



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.

WHO HAS IT?
The FBI and most other investigative bodies in the federal government, as do at least 25 different local and state police departments. Even more have access through sharing agreements with federal, state and regional task forces.

Antennas on the police vehicle determine the distance and direction of the phone in relation to the Stingray and other cell towers, telling police where the phone is in real-time. The intercepting device, known as Stingray, with related antenna and gear is sold under the names Amberjack, KingFish, Harpoon and RayFish.

Cellular tower

Stingray

Antenna

Laptop

Stingray

1
CELLPHONES

Cellphones are constantly "seeking" the nearest tower, even when you're not making a call.

Cellular tower

Stingray

2
TARGET LOCATION

Your phone will connect to the police Stingray when nearby and route data through the Stingray just like it would cell tower.

The Stingray and software collects data from all phones that connected to it.

Cellular tower

Stingray

3
TRANSLATION

The data is relayed to a connected laptop, which displays and translates it for officers.

Cellular tower

Stingray

Antenna

Laptop

Stingray

4
THROUGH TO THE CELL TOWER

Data is passed on to cell tower. The phone's user will not know the difference.

WHAT'S ACCESSIBLE
Police can get ...

- 📞 Identification/telephone numbers for all cellphones that connect. Police can use this to get historical call and text data, location data, and subscribers' payment records.
- 📱 Numbers dialed by a connected cellphone, including outgoing calls and texts.
- 📍 The location of a connected phone.

Police cannot get ...

- 🔒 Sources said the device sold to police is not set up to intercept content of calls or texts.

Cellular tower

Stingray

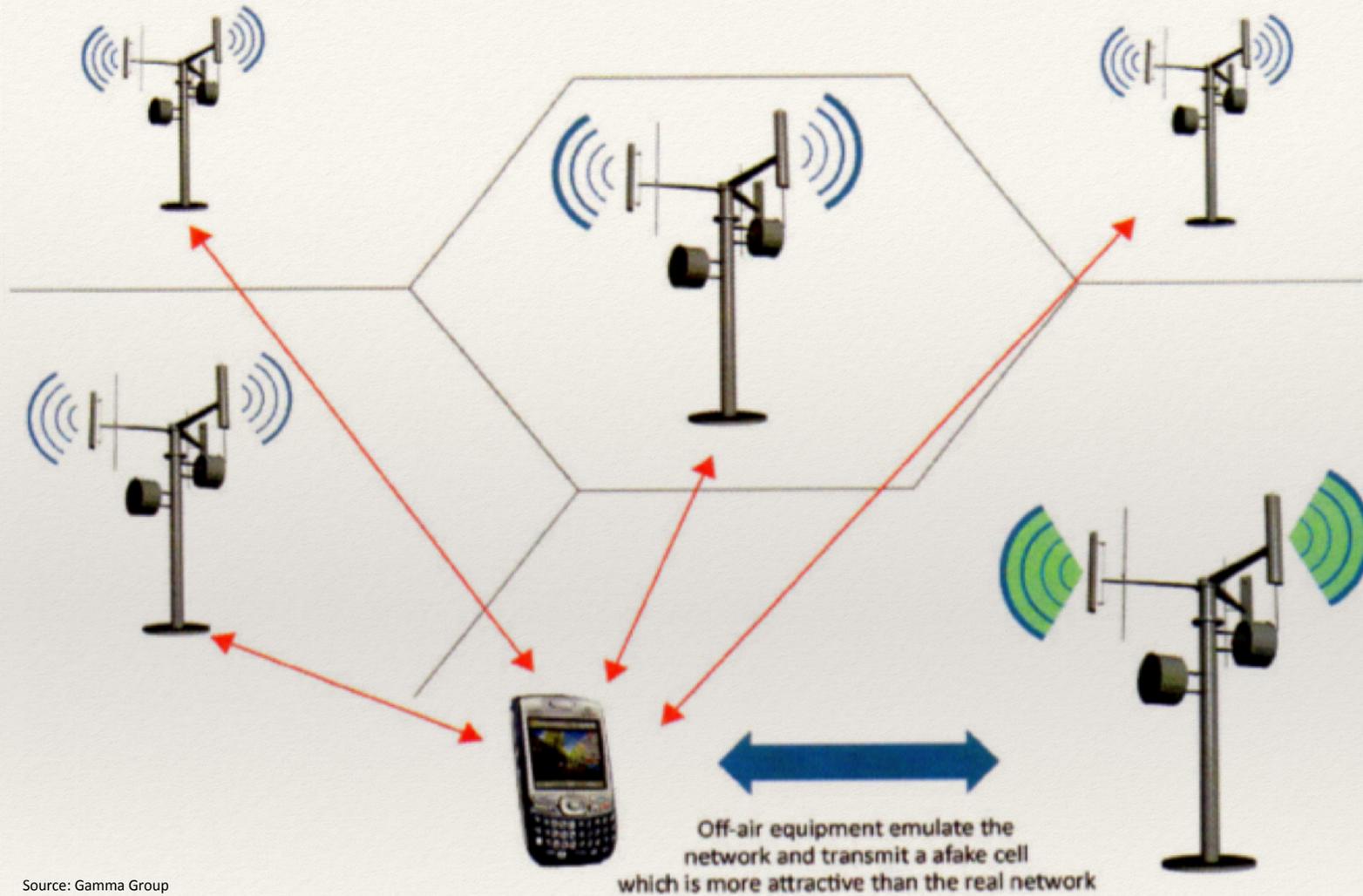


Source: [wikimedia.org](https://www.wikimedia.org/)



Source: [ibtimes.co.uk](https://www.ibtimes.co.uk/)

Subverting Cell Reselection



Source: Gamma Group

Subverting Cell (Re)Selection

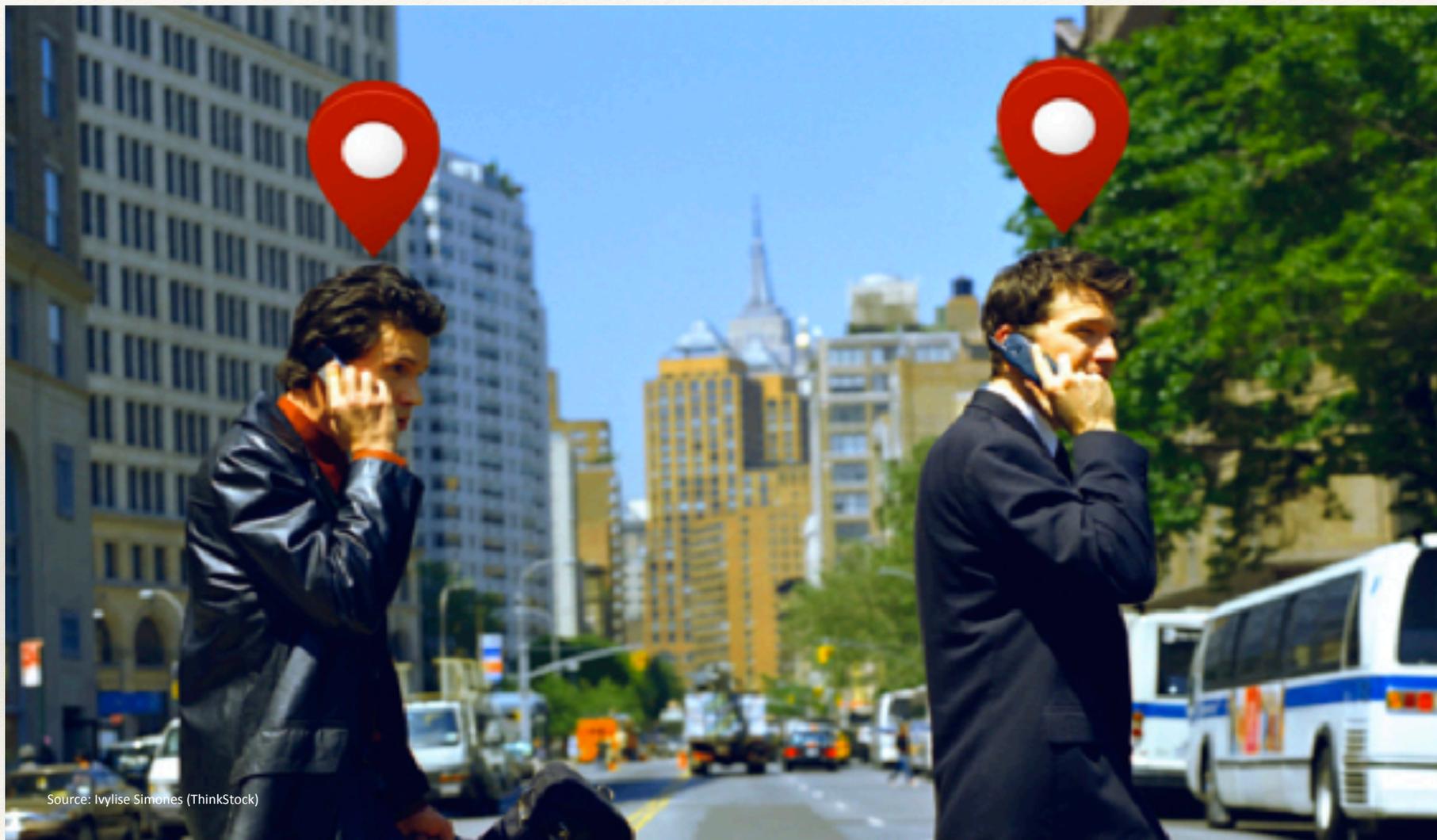
- Search all channels
- Compute C1 (path loss) for 6 channels with highest received signal strength
- Compute C2 (reselection score) for each:

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

Where:

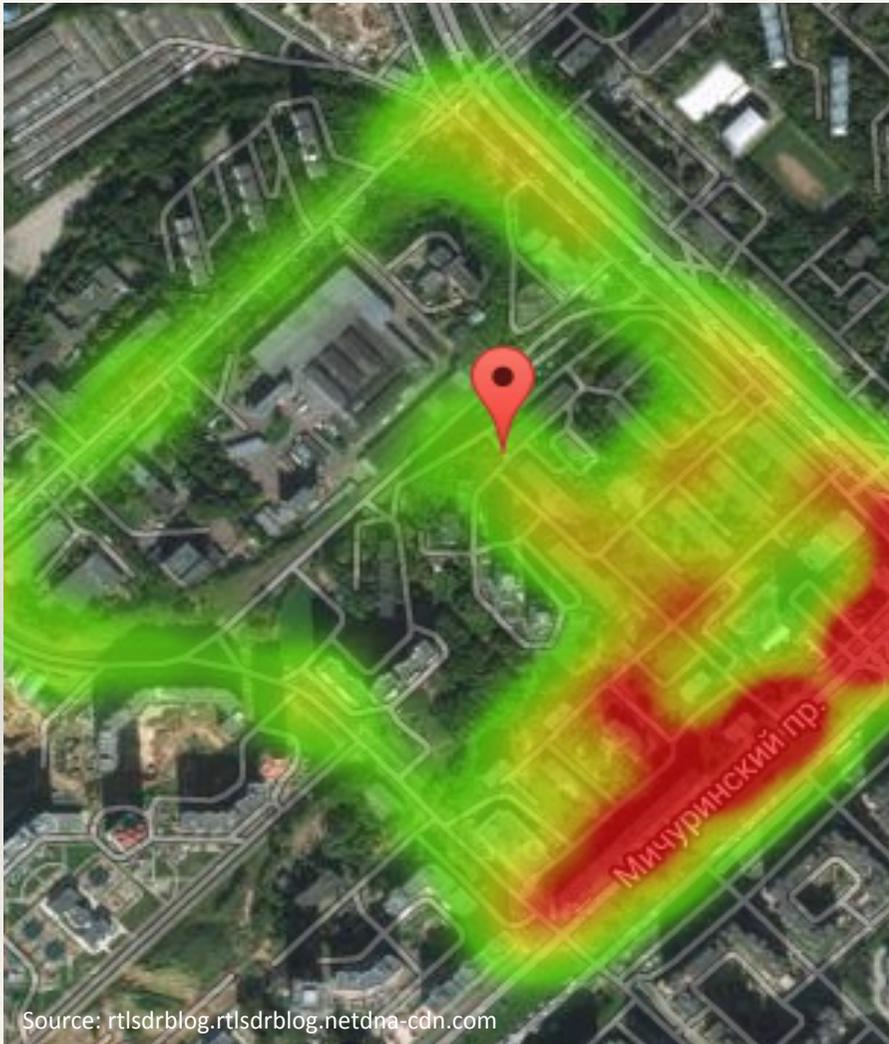
- PT is penalty time, CRO is cell reselection offset, TO is the PT offset and $H(PT - T)$ is 0 for a serving cell

Location Tracking



Source: Ivylise Simones (ThinkStock)

Location Tripwires



Source: rtsdrblog.rtsdrblog.netdna-cdn.com

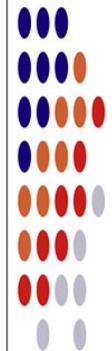
SECRET//COMINT//REL TO USA, FVEY



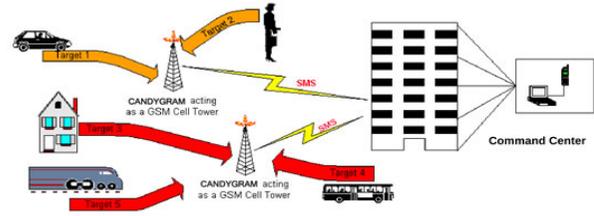
CANDYGRAM

GSM Telephone Tripwire

06/20/08



(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.



(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	(S//SI//REL) SW Features
<ul style="list-style-type: none"> • 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). <p>*Remote control software can be used with any connected to the laptop (used for communicating with the CANDYGRAM unit through text messages (SMS).</p>	<ul style="list-style-type: none"> • Configurable 200 phone number target deck. • Network auto-configuration • Area Survey Capability • Remote Operation Capability • Configurable Network emulation • Configurable RF power level • Multi-Units under single C&C • Remote restart • Remote erasure (not field recoverable) <p>Status: Available 8 mos ARO</p> <p>Unit Cost: approx \$40K</p>

POC: ██████████, S32242, ██████████, ██████████@nsa.ic.gov

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

Source: NSA SECRET//COMINT//REL TO USA, FVEY

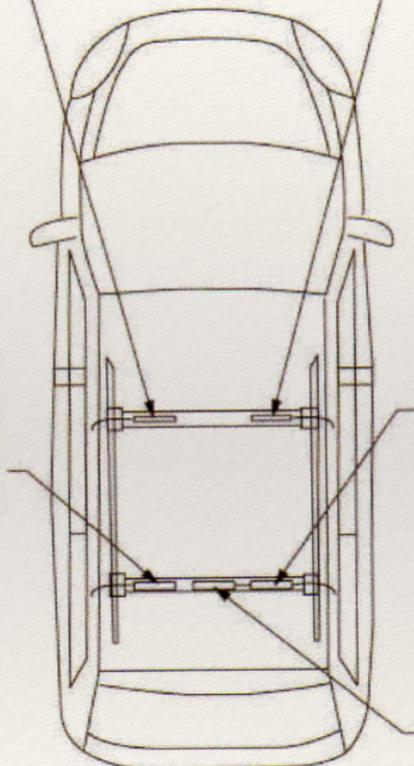
Active Tracking (Fox Hunting)

FRONT LEFT ANTENNA	
FREQ.	870 - 960 MHz
GAIN	2.3 dBi PEAK AVG.
POL.	LINEAR (HORIZONTAL)
CABLE	4m of RG316
POWER RATING	50 W

FRONT RIGHT ANTENNA	
FREQ.	1710 - 1880 MHz
GAIN	2.3 dBi PEAK AVG.
POL.	LINEAR (HORIZONTAL)
CABLE	4m of RG316
POWER RATING	50 W



REAR LEFT ANTENNA	
FREQ.	870 - 960 MHz
GAIN	4.9 dBi PEAK AVG.
POL.	LINEAR (HORIZONTAL)
CABLE	4m of RG316
POWER RATING	50 W



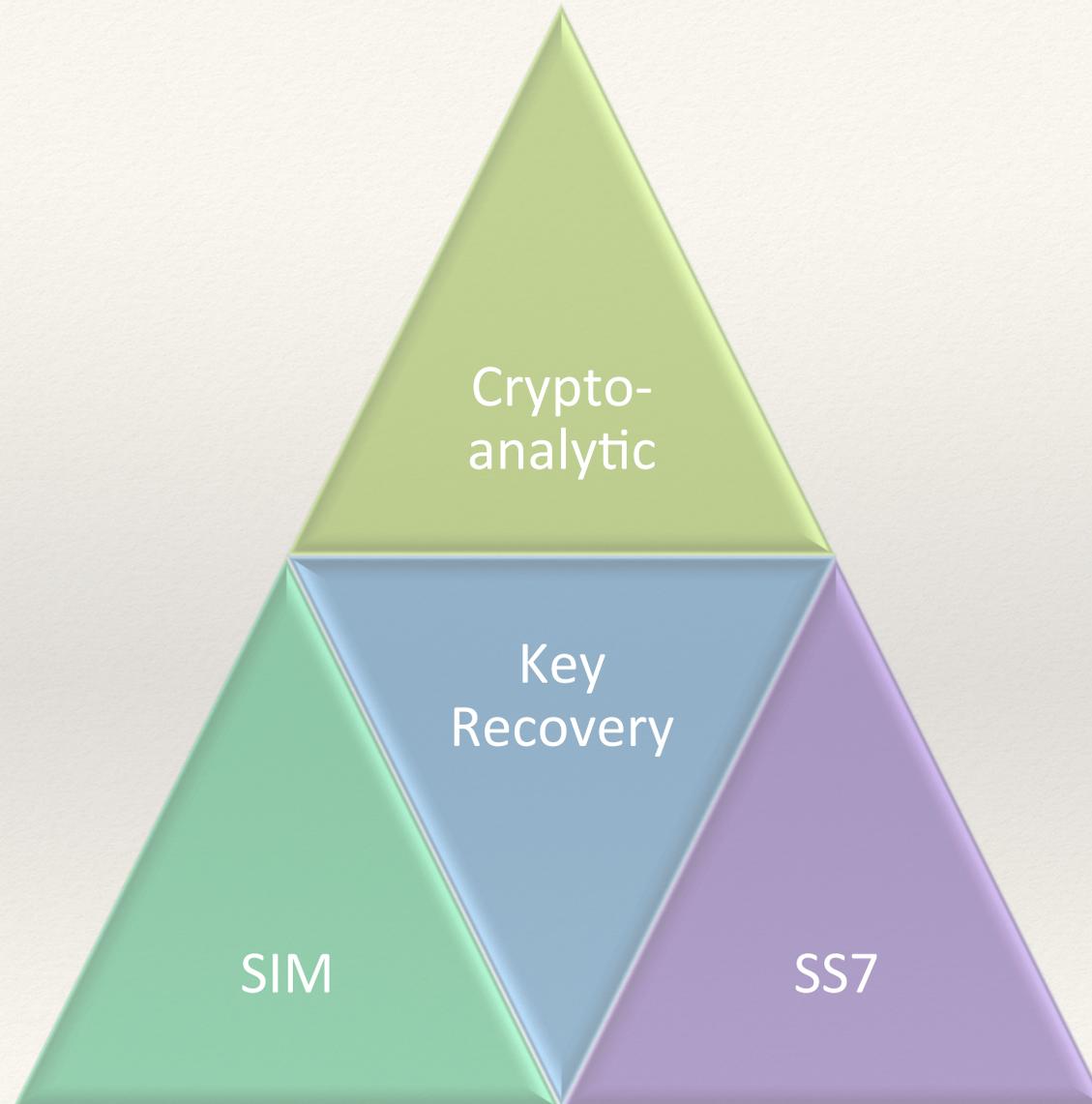
REAR RIGHT ANTENNA	
FREQ.	1710 - 1880 MHz
GAIN	5.9 dBi PEAK AVG.
POL.	LINEAR (HORIZONTAL)
CABLE	2m of RG316
POWER RATING	50 W

REAR CENTRE ANTENNA	
FREQ.	1920 - 2170 MHz
GAIN	4.9 dBi PEAK AVG.
POL.	LINEAR (HORIZONTAL)
CABLE	2m of RG316
POWER RATING	50 W



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

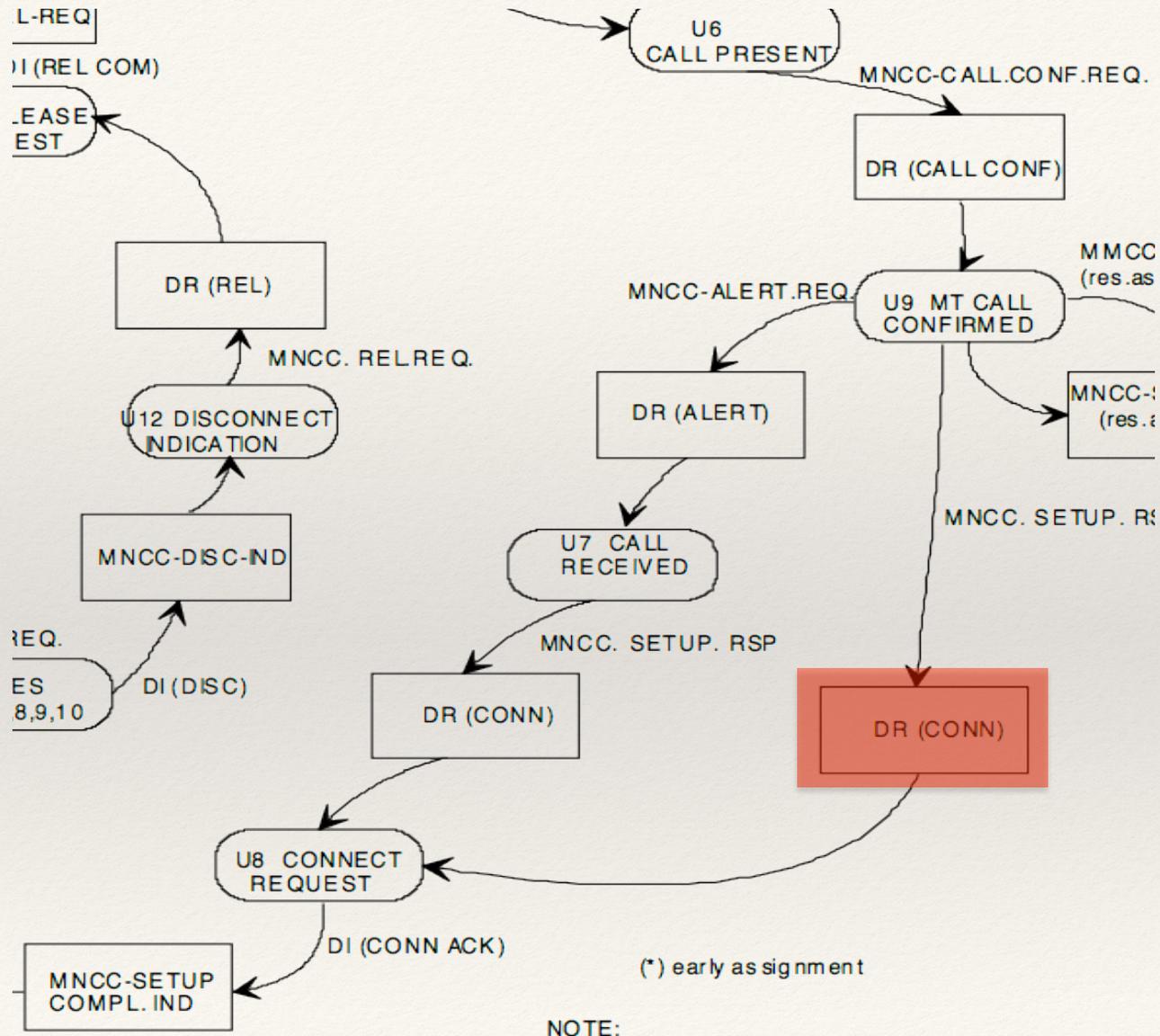
The FBI appears to have begun using a novel form of electronic surveillance in criminal investigations: remotely activating a mobile phone's microphone and using it to eavesdrop on nearby conversations.

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?

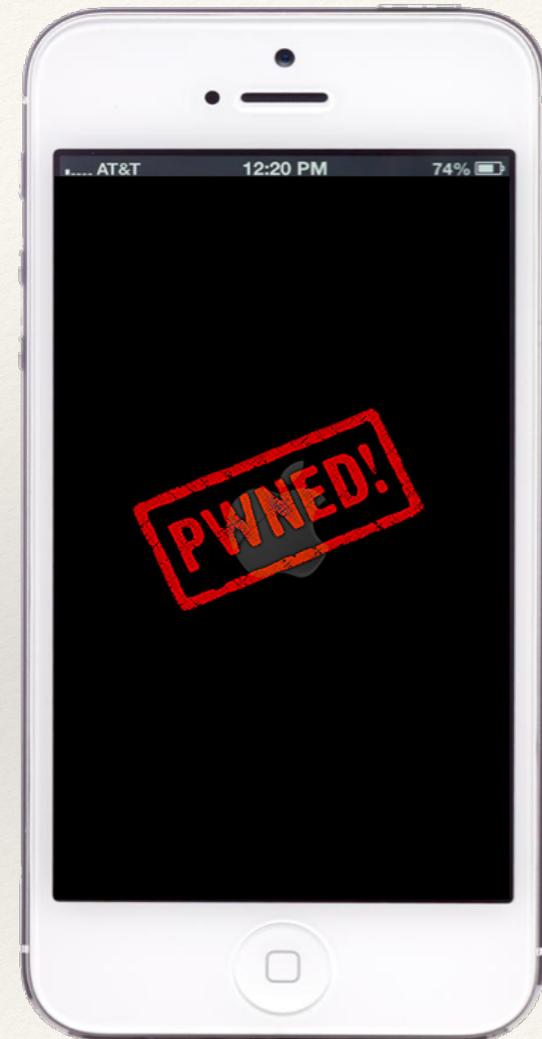


Device Compromise

“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

Secret surveillance of Norway's leaders detected

Members of parliament and the prime minister of Norway are being monitored by means of secret espionage equipment.

Andreas Bække Foss, Per Arne Johnsen, Fredrik Sævi Thorsen

Opplysningsvesenetsvesen 28.09.2013 11:11

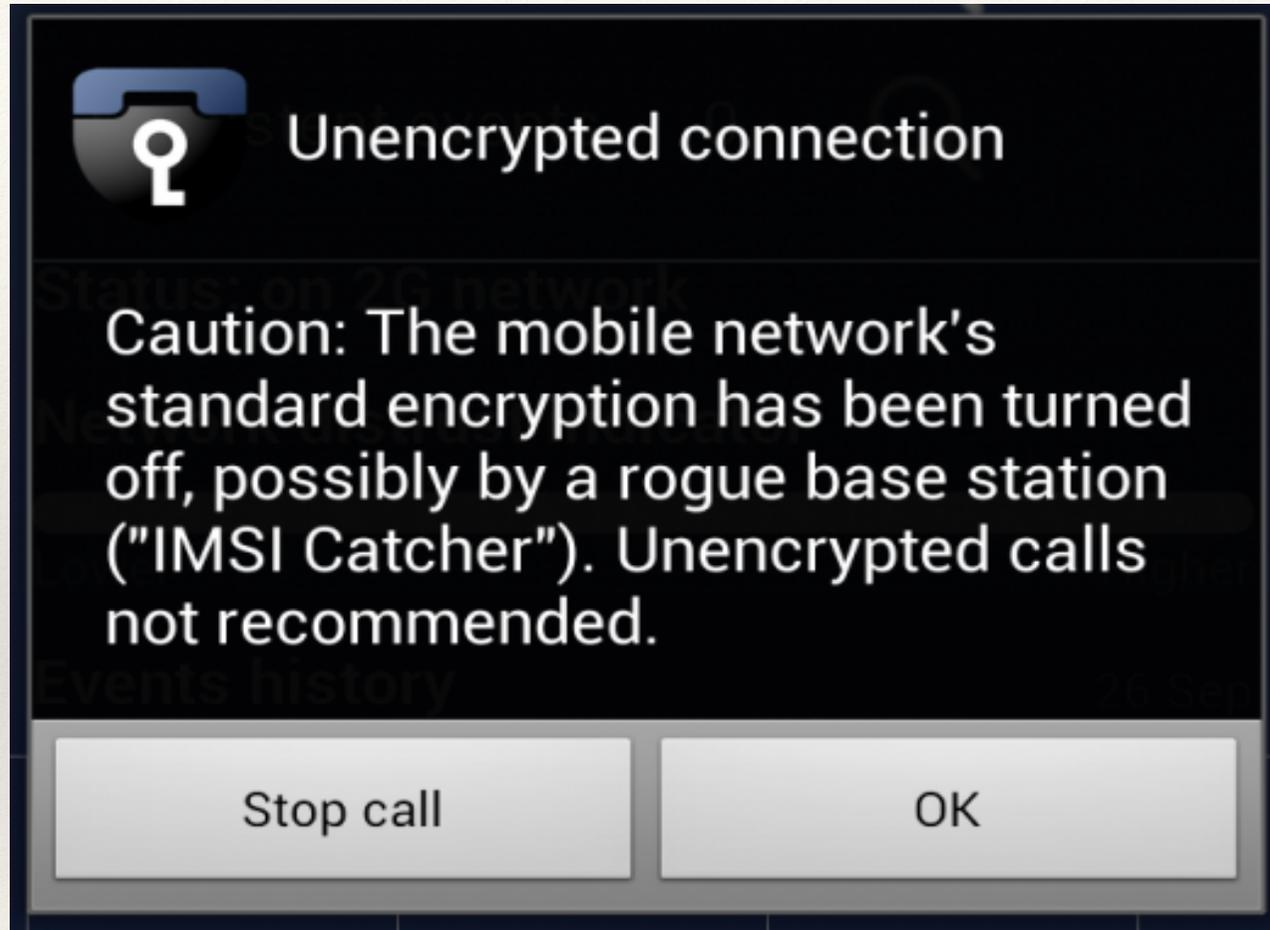


Norway's most secrets are being administered here, right in the centre of Oslo. A number of the most important state institutions are situated within a radius of one kilometre. The Prime minister's office, the Ministry of defence, Stortinget (parliament) and the central bank, Norges Bank. Ministers, state secretaries, members of parliament, state officials, business executives and other essential staff engaged in protecting the nation's security, our military and our oil wealth – totalling more than 6000 billion kroner (NOK) – are working within this area.

Source: Aftenposten

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

Detection of Fake Base Station?



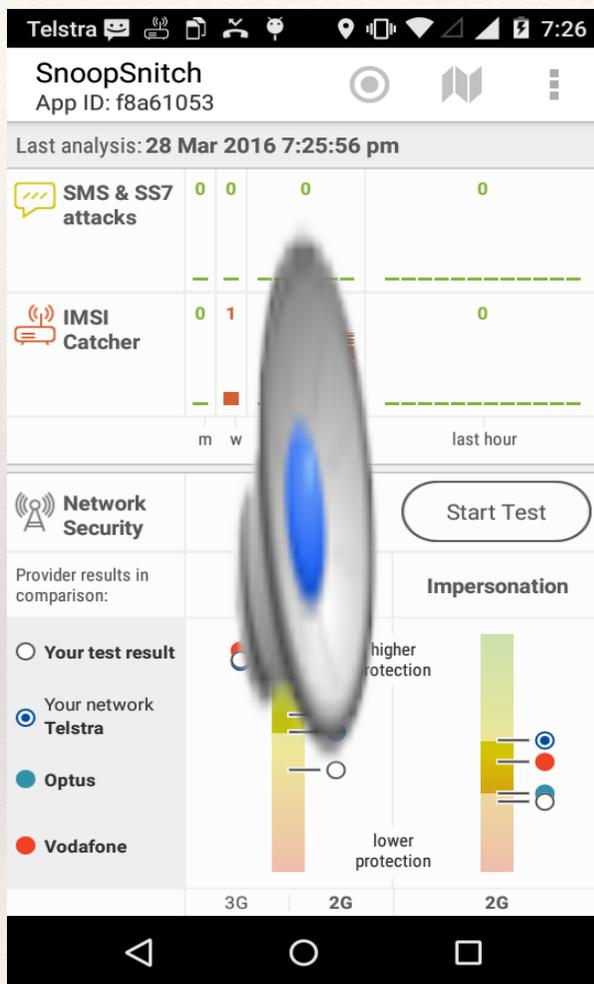
Source: Popular Science

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

Dirtboxes on a Plane | How the Justice Department spies from the sky

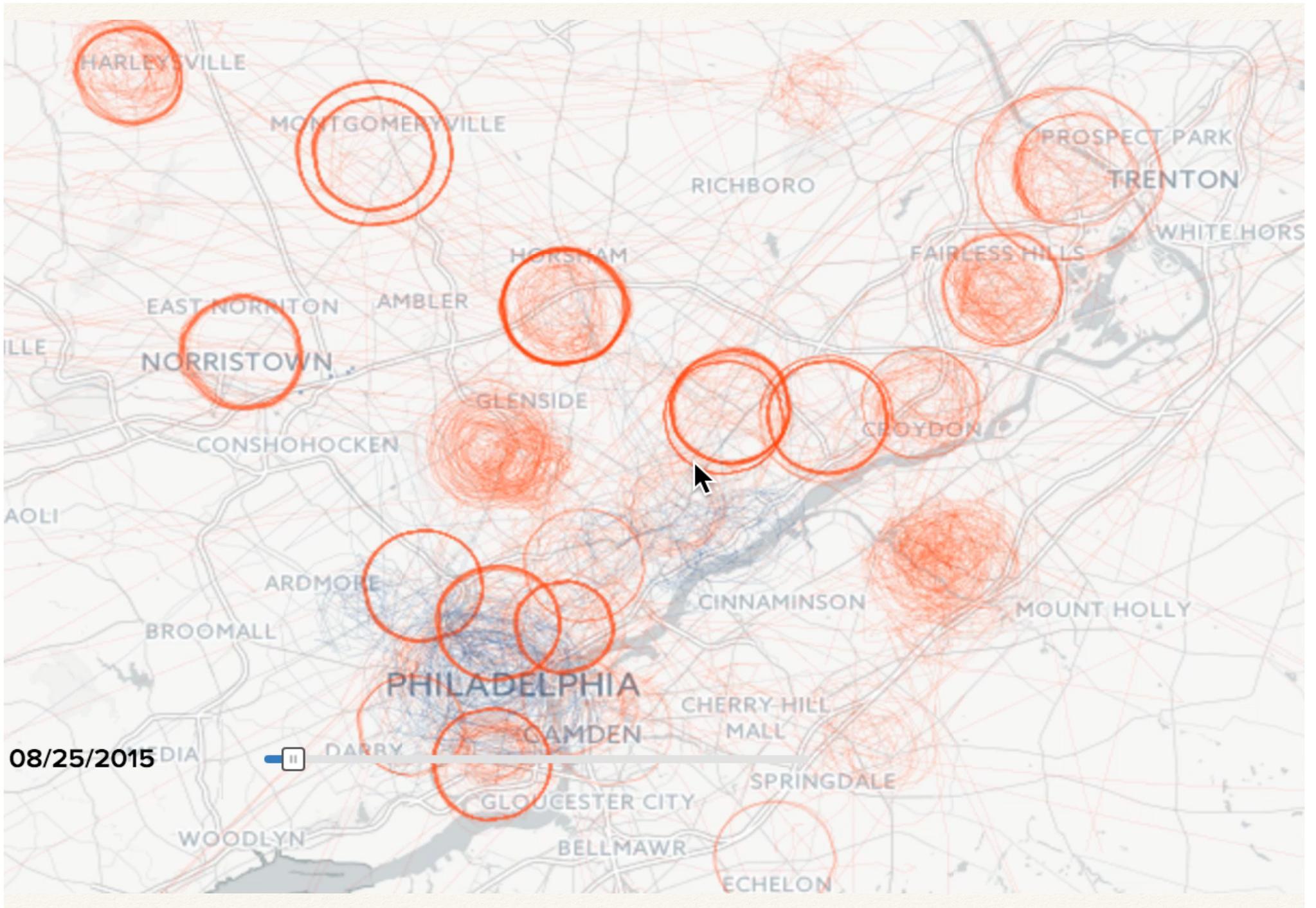
1 Planes equipped with fake cellphone-tower devices or 'dirtboxes' can scan thousands of cellphones looking for a suspect.

2 Non-suspects' cellphones are 'let go' and the dirtbox focuses on gathering information from the target.

3 The plane moves to another position to detect signal strength and location...

4 ...and the system can use that information to find the suspect within three meters, or within a specific room in a building.





Outline



• Stingray Threats



• Detection Tools



• Self-Assembly Approach



• Questions/Comments

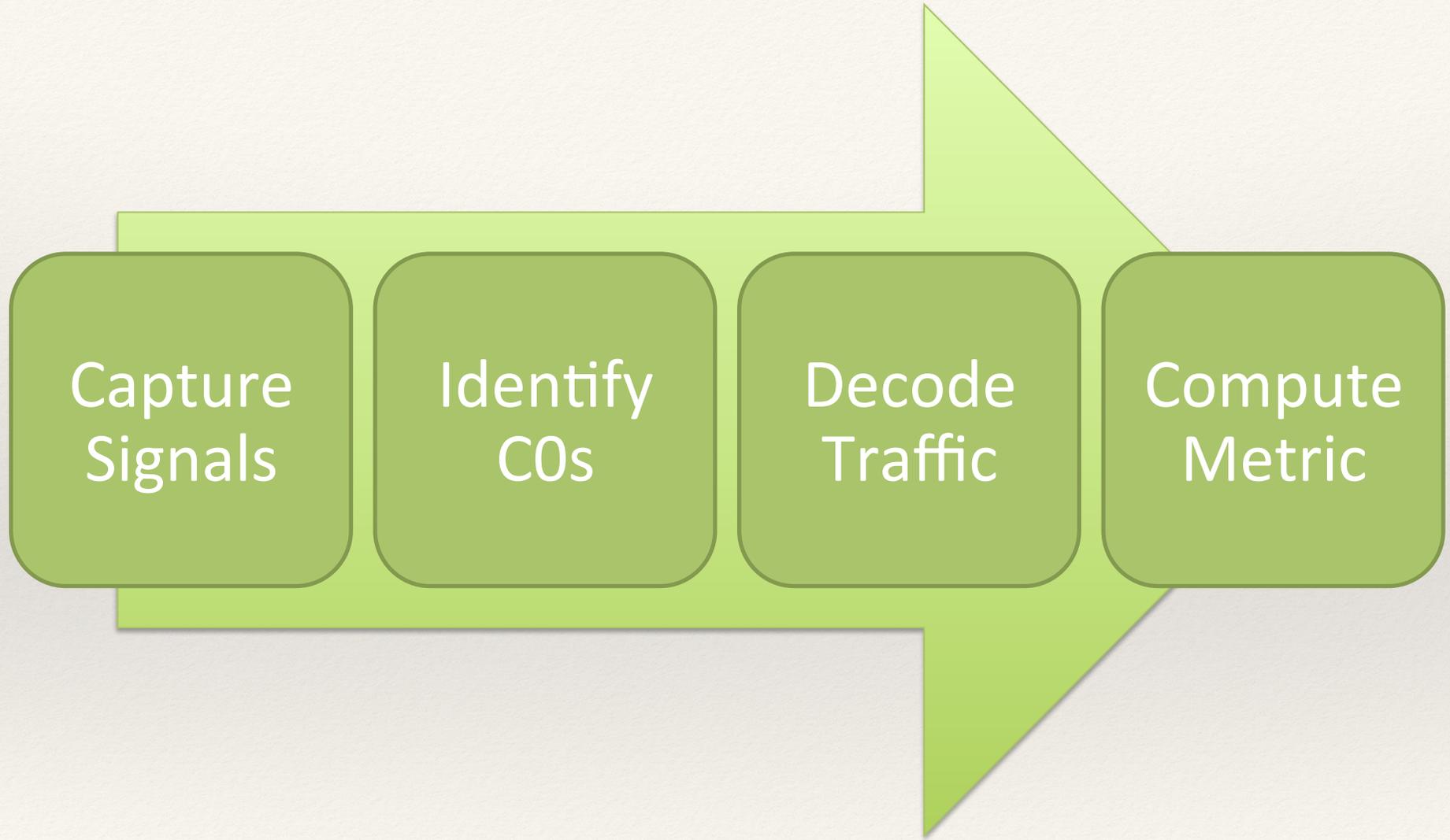
Detection Process

Capture
Signals

Identify
COs

Decode
Traffic

Compute
Metric



Australian GSM900 Frequencies

Telstra

935 MHz –
943.4 MHz

890.0 MHz –
898.4 MHz

Optus

943.4 MHz –
951.8 MHz

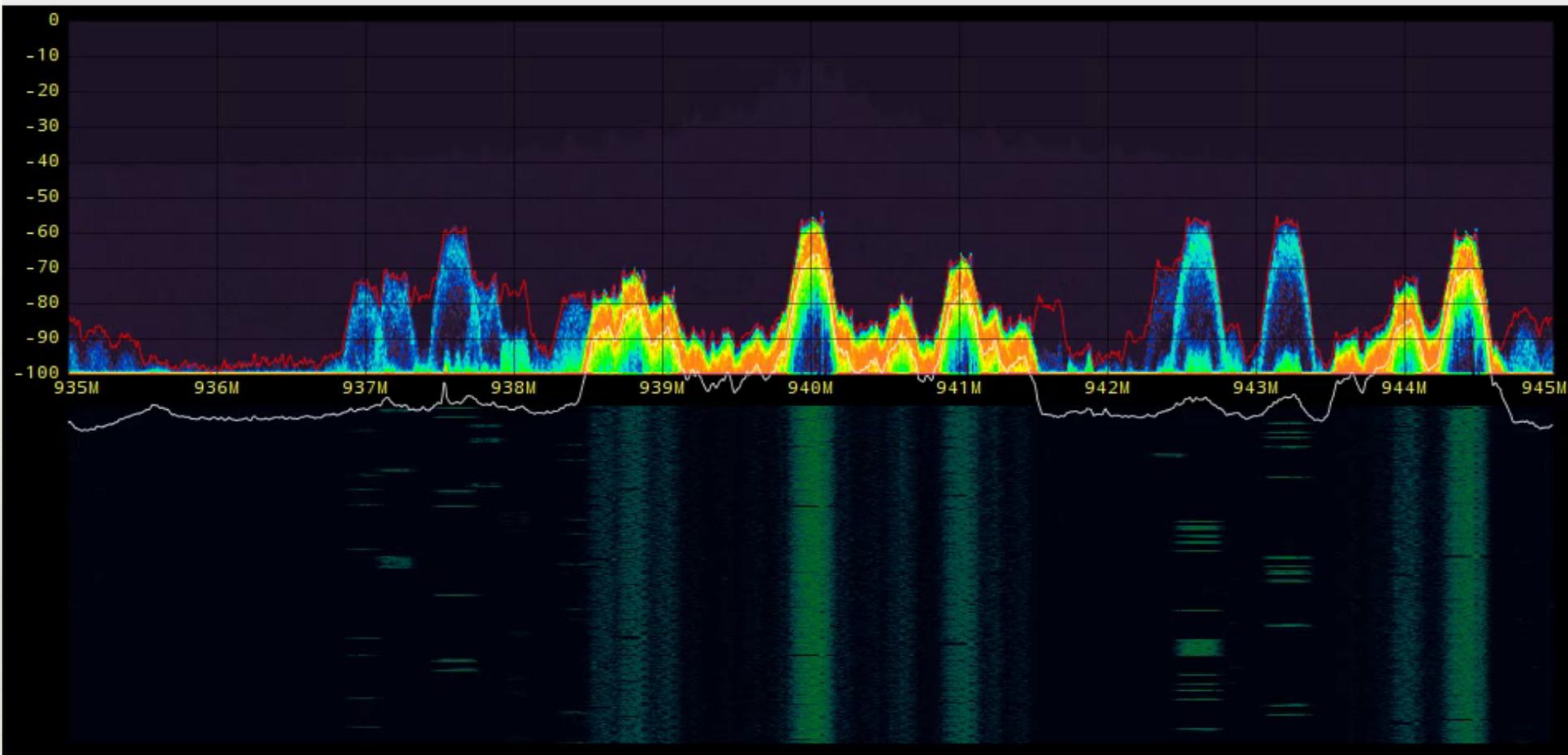
898.4 MHz –
906.8 MHz

Vodafone

951.8 MHz –
960.0 MHz

906.8 MHz –
915.0 MHz

File



UHD (003.005.004-140-gfb32ed16)

USRP: USRP2 r4 (1801), WBXv2 RX+GDB (no serial, A:0, TX/RX)

Center freq:

Gain:

15

Sample Rate:

RF Freq.: 940M

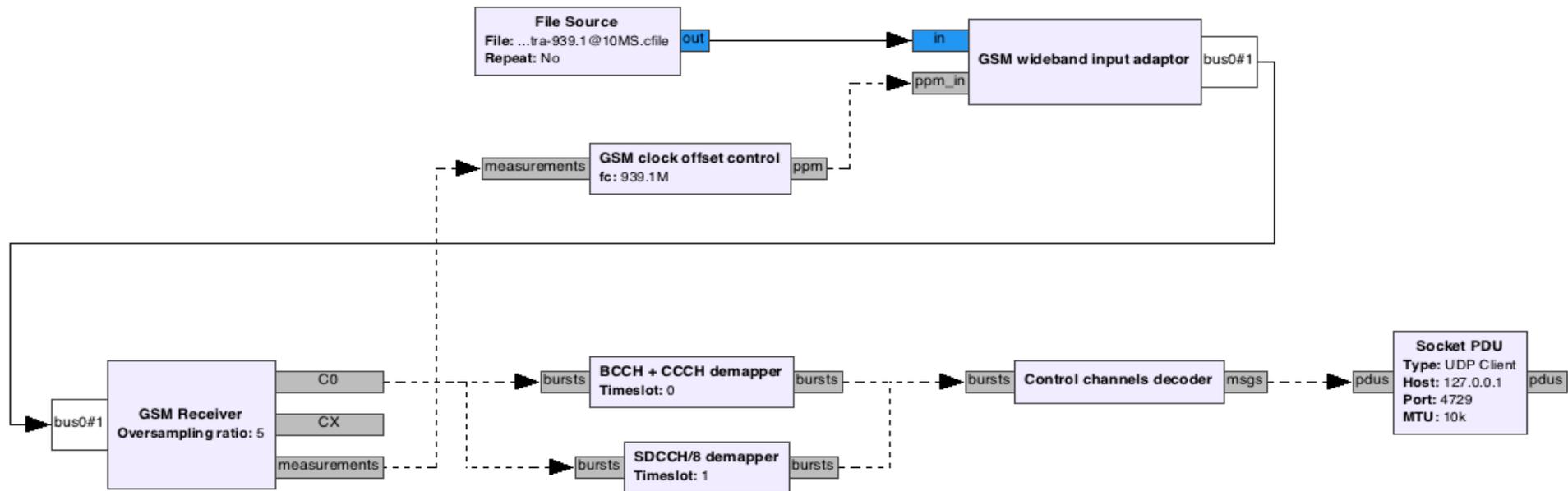
DSP Freq.: 0

OK

Traffic Reception

Options
 ID: gsmrx_uhd
 Title: C0 Decoding
 Author: Steve Glass
 Description: ARFCN...Telstra)
 Generate Options: No GUI
 Run Options: Run to Completion

Variable ID: fc Value: 939.1M	Variable ID: samp_rate_in Value: 10M	Variable ID: samp_rate_out Value: 1.35417M	Variable ID: osr Value: 5	Variable ID: ppm Value: 0	Variable ID: neighbors Value: [25, 31, 30, 29, 28...	Variable ID: ca Value: 25	Variable ID: ca_no_bch Value: 13, 38, 41
--	---	---	--	--	---	--	---



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 Information
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)

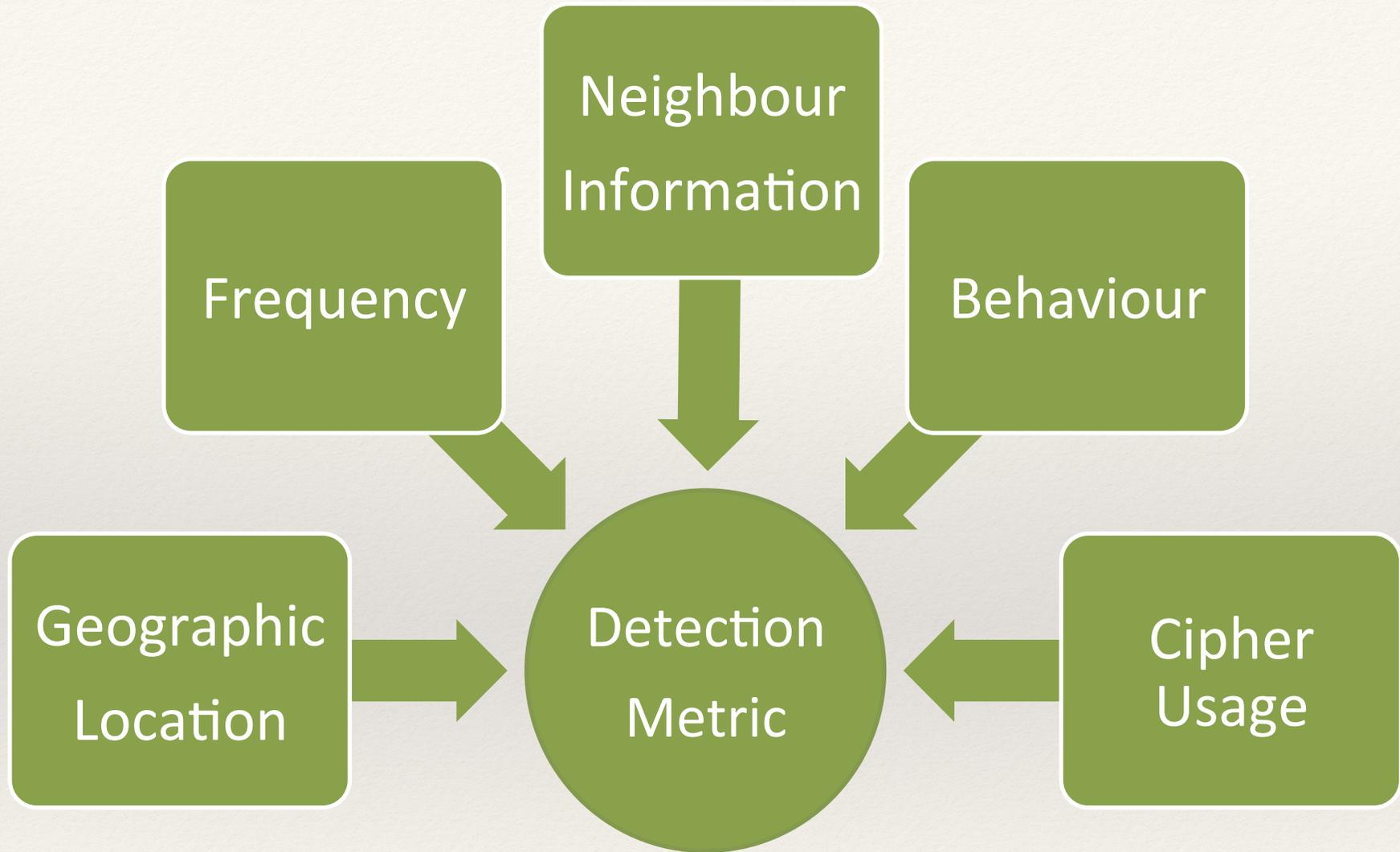
▼ Cipher Mode Setting

.... ...1 = SC: Start ciphering (1)

.... 000. = Algorithm identifier: Cipher with algorithm A5/1 (0)

▼ Cipher Mode Response

...1 = CR: IMEISV shall be included (1)



Location & Frequency

Australian Communications and Media Authority: Register of Radiocommunication Licences - Iceweasel

File Edit View History Bookmarks Tools Help

Australian Communications and ...

web.acma.gov.au/pls/radcom/assignment_search. Google

ExploitDB Linux identifier search ... mac80211 ACMA Postcode/Freq... Databases

acma.gov.au Register of Radiocommunications Licences

Assignment Details

General Details			
Licence Number	1136417	Access ID	5009645
Client	Telstra Corporation Limited		
Site	Hutchison/Vodafone Site Bldg D Gold Coast TAFE Benowa Rd & Heeb St ASHMORE		
Operating Mode	Transmit		
Access Status		Date Approved	21-JUN-13
Coverage	Local	Hours of Operation	

[New Search]

Frequencies			
Assigned	939.2 MHz	Lower	935 MHz
Carrier		Upper	943.4 MHz

Device and Antenna details			
Device ID	1391962	Emission Designator	8M40G7E
EIRP	0	Transmitter Power	20.00 pY
Antenna ID	30007		

Scapy and GSM

SI1

ARFCNs that comprise
cell

SI2

Neighbour list

SI3

Cell ID, LAI,
Reselection Info

Scapy and GSM

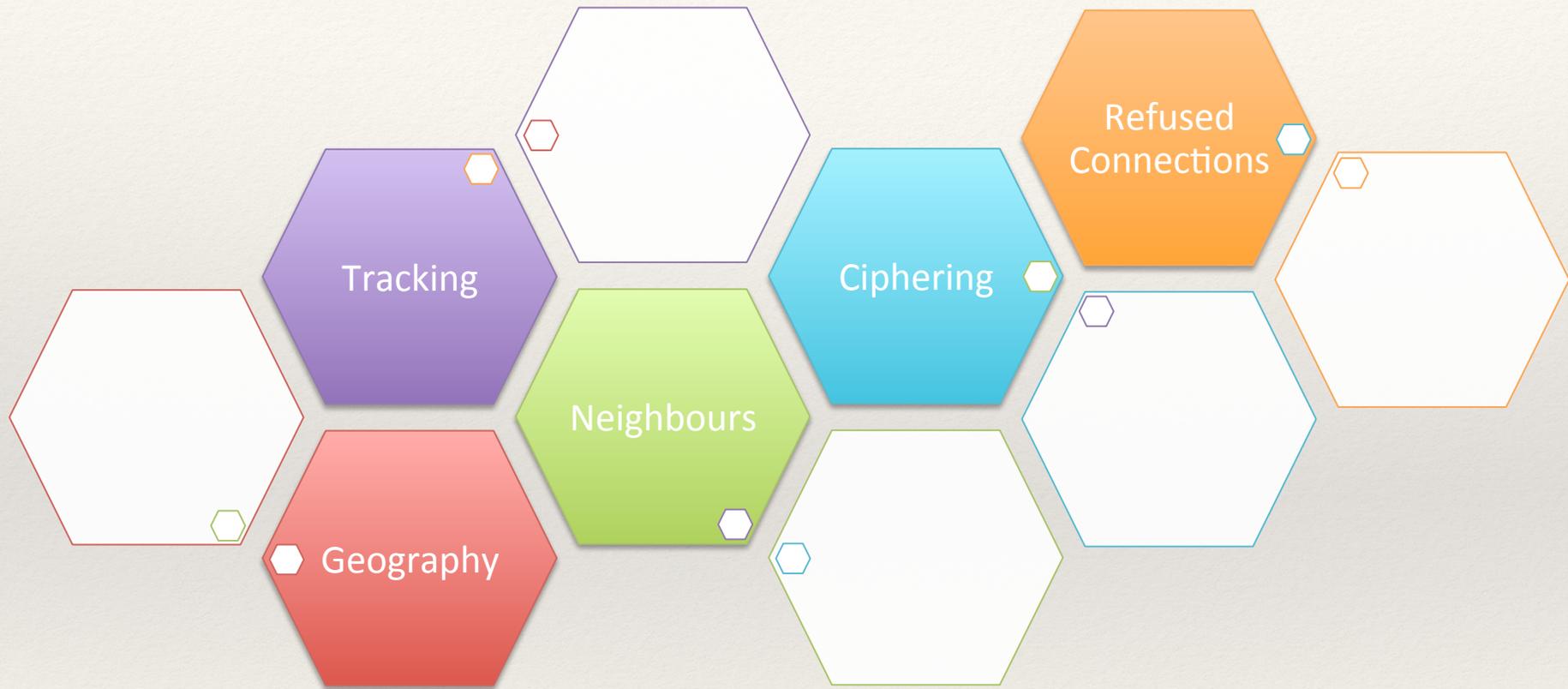
```
# GSMTap frame header
#
class GSMTap(Packet):
    """GSMTap Frame Header Version 2"""
    name = "GSMTap"
    fields_desc = [
        XByteField("version", 0x01),
        ByteField("hdr_len", 4),      # in 32bit words
        XByteField("type", 0x01),    # GSMTAP_TYPE_UM
        ByteField("timeslot", 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