*BSides Canberra 2016*

# Catching 'Rays

Steve Glass
@drsmdg

# Outline

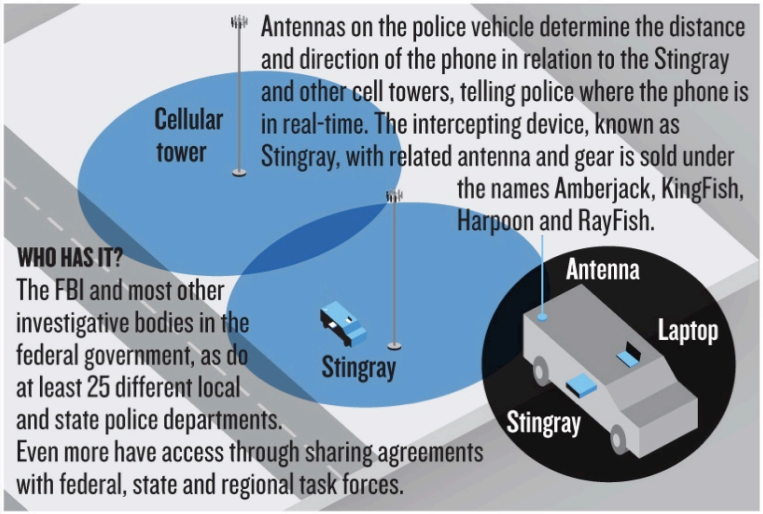
- Stingray Threats
- Detective Tools
- Self-Assembly Approach
- Questions/Comments

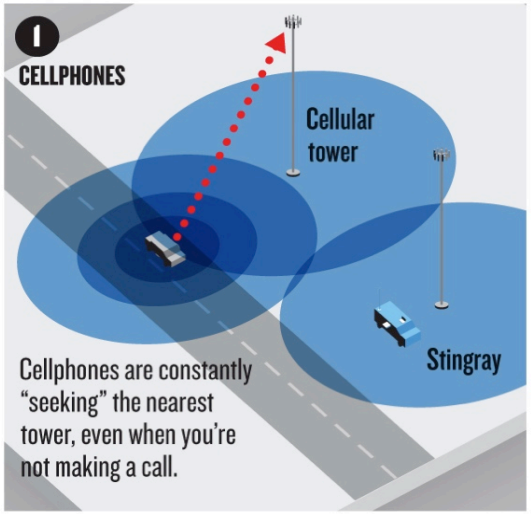
# Stingrays

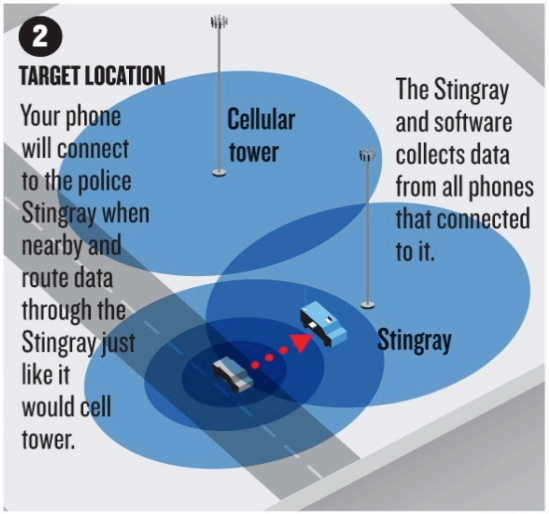

Source: Harris Corporation

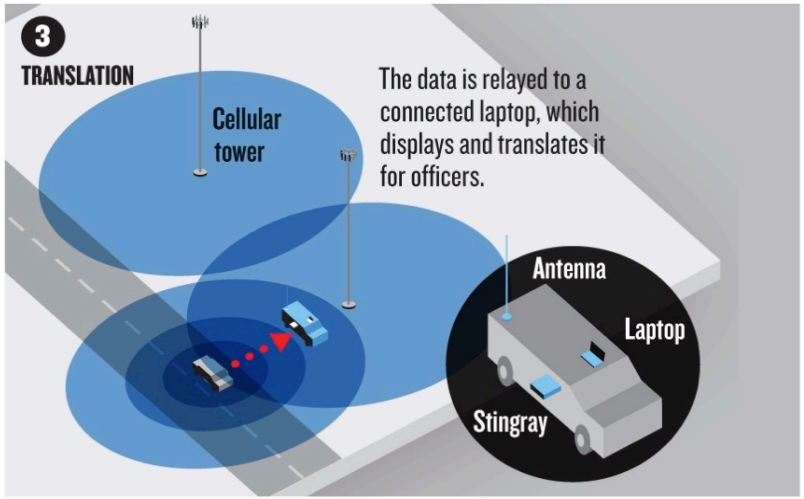
# HOW STINGRAY WORKS

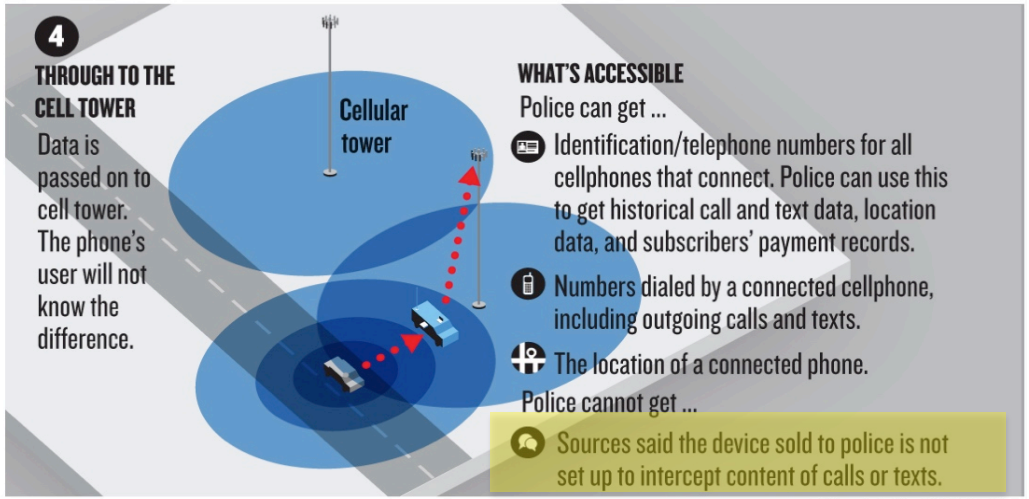
A Stingray is a mobile device that masquerades as a cellphone tower. It's usually mounted in a police surveillance vehicle.



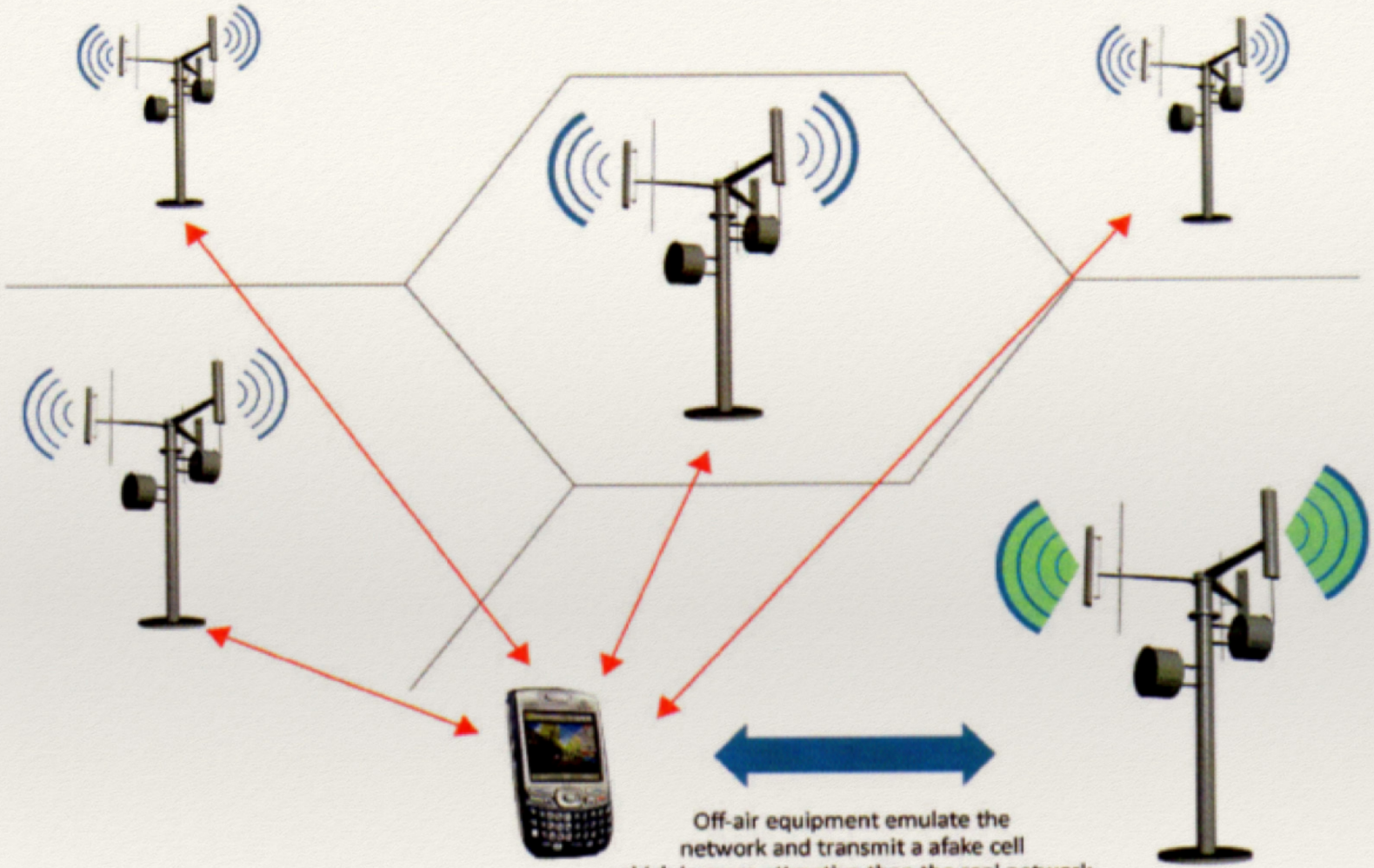




Source: USA Today


Source: wikimedia.org


Source: ibtimes.co.uk

# Subverting Cell Reselection




Source: Gamma Group

# Subverting Cell (Re)Selection

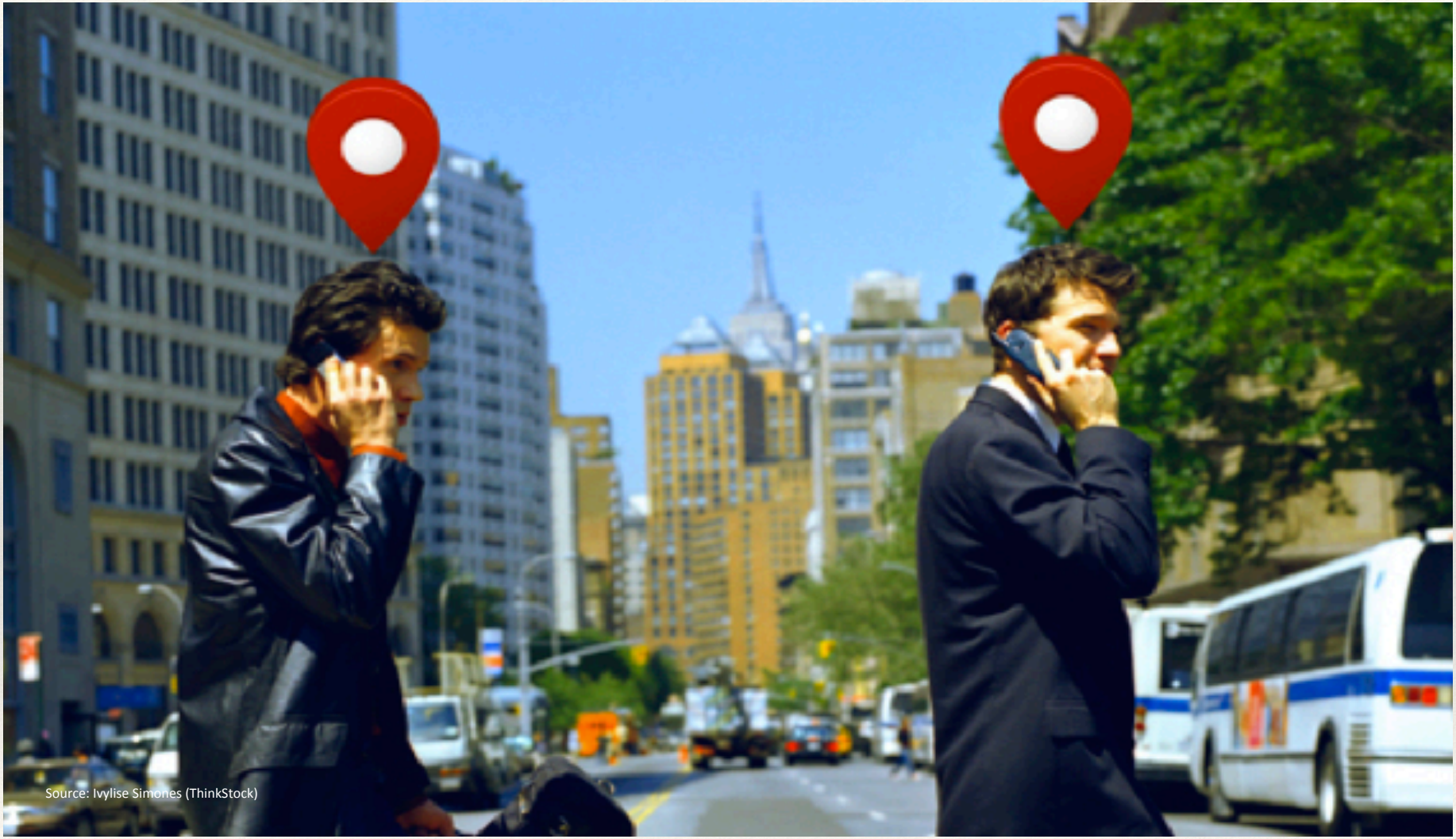
- Search all channels
- Compute C1 (path loss) for 6 channels with highest received signal strength
- Compute C2 (reselection score) for each:

$$C2 = \begin{cases} \text{C1+CRO-TO} \times \text{H(PT-T)} & \text{PT} \neq 11111 \\ \text{C1-CRO} & \text{PT=11111} \end{cases}$$

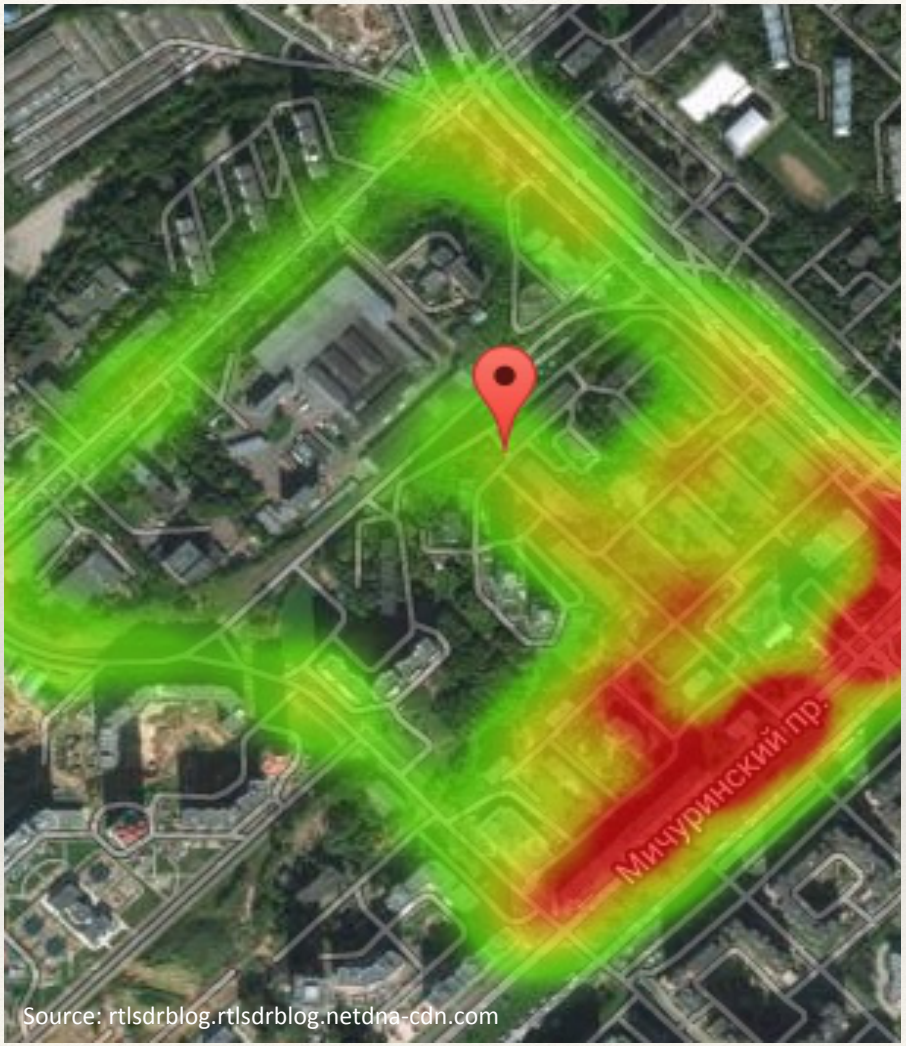
Where:

  - PT is penalty time, CRO is cell reselection offset, TO is the PT offset and H(PT-T) is 0 for a serving cell

# Location Tracking



# Location Tripwires




Source: rtlsdrblog.rtlsdrblog.netdna-cdn.com

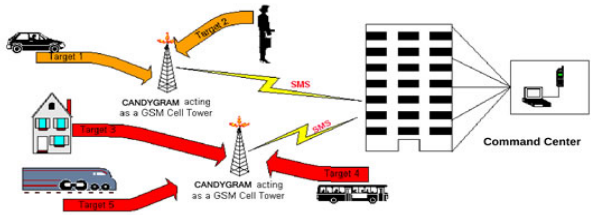
SECRET//COMINT//REL TO USA, FVEY

## CANDYGRAM

### GSM Telephone Tripwire

(S//SI//REL) Mimics GSM cell tower of a target network. Capable of operations at 900, 1800, or 1900 MHz. Whenever a target handset enters the CANDYGRAM base station's area of influence, the system sends out an SMS through the external network to registered watch phones.

06/20/08




**(S//SI//REL) CANDYGRAM Operational Concept**

(S//SI//REL) Typical use scenarios are asset validation, target tracking and identification as well as identifying hostile surveillance units with GSM handsets. Functionality is predicated on apriori target information.

**(S//SI//REL) System HW**

- GPS processing unit
- Tri-band BTS radio
- Windows XP laptop and cell phone*
- 9" wide x 12 " long x 2 " deep
- External power (9-30 VDC).

*Remote control software can be used with any connected to the laptop (used for communicating with the CANDYGRAM unit through text messages (SMS).

**(S//SI//REL) SW Features**

- Configurable 200 phone number target deck.
- Network auto-configuration
- Area Survey Capability
- Remote Operation Capability
- Configurable Network emulation
- Configurable RF power level
- Mutli-Units under single C&C
- Remote restart
- Remote erasure (not field recoverable)

**Status:** Available 8 mos ARO

**Unit Cost:** approx $40K

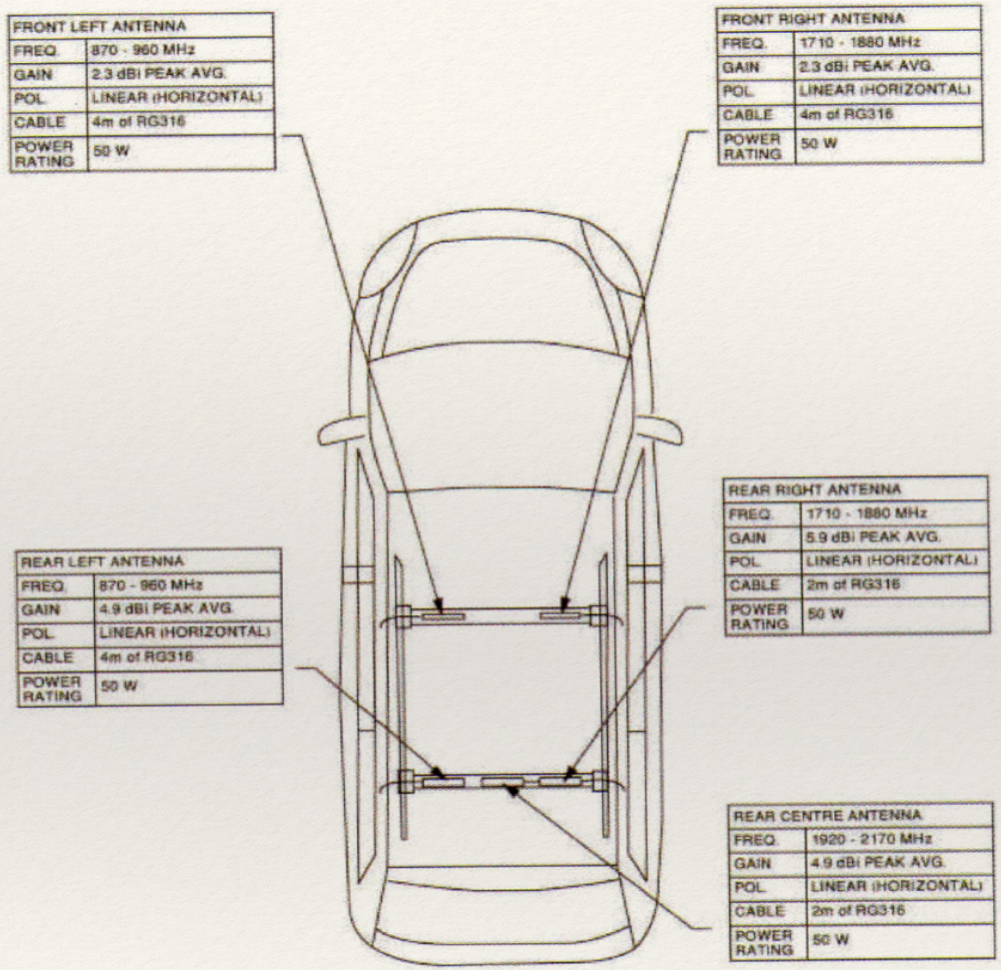
**POC:** [redacted], S32242, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

SECRET//COMINT//REL TO USA, FVEY

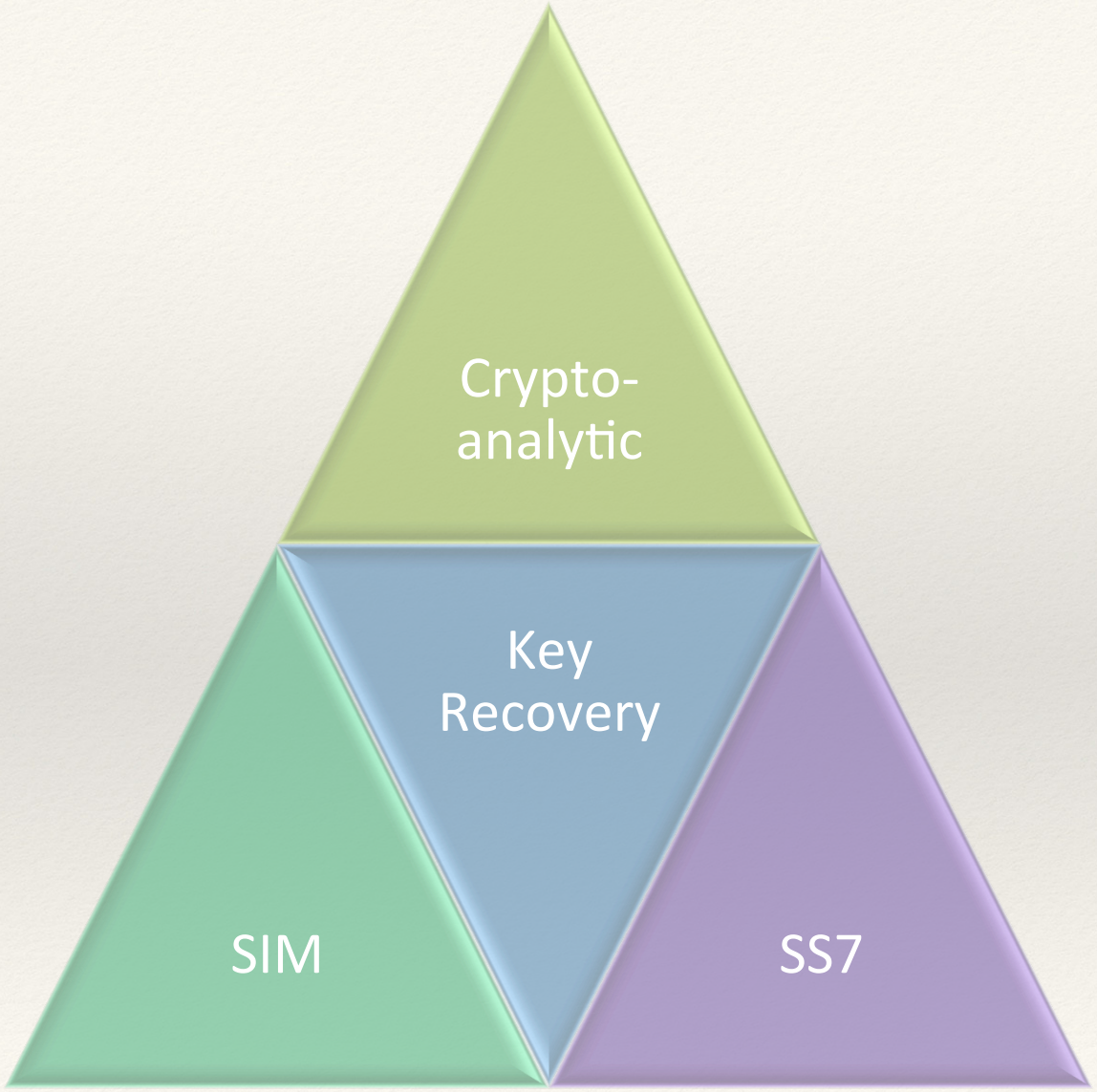
Source: NSA

# Active Tracking (Fox Hunting)




Source: Gamma International

# Eavesdropping



CNET › News › Privacy & data protection

December 1, 2006 2:20 PM PST

# FBI taps cell phone mic as eavesdropping tool

By Declan McCullagh and Anne Broache
Staff Writers, CNET News
Last modified: December 1, 2006 6:35 PM PST

**Related Stories**

Judge won't halt AT&T wiretapping lawsuit

November 17, 2006

Networking exec blasts wiretapping rules

November 16, 2006

Group appeals government eavesdropping ruling

July 21, 2006

FCC approves

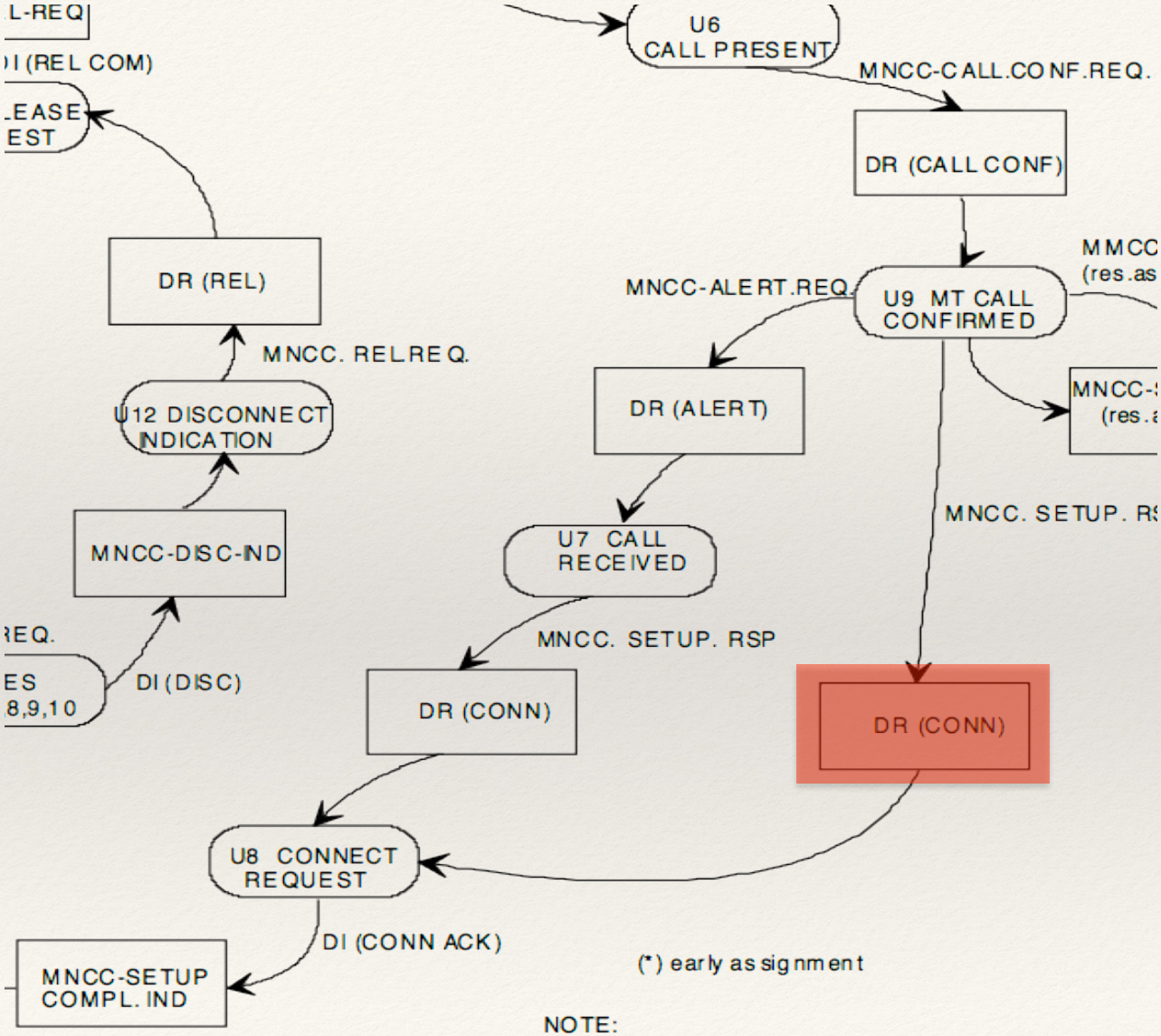
**The FBI appears to have begun using a novel form of electronic surveillance in criminal investigations: remotely activating a mobile phone's microphone and using it to eavesdrop on nearby conversations.**

The technique is called a "roving bug," and was approved by top U.S. Department of Justice officials for use against members of a New York organized crime family who were wary of conventional surveillance techniques such as tailing a suspect or wiretapping him.

Nextel cell phones owned by two alleged mobsters, John Ardito and his attorney Peter Peluso, were used by the FBI to listen in on nearby conversations. The FBI views Ardito as one of the most powerful men in the Genovese family, a major part of the national Mafia.

Source: CNET

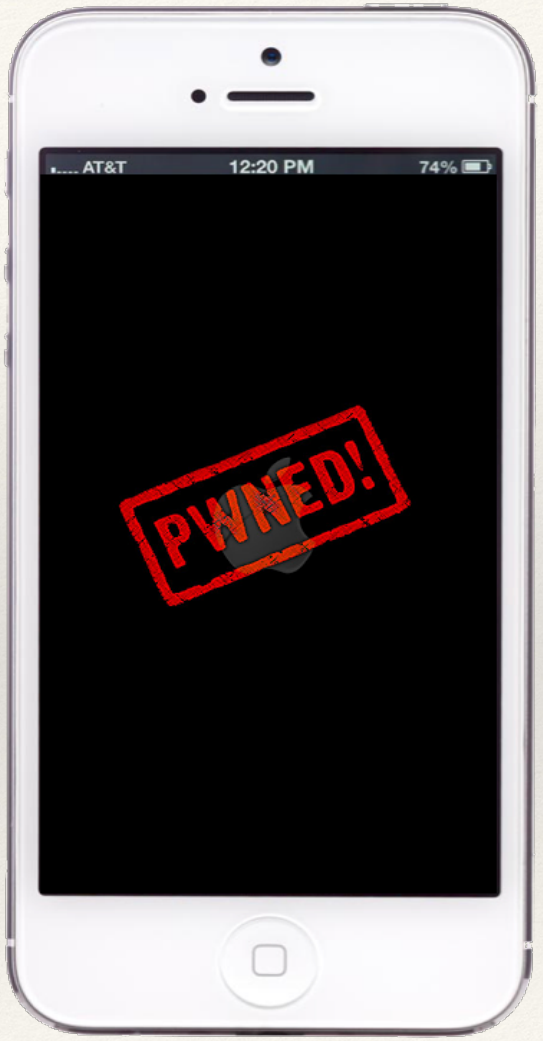
# Roving Bug Implementation?



# Device Compromise

"As soon as you turn it on it can be theirs, they can turn into a microphone they can take pictures from it, they can take the data…
They can absolutely turn them on with the power turned off to the device."

Source: Edward Snowden, interview with Brian Williams (NBC, 28 May 2014)



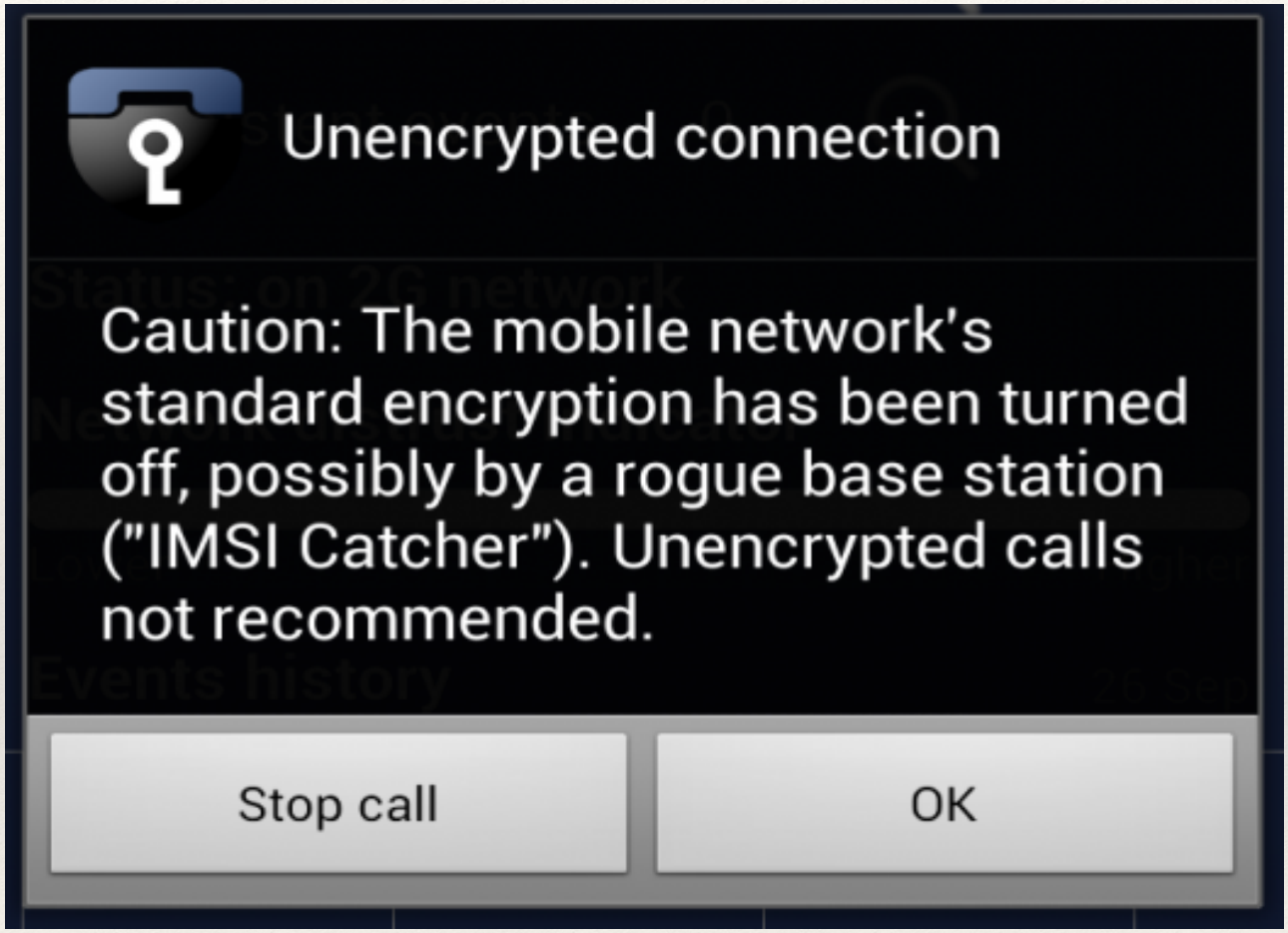
# Outline

- Stingray Threats
- Detection
- Self-Assembly Approach
- Questions/Comments


Source: Aftenposten

Base Station Security Experiments Using USRP, Torjus Bryne Retterstøl, Masters Thesis, NTNU Tronddheim, 2015

# Detection of Fake Base Station?

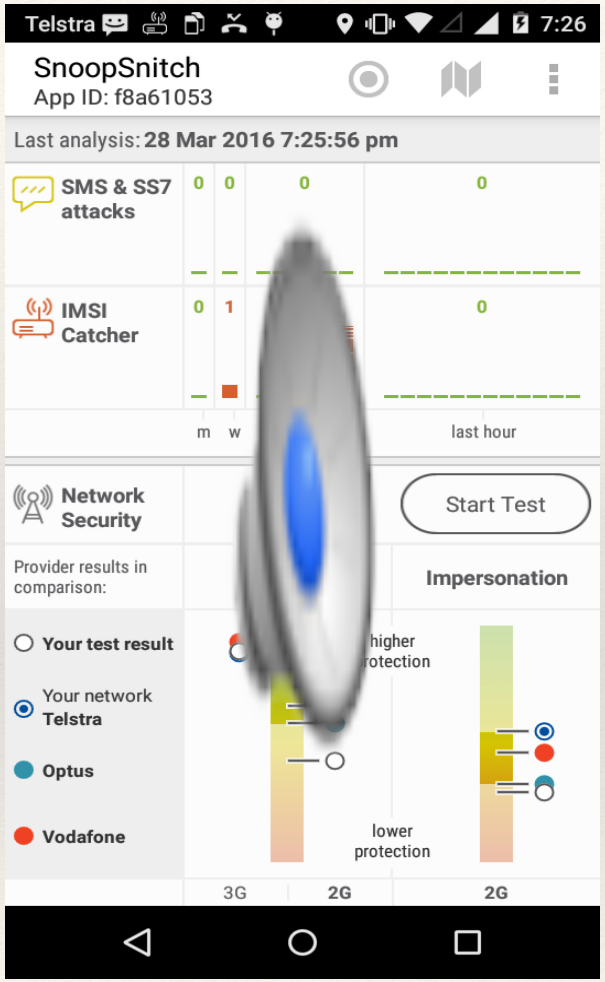



Source: Popular Science

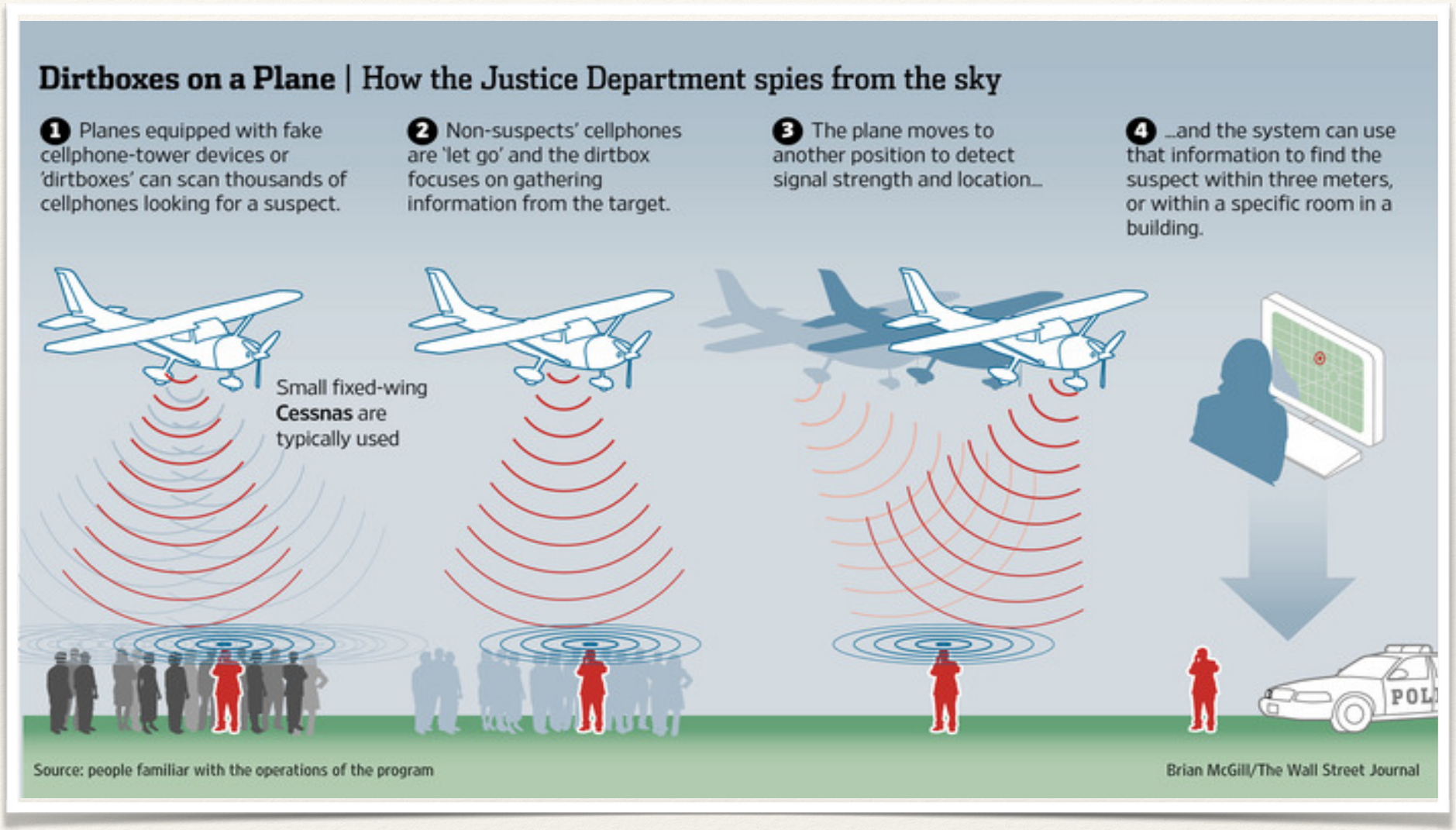
# Secure Phones


Source: Silent Circle

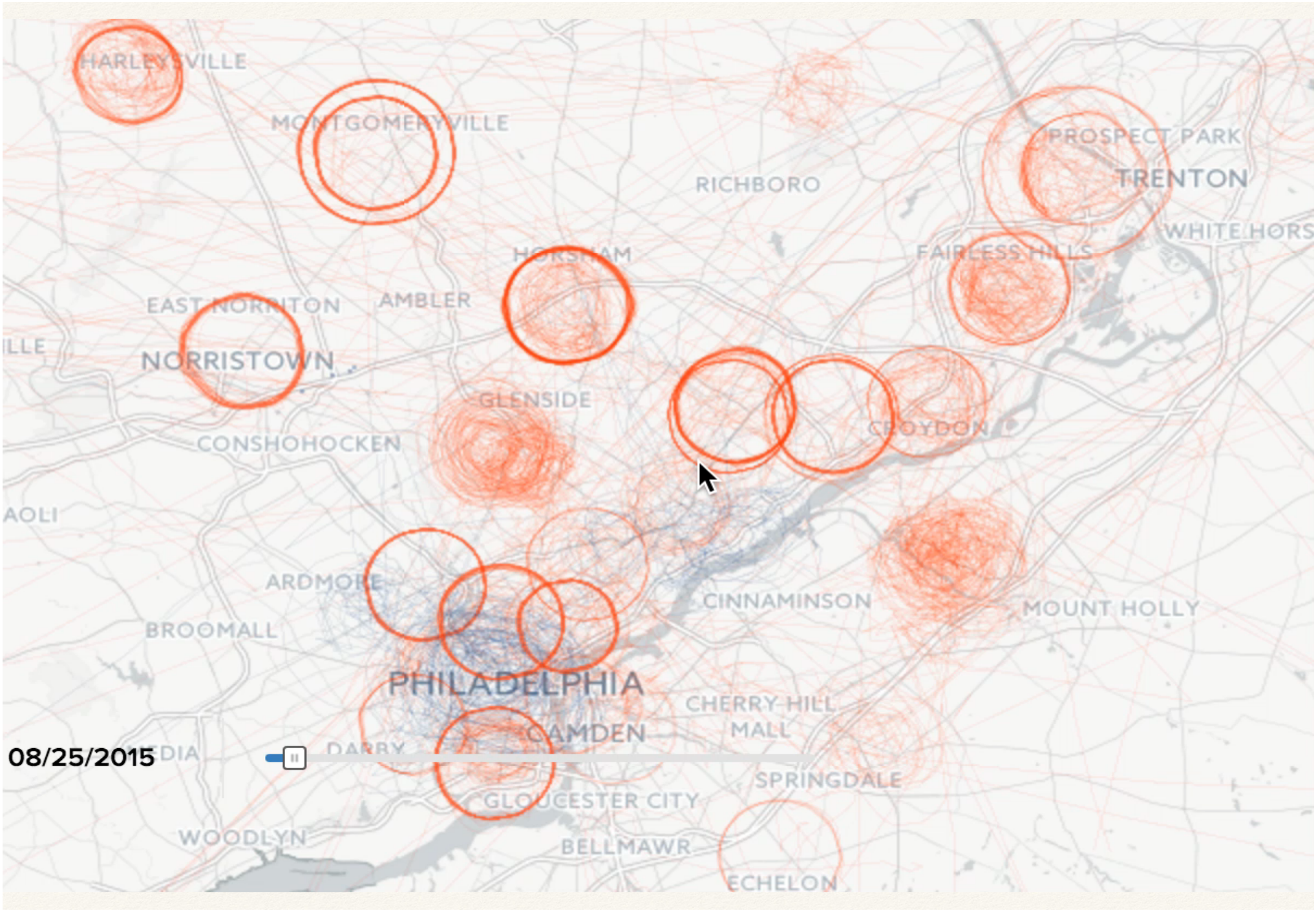
# SnoopSnitch etc.




- Various Android apps exist to detect presence of an IMSI Catcher:
  - AIMSICD
  - Darshak
  - SnoopSnitch
- Apple's telephony APIs do not provide sufficiently detailed info on cell towers/traffic



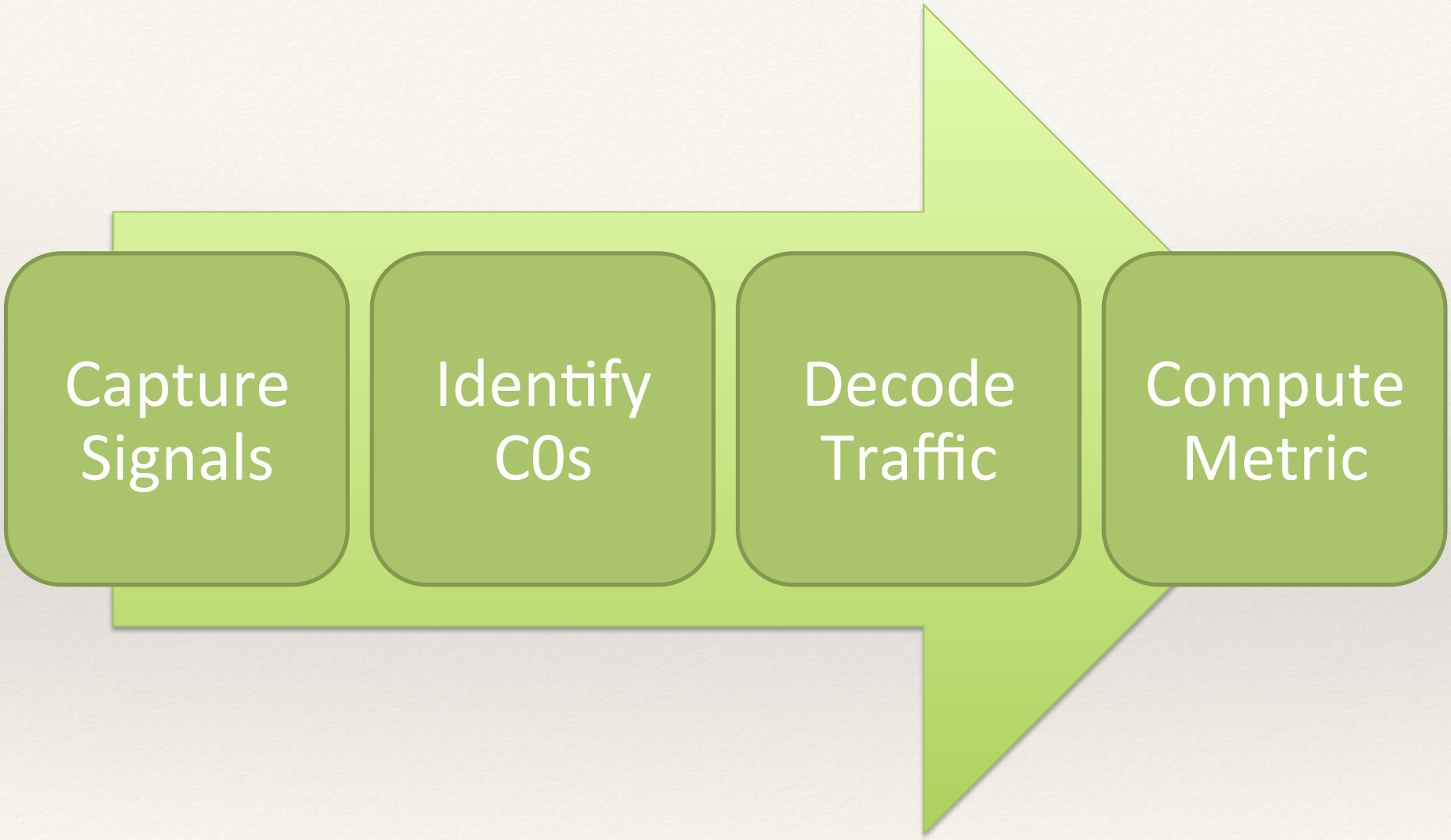

Source: The Wall Street Journal


HARLEYSVILLE
MONTGOMERYVILLE
RICHBORO
PROSPECT PARK
TRENTON
WHITE HORS
HORSHAM
FAIRLESS HILLS
EAST NORRITON
AMBLER
NORRISTOWN
GLENSIDE
CROYDON
CONSHOHOCKEN
ARDMORE
CINNAMINSON
MOUNT HOLLY
BROOMALL
PHILADELPHIA
CHERRY HILL MALL
CAMDEN
SPRINGDALE
GLOUCESTER CITY
WOODLYN
BELLMAWR
ECHELON
08/25/2015

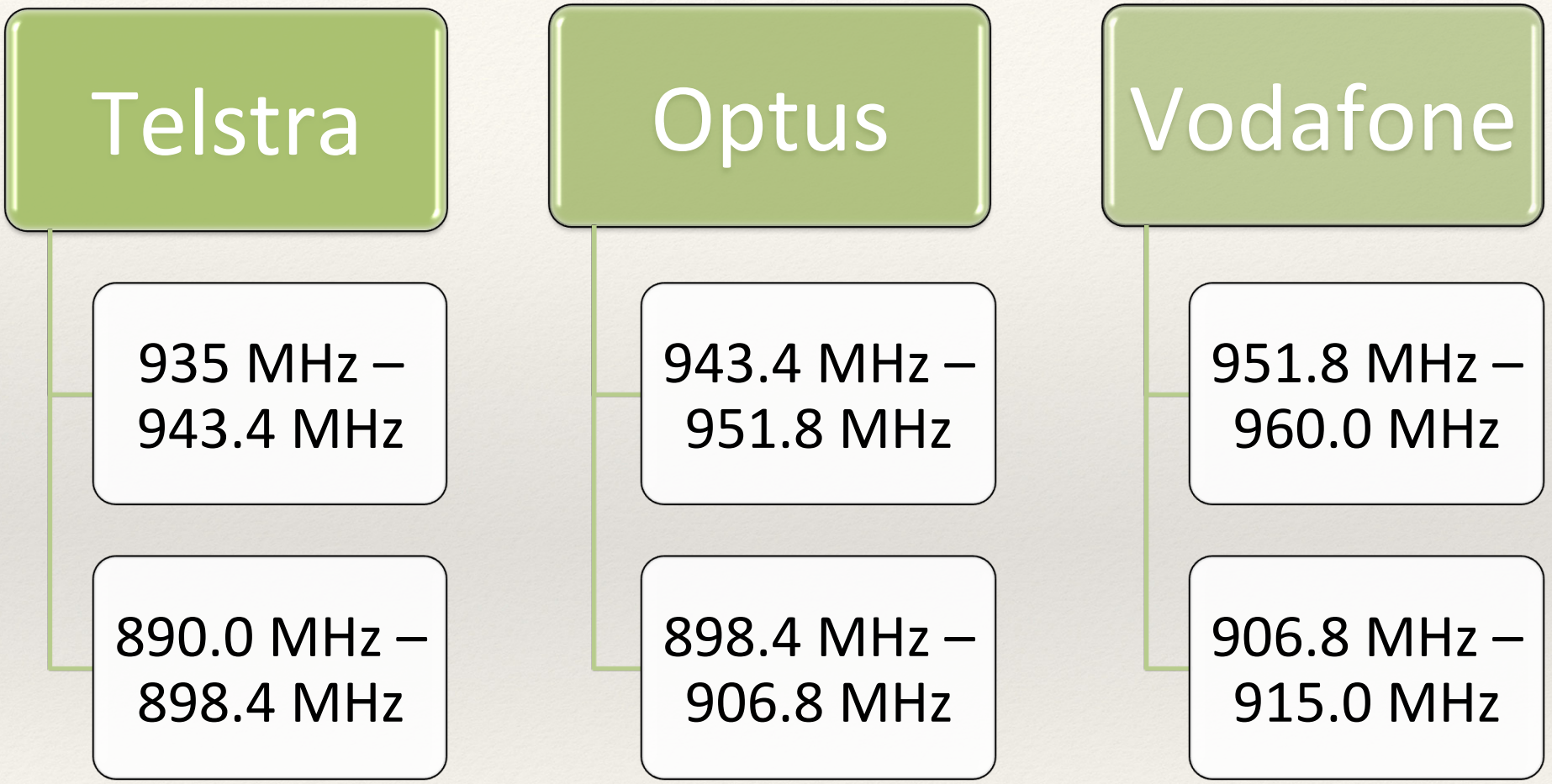
# Outline

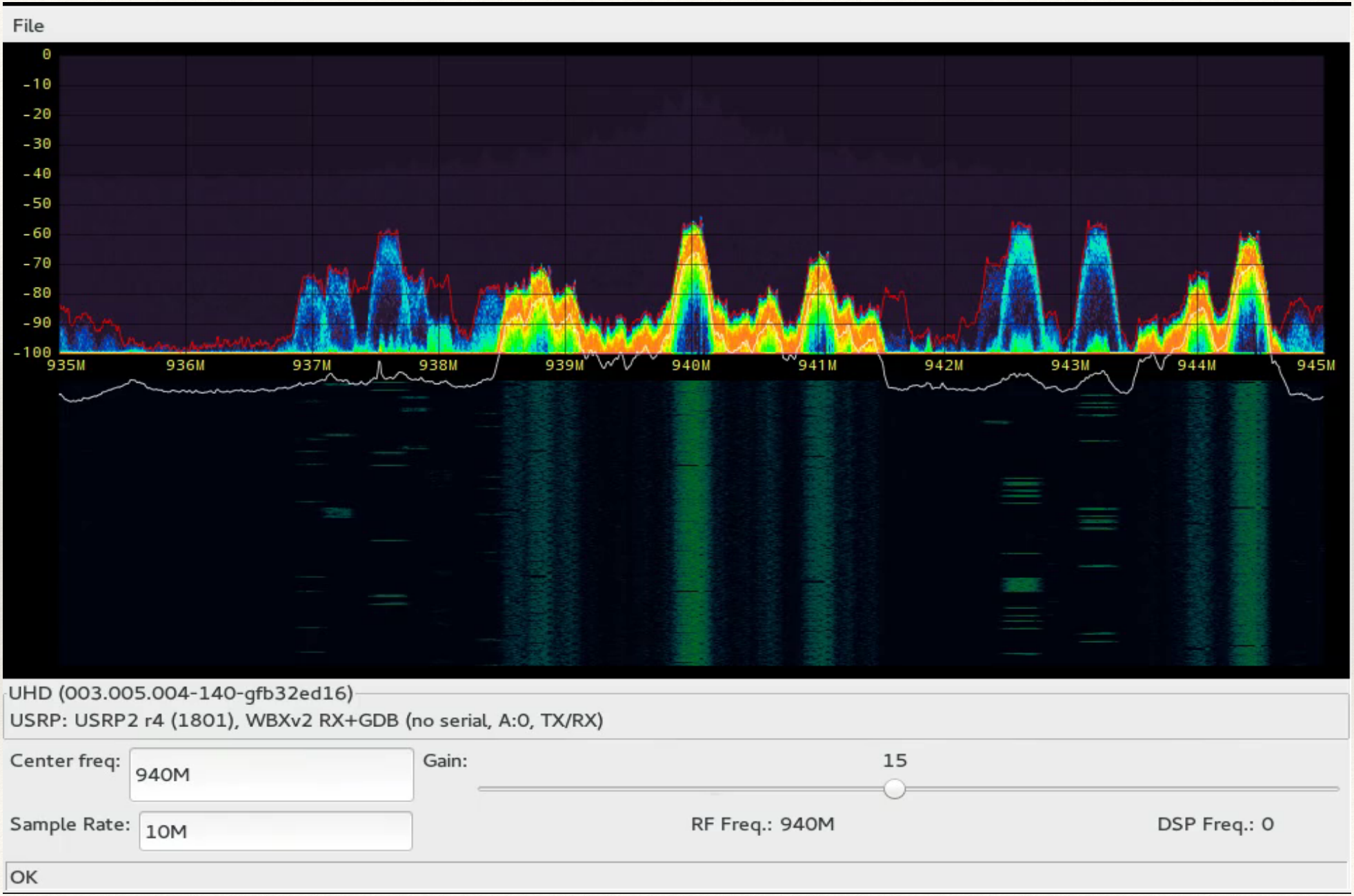
- Stingray Threats
- Detection Tools
- Self-Assembly Approach
- Questions/Comments

# Detection Process

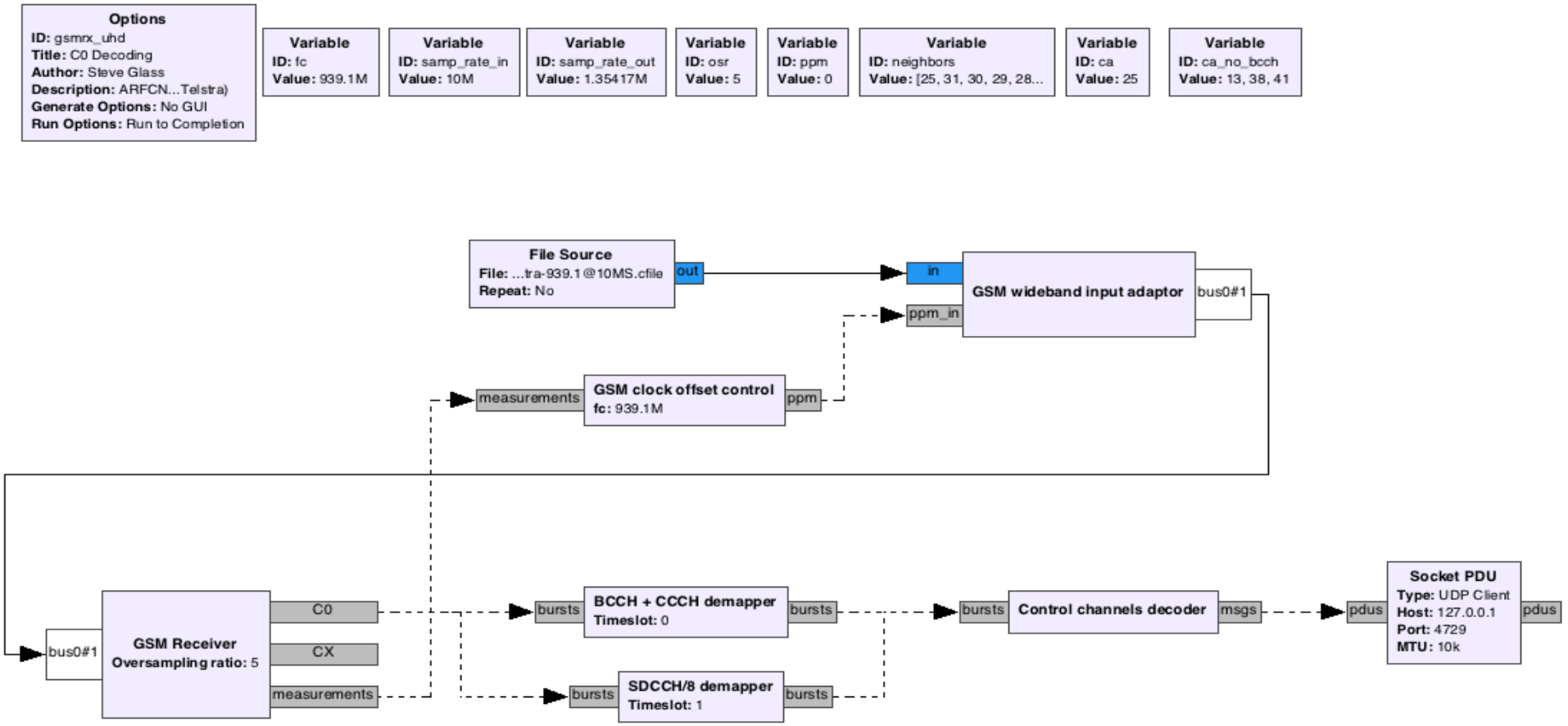


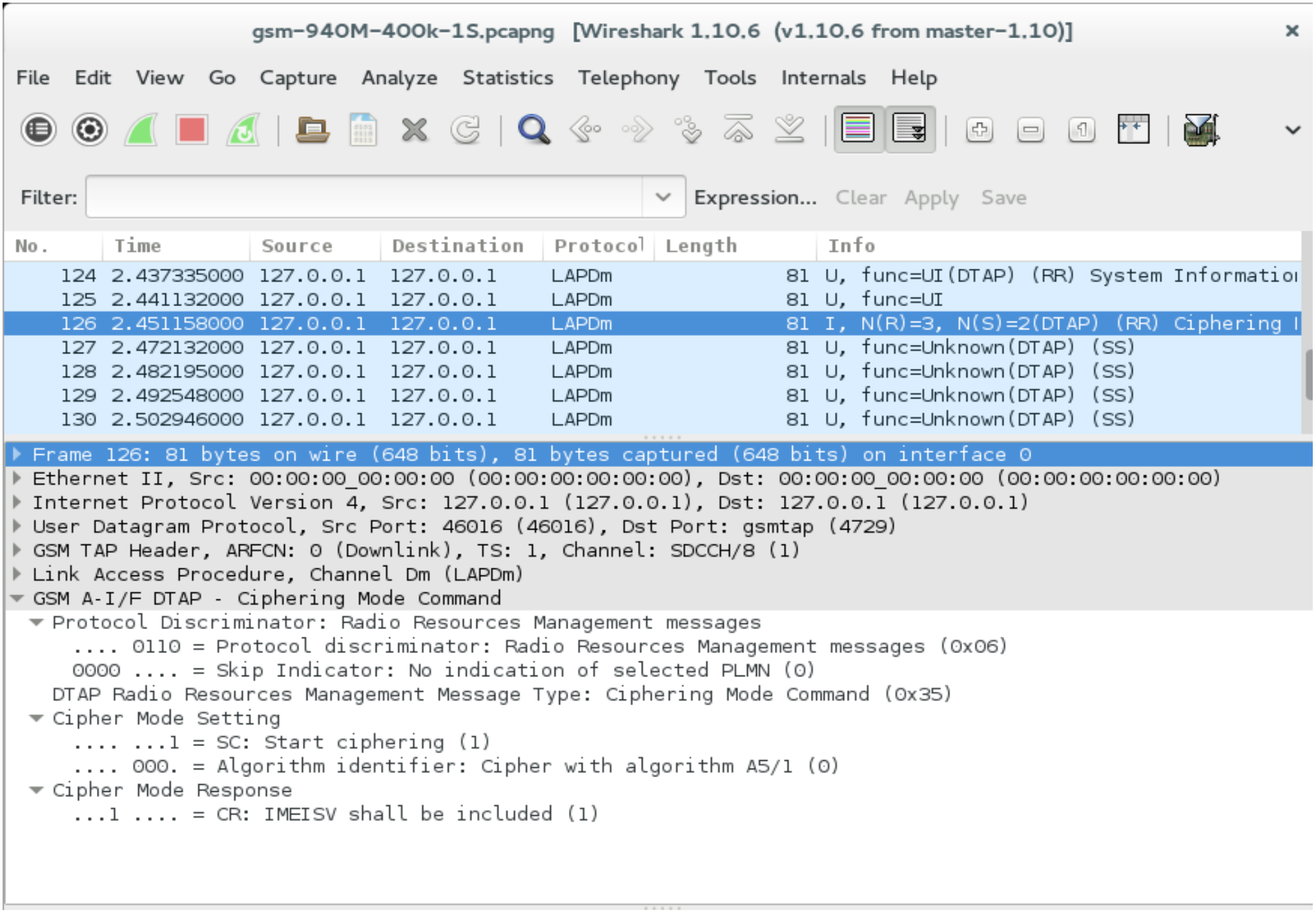
# Australian GSM900 Frequencies

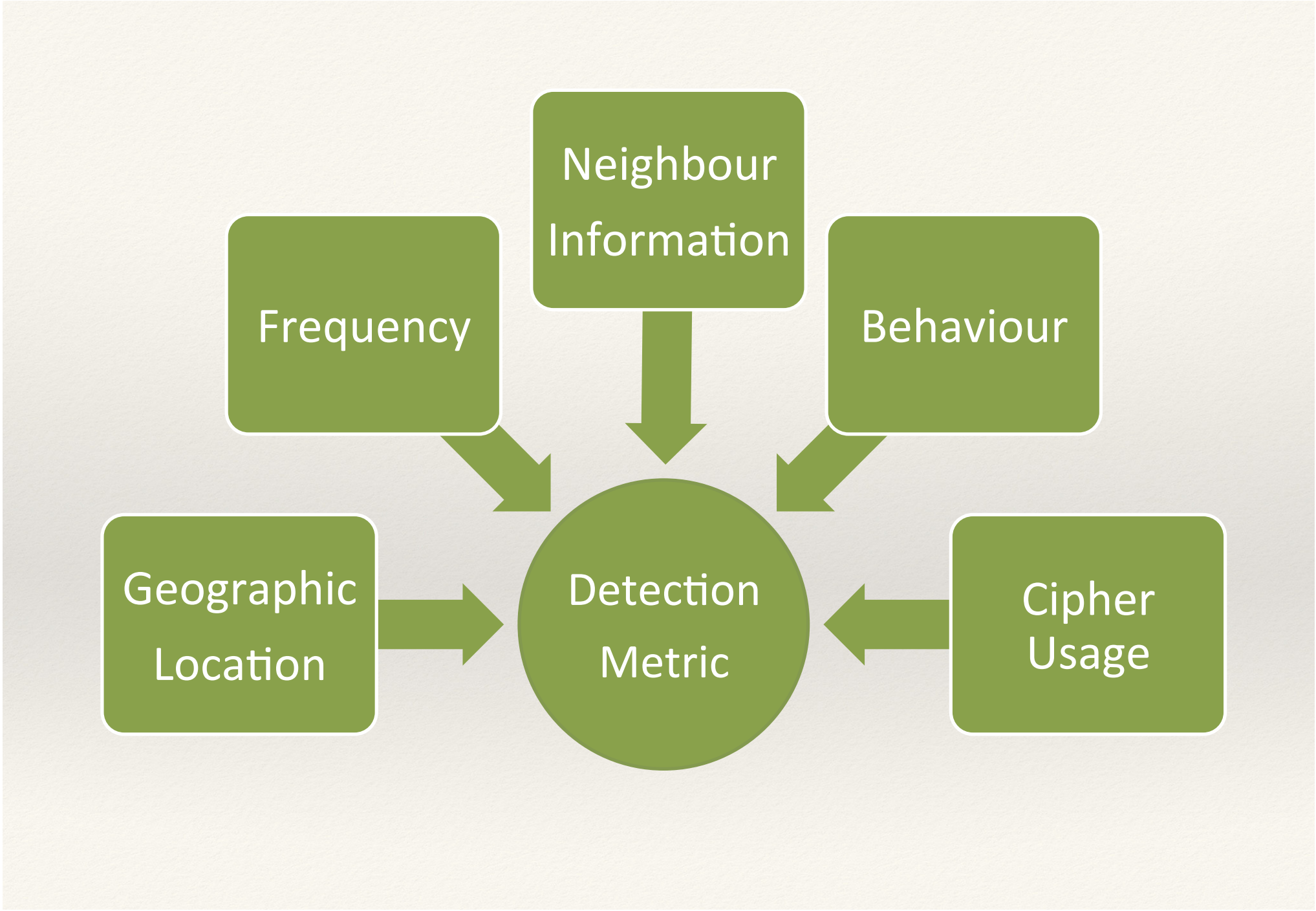



File
0
-10
-20
-30
-40
-50
-60
-70
-80
-90
-100
935M
936M
937M
938M
939M
940M
941M
942M
943M
944M
945M
UHD (003.005.004-140-gfb32ed16)
USRP: USRP2 r4 (1801), WBXv2 RX+GDB (no serial, A:0, TX/RX)
Center freq:
940M
Gain:
15
Sample Rate:
10M
RF Freq.: 940M
DSP Freq.: 0
OK

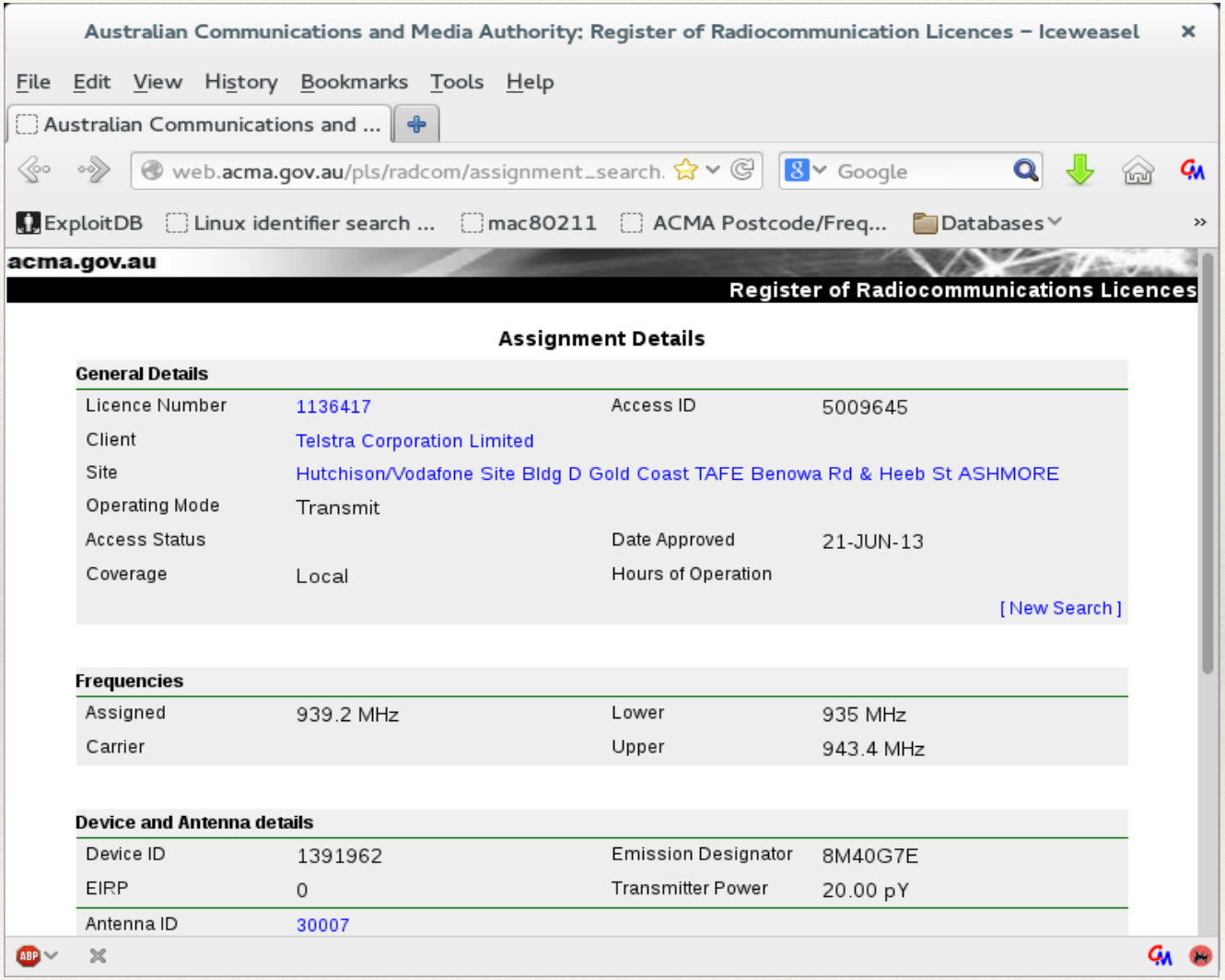
# Traffic Reception



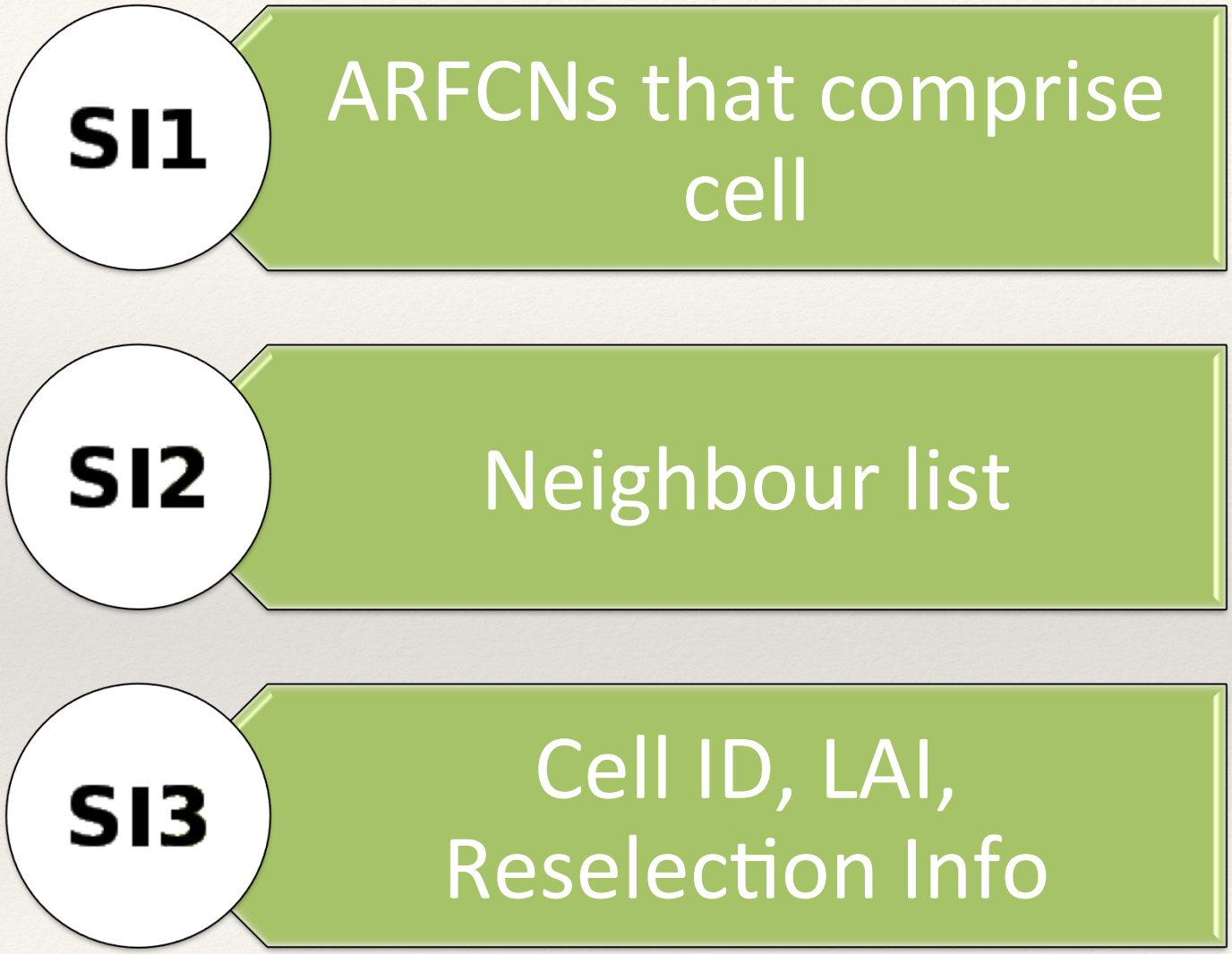

gsm-940M-400k-1S.pcapng [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
124 2.437335000 127.0.0.1 127.0.0.1 LAPDm 81 U, func=UI(DTAP) (RR) System Informatio
125 2.441132000 127.0.0.1 127.0.0.1 LAPDm 81 U, func=UI
126 2.451158000 127.0.0.1 127.0.0.1 LAPDm 81 I, N(R)=3, N(S)=2(DTAP) (RR) Ciphering I
127 2.472132000 127.0.0.1 127.0.0.1 LAPDm 81 U, func=Unknown(DTAP) (SS)
128 2.482195000 127.0.0.1 127.0.0.1 LAPDm 81 U, func=Unknown(DTAP) (SS)
129 2.492548000 127.0.0.1 127.0.0.1 LAPDm 81 U, func=Unknown(DTAP) (SS)
130 2.502946000 127.0.0.1 127.0.0.1 LAPDm 81 U, func=Unknown(DTAP) (SS)
Frame 126: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
User Datagram Protocol, Src Port: 46016 (46016), Dst Port: gsmtap (4729)
GSM TAP Header, ARFCN: 0 (Downlink), TS: 1, Channel: SDCCH/8 (1)
Link Access Procedure, Channel Dm (LAPDm)
GSM A-I/F DTAP - Ciphering Mode Command
Protocol Discriminator: Radio Resources Management messages
.... 0110 = Protocol discriminator: Radio Resources Management messages (0x06)
0000 .... = Skip Indicator: No indication of selected PLMN (0)
DTAP Radio Resources Management Message Type: Ciphering Mode Command (0x35)
Cipher Mode Setting
.... ...1 = SC: Start ciphering (1)
.... 000. = Algorithm identifier: Cipher with algorithm A5/1 (0)
Cipher Mode Response
...1 .... = CR: IMEISV shall be included (1)


Neighbour Information
Frequency
Behaviour
Geographic Location
Detection Metric
Cipher Usage

# Location & Frequency



# Scapy and GSM



# Scapy and GSM

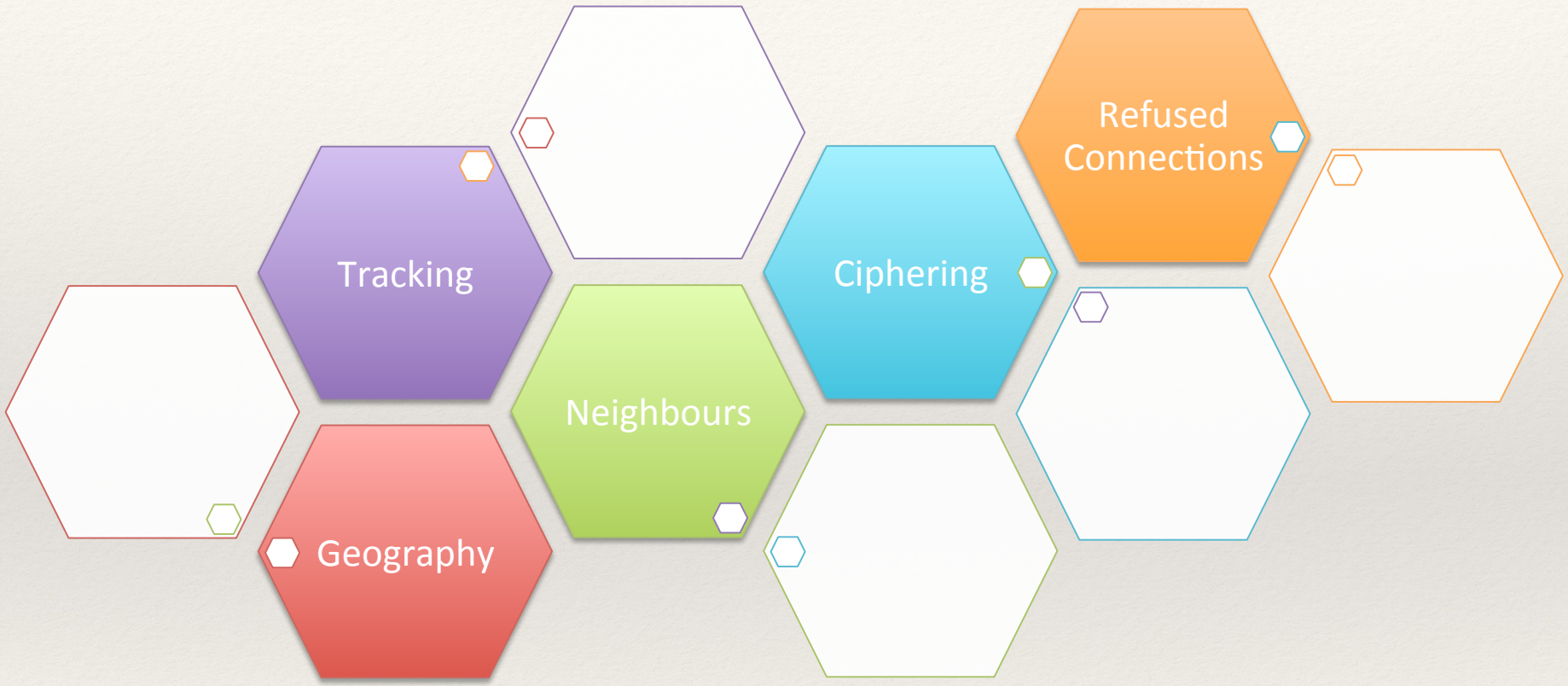
```
# GSMTap frame header
#
class GSMTap(Packet):
   """GSMTap Frame Header Version 2"""
   name = "GSMTap"
   fields_desc = [
      XByteField("version", 0x01),
      ByteField("hdr_len", 4),         # in 32bit words
      XByteField("type", 0x01),       # GSMTAP_TYPE_UM
      ByteField("timeslot", 0),        # timeslot (0..7)
      ShortField("ARFCN", 0),
      SignedByteField("signal_dBm", 0),
      SignedByteField("snr_dB", 0),
      LongField("frame_nr", 0),
      ByteEnumField("sub_type", 0,
              {
                 0x00: "UNKNOWN", 0x01: "BCCH", 0x02: "CCCH",
                 0x03: "RACH", 0x04: "AGCH", 0x05: "PCH",
                 0x06: "SDCCH", 0x07: "SDCCH4", 0x08: "SDCCH8",
                 0x09: "TCH_F", 0x0a: "TCH_H", 0x0b: "PACCH",
                 0x0c: "CBCH52", 0x0d: "PDCH", 0x0e: "PTCCH",
                 0x0f: "CBCH51",
              }),
      ByteField("antenna_nr", 0),
      ByteField("sub_slot", 0),
      ByteField("reserved", 0),
      ]

bind_layers(UDP, GSMTap, dport=4729)
```

```
# GSM L3 frame headers
#
class GSM_L3_Hdr(Packet):
   """GSM Standard L3 Header (Table 10.1)"""
   name = "GSM_L3_Hdr"
   fields_desc = [
      BitFieldLenField("l2_pseudolen", 23, 6),
      BitField("ignored", 0x0, 2),
      BitField("skip_txn_id", 0x0, 4),
      BitEnumField("proto", 0x0, 4,
        {
           0x3: "CALL_CONTROL",
           0x5: "MOBILITY_MGMT",
           0x6: "RADIO_RSRC_MGMT",
        }),
      ]

bind_layers(GSMTap, GSM_L3_Hdr)
```

# Suspicious Behaviours




Source: https://www.qrz.com/db/W0JT

# References


- The Athens Affair, Prevelakis & Spinellis, IEEE Spectrum, 2007
- Eavesdropping on and decrypting of GSM communication using readily available low-cost hardware and free open-source software in practice, Bosma *et. al.*, 2012
- Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", Barkan, Biham, Keller (2003). Crypto 2003: 600–616.
- Anatomy of Contemporary GSM Cellphone Hardware, Welte, Unpublished, 2010
- Baseband Attacks: Remote Exploitation of Memory Corruptions in Cellular Protocol Stacks, Weinmann, WooT, 2012
- Baseband exploitation in 2013: Hexagon Challenges, Weinmann, Chaos Communications Congress, 2013
- Base Station Security Experiments Using USRP, Retterstøl, Masters Thesis, Norwegian University of Science and Technology Department of Telematics, 2015