📶

REIMAGINING THE POLICE SCANNER IN THE ERA OF THE SDR

Taking scanning to the next level using distributed RTLSDR receivers & open source software

PRESENTED BY GAVIN ROZZI

Cyberspectrum #23 @ DEF CON 2018

August 9th, 2018

SDR HAS THE

POTENTIAL

TO EXPAND PUBLIC KNOWLEDGE WHILE REDUCING COST & COMPLEXITY

THE PROBLEM WITH HARDWARE SCANNERS

HARDWARE SCANNERS ARE EXPENSIVE

Digital scanners especially those capable of newer digital protocols are pricey.

P25 PHASE II SCANNER - $400

RTLSDR DONGLE - $25

HARDWARE SCANNERS HAVE LIMITATIONS

Traditional scanners can only receive one transmission at a time. But large trunked systems could have activity on multiple channels at once, forcing users to miss out.

FOR MANY, NEW DIGITAL SCANNERS ARE OUT OF REACH

As agencies continue to adopt radios that use digital modulation, many scanner enthusiasts are unable or unwilling to obtain digital scanners due to cost and complexity of programming them.

Newer scanners like the Uniden HomePatrol series have simplified things, but they still come with a high pricetag.

LIVE FEEDS AREN’T MUCH BETTER

They compensate for some shortcomings and allow portability, but are still limited by the constraints of hardware scanners.

ENTER OC RADIO LIVE

Using SDR & open source technologies, we can make scanning easier and more user-friendly. OC Radio Live is a website that I created to use SDR to stream transmissions from local radio systems. It is essentially a “Scanner as a Service” (SaaS) as it has the functions you’d expect from a traditional scanner - but with powerful new SDR-powered features.

HOW SCANNING CAN BE BETTER WITH SDR

Thanks to trunk-recorder we can record:

- Conventional analog repeater / simplex channels
- Motorola analog trunked systems
- P25 Phase 1 & 2 digital trunking systems

OCEAN COUNTY, NJ’S RADIO SYSTEMS

These capabilities allow us to record the following types of systems using the site:

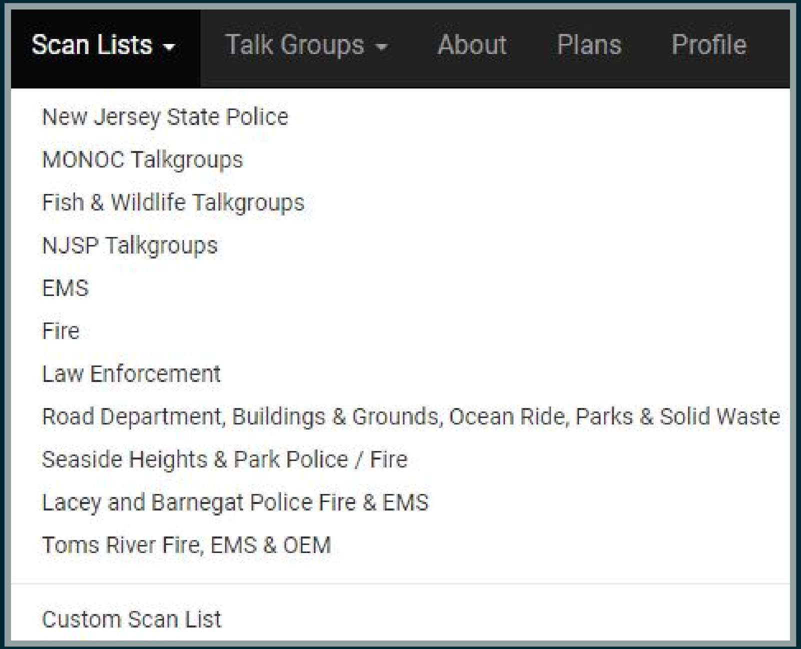
AGING 500 MHZ MOTOROLA TYPE II TRS

NEW STATE & COUNTY 700 MHZ P25 PHASE II SYSTEMS

ANALOG VHF AND UHF CONVENTIONAL CHANNELS

MORE CHOICES

Hardware scanners only offer a simple lockout and various banks of channels. OC Radio Live has data on individual channels, entire radio systems and custom scan lists for regions and types of radio traffic.

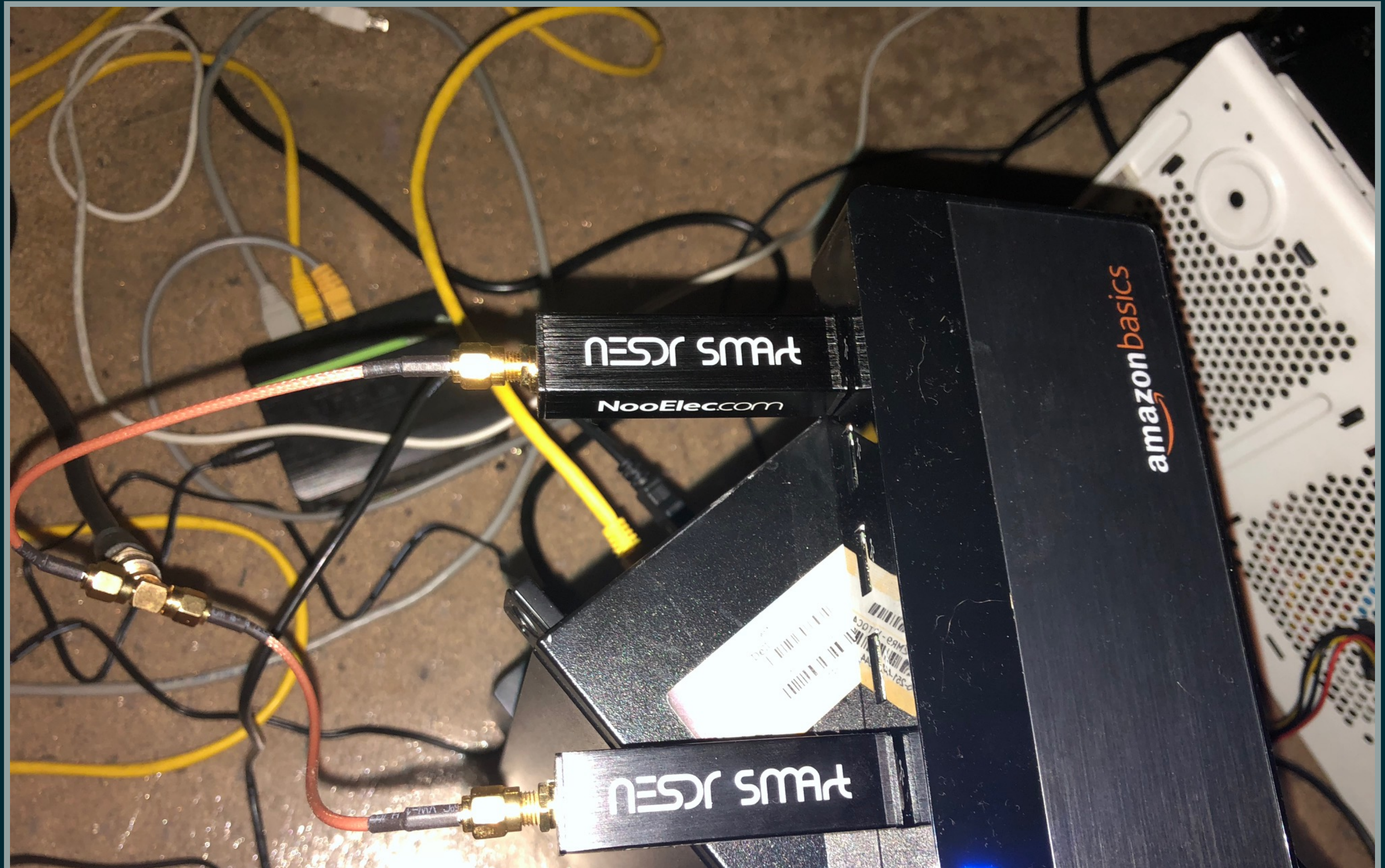

Scan Lists
Talk Groups
About
Plans
Profile
New Jersey State Police
MONOC Talkgroups
Fish & Wildlife Talkgroups
NJSP Talkgroups
EMS
Fire
Law Enforcement
Road Department, Buildings & Grounds, Ocean Ride, Parks & Solid Waste
Seaside Heights & Park Police / Fire
Lacey and Barnegat Police Fire & EMS
Toms River Fire, EMS & OEM
Custom Scan List

OUR RECEIVING SITES

Toms River, NJ (700, 460 and 155 MHz) (outside)

OUR RECEIVING SITES

Lacey, NJ (500 MHz) (inside)



THE OPEN-SOURCE

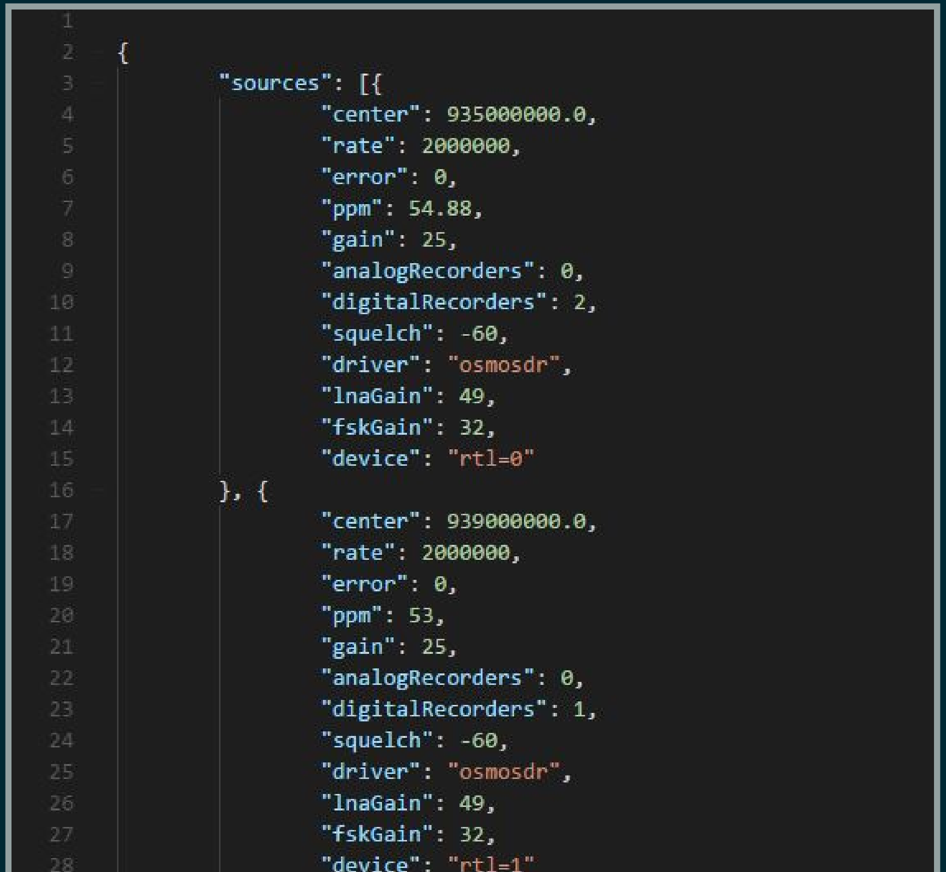
SOFTWARE POWERING THE SITE

THE BACKEND

- trunk-recorder by Luke Berndt
- Radio transmissions are saved to an Amazon S3 bucket
- Desktop with powered USB hubs at receiving site 1
- 2U server along with an Ubuntu desktop with 4 SDRs at receiving site 2

THE BACKEND

trunk-recorder uses JSON syntax for defining systems and SDRs. Some examples of the systems I defined are

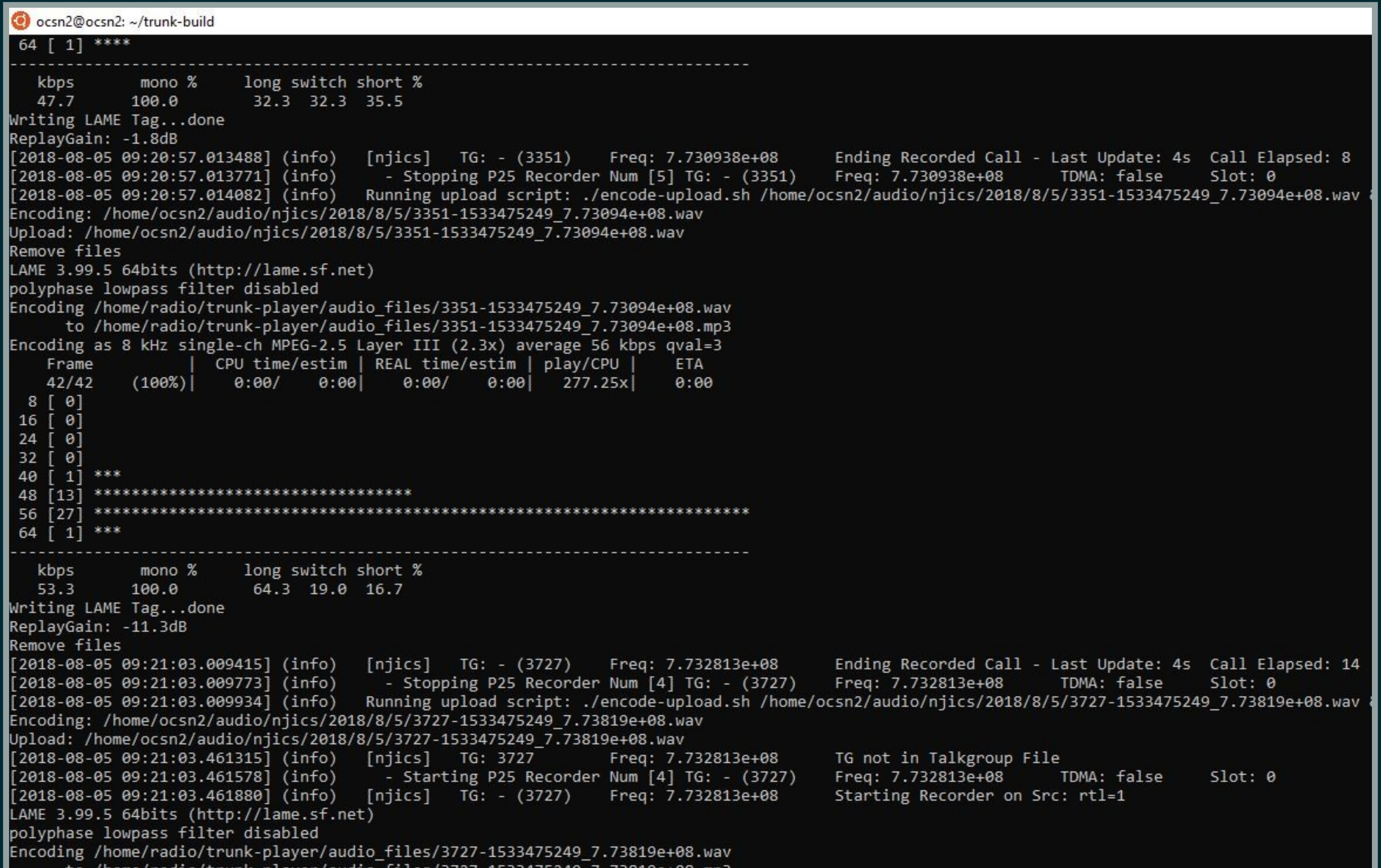


```

{
        "sources": [{
                "center": 935000000.0,
                "rate": 2000000,
                "error": 0,
                "ppm": 54.88,
                "gain": 25,
                "analogRecorders": 0,
                "digitalRecorders": 2,
                "squelch": -60,
                "driver": "osmosdr",
                "lnaGain": 49,
                "fskGain": 32,
                "device": "rtl=0"
        }, {
                "center": 939000000.0,
                "rate": 2000000,
                "error": 0,
                "ppm": 53,
                "gain": 25,
                "analogRecorders": 0,
                "digitalRecorders": 1,
                "squelch": -60,
                "driver": "osmosdr",
                "lnaGain": 49,
                "fskGain": 32,
                "device": "rtl=1"
```

THE BACKEND

Scanning the NJICS 700 MHz system



```
 64 [ 1] ****
-------------------------------------------------------------------------------
   kbps       mono %     long switch short %
   47.7      100.0        32.3  32.3  35.5
Writing LAME Tag...done
ReplayGain: -1.8dB
[2018-08-05 09:20:57.013488] (info)   [njics]   TG: - (3351)    Freq: 7.730938e+08      Ending Recorded Call - Last Update: 4s  Call Elapsed: 8
[2018-08-05 09:20:57.013771] (info)     - Stopping P25 Recorder Num [5] TG: - (3351)    Freq: 7.730938e+08      TDMA: false     Slot: 0
[2018-08-05 09:20:57.014082] (info)   Running upload script: ./encode-upload.sh /home/ocsn2/audio/njics/2018/8/5/3351-1533475249_7.73094e+08.wav
Encoding: /home/ocsn2/audio/njics/2018/8/5/3351-1533475249_7.73094e+08.wav
Upload: /home/ocsn2/audio/njics/2018/8/5/3351-1533475249_7.73094e+08.wav
Remove files
LAME 3.99.5 64bits (http://lame.sf.net)
polyphase lowpass filter disabled
Encoding /home/radio/trunk-player/audio_files/3351-1533475249_7.73094e+08.wav
      to /home/radio/trunk-player/audio_files/3351-1533475249_7.73094e+08.mp3
Encoding as 8 kHz single-ch MPEG-2.5 Layer III (2.3x) average 56 kbps qval=3
    Frame          |  CPU time/estim | REAL time/estim | play/CPU |    ETA
    42/42    (100%)|    0:00/    0:00|    0:00/    0:00|   277.25x|    0:00
  8 [ 0]
 16 [ 0]
 24 [ 0]
 32 [ 0]
 40 [ 1] ***
 48 [13] **********************************
 56 [27] **********************************************************************
 64 [ 1] ***
-------------------------------------------------------------------------------
   kbps       mono %     long switch short %
   53.3      100.0        64.3  19.0  16.7
Writing LAME Tag...done
ReplayGain: -11.3dB
Remove files
[2018-08-05 09:21:03.009415] (info)   [njics]   TG: - (3727)    Freq: 7.732813e+08      Ending Recorded Call - Last Update: 4s  Call Elapsed: 14
[2018-08-05 09:21:03.009773] (info)     - Stopping P25 Recorder Num [4] TG: - (3727)    Freq: 7.732813e+08      TDMA: false     Slot: 0
[2018-08-05 09:21:03.009934] (info)   Running upload script: ./encode-upload.sh /home/ocsn2/audio/njics/2018/8/5/3727-1533475249_7.73819e+08.wav
Encoding: /home/ocsn2/audio/njics/2018/8/5/3727-1533475249_7.73819e+08.wav
Upload: /home/ocsn2/audio/njics/2018/8/5/3727-1533475249_7.73819e+08.wav
[2018-08-05 09:21:03.461315] (info)   [njics]   TG: 3727        Freq: 7.732813e+08      TG not in Talkgroup File
[2018-08-05 09:21:03.461578] (info)     - Starting P25 Recorder Num [4] TG: - (3727)    Freq: 7.732813e+08      TDMA: false     Slot: 0
[2018-08-05 09:21:03.461880] (info)   [njics]   TG: - (3727)    Freq: 7.732813e+08      Starting Recorder on Src: rtl=1
LAME 3.99.5 64bits (http://lame.sf.net)
polyphase lowpass filter disabled
Encoding /home/radio/trunk-player/audio_files/3727-1533475249_7.73819e+08.wav
      to /home/radio/trunk-player/audio_files/3727-1533475249_7.73819e+08.mp3
```

THE FRONTEND

The frontend is hosted on a simple Ubuntu 16.04 VPS on a cloud hosting provider.

- Django web framework
- Nginx as a reverse proxy to daphne
- trunk-player handles the scanning interface

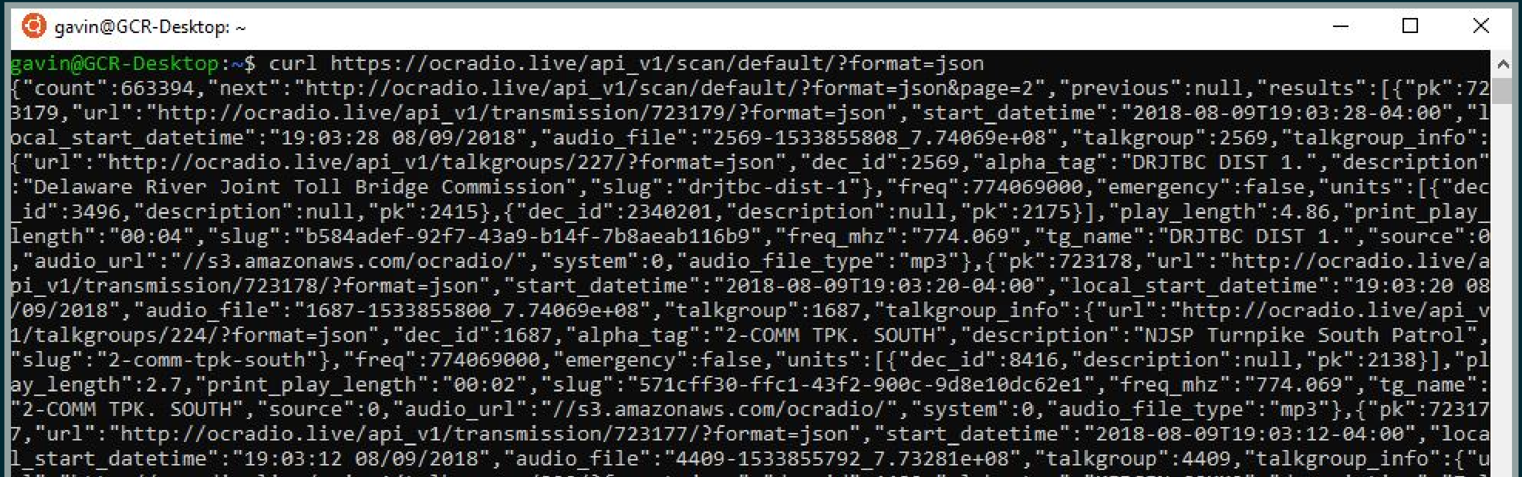
BRINGING IT ALL TOGETHER

- trunk-recorder reads in the JSON configuration file for the system(s) and allocates recorders on multiple RF channels within the SDR’s bandwidth.
- A bash script passes the transmissions along with JSON metadata to the frontend server, where it is written to a database.
- The transmissions are uploaded to Amazon S3 for storage and deleted from the frontend.

A REST API ENDPOINT FOR EVERY RADIO SYSTEM

Example request:

curl https://ocradio.live/api_v1/scan/default/?format=json



```
gavin@GCR-Desktop:~$ curl https://ocradio.live/api_v1/scan/default/?format=json
{"count":663394,"next":"http://ocradio.live/api_v1/scan/default/?format=json&page=2","previous":null,"results":[{"pk":72
3179,"url":"http://ocradio.live/api_v1/transmission/723179/?format=json","start_datetime":"2018-08-09T19:03:28-04:00","l
ocal_start_datetime":"19:03:28 08/09/2018","audio_file":"2569-1533855808_7.74069e+08","talkgroup":2569,"talkgroup_info":
{"url":"http://ocradio.live/api_v1/talkgroups/227/?format=json","dec_id":2569,"alpha_tag":"DRJTBC DIST 1.","description"
:"Delaware River Joint Toll Bridge Commission","slug":"drjtbc-dist-1"},"freq":774069000,"emergency":false,"units":[{"dec
_id":3496,"description":null,"pk":2415},{"dec_id":2340201,"description":null,"pk":2175}],"play_length":4.86,"print_play_
length":"00:04","slug":"b584adef-92f7-43a9-b14f-7b8aeab116b9","freq_mhz":"774.069","tg_name":"DRJTBC DIST 1.","source":0
,"audio_url":"//s3.amazonaws.com/ocradio/","system":0,"audio_file_type":"mp3"},{"pk":723178,"url":"http://ocradio.live/a
pi_v1/transmission/723178/?format=json","start_datetime":"2018-08-09T19:03:20-04:00","local_start_datetime":"19:03:20 08
/09/2018","audio_file":"1687-1533855800_7.74069e+08","talkgroup":1687,"talkgroup_info":{"url":"http://ocradio.live/api_v
1/talkgroups/224/?format=json","dec_id":1687,"alpha_tag":"2-COMM TPK. SOUTH","description":"NJSP Turnpike South Patrol",
"slug":"2-comm-tpk-south"},"freq":774069000,"emergency":false,"units":[{"dec_id":8416,"description":null,"pk":2138}],"pl
ay_length":2.7,"print_play_length":"00:02","slug":"571cff30-ffc1-43f2-900c-9d8e10dc62e1","freq_mhz":"774.069","tg_name":
"2-COMM TPK. SOUTH","source":0,"audio_url":"//s3.amazonaws.com/ocradio/","system":0,"audio_file_type":"mp3"},{"pk":72317
7,"url":"http://ocradio.live/api_v1/transmission/723177/?format=json","start_datetime":"2018-08-09T19:03:12-04:00","loca
l_start_datetime":"19:03:12 08/09/2018","audio_file":"4409-1533855792_7.73281e+08","talkgroup":4409,"talkgroup_info":{"u
```

CONCLUSION

SDR can break down cost & complexity barriers to monitoring public safety radio systems. SDR combined with web services can allow receiving setups previously not possible with past hardware radios.

SITE DEMONSTRATION + Q & A