

SITCH

Inexpensive, coordinated GSM anomaly detection

About Me

- 2000: Technology career started (I can get paid for this??)
- 2003: Started building with Linux
- Came to infosec through systems and network engineering, integration
- Security tools and integration (SIEM, HIDS, etc...)
- Current: R&D

About You

- Background in systems and network engineering
- Interested in GSM threat detection
- Tinfoil hat not required... but not unwelcome!

“Thoughts and opinions expressed are my own. If you take anything away from this talk and act on it, I’m not responsible if you go to jail, become a pariah, or your dog stops liking you. Know the laws you’re subject to and operate accordingly.”

–Ashmastaflash

What We're Covering Today

- Why Care?
- Current Threat and Detection Landscape
- Project Goals
- SITCH: MkI
- SITCH: MkII
- Service Architecture
- Future Plans
- Prior Art
- Q&A

Why Care?

- Invasions of privacy are bad, even when they're unnoticed.
- Industrial espionage costs money and jobs.

WTF Is Under All That??



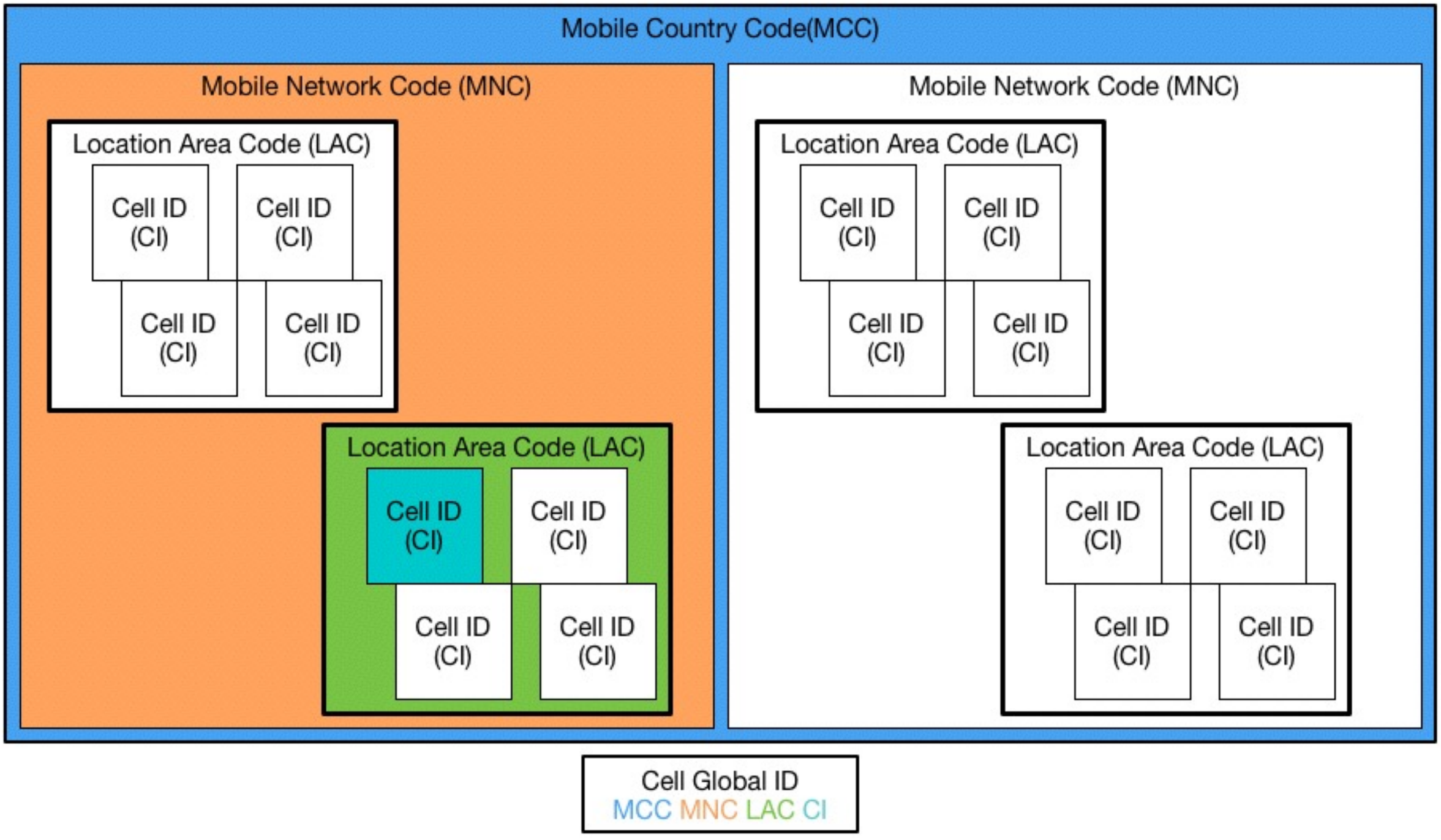
Is Anybody Home?



Terminology

- Software Defined Radio (SDR): Using software to perform signal processing in concert with an adjustable-frequency RF receiver
- ARFCN: Absolute Radio Frequency Channel Number
- BTS: Base Transceiver Station
- CGI: Cell Global ID (MCC + MNC + LAC + CI)
    - MCC: Mobile Country Code
    - MNC: Mobile Network Code
    - LAC: Location Area Code
    - CI: Cell ID
- IMSI: International Mobile Subscriber Identity

GSM Addressing



Cell Global ID
MCC MNC LAC CI

Threat and Detection Landscape

- Malicious Devices
- Indicators of Attack
- Existing Detection Methods

Hacked Femtocell

Trusted part of provider's network
Your phone doesn't know it's evil



Evil BTS

Handset will automatically associate, unable to assert trustworthiness



Indicators of Attack

- ARFCN over threshold
- ARFCN outside forecast
- Unrecognized CGI
- Gratuitous BTS re-association
- BTS detected outside of range

Detection Methods

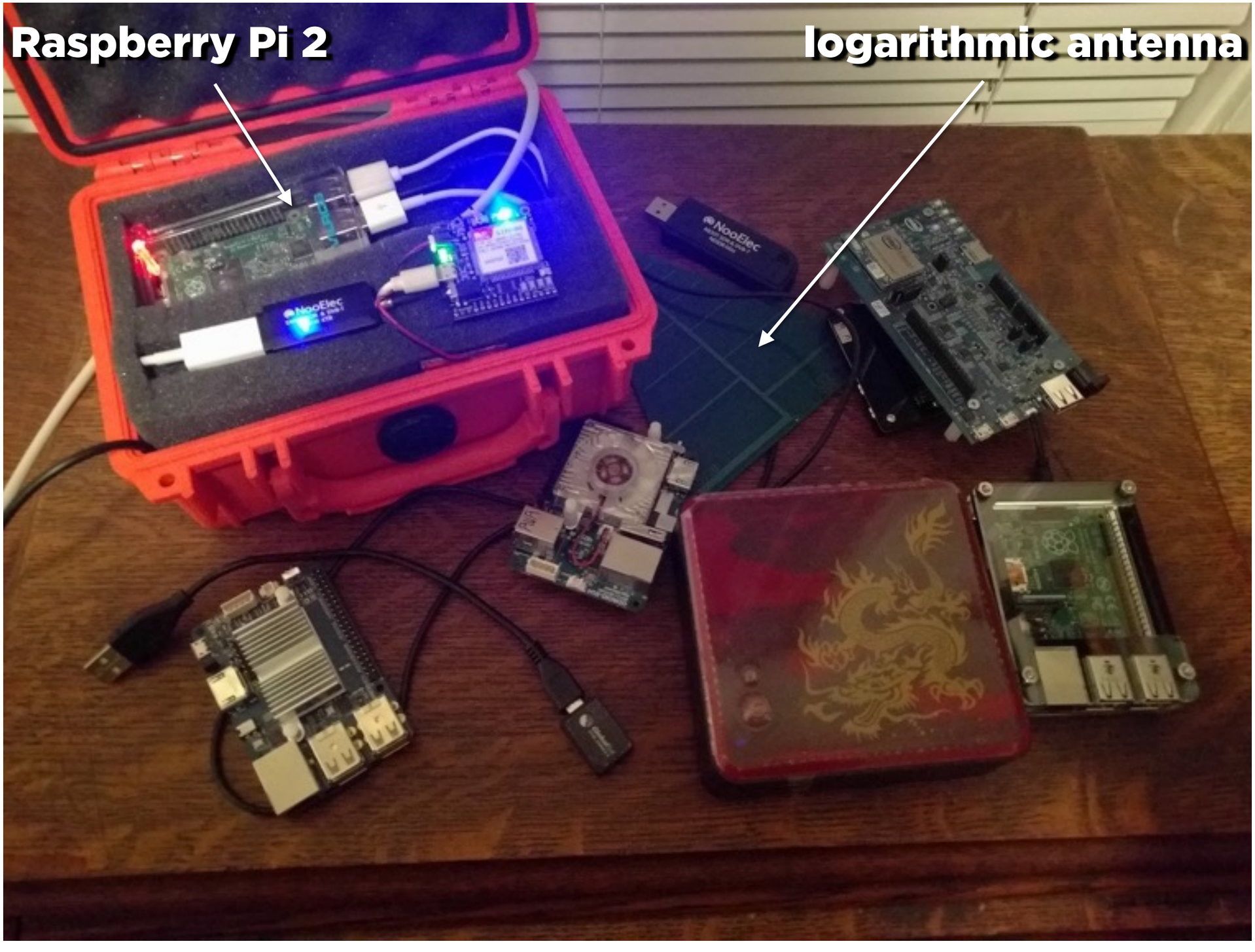
- Commercial Options:
  - Pwnie Express
  - Bastille Networks
- Open Source:
  - Fake BTS
  - AIMSICD
  - Femto Catcher

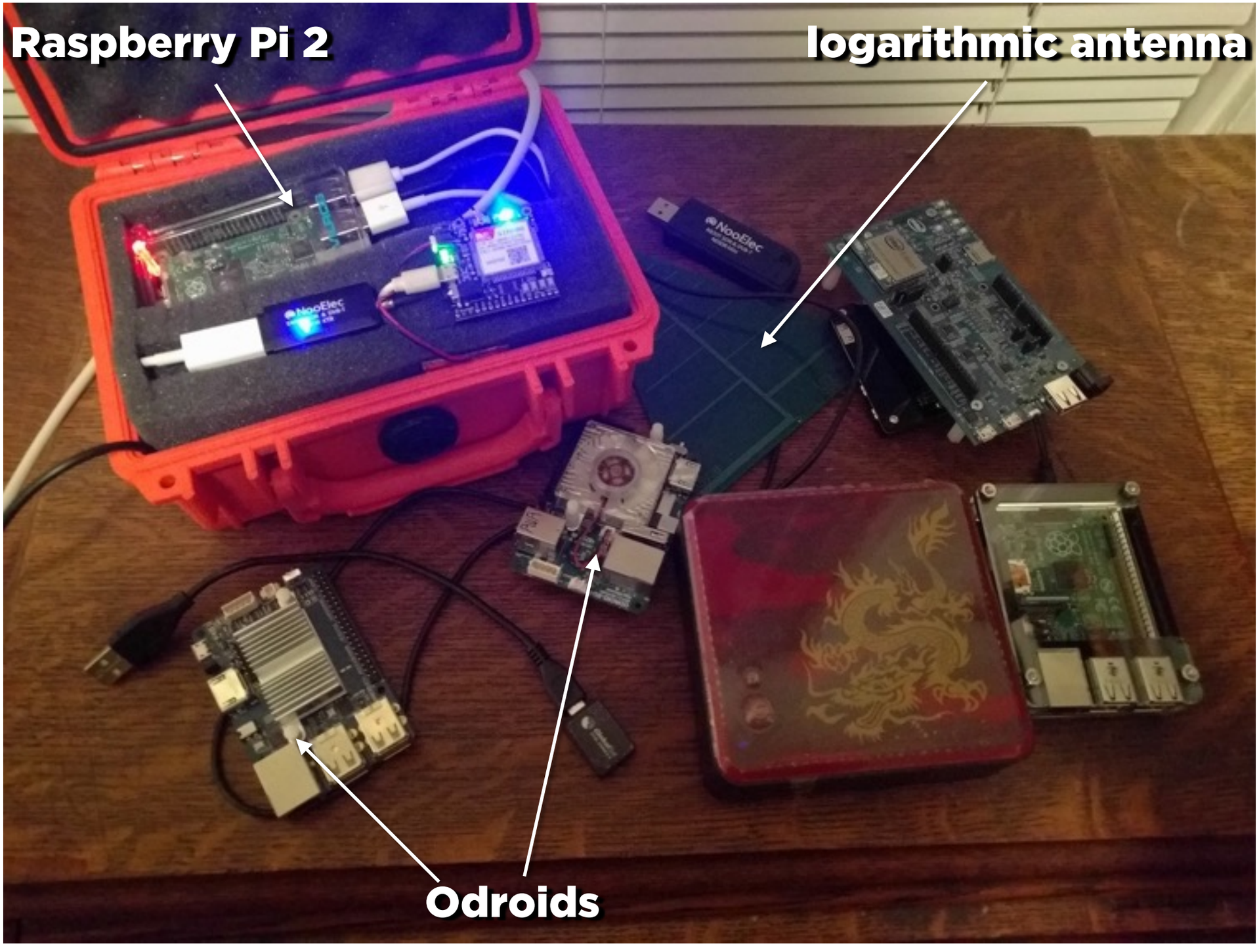
Project Goals

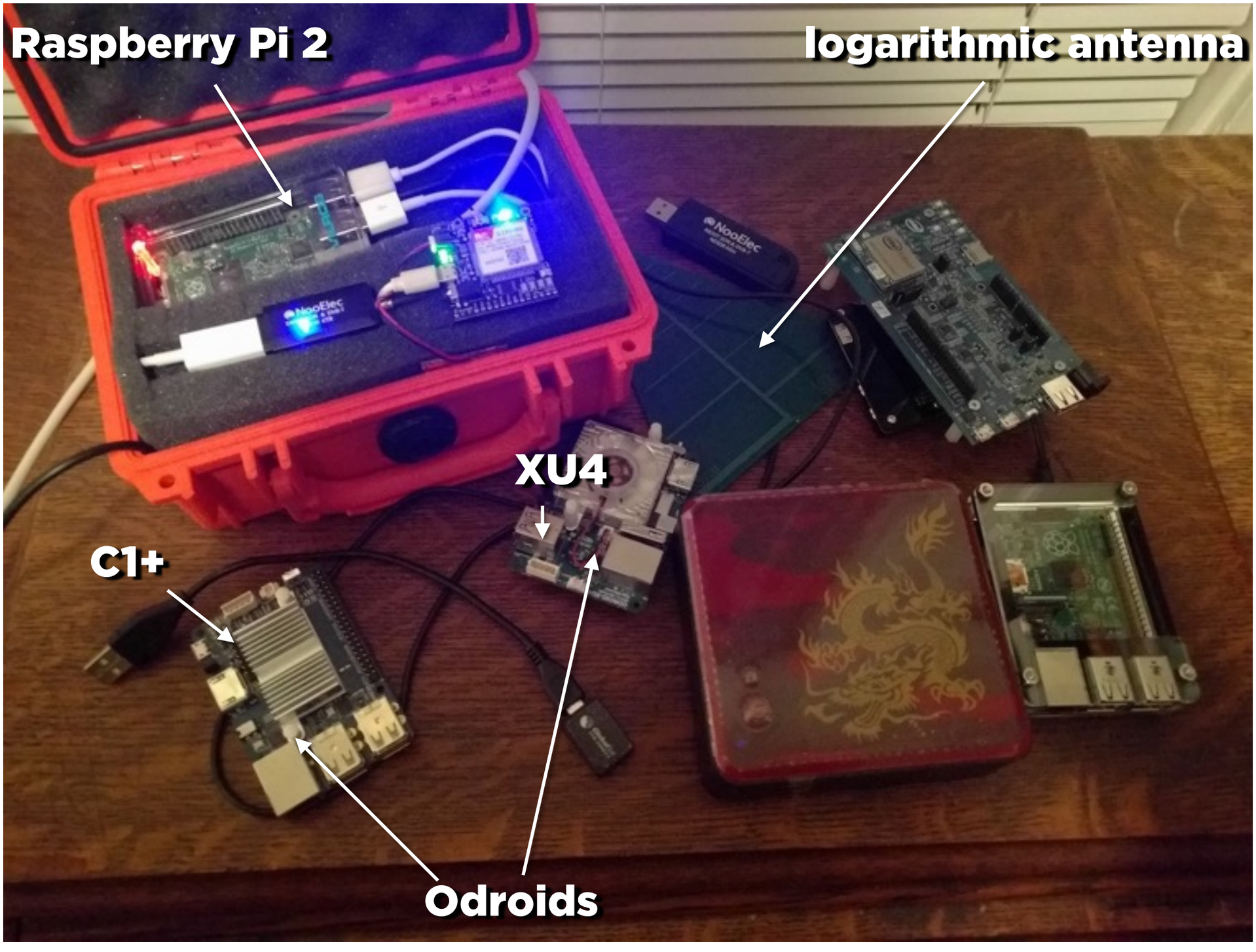
- Inexpensive (what can I get for $100?)
- Small footprint, low power requirements preferred
- Functional Targets: Indicators of Attack (IOA) Coverage
- Centrally managed software and configuration

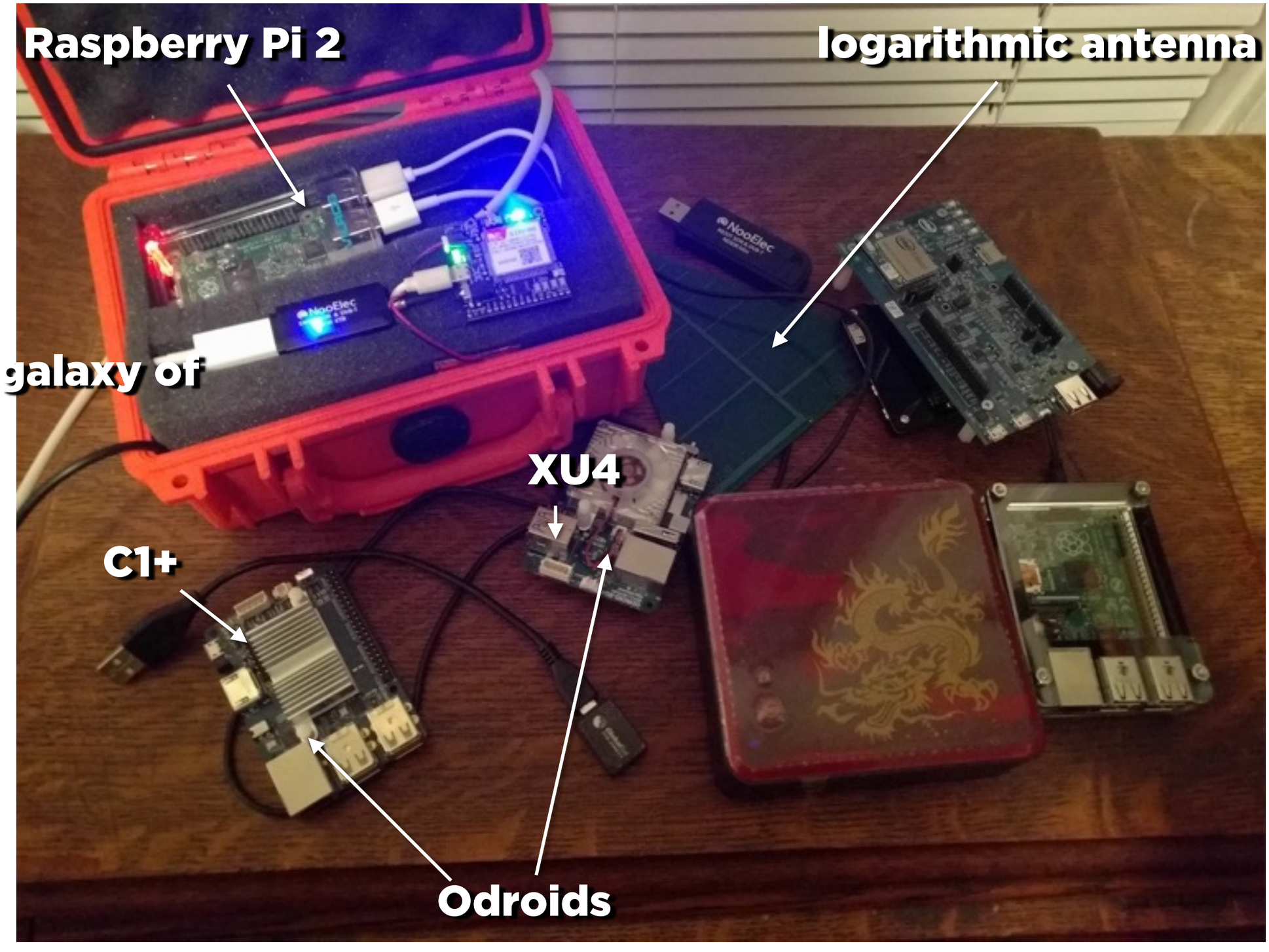

NooElec
NooElec

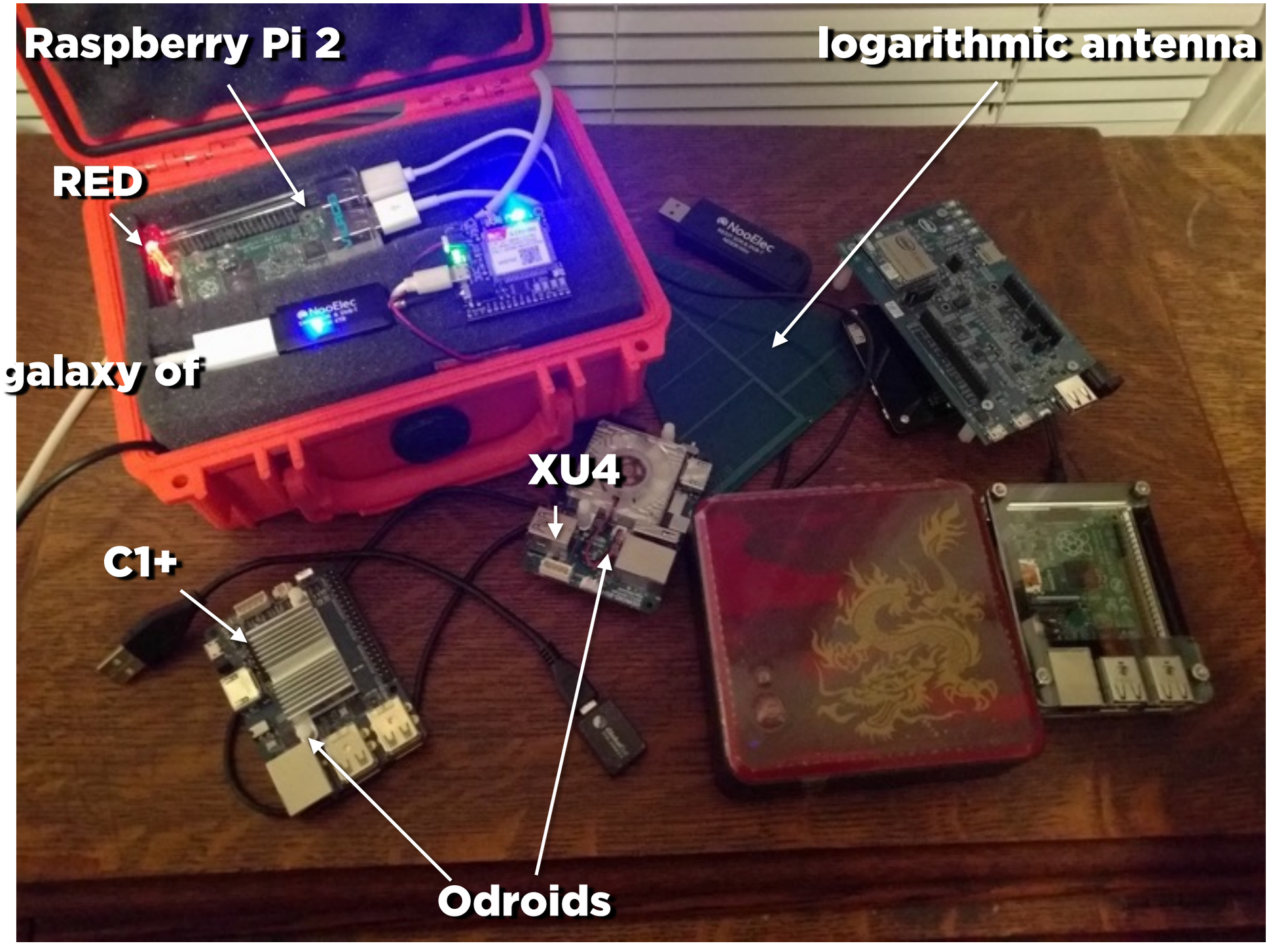

Raspberry Pi 2

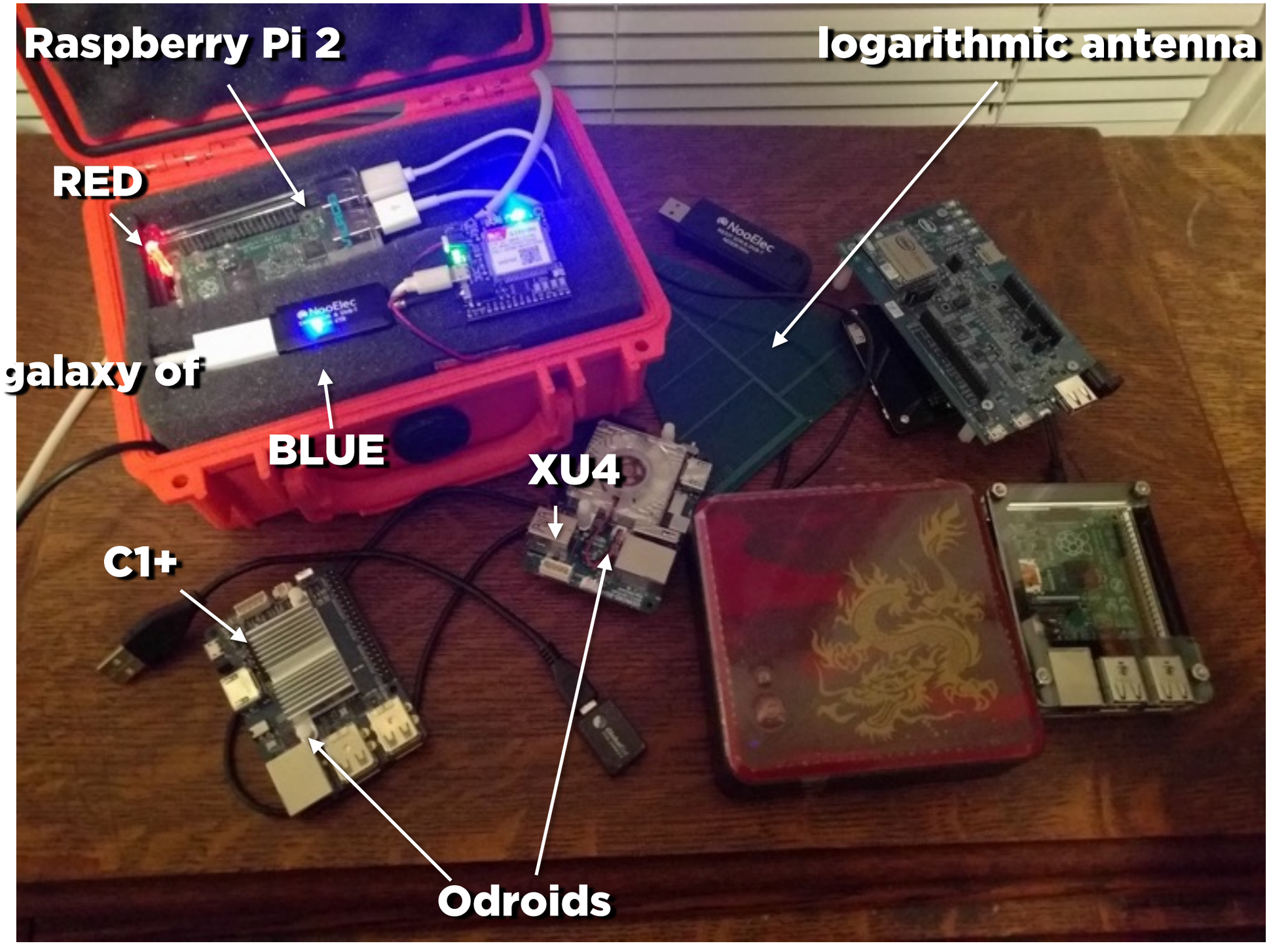

Raspberry Pi 2
logarithmic antenna

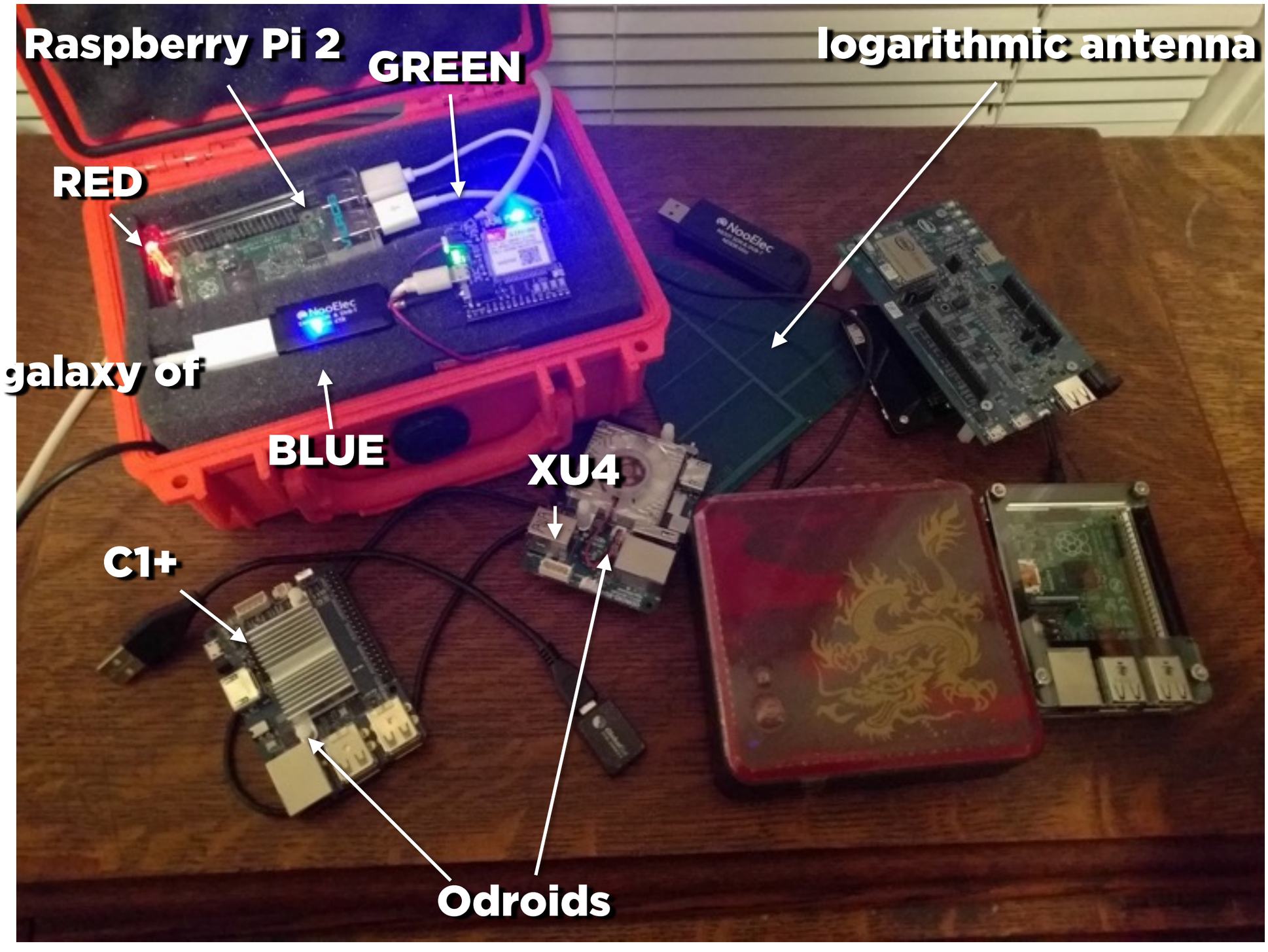

Raspberry Pi 2
logarithmic antenna
Odroids

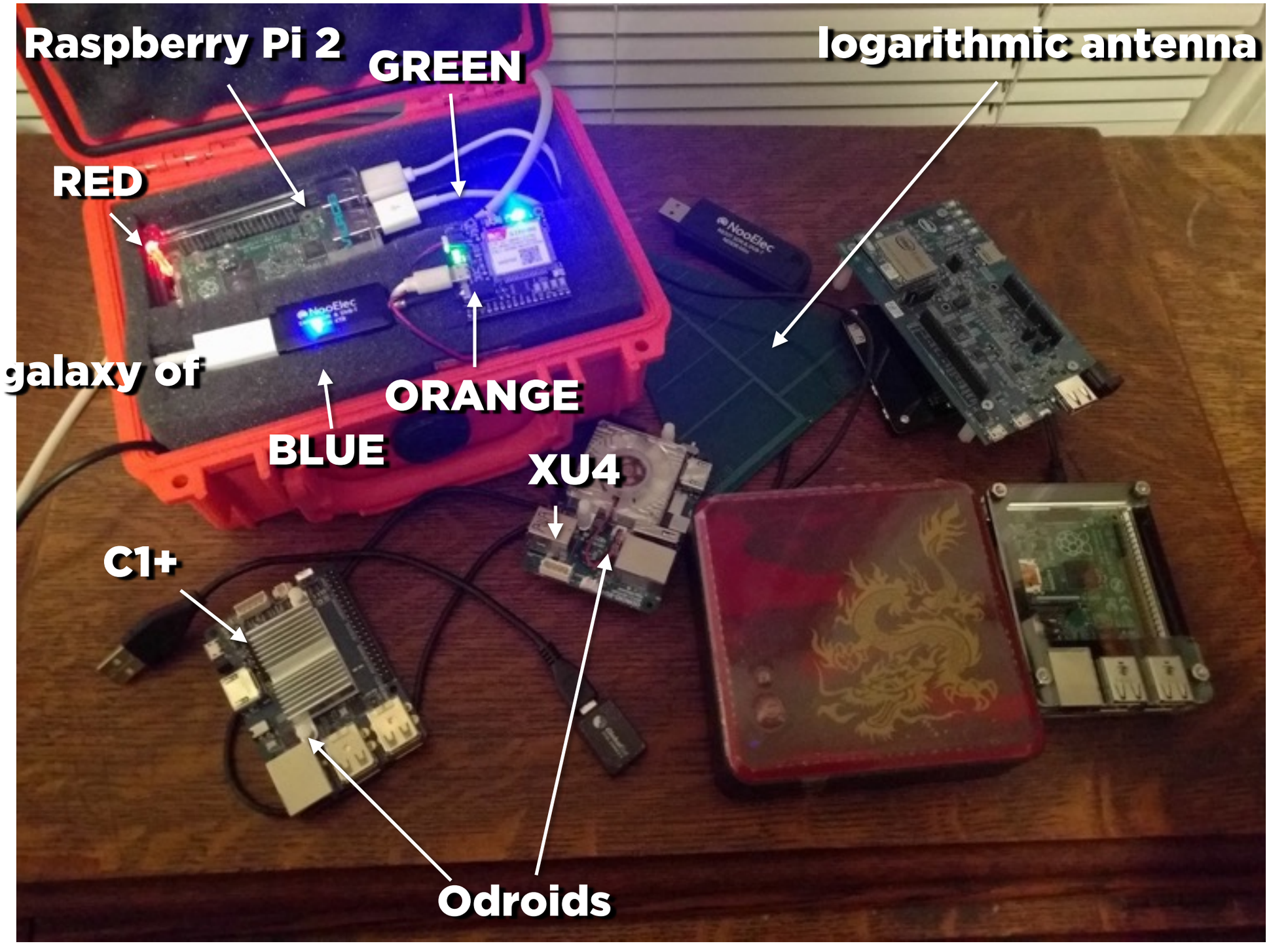

Raspberry Pi 2
logarithmic antenna
XU4
C1+
Odroids

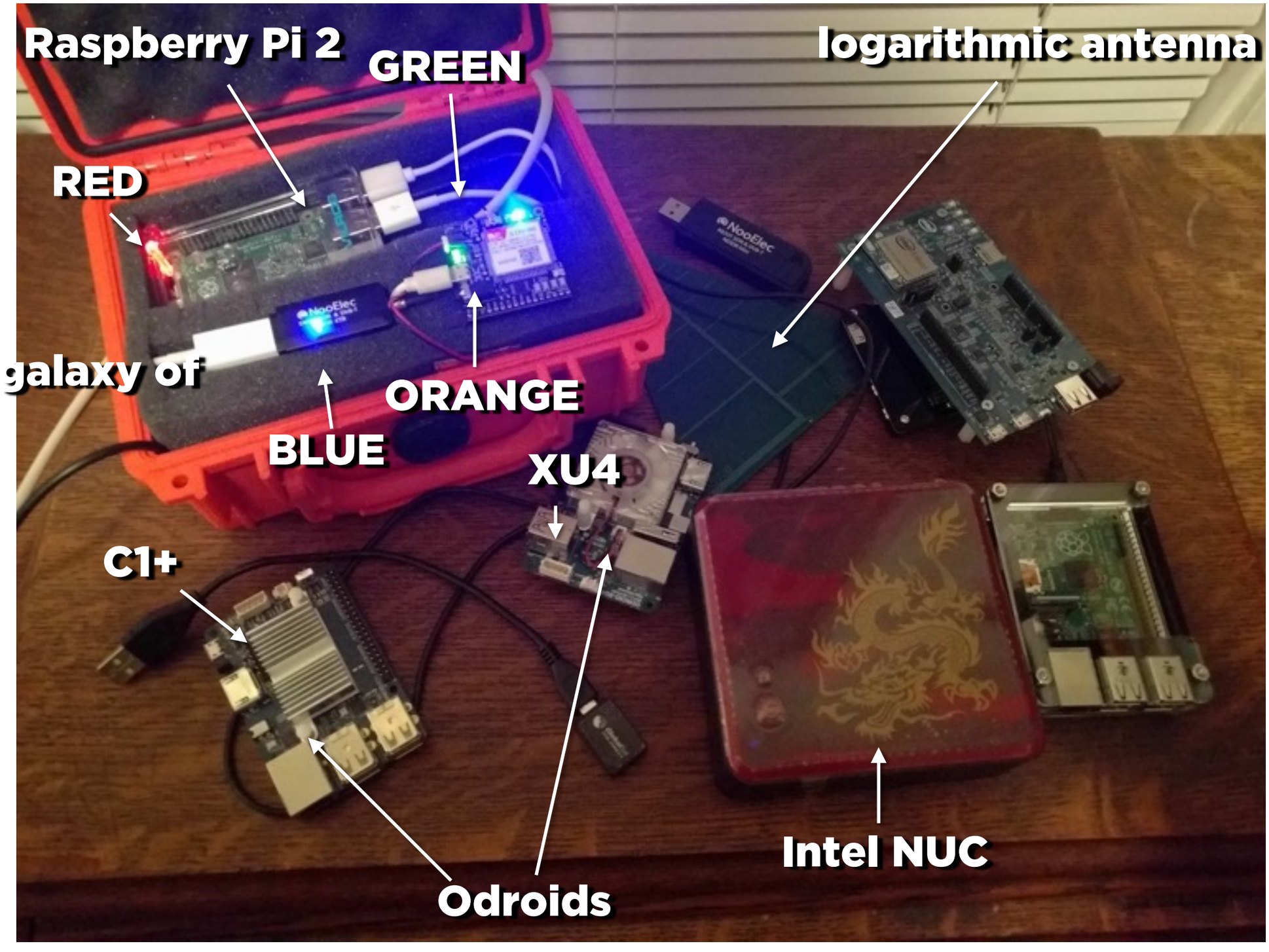

Raspberry Pi 2
logarithmic antenna
galaxy of
XU4
C1+
Odroids

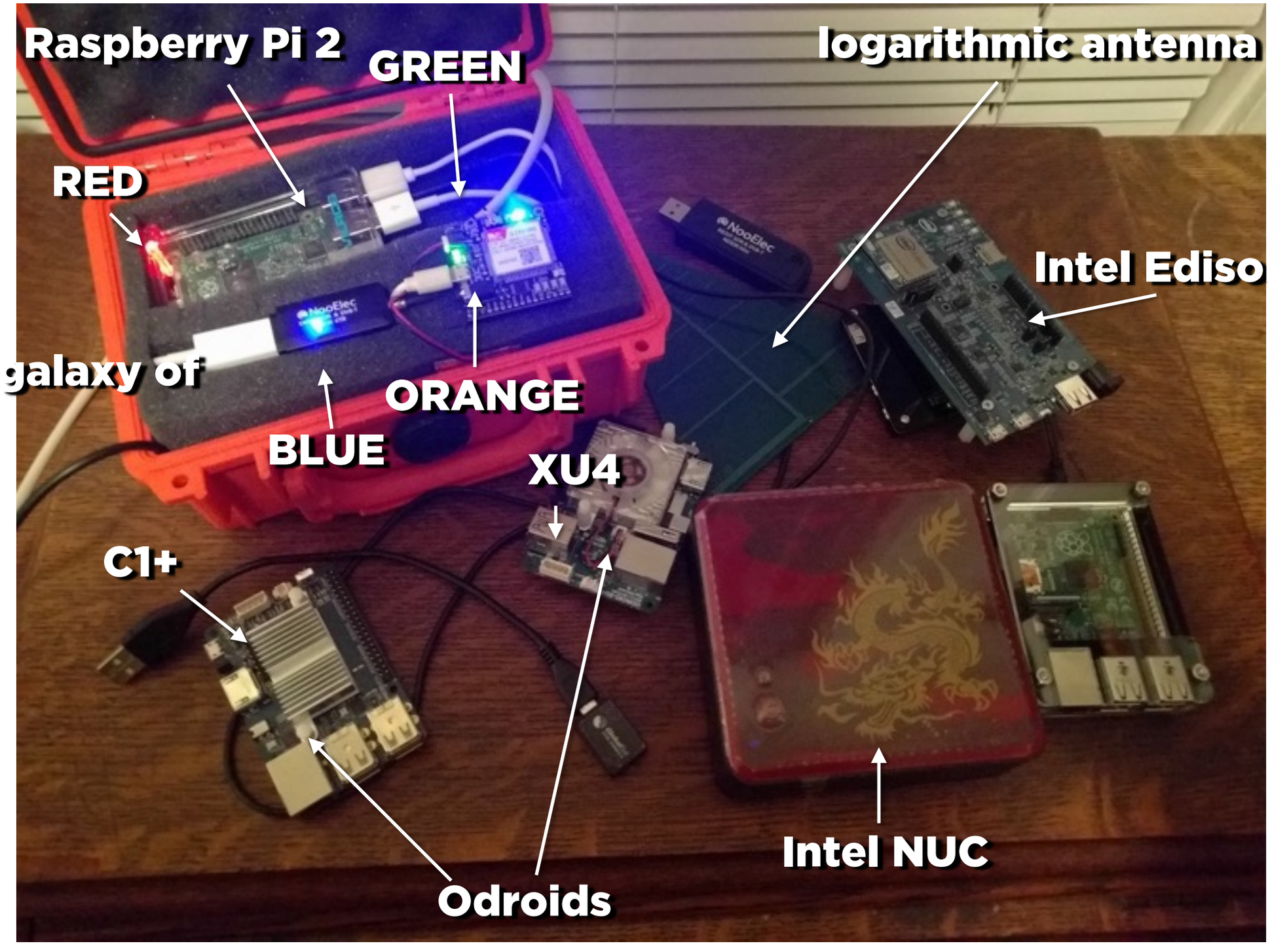

Raspberry Pi 2
logarithmic antenna
RED
galaxy of
XU4
C1+
Odroids

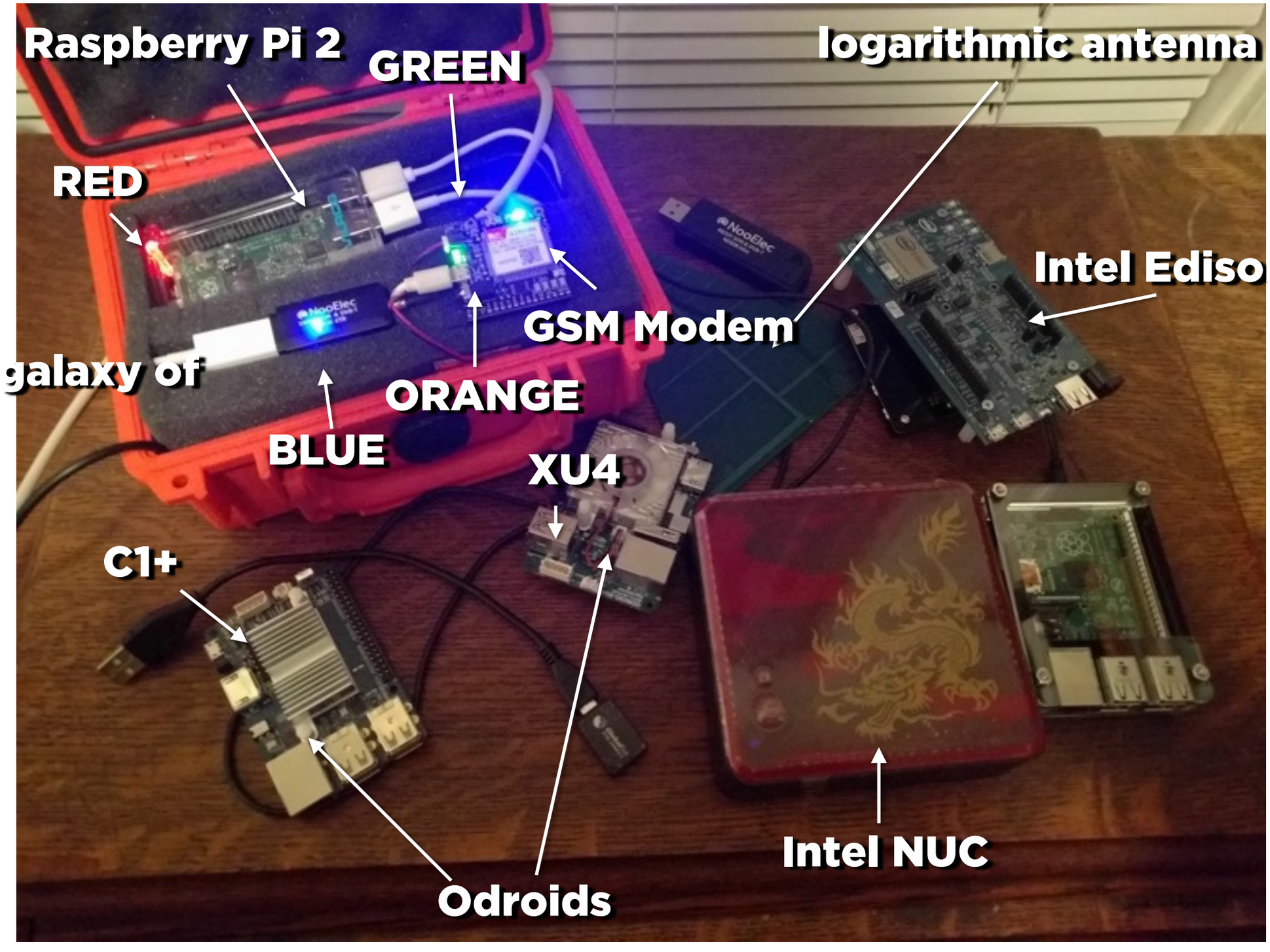

Raspberry Pi 2
logarithmic antenna
RED
galaxy of
BLUE
XU4
C1+
Odroids

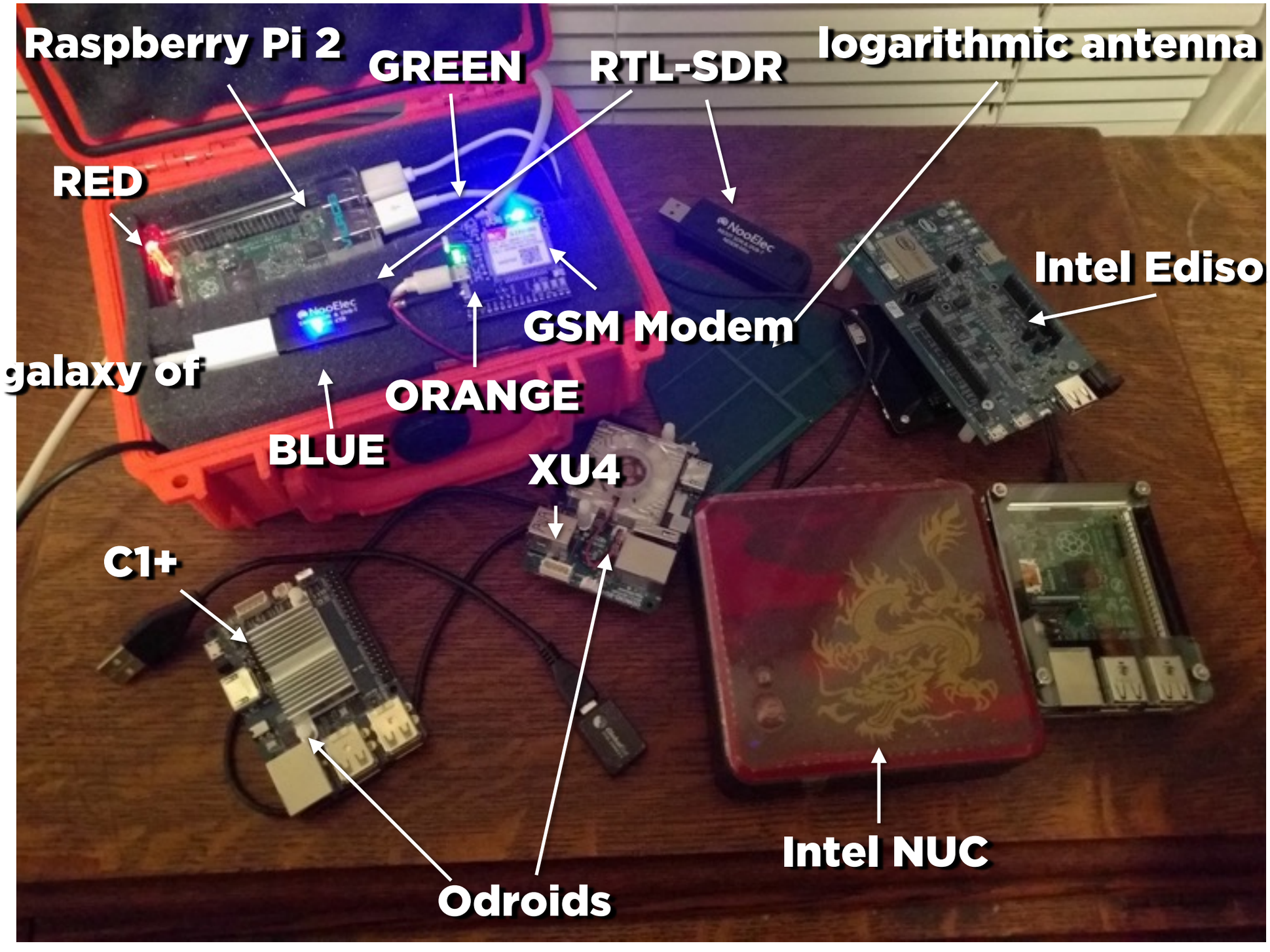

Raspberry Pi 2
GREEN
logarithmic antenna
RED
galaxy of
BLUE
XU4
C1+
Odroids


Raspberry Pi 2
GREEN
logarithmic antenna
RED
galaxy of
ORANGE
BLUE
XU4
C1+
Odroids


Raspberry Pi 2
GREEN
logarithmic antenna
RED
galaxy of
ORANGE
BLUE
XU4
C1+
Odroids
Intel NUC


Raspberry Pi 2
GREEN
logarithmic antenna
RED
Intel Edison
galaxy of
ORANGE
BLUE
XU4
C1+
Intel NUC
Odroids


Raspberry Pi 2
GREEN
logarithmic antenna
RED
Intel Edison
GSM Modem
galaxy of
ORANGE
BLUE
XU4
C1+
Intel NUC
Odroids


Raspberry Pi 2
GREEN
RTL-SDR
logarithmic antenna
RED
Intel Edison
galaxy of
GSM Modem
ORANGE
BLUE
XU4
C1+
Intel NUC
Odroids

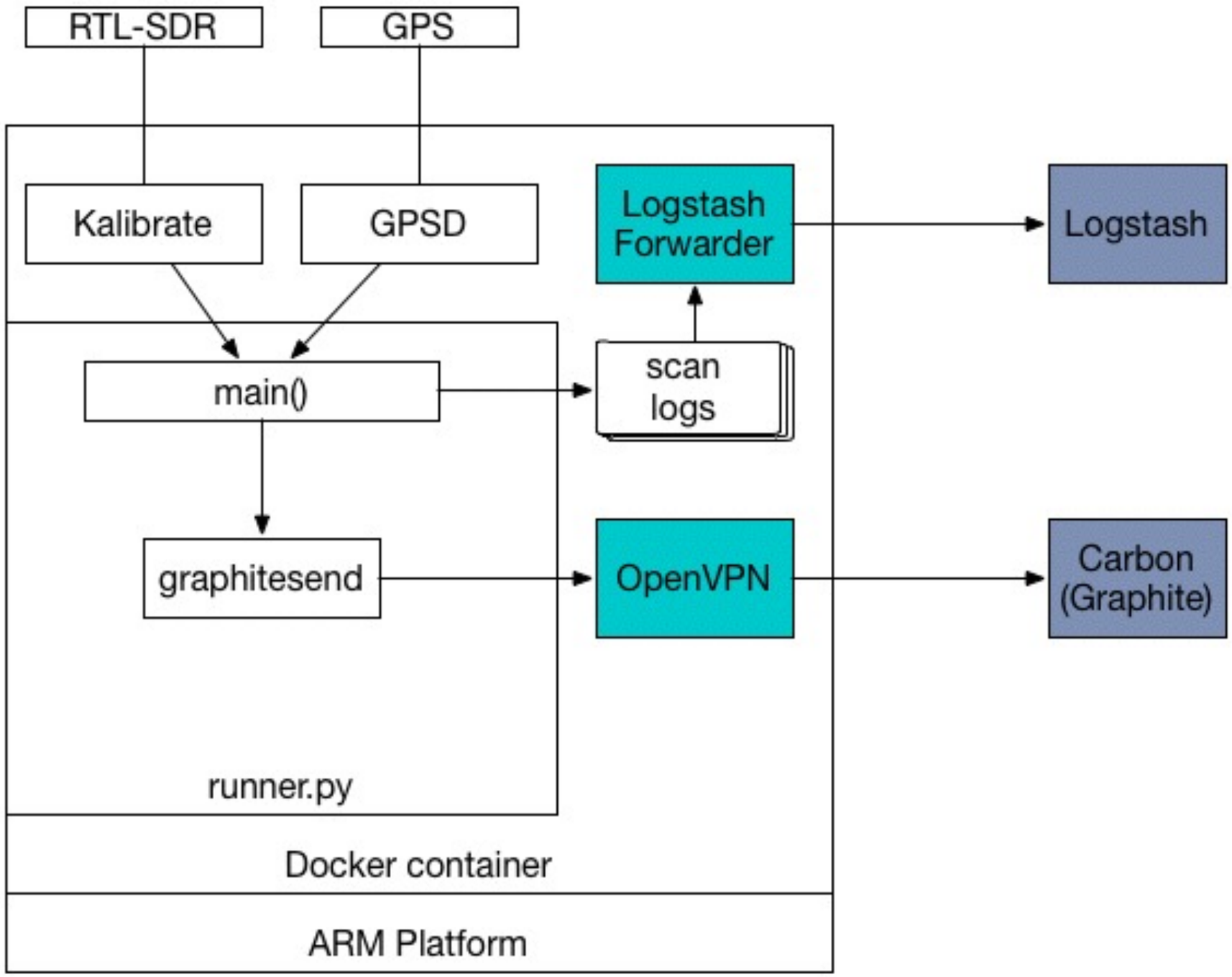

Raspberry Pi 2
GREEN
RTL-SDR
logarithmic antenna
RED
Intel Edison
GSM Modem
galaxy of
ORANGE
BLUE
XU4
C1+
I didn't really *need* all of this...
Intel NUC
Odroids



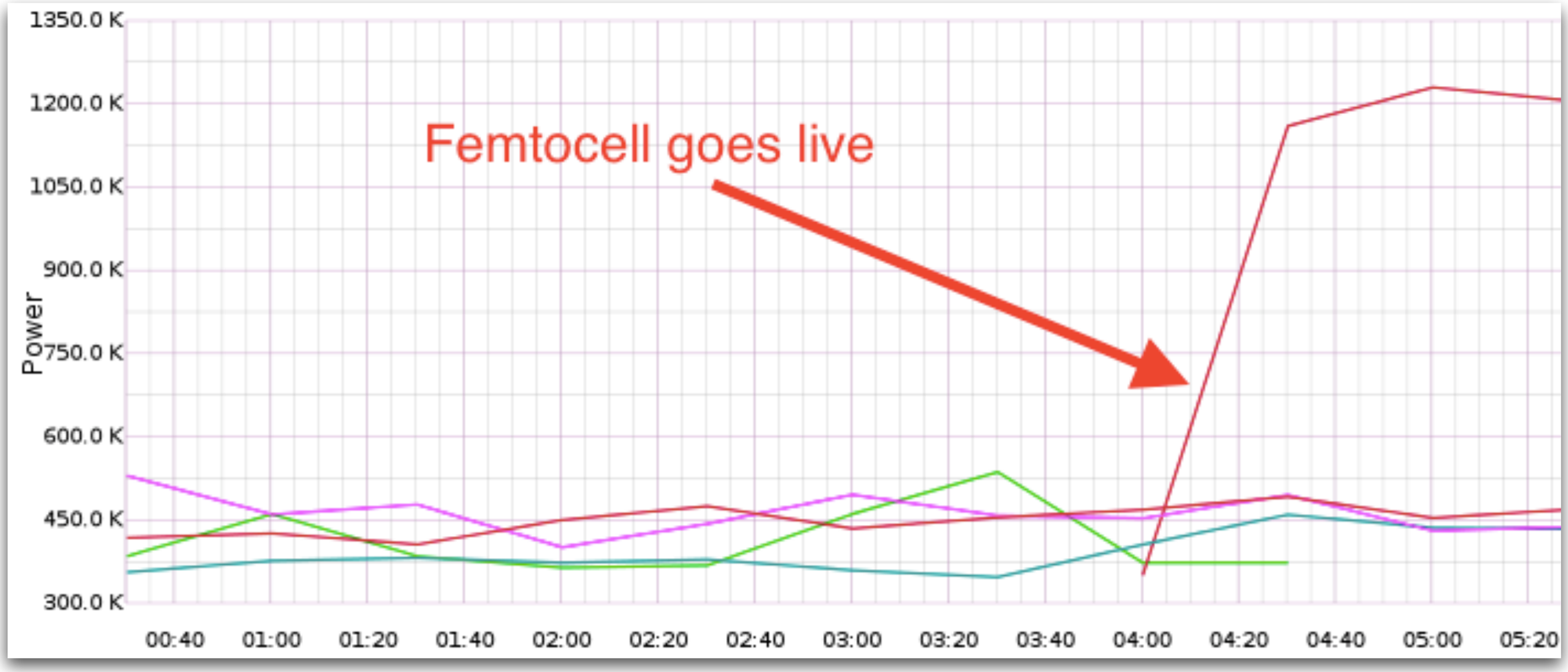
SITCH

Situational Information from Telemetry and Correlated Heuristics

SITCH Sensor MkI



SITCH Sensor MkI



MkI Results

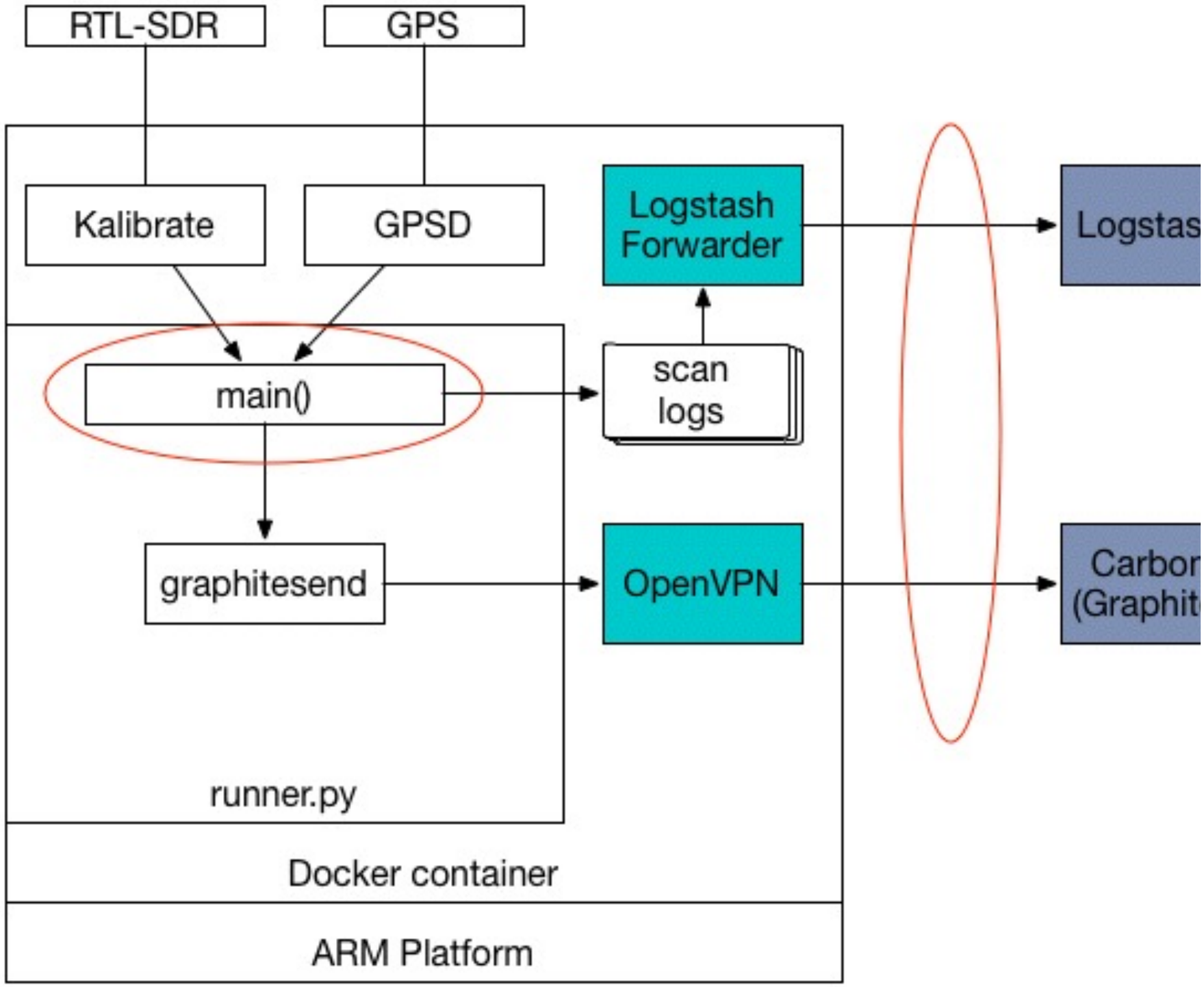
Targets	MkI Coverage
ARFCN over threshold	YES
ARFCN outside of forecast	YES
Unrecognized CGI	NO
Gratuitous BTS re-association	NO
BTS detected outside of range	NO
Price	~$100

Releasing MKL?

No.



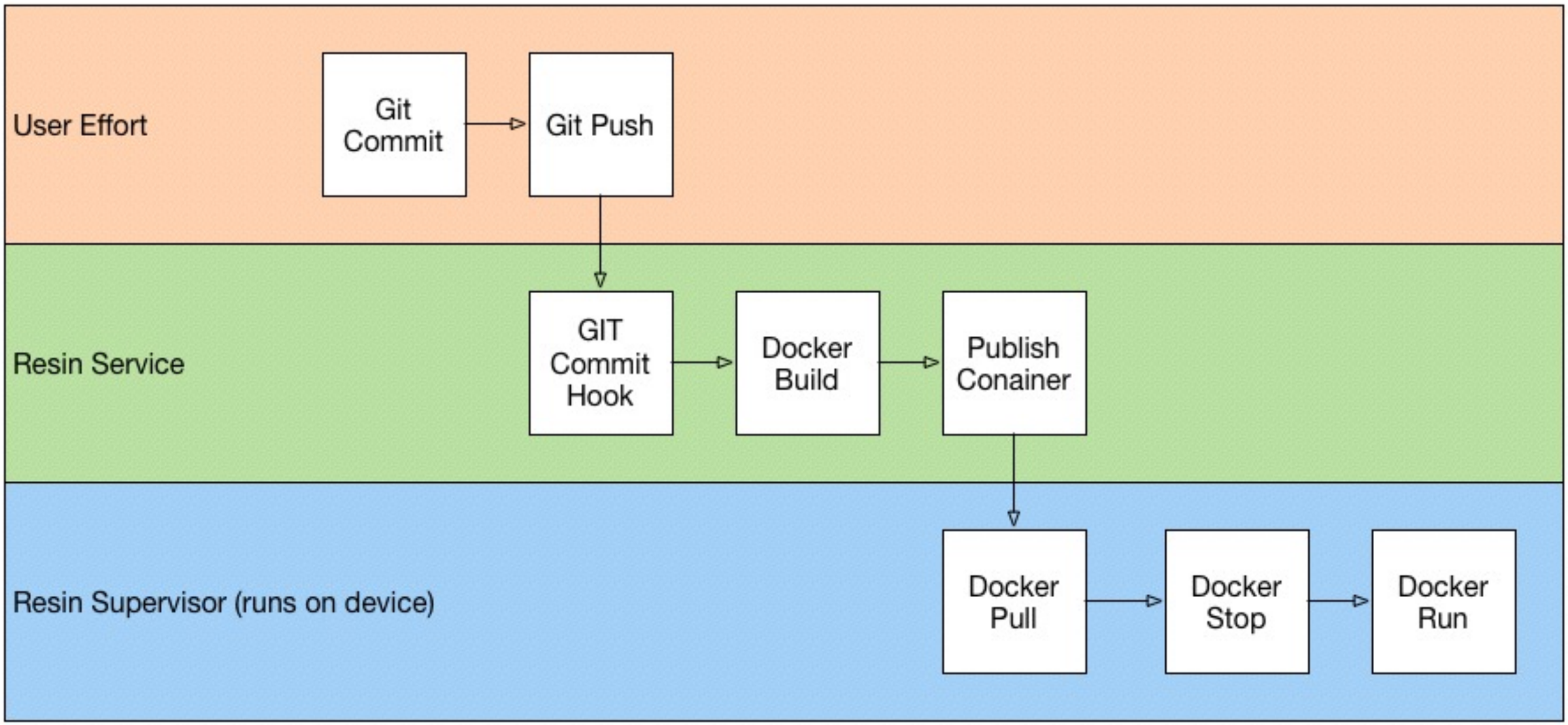
What's wrong with MkI?



Start Demo Here!

- Confirm device registration
- Image download starts

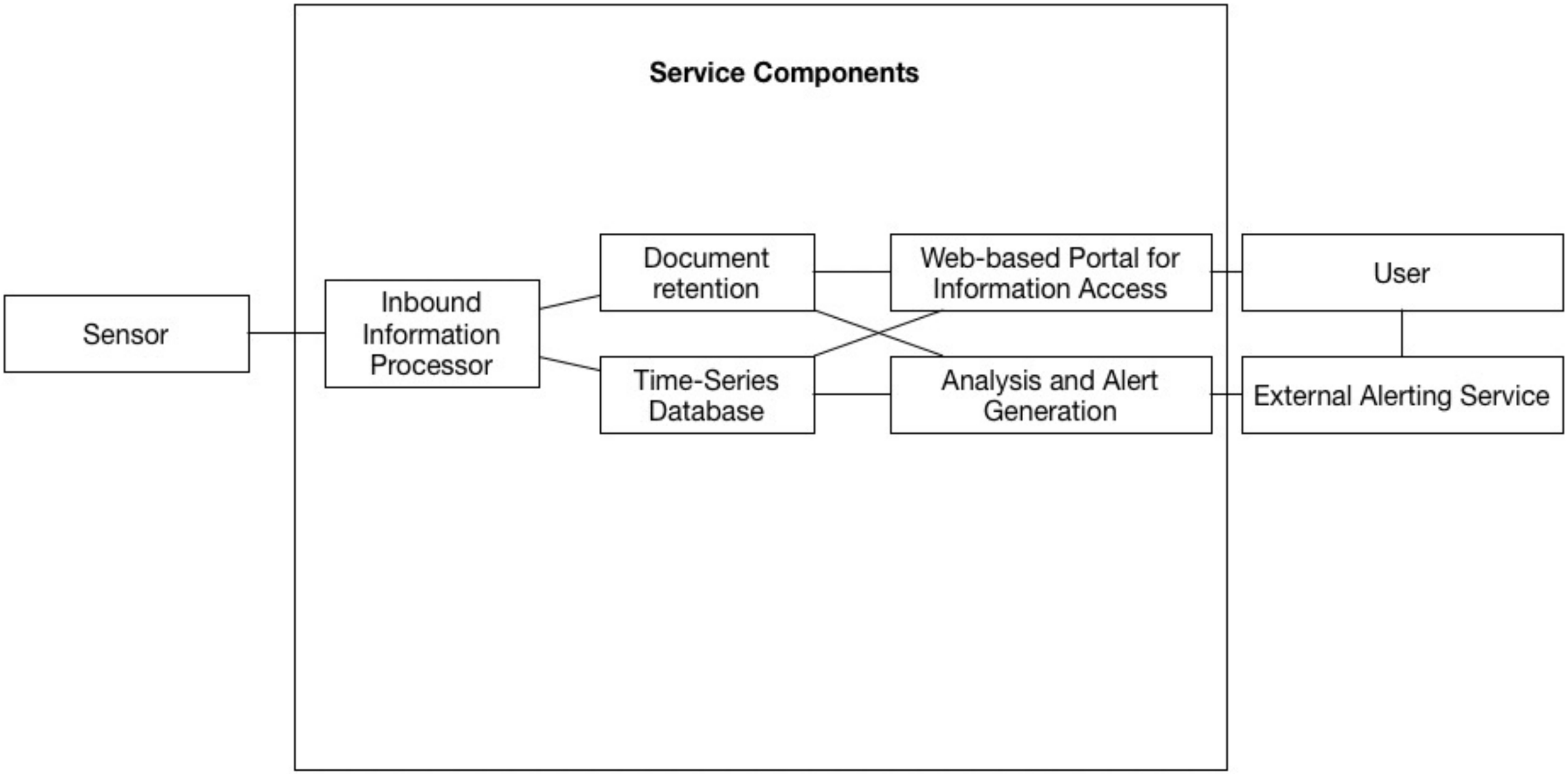
Deployment Pipeline



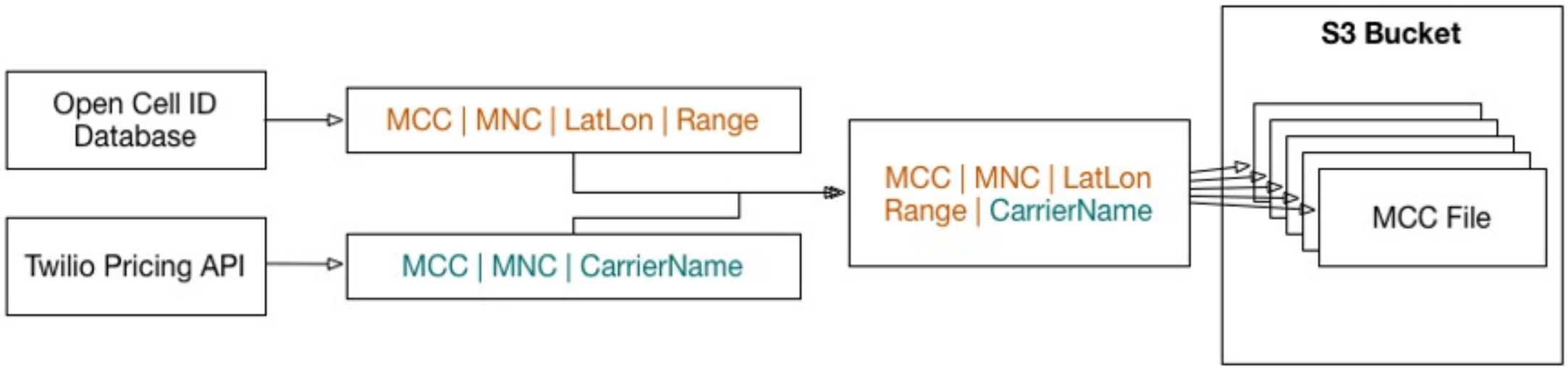
Service-Side Software

Tool	Purpose
Logstash	Inbound Information Processing Alert delivery
Elasticsearch	Scan document retention
Carbon/Graphite	Time-series database Statistical analysis of time-series data
Kibana	Browse scans
Tessera	Dashboard for Graphite
Graphite Beacon	Alert Generation
Vault	Secret management
Resin	Software Deployment
Slack	Notifications

SITCH Service Architecture

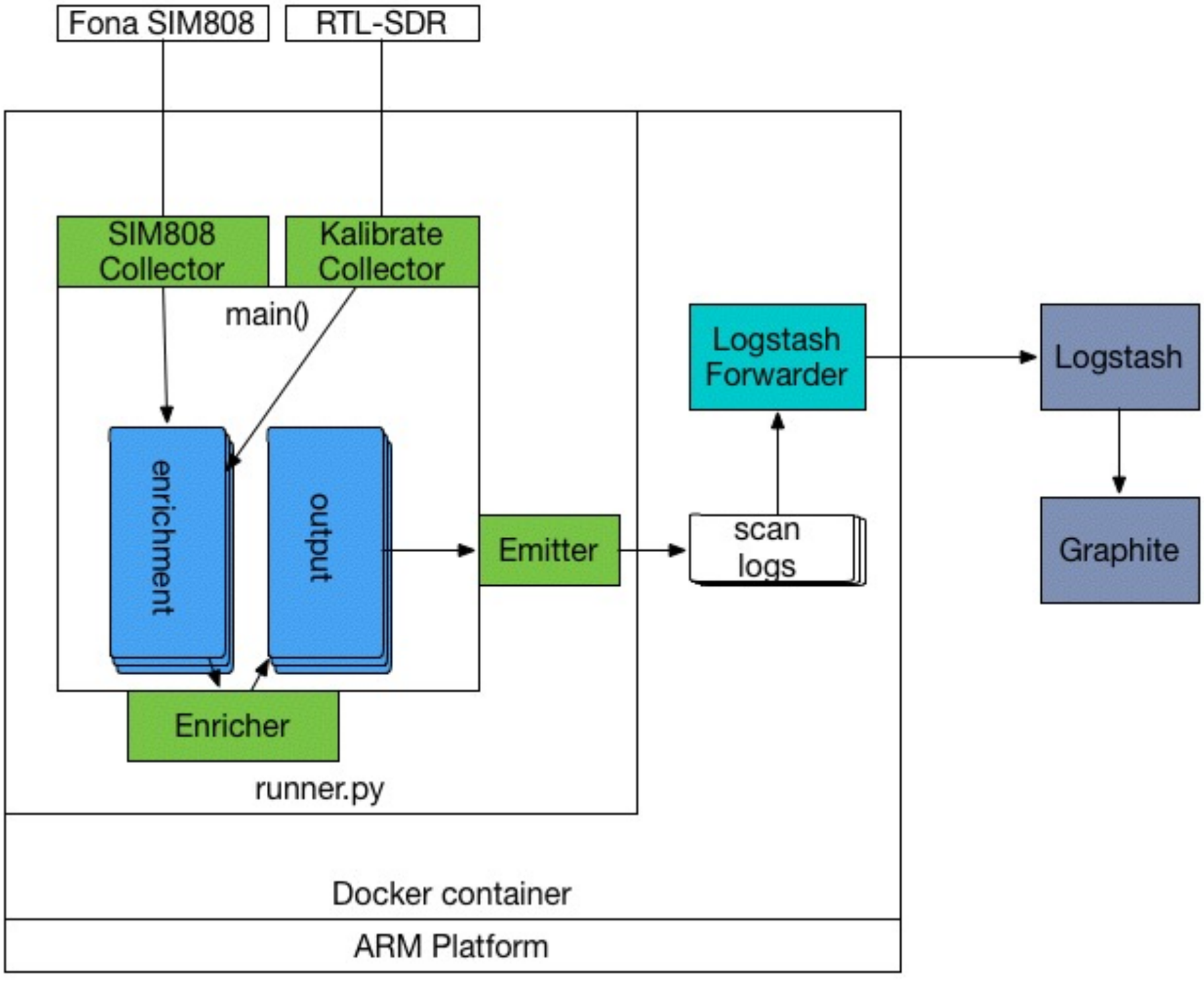


SITCH Intelligence Feed

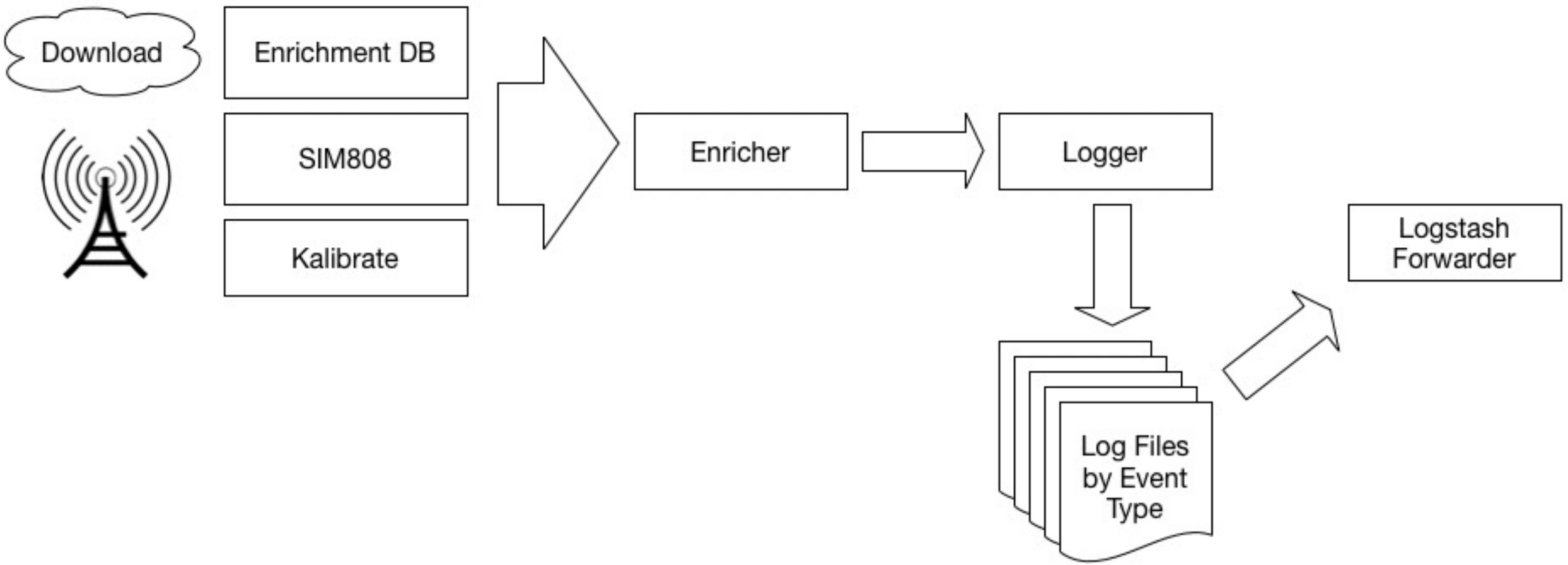


- OpenCellID Database:
  - MCC, MNC, Lat, Lon, Range
- Twilio:
  - MCC, MNC, CarrierName

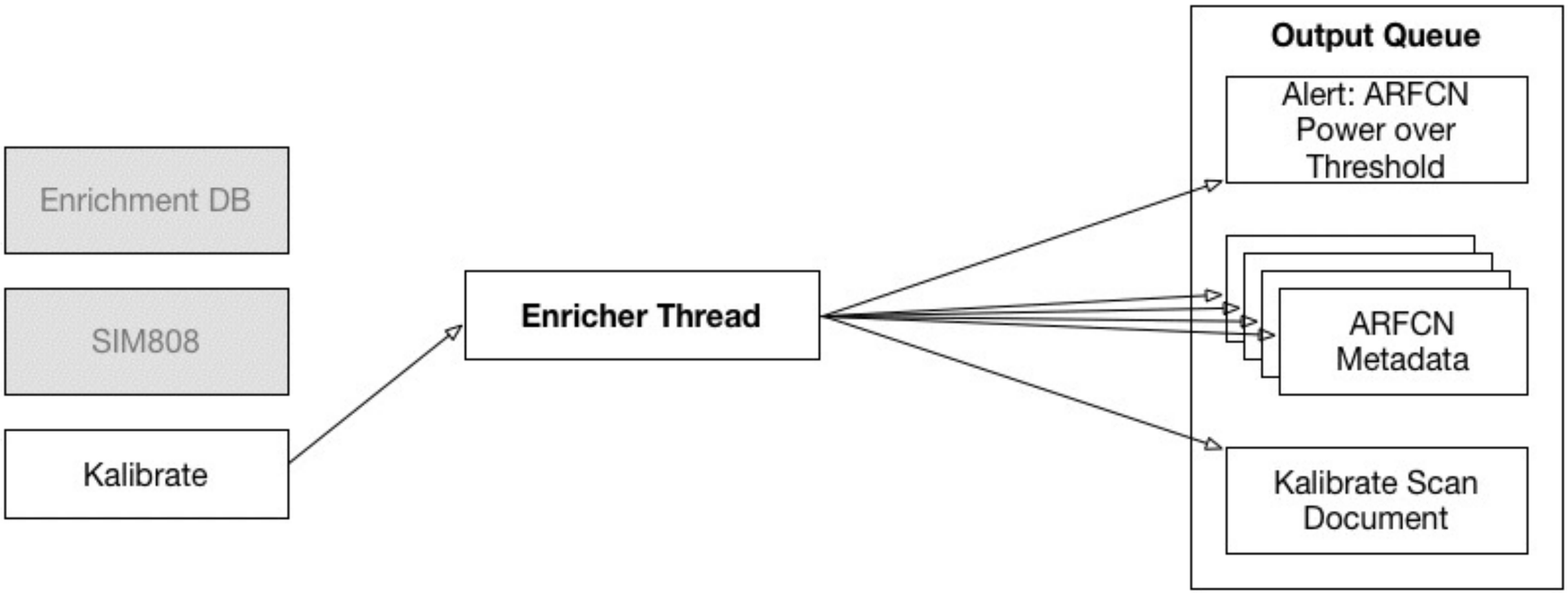
SITCH Sensor MkII



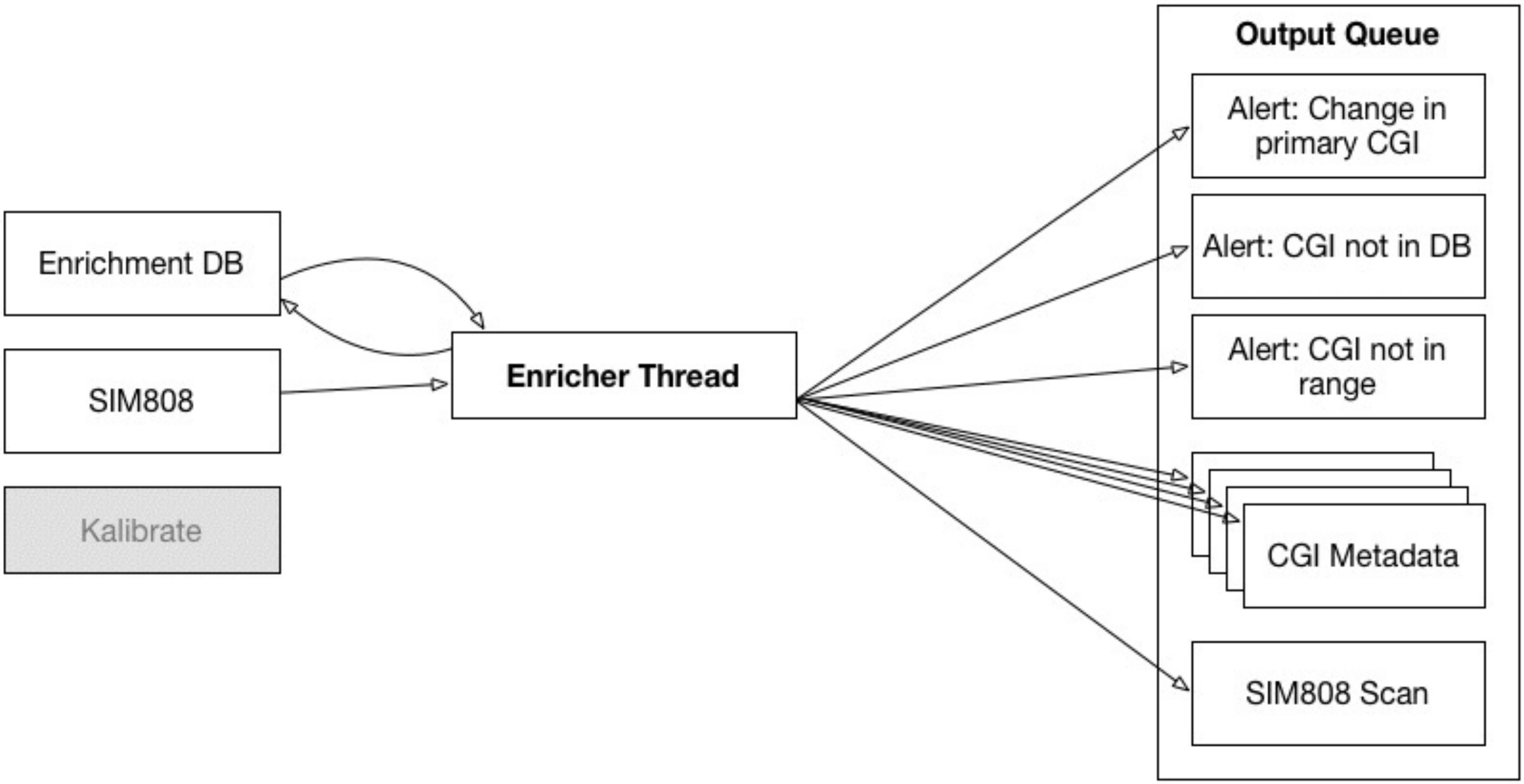
SITCH Sensor MkII



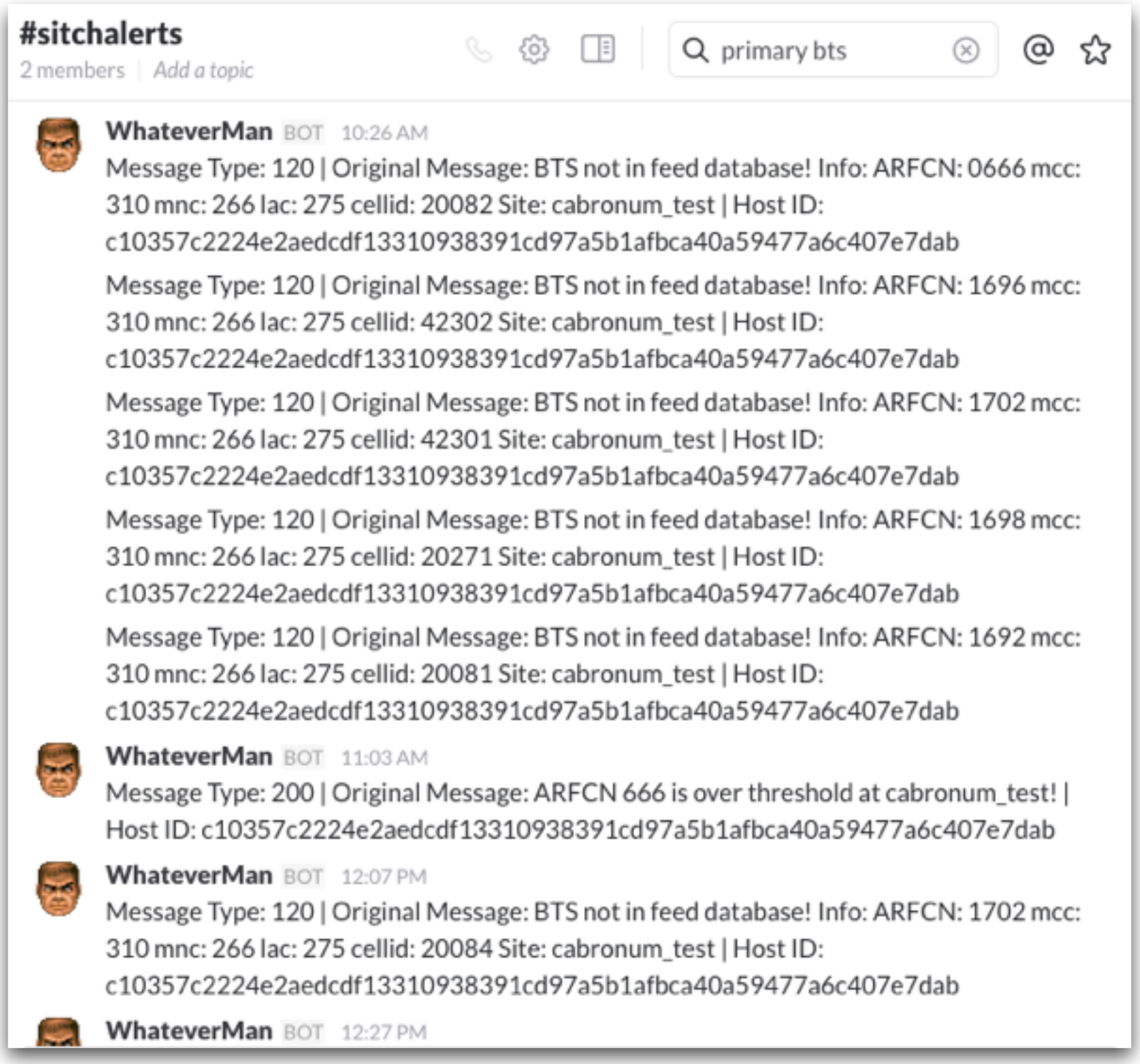
SITCH Sensor MkII



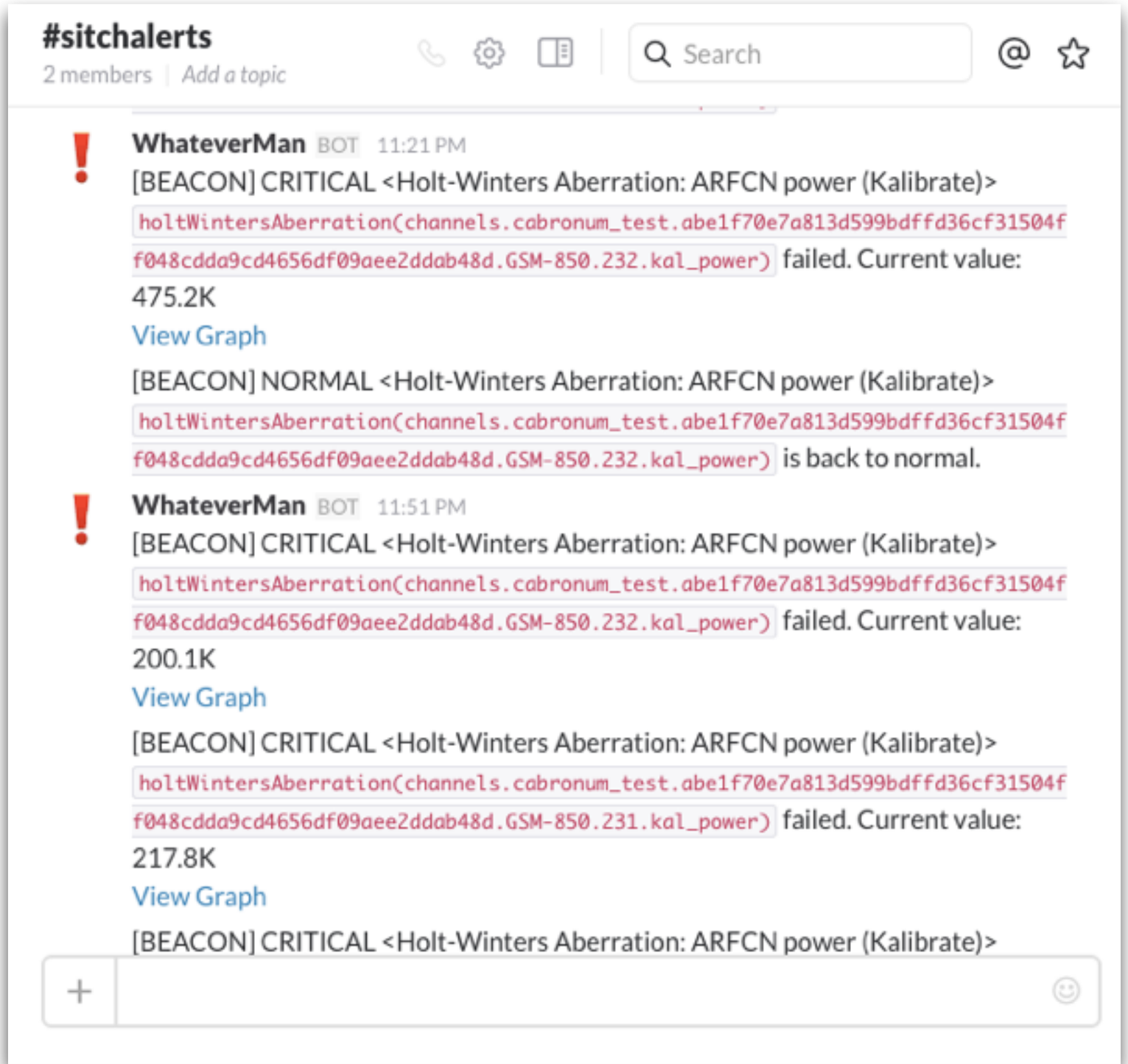
SITCH Sensor MkII



SITCH Sensor MkII



SITCH Sensor MkII



Return to Demo!

- Slack alerts
- Tessera graphs
- Kibana scan search
- Resin logs

MkI, MkII Summary

Targets	MkI Coverage	MkII Coverage
ARFCN over threshold	YES	YES
ARFCN outside of forecast	YES	YES
Unrecognized CGI	NO	YES
Gratuitous BTS re-association	NO	YES
BTS detected outside of range	NO	YES
Price	~$100	~$150

Going Forward

- Automatic device detection
- Device and service heartbeats
- Gnuradio = pure SDR:
    - GR-GSM
    - ADS-B
    - FPV drone
- Dedicated radios:
    - Ubertooth One
    - YARD Stick One

Prior Art

- DIY Cellular IDS (Davidoff, Fretheim, Harrison, & Price, Defcon 21)
- Traffic Interception and Remote Mobile Phone Cloning with a Compromised Femtocell (DePerry, Ritter, & Rahimi, Defcon 21)
- Introduction to SDR and the Wireless Village (DaKahuna & Satanklawz, Defcon 23)
- http://fakebts.com - Fake BTS Project (Cabrera, 2014)
- How to Build Your Own Rogue GSM BTS for Fun and Profit (Simone Margaritelli)
- Gnuradio (many)
- Gr-gsm (Krysik, et al.)
- Kalibrate (thre.at)

THANKS!

- John Menerick
- Gillis Jones
- Christian Wright
- Dave Doolin
- Silent Contributors...

Q&A

#OMW2 Scan Your GSM

