Scanning the Airwaves

or: how to build a trunked radio scanner with a $20 USB stick

BRYAN PASSIFIUME & RICHARD HENDERSON

DefCon 25, Las Vegas – July 2017

Welcome!

Who We Are

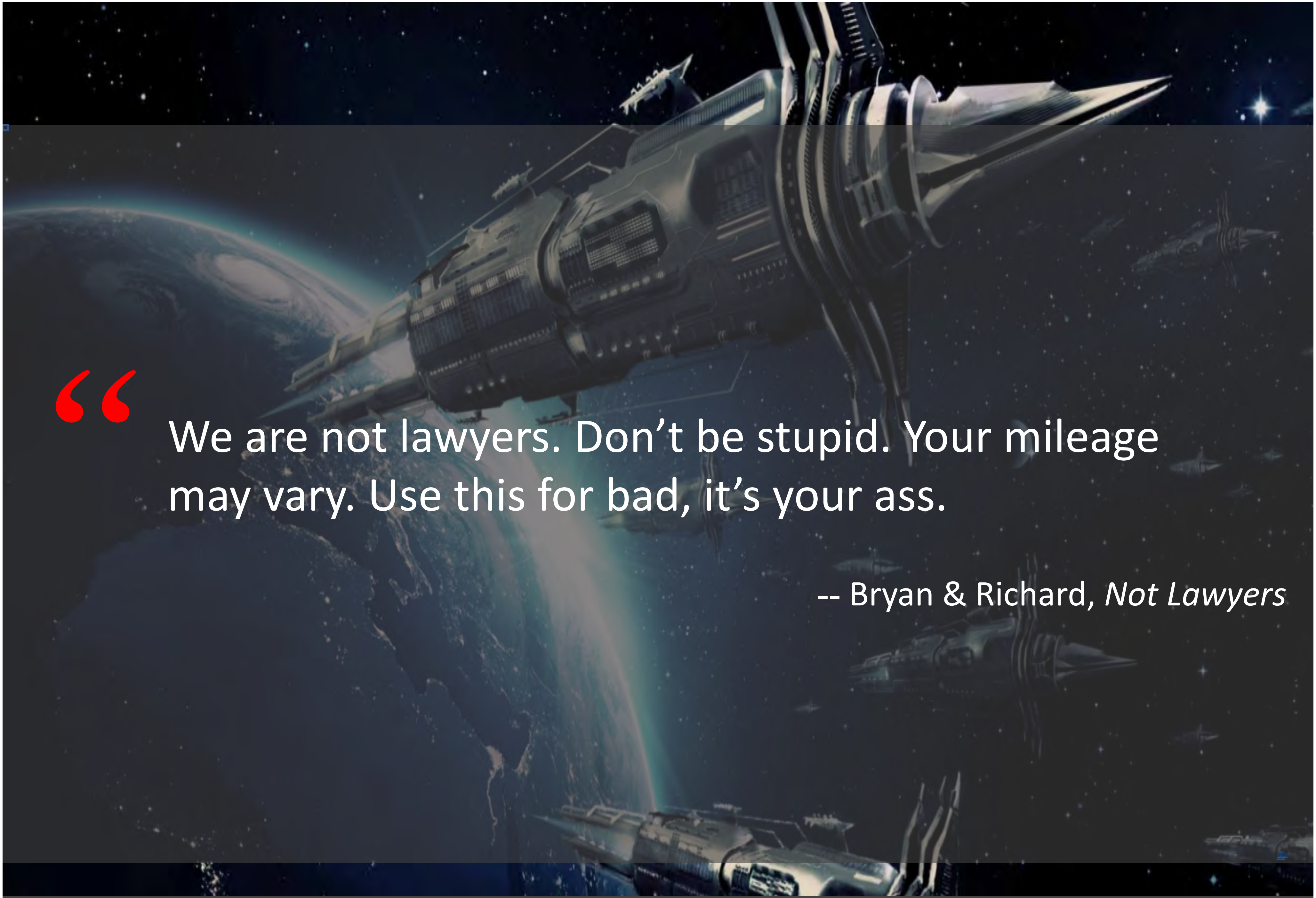
Bryan:
Ham, Crime Reporter/Photog for Calgary Sun. Co-founder of Ham Radio satire site Hamsexy.com
@BryanPassifiume

Richard:
Ham, writer, infosec professional.
@RichSentMe

What this is VS What this is not

Is:
a way to learn more about SDR, listening in, modern frequency scanning
teaching the basic tools to get started

Is NOT:
an all-encompassing walkthrough of how to listen to everything out there.
a way to crack encrypted comms… well, not **all** encrypted comms (voice inversion is NOT crypto lulz)
a hand-holding exercise to set you up with a scanner and let you loose – you'll need to take what you learn and apply it to your own local environment



> “We are not lawyers. Don’t be stupid. Your mileage may vary. Use this for bad, it’s your ass.
>
> -- Bryan & Richard, *Not Lawyers*

Why Get a License?

It’s Worth It!

Having a license opens up all sorts of new gadgets, power levels, and ideas.

It’s Easy

Getting started in most places is super easy. ***No advanced electronics knowledge is needed.***

Community

It may be a dying hobby, but there are still a LOT of hams out there.

Key to RF Experimentation

1000 Watts of power can carry. High power levels, data links, moon bounce, satellites, etc.

Resources

Like most things, you can find tons of help online.

Trouble?

In some places, having a ham license is the only legally allowed use of certain scanning equipment

SYSTEM REQUIREMENTS

----- Windows. No VMs. Srs. -----

Agenda

1 A Quick History

How did we get to here?

2 Practical Introduction

Current state of hardware, antenna types, why heat matters, etc.

3 Software Installation & Setup

Getting started with the introductory software (HDSDR)

4 Advanced Monitoring

Moving into trunked radio systems – how they work, installing other software to monitor

5 Where to Go from Here?

Multi-stick monitoring, pager decoding, where to find more info

PART ONE:

----- In the Beginning… -----

Early Radio Scanners...

The Birth of SDR

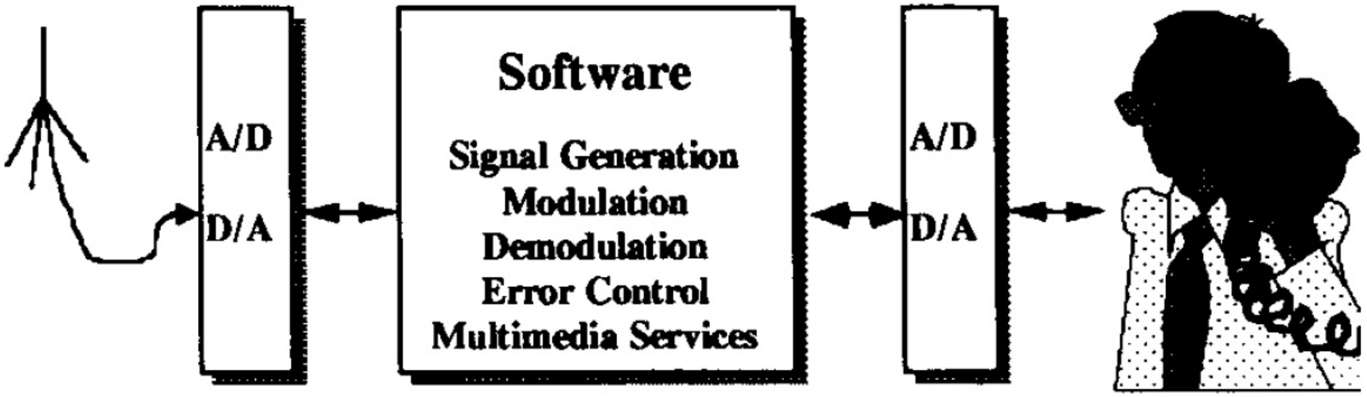
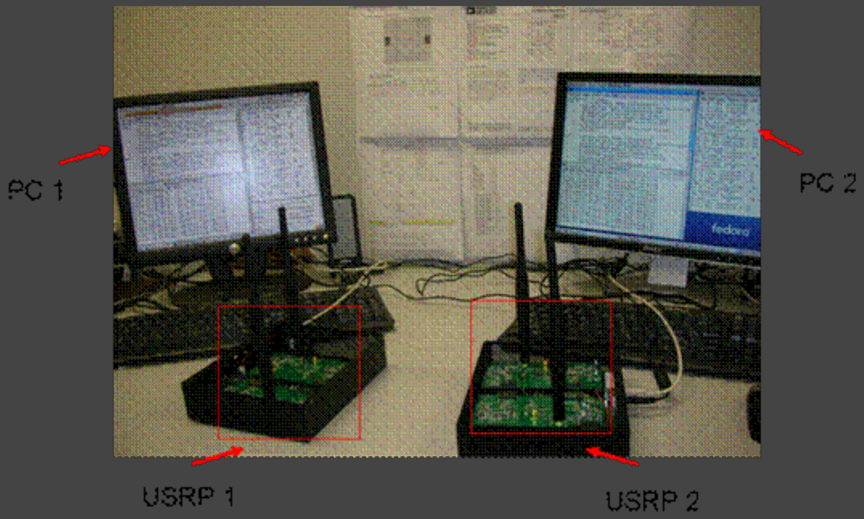


Figure 1, An Idealized Software Radio

Universal Software Radio Peripheral (USRP)



Enter the Realtek RTL2832U…

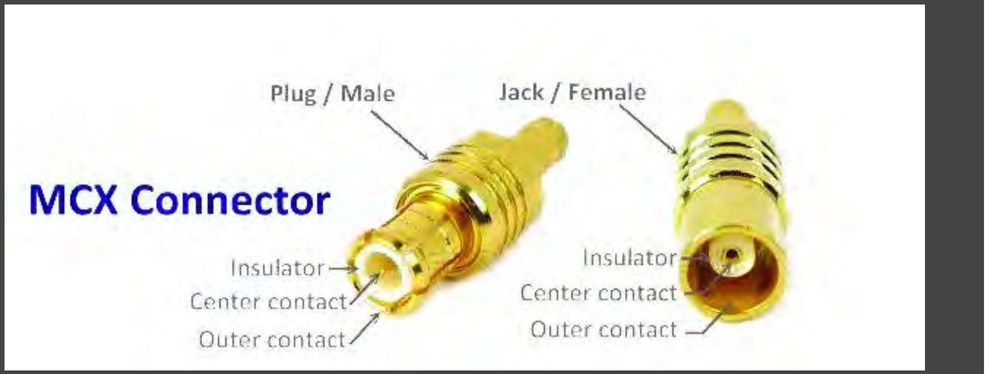
PART TWO:

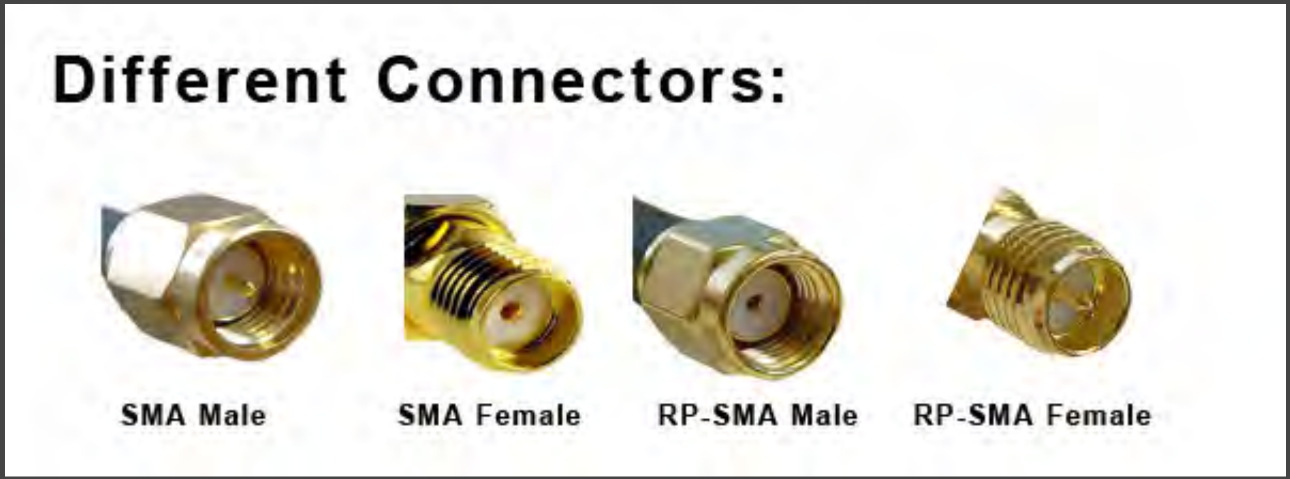
----- Introduction to SDR Scanning Today -----

The Basics:

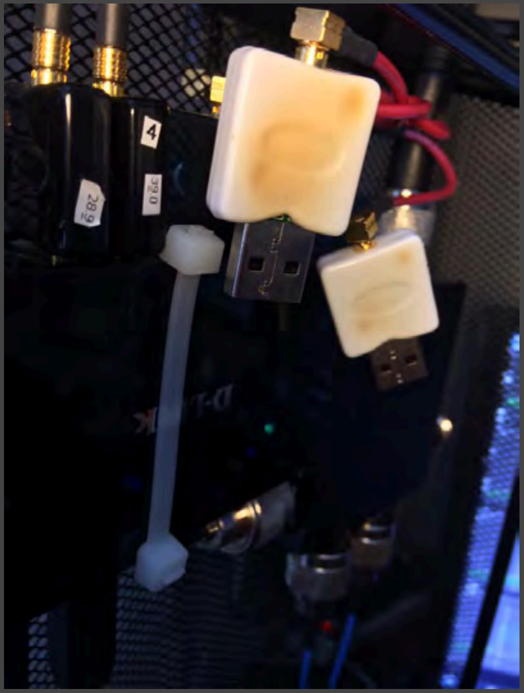
Other Sticks:

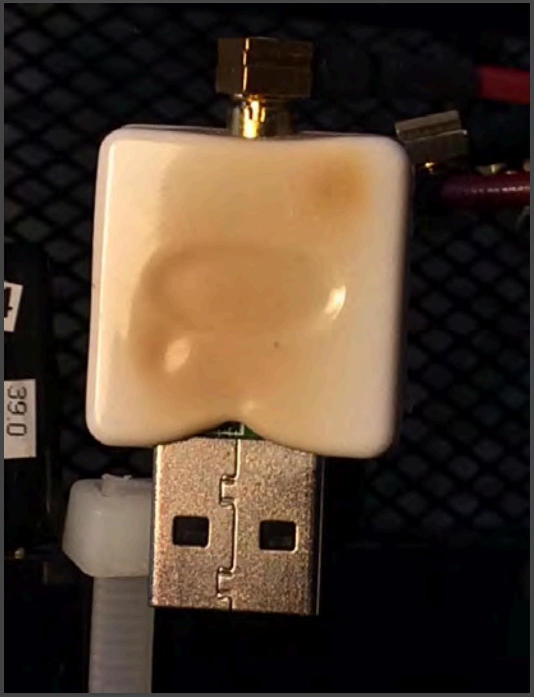
A Quick Note on Antenna Connectors:



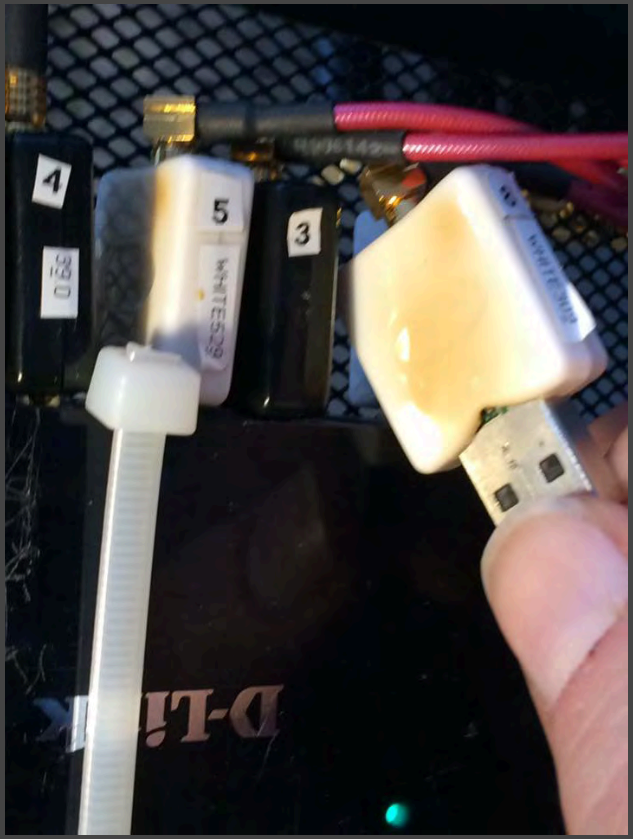


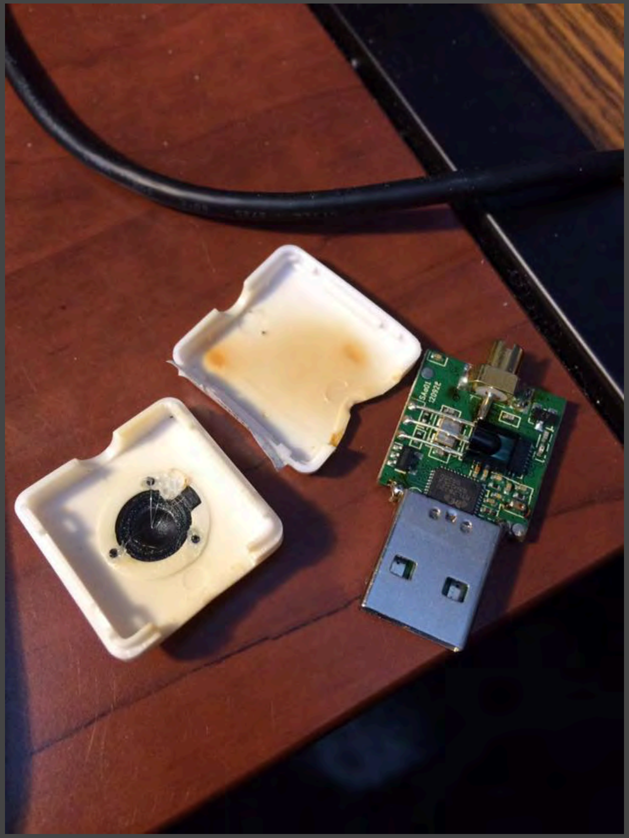
A Word or Two on Heat:





A Word or Two on Heat:





PART THREE:

----- Getting Started with Basic Scanning -----

Getting the Software

Drivers:

- •WinUSB drivers via Zadig installer (http://zadig.akeo.ie/)
- •ExtIO.DLL (https://github.com/josemariaaraujo/ExtIO_RTL)

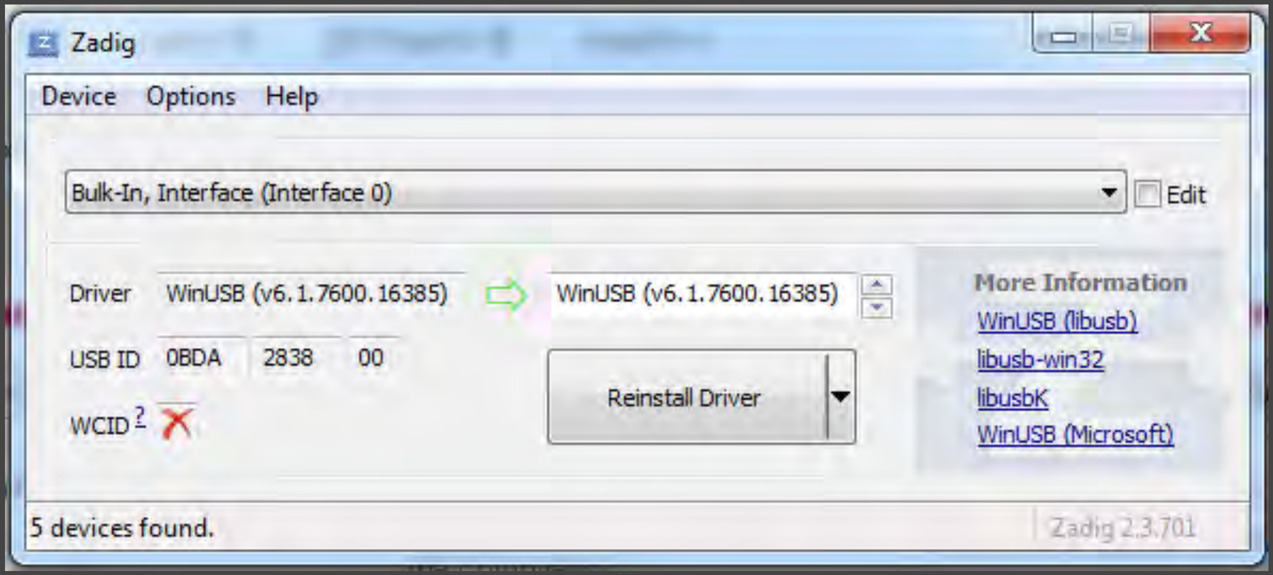
Software:

- •HDSDR (http://www.hdsdr.de/)
- •UniTrunker 1.0.32.5 (http://www.unitrunker.com/)
- •DSDPlus 1.101 (https://www.dsdplus.com/)
- •VB Cable 4.5 (http://www.vb-audio.com/Cable/index.htm)

Installing the Software

WinUSB:

- Run ZADIG installer to load WinUSB drivers for each “bulk-in, interface” instance noted (if needed)



Bulk-In, Interface (Interface 0)

Driver WinUSB (v6.1.7600.16385) ⇨ WinUSB (v6.1.7600.16385)

USB ID 0BDA 2838 00

WCID ? ✗

5 devices found.

Zadig 2.3.701

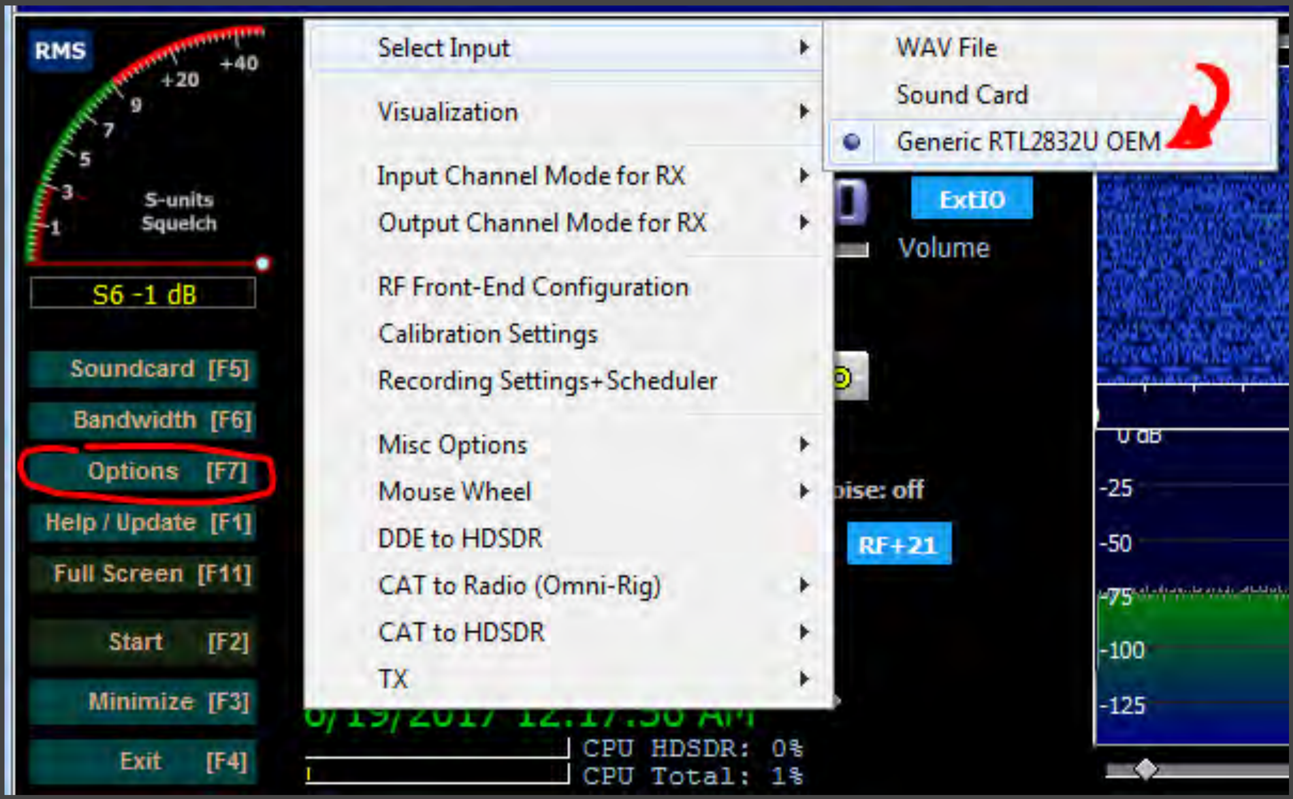
Installing the Software

SDR Driver/Libraries:
Unzip **ExtIO_RTL-master.zip**
Copy zip file contents to C:\Program Files (x86)\HDSDR

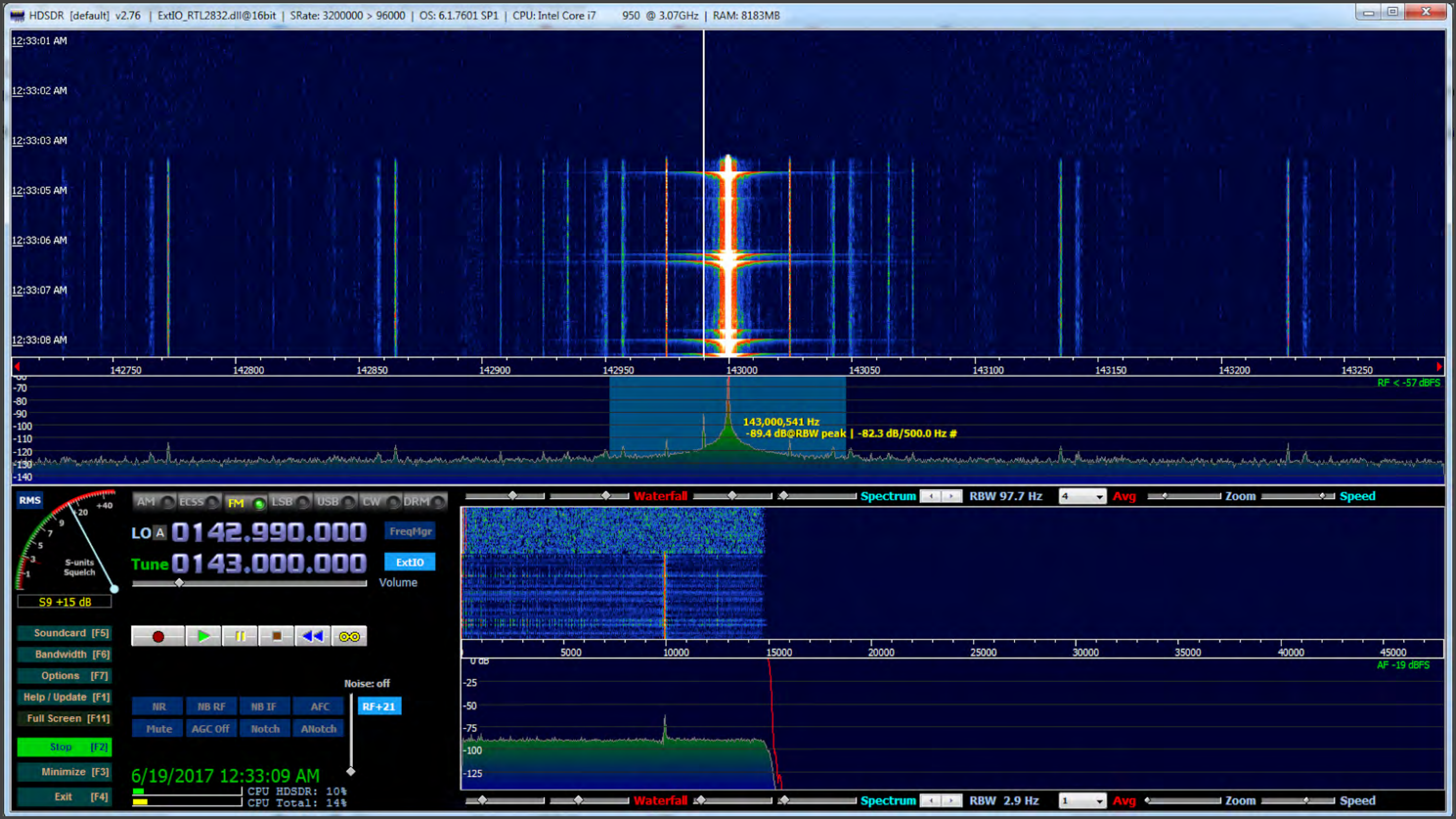
HDSDR:

- Run HDSDR_install.exe, follow etc.
- Run program
- Load EXT_IO for SDR dongle:
    - Options (F7)
    - Select Input
    - Point to ExtIO_RTL.DLL in /release/ folder

Installing the Software



Calibration & Operation



HDSDR [default] v2.76 | ExtIO_RTL2832.dll@16bit | SRate: 3200000 > 96000 | OS: 6.1.7601 SP1 | CPU: Intel Core i7 950 @ 3.07GHz | RAM: 8183MB

143,000,541 Hz
-89.4 dB@RBW peak | -82.3 dB/500.0 Hz #

RF < -57 dBFS

LO A 0142.990.000

Tune 0143.000.000

S9 +15 dB

RBW 97.7 Hz

Avg 4

RBW 2.9 Hz

Avg 1

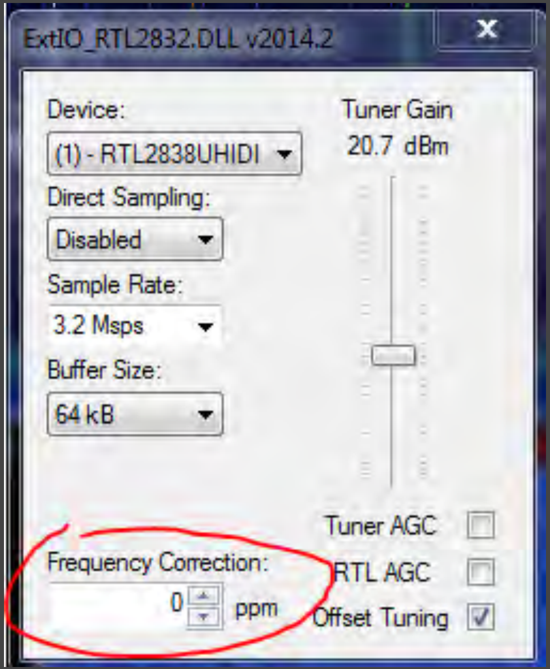
AF -19 dBFS

Noise: off

6/19/2017 12:33:09 AM

CPU HDSDR: 10%
CPU Total: 14%

Calibration & Operation



ExtIO_RTL2832.DLL v2014.2

Device: (1) - RTL2838UHIDI

Direct Sampling: Disabled

Sample Rate: 3.2 Msps

Buffer Size: 64 kB

Tuner Gain 20.7 dBm

Frequency Correction: 0 ppm

Tuner AGC □

RTL AGC □

Offset Tuning ☑

Time to Do Some Scanning!

Let’s take 30 minutes (or more!) to experiment.

Tune around, see what interesting signals you can find!

Suggestions:

- Local broadcast FM (87-108MHz)
- Other signals in the 450-520MHz range (FRS radio, commercial UHF)
- We’ll key up radios and show you what low power vs. high power signals might look like on your computer
- Can you find local ATC?

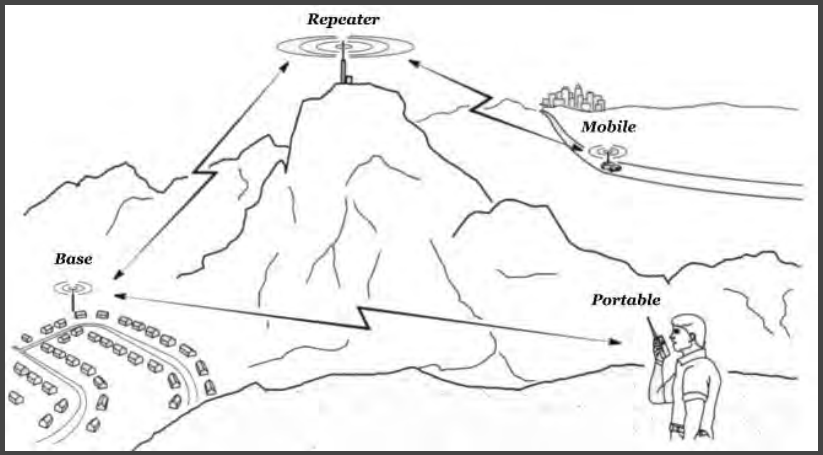
- Troubleshooting, initial questions, help, etc.

PART FOUR:

----- Advanced Monitoring -----

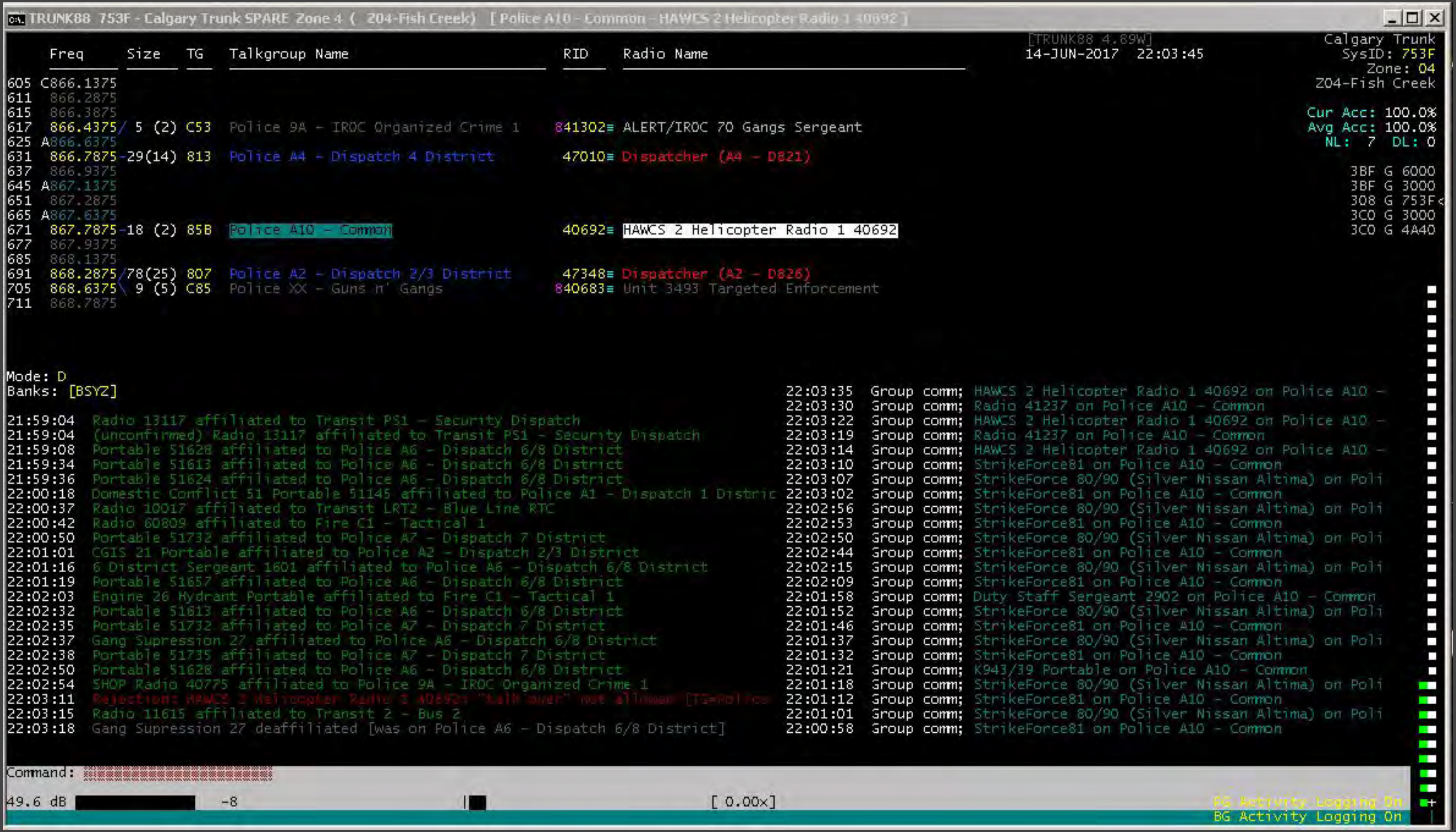
Trunking

Most large municipal radio systems employ some form of trunked radio system, a repeater-based, scalable packet-switching radio network that permits a large amount of users to use a small amount of frequencies:



Trunking

Most common are variants of Motorola Type II networks system, using single control channel to allocate & assign frequencies to talkgroups. Example of Trunk88 running on my home computer:



TRUNK88 753F - Calgary Trunk SPARE Zone 4 (204-Fish Creek) [Police A10 - Common - HAWCS 2 Helicopter Radio 1 40692]

```
                                                                               [TRUNK88 4.89W]               Calgary Trunk
     Freq      Size    TG   Talkgroup Name                    RID     Radio Name                       14-JUN-2017   22:03:45           SysID: 753F
                                                                                                                                      Zone: 04
605 C866.1375                                                                                                                  Z04-Fish Creek
611  866.2875
615  866.3875                                                                                                                  Cur Acc: 100.0%
617  866.4375/ 5 (2) C53  Police 9A - IROC Organized Crime 1  841302≡ ALERT/IROC 70 Gangs Sergeant                              Avg Acc: 100.0%
625 A866.6375                                                                                                                    NL:  7  DL: 0
631  866.7875-29(14) 813  Police A4 - Dispatch 4 District      47010≡ Dispatcher (A4 - D821)
637  866.9375                                                                                                                    3BF G 6000
645 A867.1375                                                                                                                    3BF G 3000
651  867.2875                                                                                                                    308 G 753F<
665 A867.6375                                                                                                                    3C0 G 3000
671  867.7875-18 (2) 85B  Police A10 - Common                  40692≡ HAWCS 2 Helicopter Radio 1 40692                          3C0 G 4A40
677  867.9375
685  868.1375
691  868.2875/78(25) 807  Police A2 - Dispatch 2/3 District    47348≡ Dispatcher (A2 - D826)
705  868.6375\ 9 (5) C85  Police XX - Guns n' Gangs           840683≡ Unit 3493 Targeted Enforcement
711  868.7875


Mode: D
Banks: [BSYZ]                                                                         22:03:35  Group comm; HAWCS 2 Helicopter Radio 1 40692 on Police A10 -
                                                                                      22:03:30  Group comm; Radio 41237 on Police A10 - Common
21:59:04  Radio 13117 affiliated to Transit PS1 - Security Dispatch                   22:03:22  Group comm; HAWCS 2 Helicopter Radio 1 40692 on Police A10 -
21:59:04  (unconfirmed) Radio 13117 affiliated to Transit PS1 - Security Dispatch     22:03:19  Group comm; Radio 41237 on Police A10 - Common
21:59:08  Portable 51628 affiliated to Police A6 - Dispatch 6/8 District              22:03:14  Group comm; HAWCS 2 Helicopter Radio 1 40692 on Police A10 -
21:59:34  Portable 51613 affiliated to Police A6 - Dispatch 6/8 District              22:03:10  Group comm; StrikeForce81 on Police A10 - Common
21:59:36  Portable 51624 affiliated to Police A6 - Dispatch 6/8 District              22:03:07  Group comm; StrikeForce 80/90 (Silver Nissan Altima) on Poli
22:00:18  Domestic Conflict 51 Portable 51145 affiliated to Police A1 - Dispatch 1 Distric 22:03:02  Group comm; StrikeForce81 on Police A10 - Common
22:00:37  Radio 10017 affiliated to Transit LRT2 - Blue Line RTC                      22:02:56  Group comm; StrikeForce 80/90 (Silver Nissan Altima) on Poli
22:00:42  Radio 60809 affiliated to Fire C1 - Tactical 1                              22:02:53  Group comm; StrikeForce81 on Police A10 - Common
22:00:50  Portable 51732 affiliated to Police A7 - Dispatch 7 District                22:02:50  Group comm; StrikeForce 80/90 (Silver Nissan Altima) on Poli
22:01:01  CGIS 21 Portable affiliated to Police A2 - Dispatch 2/3 District            22:02:44  Group comm; StrikeForce81 on Police A10 - Common
22:01:16  6 District Sergeant 1601 affiliated to Police A6 - Dispatch 6/8 District    22:02:15  Group comm; StrikeForce 80/90 (Silver Nissan Altima) on Poli
22:01:19  Portable 51657 affiliated to Police A6 - Dispatch 6/8 District              22:02:09  Group comm; StrikeForce81 on Police A10 - Common
22:02:03  Engine 26 Hydrant Portable affiliated to Fire C1 - Tactical 1               22:01:58  Group comm; Duty Staff Sergeant 2902 on Police A10 - Common
22:02:32  Portable 51613 affiliated to Police A6 - Dispatch 6/8 District              22:01:52  Group comm; StrikeForce 80/90 (Silver Nissan Altima) on Poli
22:02:35  Portable 51732 affiliated to Police A7 - Dispatch 7 District                22:01:46  Group comm; StrikeForce81 on Police A10 - Common
22:02:37  Gang Supression 27 affiliated to Police A6 - Dispatch 6/8 District          22:01:37  Group comm; StrikeForce 80/90 (Silver Nissan Altima) on Poli
22:02:38  Portable 51735 affiliated to Police A7 - Dispatch 7 District                22:01:32  Group comm; StrikeForce81 on Police A10 - Common
22:02:50  Portable 51628 affiliated to Police A6 - Dispatch 6/8 District              22:01:21  Group comm; K943/39 Portable on Police A10 - Common
22:02:54  SHOP Radio 40775 affiliated to Police 9A - IROC Organized Crime 1           22:01:18  Group comm; StrikeForce 80/90 (Silver Nissan Altima) on Poli
22:03:11  Rejection: HAWCS 2 Helicopter Radio 1 40692: "talk over" not allowed [TG=Police 22:01:12  Group comm; StrikeForce81 on Police A10 - Common
22:03:15  Radio 11615 affiliated to Transit 2 - Bus 2                                 22:01:01  Group comm; StrikeForce 80/90 (Silver Nissan Altima) on Poli
22:03:18  Gang Supression 27 deaffiliated [was on Police A6 - Dispatch 6/8 District]  22:00:58  Group comm; StrikeForce81 on Police A10 - Common

Command:
49.6 dB              -8                  |                    [ 0.00x]                              FG Activity Logging On
                                                                                                    BG Activity Logging On
```

How Do Trunking Systems Work?

- Talkgroups analogous to ‘virtual channels’
- Frequency assignment is transparent to the user
- Systems are typically designed, built, and operated around the ”5x5” principle
- Therefore, most systems have a large number of TGs and a small number of available frequencies and voice channels
- The number of maximum active TGs at once is, as you’d expect, limited by the number of voice channels

- Development of commercial *TrunkTracking* scanners required reverse engineering of each vendor’s proprietary control channel data

How Do Trunking Systems Work?

- Talkgroups analogous to ‘virtual channels’
- Frequency assignment is transparent to the user
- Systems are typically designed, built, and operated around the ”5x5” principle
- Therefore, most systems have a large number of TGs and a small number of available frequencies and voice channels
- The number of maximum active TGs at once is, as you’d expect, limited by the number of voice channels

- Development of commercial *TrunkTracking* scanners required reverse engineering of each vendor’s proprietary control channel data

How Do Trunking Systems Work?

How a trunked transmission works in the picture here:

1. User presses PTT key on radio, while tuned to TG A3
2. Trunk controller searches for a free frequency (in this case 864.000 MHz), and then issues channel grant to all radios tuned to TG A3 to use 864.000 MHz.
3. When user releases PTT, trunk controller orders all radios on TG A3 to standby, and then releases 864.000 back into the available frequency pool.

Some Background on the History of System Hacking

- Work built on shoulders of decades of radio hacking communities centered around the Batlabs website, several Russian-based hacking collectives and later the now-defunct P25.ca/communications,support forums.
- Motorola RSS/CPS software very expensive and fiercely protected, online file sharing helped spread the hobby
- Rudimentary protection schemes by Motorola easily circumvented, such as software (and later hardware) system keys for trunked radio programming, the leak of lab/depot versions of programming software, and what was once a thriving community of hackers and users, developing workarounds and countermeasures to Motorola's latest efforts to shut out unauthorized users
- Innovation and workarounds mean almost every trunked police radio system operating in North America has at least a couple of unauthorized radios silently affiliated and listening in
- Biggest detriment now is encryption — AES256-based

Introduction to UniTrunker

- A ready-to-roll copy of UniTrunker will be provided to attendees, instead of forcing everyone to roll their own (which would take forever to get set up).

Introduction to MOTOTRBO and DSD+

- Demonstration of DSD+ and its ability to decode the local MotoTrbo system. ;)
- Discussion on how DSD+ can decode P25 audio via piped audio from other software (like HDSDR, UniTrunker, etc.)

Introduction to MOTOTRBO and DSD+

- Quick primer on MotoTrbo/DMR methodology (more slides to come here)
  - TDMA
  - Timeslots
  - sidealong data/telemetry, etc.

PART FIVE:

----- Where to Go From Here -----

Online Resources for Frequency Data

- RadioReference
- Other sites

- We’ll demo finding info for your area!

Online Resources for Getting a Ham Radio License

- ARRL
- RAC
- Question Pools

- How to find an examiner, what the exam is like, etc.

Specific Questions?

- We’ll use the rest of the time to play, experiment, TX/RX!