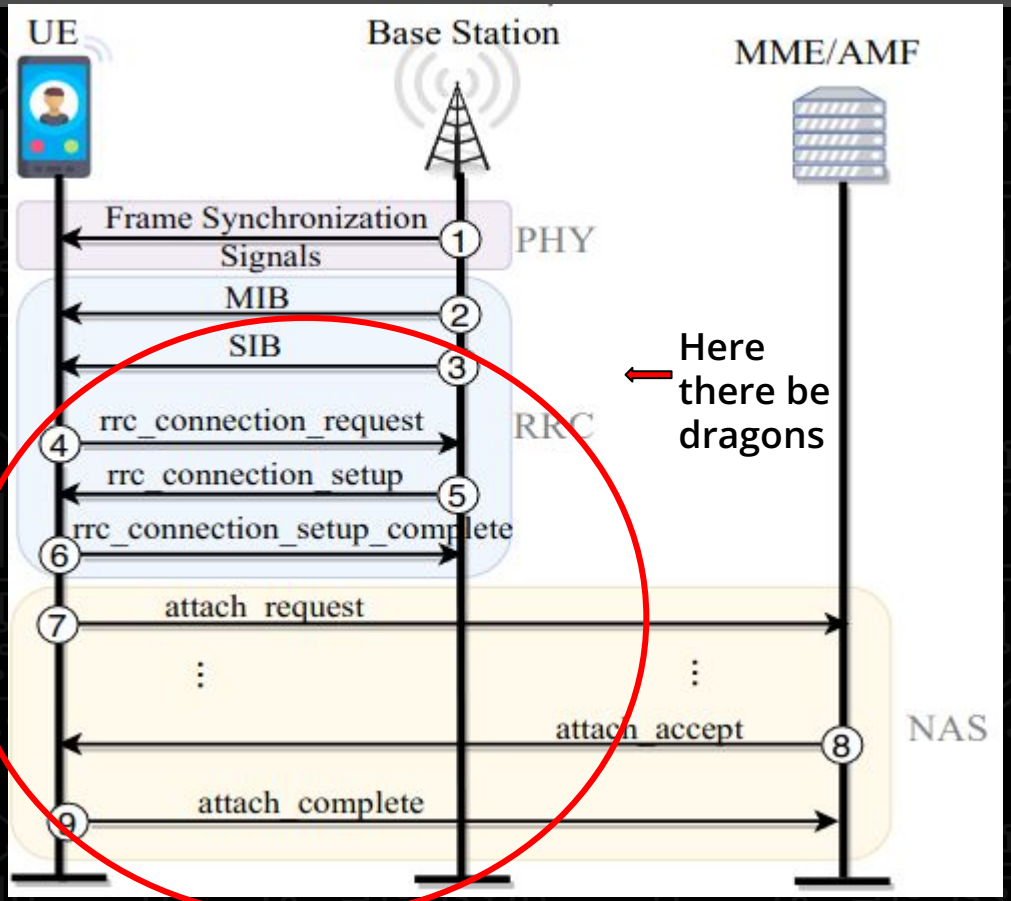
Gotta catch em all whitepaper by Advisory Board member Yomna

Pre-Authentication Vulnerabilities

- 4G has a glass jaw
- Even though the UE authenticates the tower there are still several messages that it sends, receives, and trusts before authentication happens or w/o authentication
- This is the weak spot in which the vast majority of 4G attacks happen.
- Even downgrade attacks!



Insecure Connection Bootstrapping in Cellular Networks:The Root of All Evil - Hussain et al 2019



Insecure Connection Bootstrapping in Cellular Networks:The Root of All Evil -

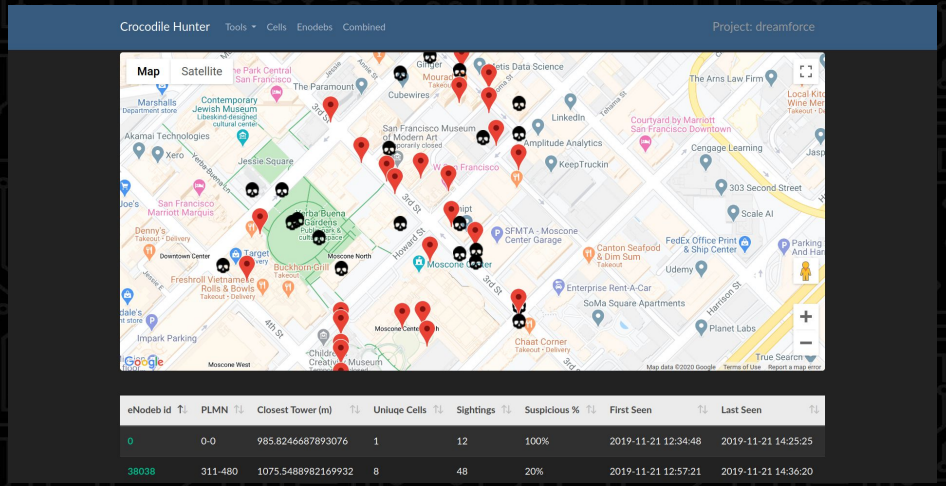
Doesn't 5G Fix This Whole Problem?

No, not really. 5G can be jammed. Or turned off.

> With a simple button in the Companion App, the 5G cells will be locked quickly and efficiently with minimum impact on subscribers in the area. With 5G cells being unavailable, all mobile devices in the area are forced to look for and attach to available 2G, 3G or 4G cell towers.

Source: Group2000 - Lima 5g Cellpro

Previous Detection Methods 2G Only



eNodeb id	PLMN	Closest Tower (m)	Uniuqe Cells	Sightings	Suspicious %	First Seen	Last Seen
0	0-0	985.8246687893076	1	12	100%	2019-11-21 12:34:48	2019-11-21 14:25:25
38038	311-480	1075.5488982169932	8	48	20%	2019-11-21 12:57:21	2019-11-21 14:36:20

CROCODILE HUNTER

Problems

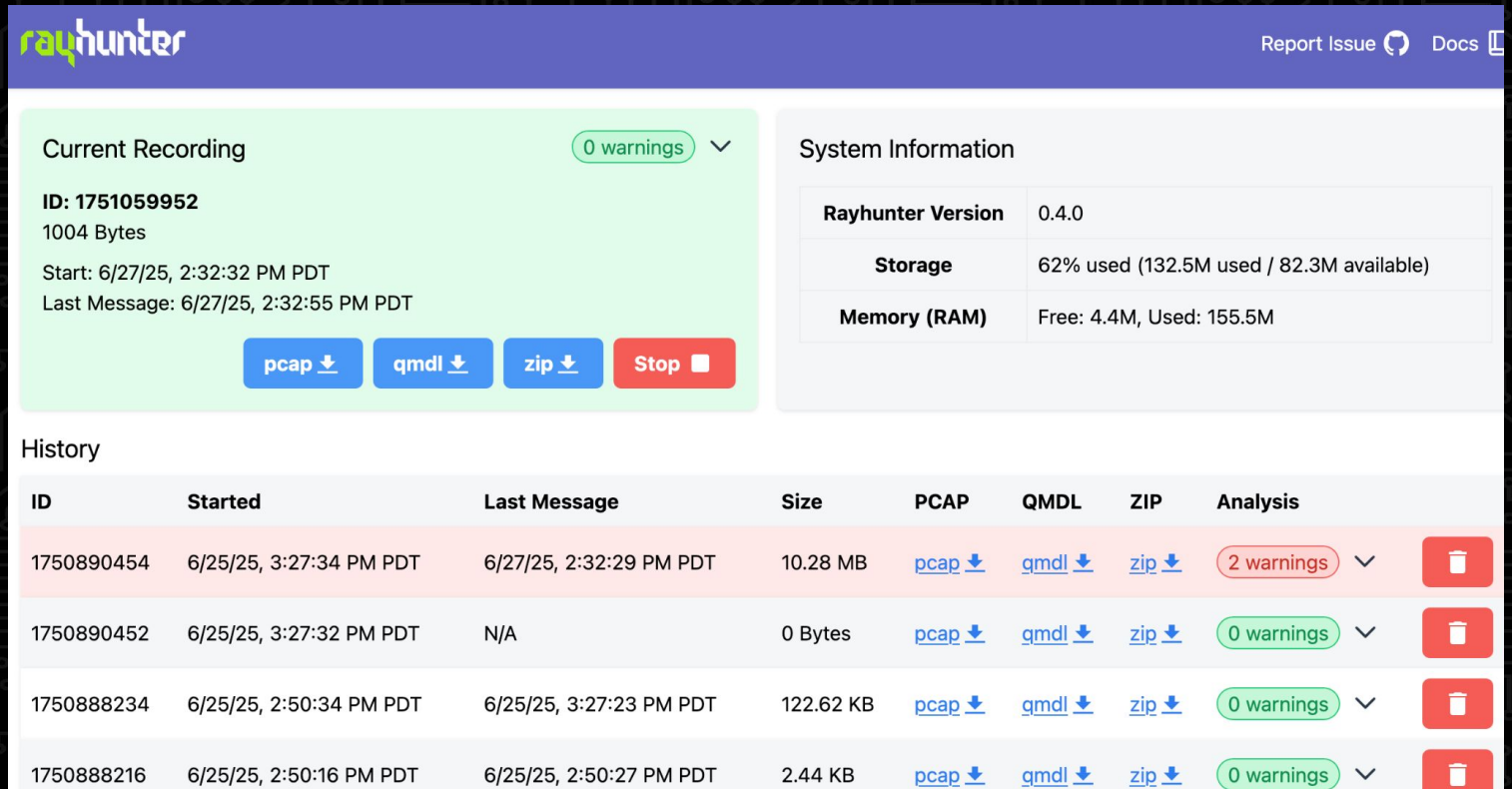
- Too expensive
- Too hard to set up
- Difficult to interpret the results for laypersons

Can we do better? Yes!

Introducing Rayhunter!

- Runs on a $20 mobile hotspot
- Easy(ish) to install
- Simple UI
- Written in Rust so it's ~~trendy~~ memory safe!
- A quick note on the name
  - It's the only thing we could come up with that wasn't already trademarked

Web UI

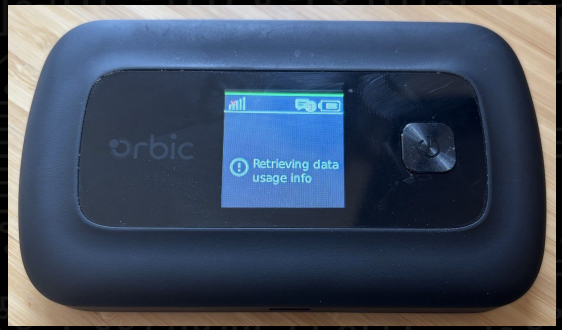

rayhunter
Report Issue
Docs
Current Recording
0 warnings
ID: 1751059952
1004 Bytes
Start: 6/27/25, 2:32:32 PM PDT
Last Message: 6/27/25, 2:32:55 PM PDT
pcap
qmdl
zip
Stop
System Information
Rayhunter Version
0.4.0
Storage
62% used (132.5M used / 82.3M available)
Memory (RAM)
Free: 4.4M, Used: 155.5M
History
ID
Started
Last Message
Size
PCAP
QMDL
ZIP
Analysis
1750890454
6/25/25, 3:27:34 PM PDT
6/27/25, 2:32:29 PM PDT
10.28 MB
pcap
qmdl
zip
2 warnings
1750890452
6/25/25, 3:27:32 PM PDT
N/A
0 Bytes
pcap
qmdl
zip
0 warnings
1750888234
6/25/25, 2:50:34 PM PDT
6/25/25, 3:27:23 PM PDT
122.62 KB
pcap
qmdl
zip
0 warnings
1750888216
6/25/25, 2:50:16 PM PDT
6/25/25, 2:50:27 PM PDT
2.44 KB
pcap
qmdl
zip
0 warnings

Rayhunter Project Goals

- Determine in real time whether CSS are being used to surveil free speech activities
- Get lots of people using it to determine extent of CSS use
- Get a clearer picture of CSS use outside the US
- Get data about exploits CSS are actually using in the wild
- Clear up FUD and more accurate threat modeling for activists

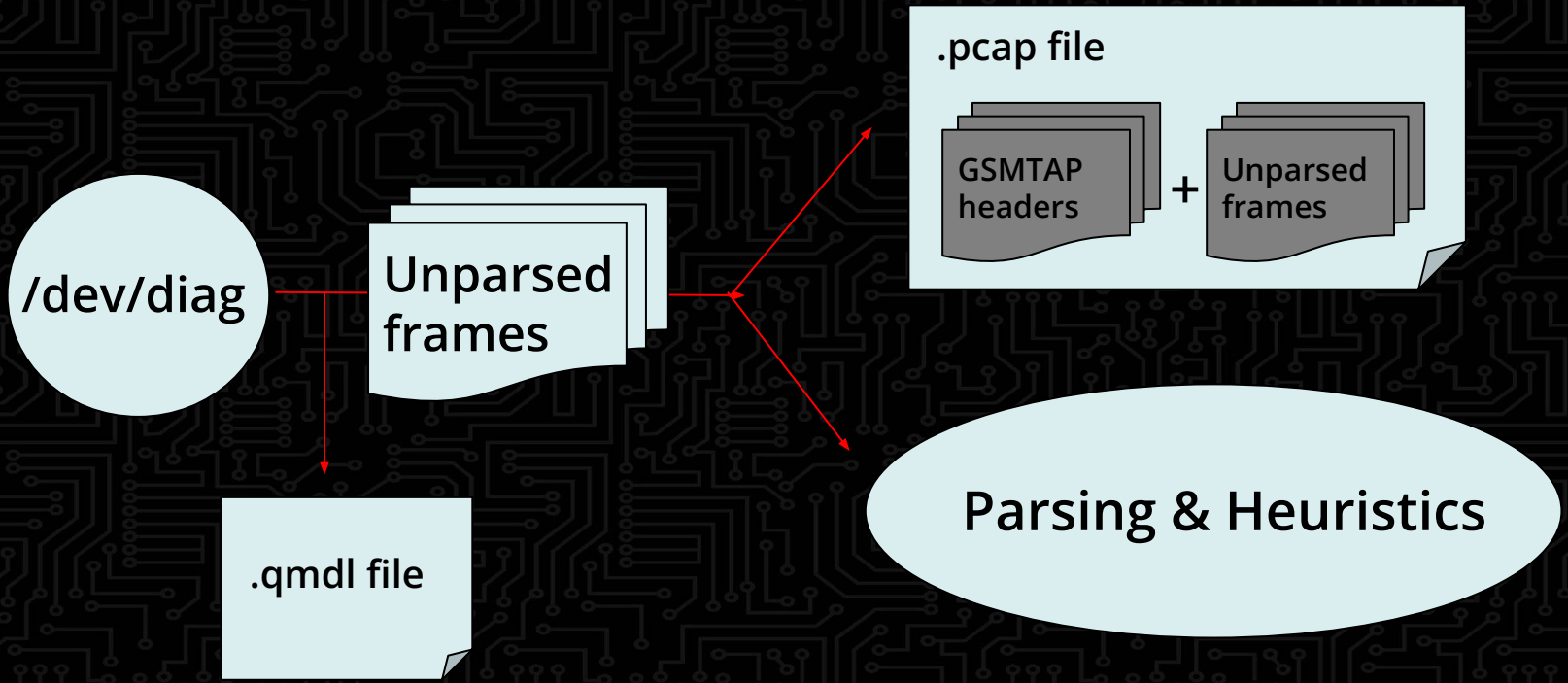
How Rayhunter works

- Consumes the Qualcomm Diag protocol
- Captures the traffic going between device and base station (pcap)
- Looks for anomalies
- Reports to user via screen (user can also download pcap)



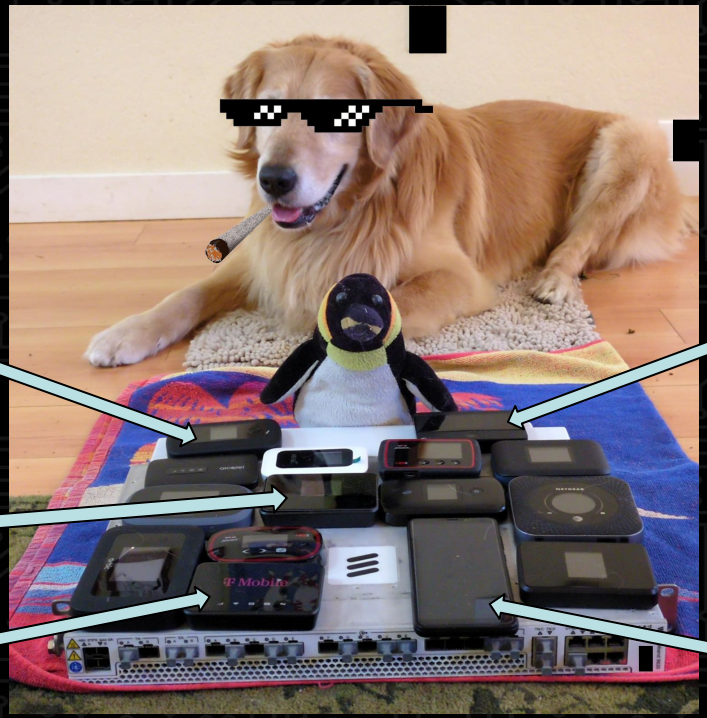
From a user perspective: Turn it on, put it in your pocket, and go about your day

Parsing frames



What hardware do we support?

Orbic RC400L



TP-Link M7350

(Celeste port by untitaker)

Wingtech CT2MHS01

T-Mobile TMOHS1

PinePhone
PinePhone Pro

What does Rayhunter run on today?

- **Qualcomm MDM modems**
  - mdm9x07
  - mdm9650
  - Integrated Cortex-A7 (A5) core
  - (Open Embedded) Linux 3.18
  - Android USB gadget functionality

- **Rayhunter needs 5-20MB of RAM**
- **Logs need low MBs of storage**
- **Devices with a fb display are best**
- **LEDs are okay**
- **Helpful if busybox has telnetd**

What hardware *could* we support?

... ALL the devices

Why is it hard to find IMSI Catchers

Threat Hunting, is it art or science?
There are SO MANY false positives ...

Heuristics So Far

- **2G Downgrade**
  - This is the attack used by crimeware IMSI catchers, necessary if you want to send content / inject
  - Monitor the SIB6/7 for downgrade attacks
  - Hasn't been detected in the US yet
  - Problematic in countries where 2g is still a thing
- **Null Cipher Use**
  - Check if the base station suggests null ciphers
  - Good for content interception / injection

Heuristics So Far

- **Incomplete SIB Chains**
  - Developers are lazy!
  - Take IMSI Catchers tend to only send the necessary SIB messages
- **IMSI Attach (Device IMSI is requested)**
  - Look for IMSI/IMEI requested in NAS messages without authentication.
  - This one is our problem child - hard to get right
  - But we know its used by commercial IMSI catchers!

Problems with the IMSI Attach Heuristic

- **IMSI Attach happens sometimes for legit reasons**
  - Roaming when there are no towers in your home PLMN
  - Attach on first startup in a long time
- **A better test! IMSI Request -> No Auth -> Detach**
  - Wallet inspector attack
  - But this happens sometimes for “legit reasons” still 😭

Commercial IMSI Catcher Attack Testing - CAPE

Info	IMSI	IMEISV	ARFCN	cellIdentity	trackingArea
Paging (1 PagingRecord)			[redacted]		
Paging (1 PagingRecord)					
Paging (1 PagingRecord)					
SystemInformationBlockType1				[redacted]	1ee6
SystemInformation [SIB2 SIB3]					
SystemInformationBlockType1				[redacted]	1ee6
SystemInformationBlockType1				[redacted]	1ee6
Tracking area update request					
RRCConnectionRequest					
RRCConnectionSetup					
RRCConnectionSetupComplete, Tracking area update request					
DLInformationTransfer, Identity request					
Identity request					
Identity response	[redacted]				
ULInformationTransfer, Identity response	[redacted]				
DLInformationTransfer, Tracking area update reject (Ill…					
Tracking area update reject (Illegal UE)					
RRCConnectionRelease [cause=other]					
SystemInformationBlockType1				[redacted]	1ee6
SystemInformation [SIB2 SIB3]					
SystemInformationBlockType1				[redacted]	3703

Commercial IMSI Catcher Attack Testing - CAPE

```
→  pcaps rayhunter-check -p 2_diff_tac_cause_3.pcap
INFO  [rayhunter_check] Analyzers:
INFO  [rayhunter_check]     - Identity (IMSI or IMEI) requested in suspicious manner (v2): Tests whether the ME sends an Identity Request NAS message without either an associated atta
 accept message
INFO  [rayhunter_check]     - Connection Release/Redirected Carrier 2G Downgrade (v1): Tests if a cell releases our connection and redirects us to a 2G cell.
INFO  [rayhunter_check]     - LTE SIB 6/7 Downgrade (v1): Tests for LTE cells broadcasting a SIB type 6 and 7 which include 2G/3G frequencies with higher priorities.
INFO  [rayhunter_check]     - Null Cipher (v1): Tests whether the cell suggests using a null cipher (EEA0)
INFO  [rayhunter_check]     - NAS Null Cipher Requested (v1): Tests whether the MME requests to use a null cipher in the NAS security mode command
INFO  [rayhunter_check]     - Incomplete SIB (v1): Tests whether a SIB1 message contains a full chain of followup sibs
INFO  [rayhunter_check] **** Beginning analysis of 2_diff_tac_cause_3.pcap
WARN  [rayhunter_check] 2_diff_tac_cause_3.pcap: WARNING (Severity: High) - 1980-01-26 05:46:22.182570 +00:00 SIB1 scheduling info list was malformed (packet 108)
WARN  [rayhunter_check] 2_diff_tac_cause_3.pcap: WARNING (Severity: High) - 1980-01-26 05:46:22.182688 +00:00 SIB1 scheduling info list was malformed (packet 110)
WARN  [rayhunter_check] 2_diff_tac_cause_3.pcap: WARNING (Severity: High) - 1980-01-26 05:46:22.182688 +00:00 SIB1 scheduling info list was malformed (packet 111)
WARN  [rayhunter_check] 2_diff_tac_cause_3.pcap: WARNING (Severity: High) - 1980-01-26 05:46:22.183072 +00:00 Disconnected after Identity Request without Auth Accept (frame 121)
WARN  [rayhunter_check] 2_diff_tac_cause_3.pcap: WARNING (Severity: High) - 1980-01-26 05:46:22.183411 +00:00 SIB1 scheduling info list was malformed (packet 123)
INFO  [rayhunter_check] 2_diff_tac_cause_3.pcap: 350 messages analyzed, 5 warnings, 1 messages skipped
```

In the Field - Turks and Caicos

```
i-goodsim.qmdl: INFO - 2025-06-07 21:22:06.117 +00:00 Disconnected after Identity Request without Auth Accept
i-goodsim.qmdl: INFO - 2025-06-08 00:22:28.411 +00:00 Disconnected after Identity Request without Auth Accept
i-goodsim.qmdl: WARNING (Severity: High) - 2025-06-08 08:46:57.462 +00:00 Identity requested without Attach Request
i-goodsim.qmdl: INFO - 2025-06-08 08:46:58.206 +00:00 Disconnected after Identity Request without Auth Accept
i-goodsim.qmdl: WARNING (Severity: High) - 2025-06-08 09:22:13.650 +00:00 Identity requested without Attach Request
i-goodsim.qmdl: INFO - 2025-06-08 09:22:14.536 +00:00 Disconnected after Identity Request without Auth Accept
i-goodsim.qmdl: WARNING (Severity: High) - 2025-06-08 12:20:30.716 +00:00 Identity requested without Attach Request
i-goodsim.qmdl: INFO - 2025-06-08 12:20:31.448 +00:00 Disconnected after Identity Request without Auth Accept
i-goodsim.qmdl: WARNING (Severity: High) - 2025-06-08 21:22:34.877 +00:00 Identity requested without Attach Request
i-goodsim.qmdl: INFO - 2025-06-08 21:22:35.574 +00:00 Disconnected after Identity Request without Auth Accept
i-goodsim.qmdl: WARNING (Severity: High) - 2025-06-08 23:46:24.430 +00:00 Identity requested without Attach Request
i-goodsim.qmdl: INFO - 2025-06-08 23:46:25.220 +00:00 Disconnected after Identity Request without Auth Accept
i-goodsim.qmdl: WARNING (Severity: High) - 2025-06-09 09:22:42.106 +00:00 Identity requested without Attach Request
i-goodsim.qmdl: INFO - 2025-06-09 09:22:42.787 +00:00 Disconnected after Identity Request without Auth Accept
i-goodsim.qmdl: WARNING (Severity: High) - 2025-06-09 10:43:39.567 +00:00 Identity requested without Attach Request
i-goodsim.qmdl: INFO - 2025-06-09 10:43:40.258 +00:00 Disconnected after Identity Request without Auth Accept
i-goodsim.qmdl: WARNING (Severity: High) - 2025-06-09 23:49:13.069 +00:00 Identity requested without Attach Request
i-goodsim.qmdl: INFO - 2025-06-09 23:49:13.802 +00:00 Disconnected after Identity Request without Auth Accept
```

Courtesy of ZeroChaos

In the Field - Turks and Caicos

```
WARNING (Severity: High) - 2025-06-10 14:21:55.975 +00:00 NAS Security mode command requested null cipher(packet 166851)
WARNING (Severity: High) - 2025-06-10 14:22:06.562 +00:00 NAS Security mode command requested null cipher(packet 166877)
WARNING (Severity: High) - 2025-06-10 14:44:15.245 +00:00 NAS Security mode command requested null cipher(packet 167483)
WARNING (Severity: High) - 2025-06-10 14:45:05.109 +00:00 NAS Security mode command requested null cipher(packet 167591)
WARNING (Severity: High) - 2025-06-10 14:45:15.717 +00:00 NAS Security mode command requested null cipher(packet 167612)
WARNING (Severity: High) - 2025-06-10 14:45:26.340 +00:00 NAS Security mode command requested null cipher(packet 167633)
WARNING (Severity: High) - 2025-06-10 14:45:36.852 +00:00 NAS Security mode command requested null cipher(packet 167654)
WARNING (Severity: High) - 2025-06-10 14:45:47.430 +00:00 NAS Security mode command requested null cipher(packet 167675)
WARNING (Severity: High) - 2025-06-10 15:42:52.250 +00:00 NAS Security mode command requested null cipher(packet 170505)
WARNING (Severity: High) - 2025-06-10 15:43:02.816 +00:00 NAS Security mode command requested null cipher(packet 170526)
WARNING (Severity: High) - 2025-06-10 15:43:13.335 +00:00 NAS Security mode command requested null cipher(packet 170547)
WARNING (Severity: High) - 2025-06-10 15:43:24.007 +00:00 NAS Security mode command requested null cipher(packet 170568)
WARNING (Severity: High) - 2025-06-10 15:43:34.513 +00:00 NAS Security mode command requested null cipher(packet 170589)
WARNING (Severity: High) - 2025-06-10 15:56:28.342 +00:00 NAS Security mode command requested null cipher(packet 171416)
WARNING (Severity: High) - 2025-06-10 15:56:38.885 +00:00 NAS Security mode command requested null cipher(packet 171442)
WARNING (Severity: High) - 2025-06-10 15:56:49.612 +00:00 NAS Security mode command requested null cipher(packet 171463)
WARNING (Severity: High) - 2025-06-10 15:57:03.956 +00:00 NAS Security mode command requested null cipher(packet 171484)
WARNING (Severity: High) - 2025-06-10 15:57:14.478 +00:00 NAS Security mode command requested null cipher(packet 171505)
WARNING (Severity: High) - 2025-06-10 16:10:07.127 +00:00 NAS Security mode command requested null cipher(packet 172263)
WARNING (Severity: High) - 2025-06-10 16:10:18.090 +00:00 NAS Security mode command requested null cipher(packet 172289)
WARNING (Severity: High) - 2025-06-10 16:10:29 +00:00 NAS Security mode command requested null cipher(packet 172321)
```

Courtesy of ZeroChaos

In the Field - Chicago

```
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:15:02.598 +00:00 Disconnected after Identity Request without Auth Accept (frame 1036)
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:15:39.066 +00:00 Disconnected after Identity Request without Auth Accept (frame 1056)
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:16:21.876 +00:00 Disconnected after Identity Request without Auth Accept (frame 1078)
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:16:47.325 +00:00 Disconnected after Identity Request without Auth Accept (frame 1100)
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:17:05.607 +00:00 Disconnected after Identity Request without Auth Accept (frame 1121)
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:17:31.074 +00:00 Disconnected after Identity Request without Auth Accept (frame 1141)
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:17:45.371 +00:00 Disconnected after Identity Request without Auth Accept (frame 1159)
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:18:04.609 +00:00 Disconnected after Identity Request without Auth Accept (frame 1179)
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:19:00.843 +00:00 Disconnected after Identity Request without Auth Accept (frame 1204)
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:19:58.452 +00:00 Disconnected after Identity Request without Auth Accept (frame 1224)
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:21:02.466 +00:00 Disconnected after Identity Request without Auth Accept (frame 1250)
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:22:00.123 +00:00 Disconnected after Identity Request without Auth Accept (frame 1275)
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:23:06.593 +00:00 Disconnected after Identity Request without Auth Accept (frame 1303)
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:24:00.435 +00:00 Disconnected after Identity Request without Auth Accept (frame 1327)
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:25:04.431 +00:00 Disconnected after Identity Request without Auth Accept (frame 1352)
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:26:02.012 +00:00 Disconnected after Identity Request without Auth Accept (frame 1373)
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:28:02.370 +00:00 Disconnected after Identity Request without Auth Accept (frame 1397)
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:30:02.705 +00:00 Disconnected after Identity Request without Auth Accept (frame 1425)
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:37:51.056 +00:00 Disconnected after Identity Request without Auth Accept (frame 1464)
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:38:09.060 +00:00 Disconnected after Identity Request without Auth Accept (frame 1482)
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:41:41.630 +00:00 Disconnected after Identity Request without Auth Accept (frame 1518)
WARN  [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) – 2025-05-06 17:42:32.237 +00:00 Disconnected after Identity Request without Auth Accept (frame 1542)
```

Courtesy of Ryan

In the Field - Penn Station - NYC

```
INFO  [rayhunter_check] **** Beginning analysis of 1746553345-2.qmdl
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 22:46:07.027 +00:00 Disconnected after Identity Request without Auth Accept (frame 13411)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 22:50:57.546 +00:00 Disconnected after Identity Request without Auth Accept (frame 13572)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 22:51:02.685 +00:00 Disconnected after Identity Request without Auth Accept (frame 13601)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 22:52:43.567 +00:00 Disconnected after Identity Request without Auth Accept (frame 13743)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 22:53:06.714 +00:00 Disconnected after Identity Request without Auth Accept (frame 13760)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 22:53:57.111 +00:00 Disconnected after Identity Request without Auth Accept (frame 13797)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 23:13:23.503 +00:00 Disconnected after Identity Request without Auth Accept (frame 14530)
INFO  [rayhunter_check] 1746553345-2.qmdl: INFO - 2025-05-07 23:14:47.870 +00:00 Identity request happened without auth request followup (frame 14646)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 23:14:54.907 +00:00 Disconnected after Identity Request without Auth Accept (frame 14650)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 23:19:25.402 +00:00 Disconnected after Identity Request without Auth Accept (frame 14830)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 23:21:46.438 +00:00 Disconnected after Identity Request without Auth Accept (frame 14972)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 23:28:29.688 +00:00 Disconnected after Identity Request without Auth Accept (frame 15218)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 23:28:51.864 +00:00 Disconnected after Identity Request without Auth Accept (frame 15235)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 23:29:31.928 +00:00 Disconnected after Identity Request without Auth Accept (frame 15279)
INFO  [rayhunter_check] 1746553345-2.qmdl: 16638 messages analyzed, 13 warnings, 299 messages skipped
```

Courtesy of Alliraine

In the Field - No Kings Protests

Many More

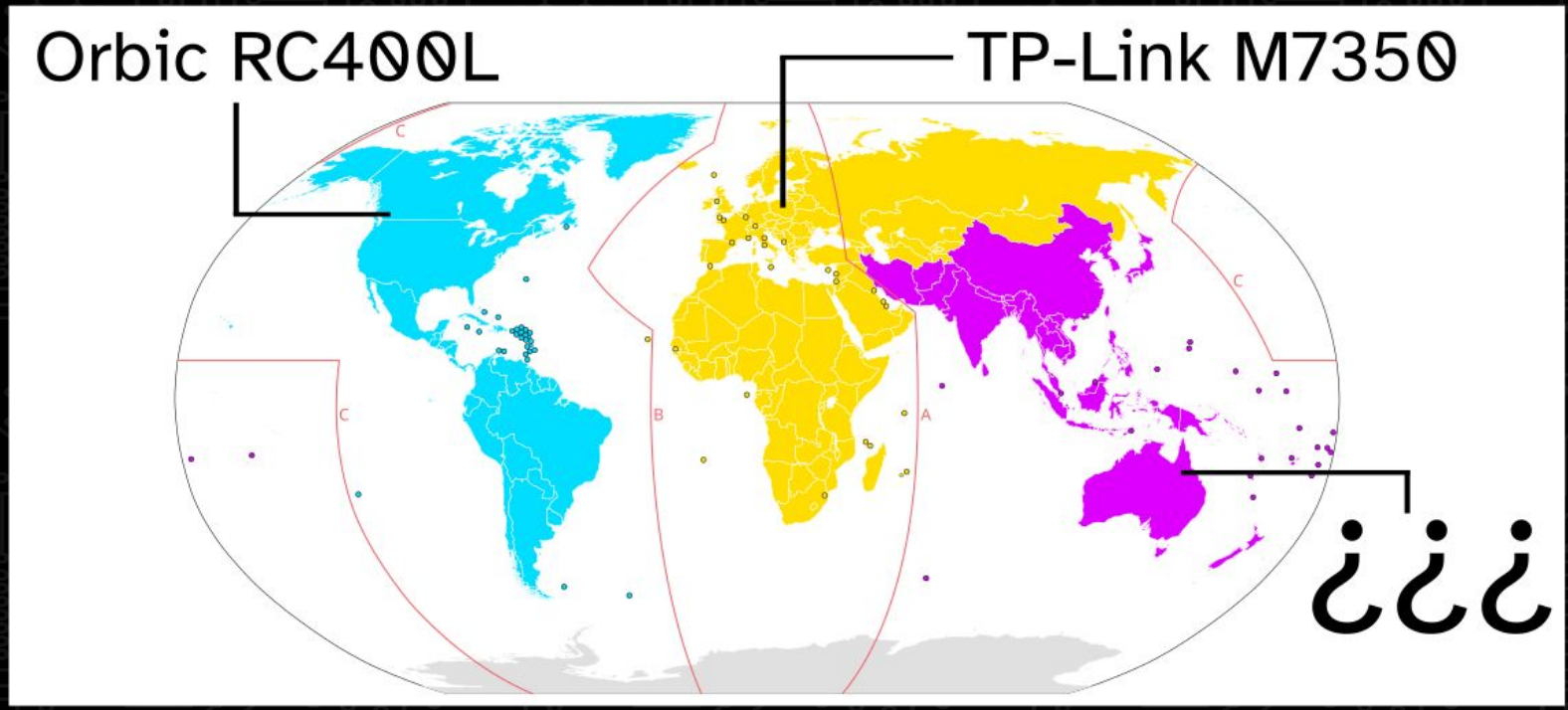
- We have several more results that are more ambiguous than this.
- Embassies
- DNC
- Various cities!

Still lots to do

- More testing with simulated attack environments
- User Testing
- UI Improvements
- More Heuristics
- International testing and support of all ITU regions

Let’s take Rayhunter global…

ITU Region 1, 2, ...3?



https://efforg.github.io/rayhunter/supported-devices.html

Adding a new device

1. **Select a Qualcomm based device**
2. **Root the device**
    a. Almost all binaries run as root
    b. Vendors often have hidden unlock methods
    c. Root password is often oelinux123
3. **Start with headless mode, ensure Rayhunter gets useful data from /dev/diag**
4. **Add display support using our generic_framebuffer module**
5. **Add an installer module**
    a. Unlocking and installing over telnet instead of adb is preferred

Interesting userspace binaries

Binary	Description
qcmap_web_cgi	Web request logic (may contain RCEs)
qcmap_auth	Web authentication logic (may also contain RCEs)
qcmap_web_client	More web request logic (believe it or not, may contain more RCEs)
atfwd_daemon	Undocumented AT commands (you'll never guess what those may contain…)
boot_hsusb_composition	USB mode switching (enable ADB, after you get RCE)

Solving problems with Rust 

Before

- gcc, glibc required
- Rust bindings to C libs
- Overcomplicated toolchain
- Install via shell scripts and one Rust binary to unlock adb on the Orbic
- Needed upstream adb
- No NAS parsing

After

- musl target
- llvm linker
- Pure Rust libraries only
- Only need what you get from rustup
- Portable statically-linked installer
- Uses just-enough adb_client
- Pure Rust NAS parser generated from pycrate

How can you get involved?

- Device porting
- GPS functionality on-device
- USB host mode
- macOS kernel driver detaching in nusb crate
- adb forward in adb_client crate
- Windows installer troubleshooting
- Write an iOS companion app, or improve our Android app
- Keep wardriving! OpenCelliD data is often a decade old

We Want Your Help!

- Do you know people who would be interested in field testing this?
- Do you know telephony experts who can help us come up with good heuristics?
- Do you want to distribute a bunch of these in your other networks?

Advice from My Kid

Acknowledgements

- Sangwook Bae, Ruddy Wang and CAPE for help testing and thinking about heuristics.
- Matthew Garrett for rooting the Orbic and letting us know about it and the diag protocol.
- Andy Carra from Wigle, Russ Hanneman, and Dragorn for advice and testing.
- EFF Staff and others for field testing.
- Gary Miller, Yoshi Kono, Alex Gantman, Subrato De, Alex Ross, and Bradley Reaves for advice and connections.
- Folks at OSMOCOM, QCSuper, and Snoopsnitch for paving the way.
- Yomna for her work at EFF and elsewhere better understanding and protecting against cell site simulators.
- All our open source contributors! Esp. untitaker, sashanoraa, alliraine, MatejKovacic, m0veax, and everyone else!
- oopsbagel thanks: Abby, ahills, Aldera, Alex, Ammar, Cody Harris, daygr, Edwin's Angels, Nathan, q, Rachel, Sharon, Tony
- EFF Members for supporting this work!!!

Thank you!

https://github.com/efforg/rayhunter

Cooper Quintin
Senior Staff Technologist
cooperq@eff.org - bsky: @cooperq.com

Will Greenberg
Senior Staff Technologist
willg@eff.org

oopsbagel
Rayhunter Maintainer
oopsbagel@disroot.org

References

1. https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks
2. https://www.google.com/url?q=https://www.documentcloud.org/documents/24733508-2024_ma-state-police_css-proposal_jacobs/?mode%3Ddocument%23document/p16/a2562758&sa=D&source=editors&ust=1754002755410072&usg=AOvVaw2AM-eIH1FK-BOrlb9AdpZC
3. https://github.com/srsLTE/srsLTE
4. https://arxiv.org/pdf/1710.08932.pdf
5. https://www.usenix.org/system/files/conference/woot17/woot17-paper-park.pdf
6. https://petsymposium.org/popets/2017/popets-2017-0027.pdf
7. https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf