ADS-B SDR Workshop

David “Karit” Robinson
TuskCon 2018

whoami

- David Robinson
- @nzkarit
- Penetration Tester at ZX Security in Wellington
- Enjoy SDR and physical (e.g. lock picking)

Before we start

- If you want to play along with workshop parts
- There is a VM I can pass around on thumb drive
  - The same one I said was available for download the other day
  - This is all setup ready to go
  - Though may be worth doing a “git pull” , see running.md on the desktop
- If want to set up yourself see https://github.com/nzkarit/tuskcon-2018-vm
  - That Repo has the setup instructions and also the commands to make it work
  - (Happy for pull requests (or bugs) if doesn’t work for you)

Today

- ADS-B Background
- SDR ADS-B Receiving
- SDR ADS-B Broadcast
- Making it more hacker friendly
- What the Aviation Industry is doing

ADS-B

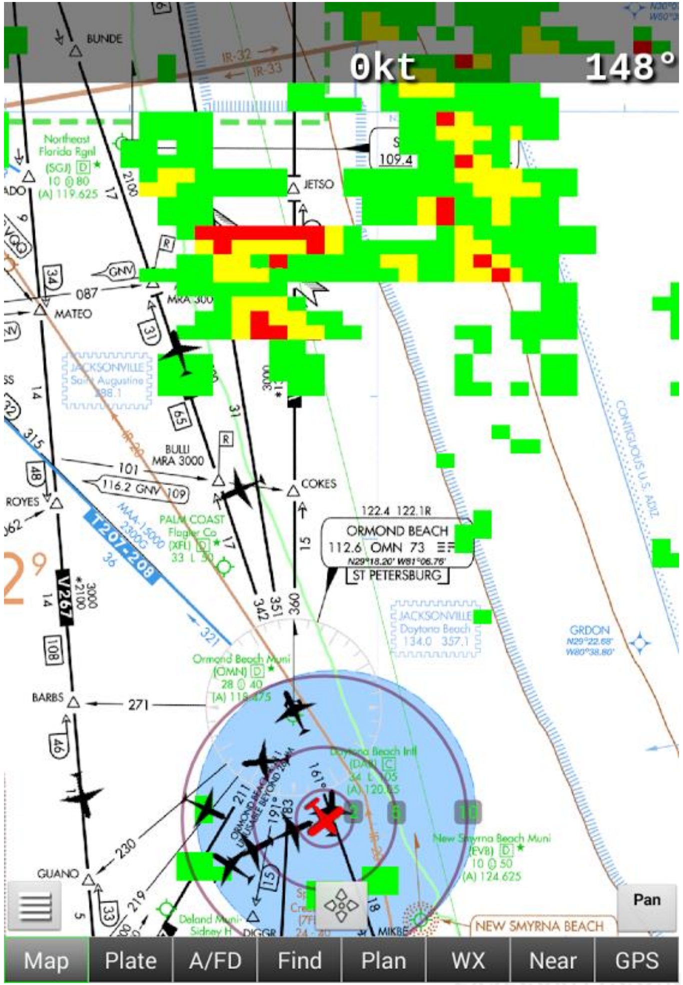
- Automatic dependent surveillance – broadcast (ADS-B)
- The new* standard for how plane report their location to ATC (Air Traffic Control)
    - ID, Latitude, Longitude, Altitude (plus some other things)

* And by new I mean:

    - Standard from 2002
    - US by 2020 for A, B, C and part of E Air Space
    - Aussie 2013 for >=29000 feet
    - NZ 2018-12-31 >=24500 feet, 2021-12-31 Controlled Airspace
        - https://www.nss.govt.nz/dmsdocument/18-ads-b-in-new-zealand-faqs
    - Aviation is a slow system to pick up new standards

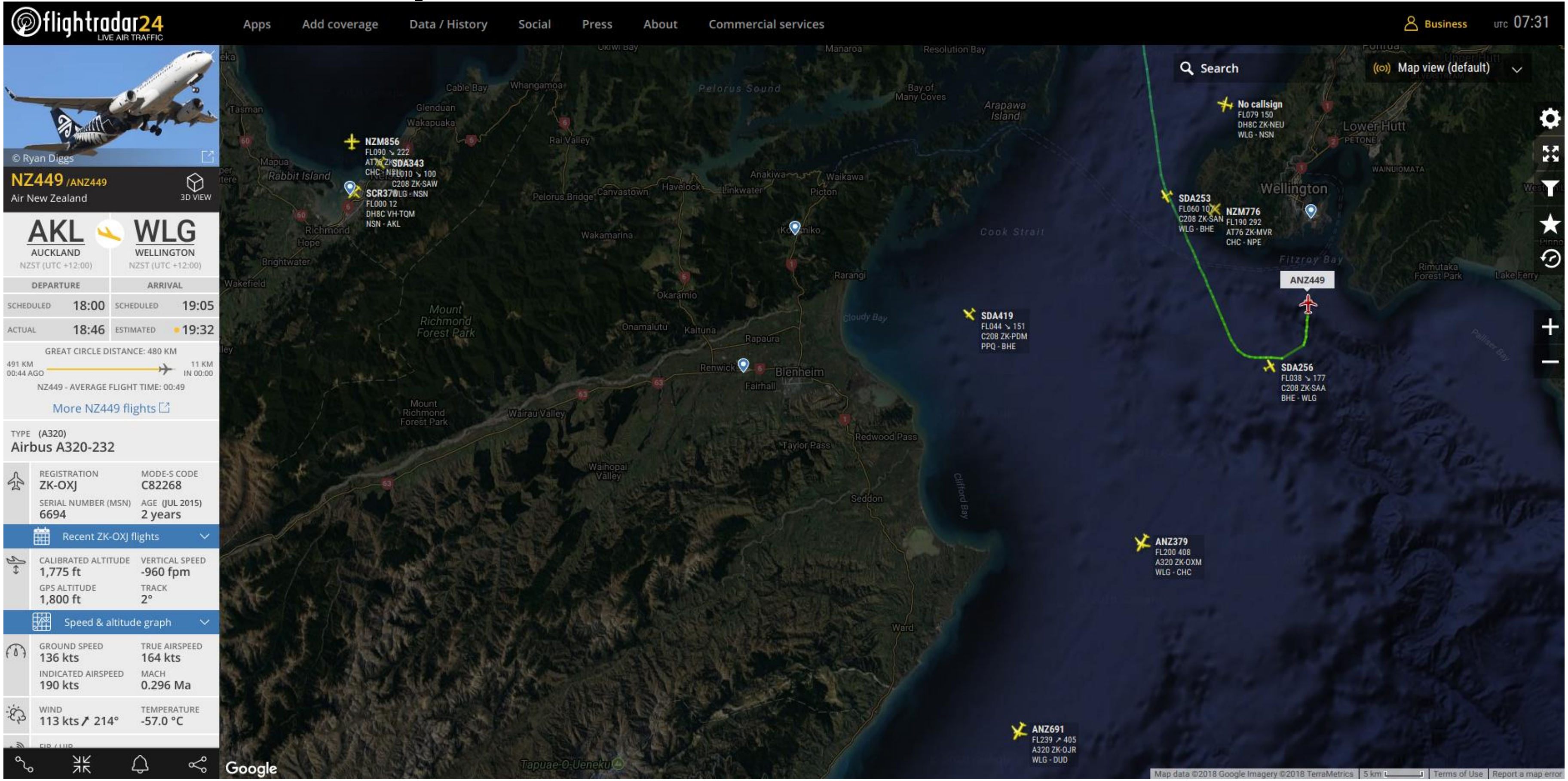
ADS-B Terms

- ADS-B Out – When a plane or ground vehicle broadcasts ADS-B messages
- ADS-B In – An ADS-B receiver e.g. Air Traffic Control, a plane with a moving map



http://sportysnetwork.com/ipad/files/2015/09/Avare2.pn
g

ADS-B Example



NZ449 /ANZ449
Air New Zealand

AKL	WLG
AUCKLAND	WELLINGTON
NZST (UTC +12:00)	NZST (UTC +12:00)

DEPARTURE		ARRIVAL	
SCHEDULED	18:00	SCHEDULED	19:05
ACTUAL	18:46	ESTIMATED	19:32

GREAT CIRCLE DISTANCE: 480 KM

491 KM
00:44 AGO

11 KM
IN 00:00

NZ449 - AVERAGE FLIGHT TIME: 00:49

More NZ449 flights

TYPE (A320)
Airbus A320-232

REGISTRATION ZK-OXJ	MODE-S CODE C82268
SERIAL NUMBER (MSN) 6694	AGE (JUL 2015) 2 years

Recent ZK-OXJ flights

CALIBRATED ALTITUDE 1,775 ft	VERTICAL SPEED -960 fpm
GPS ALTITUDE 1,800 ft	TRACK 2°

Speed & altitude graph

GROUND SPEED 136 kts	TRUE AIRSPEED 164 kts
INDICATED AIRSPEED 190 kts	MACH 0.296 Ma
WIND 113 kts ↗ 214°	TEMPERATURE -57.0 °C

History of Surveillance

- Primary Surveillance – RADAR
    - Spinning RADAR dish
    - Radio signal bounces off Plane
- Secondary Surveillance
    - Mode A/B, C, S
    - When RADAR sweeps the plane it can return more information e.g.
        - Squawk
        - Altitude
        - ID
        - Autopilot settings
        - Weather

Where ADS-B sits

- It is an extension of Mode-S message format
- Sometime referred to as Mode-S ES (Extender Squitter)
- Different from previous forms as it broadcasts all the time opposed to when requested by a RADAR

ADS-B Message

- An ADS-B message is actually two Mode-S data packets
- It is broadcasted at 1Hz
    - So each plane sends two Mode-S ES messages per second

- It sends two messages because the 112 bits per message is not enough for all the data needed
- Need both messages to get the full location details
    - Can roughly infer location from one message

ADS-B Message

- 1090MHz
- Pulse Position Modulation (PPM)
- One bit per µs
- 8µs of preamble
- 112µs of data

Receiving Messages

- RTL-SDR
- dump1090
    - https://github.com/MalcolmRobb/dump1090

Workshop – dump1090

- running.md has the commands to run
- Fingers crossed there are some flights near by
  - (Don’t worry we will make our own planes later)

- Will need an RTLSDR for this

Broadcast

- The following tool on GitHub can perform the broadcast
- https://github.com/lyusupov/ADSB-Out

- Works well out of the box
    - Though is tied to the hackRF

My Changes

- Broke it up into class files (was a singular Python file before)
  - Basically as a way to help me learn what it was doing
  - Tried to add notes and comments when I figured out what was going on
  - Hopefully easier for others to pick up now
- Added
  - Config file
  - Command line flags
  - CSV import
- Made a CSV generator

- My repo https://github.com/nzkarit/ADSB-Out

Safety Considerations

- 1090MHz is licensed spectrum and can be regarded as Safety of Life
- Do NOT broadcast on 1090MHz
- Use an ISM band
  - The example on GitHub/my example command scripts use the ISM band
- 915MHz is fine in NZ and Aussie
  - Example commands all use this
- 915-928MHZ
- https://www.rsm.govt.nz/about-rsm/spectrum-policy/gazette/gurl/short-range-devices
- https://www.acma.gov.au/Industry/Spectrum/Radiocomms-licensing/Class-licences/shortrange-spreadspectrum-devices-fact-sheet

Workshop – ADS-B Broadcast

- Commands in running.py

- You will need a hackRF for the broadcast
- If you have a RTLSDR you can listen to the others broadcasting

Yawn Broadcast

- *Yawn* I can broadcast a plane at one location, boring
- I want to broadcast all the planes, locations, etc

- Take in a CSV file
- Will broadcast one message per row
- If a column is not specified it will populate based on default in config
  - So you can focus testing on a singular item

- Gotcha: big files can take a while to convert into radio
  - Chunk it
  - Possible because it puts it all in memory then gets swapped out
  - Want to fix by making it realtime (more on that later)

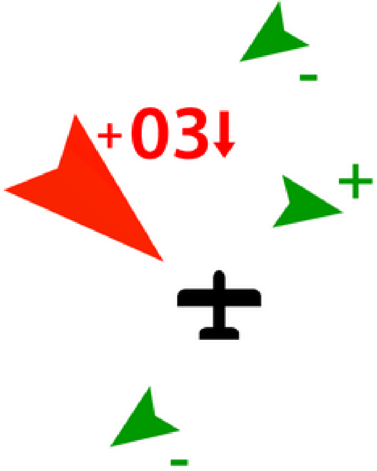
Workshop – Generate a CSV

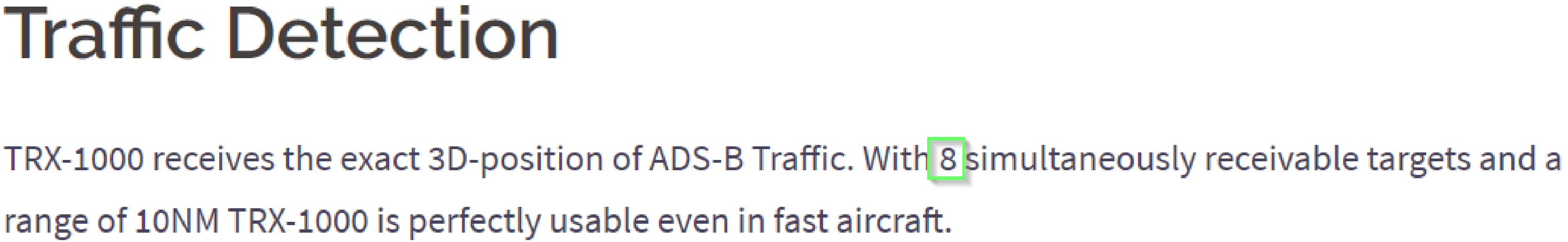
- Have some scripts which generate all the possible:
  - ICAOs
  - Latitudes

Where to?

- These changes have been made to make it more friendly for me to do stuff with an attackers hat on
- The problem is I don't have a plane or an Air traffic Control tower

Then a Moving Map says





Traffic Detection

TRX-1000 receives the exact 3D-position of ADS-B Traffic. With 8 simultaneously receivable targets and a range of 10NM TRX-1000 is perfectly usable even in fast aircraft.

http://nzsoaring.solutions/trx-1000/

Air Services Australia

- TAAATS has been upgraded to process as many as 1,000 ADS-B flights simultaneously from up to 200 ground stations.
  - http://www.airservicesaustralia.com/projects/ads-b/tracking-ads-b/

Adding soapySDR

- This is library which should allow broadcast at generation time
- Also will make the support for other transmitters easy, so could use
  - LimeSDR
  - LimeSDR Mini
  - BladeRF
  - Etc
- If anyone has experience in and could give me some pointers that would be awesome
  - Always open to pull requests ☺

Why haven’t people talked this?????

- There have been many talks about ADS-B not being signed
  - RenderMan has some good ones
- Aviation is slow to pick up new standards
- Even then ADS-B isn’t a new standard , its just shoehorned in Mode-S 112 bit packets
  - No room for a signature
- How are you going to do PKI for planes?
  - CA sign each new plane and do revoke lists somehow
  - Every plane has every other plane’s public key
  - Planes don’t have reliable internet connections and pilots just want to fly
    - Not wait for updates on reboot like Window’s Updates

Timeline

- Considering ADS-B not mandatory yet and has been rolled out for years
- Even if they were to make an ADS-B v2, looking at 20+ years most likely for a change
- So standard can’t change, we need to look at other ways

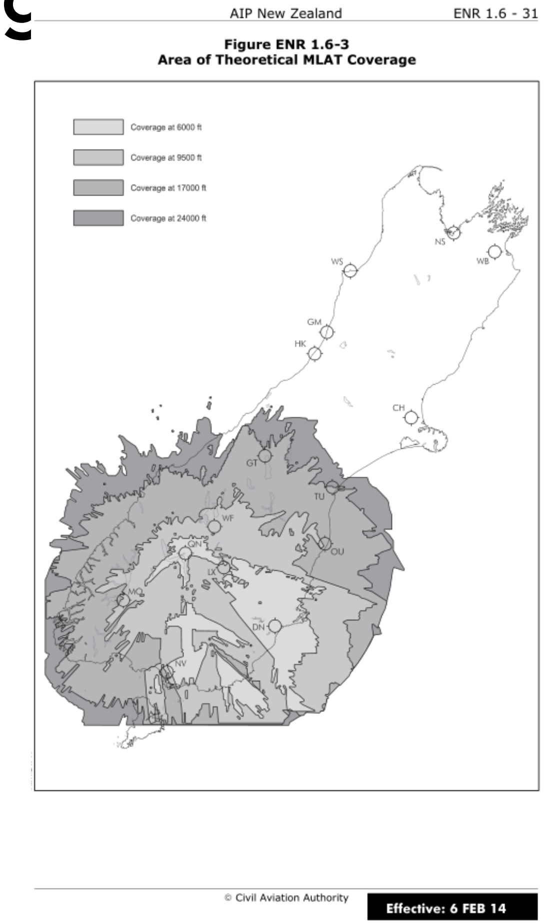
Defence

- ATC on ground can do MLAT

MLAT

- Time Difference of Arrival
- Requires four+ with a known clock

NZ MLAT Coverage



AIP New Zealand ENR 1.6 - 31

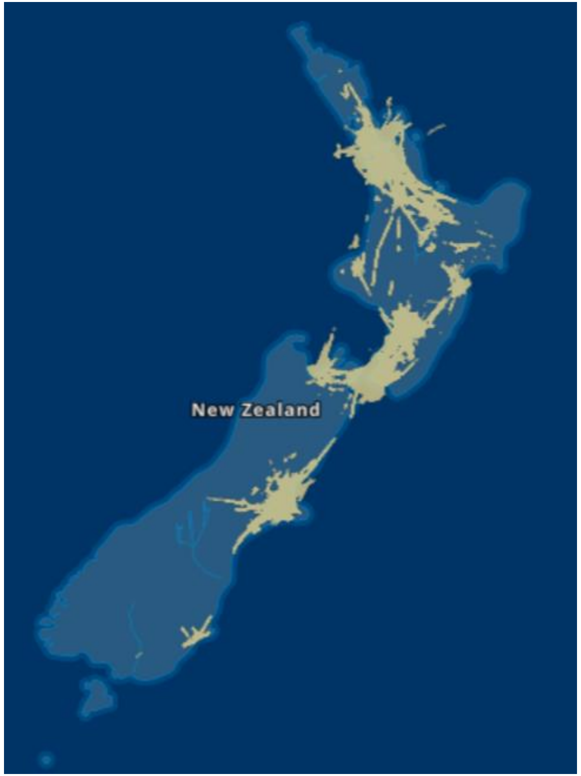
Figure ENR 1.6-3
Area of Theoretical MLAT Coverage

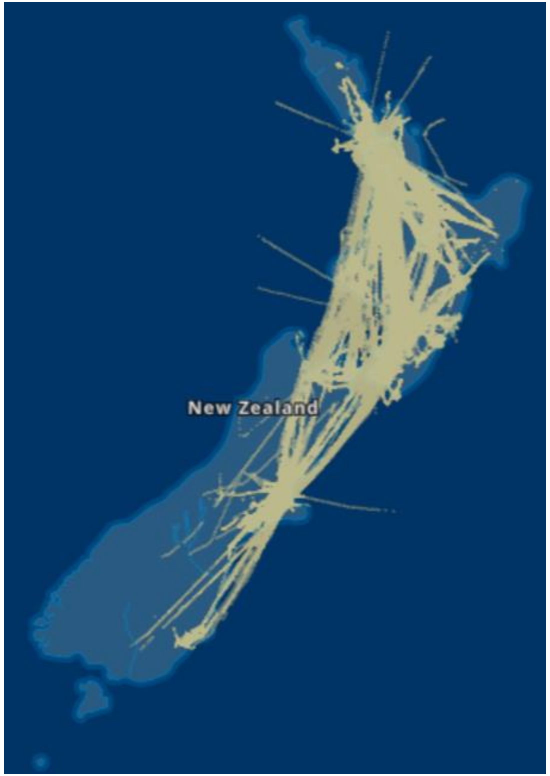
© Civil Aviation Authority

Effective: 6 FEB 14

http://www.aip.net.nz/pdf/ENR_1.6.pdf

Flightaware MLAT Coverage





https://flightaware.com/adsb/coverage#data-coverag

On planes with ADS-B In

- Only a single receiver and needs to be standalone
- Can’t do MLAT

TCAS

- Traffic collision avoidance system
- Does have direction checking
- But haven’t seen ADS-B In with this
    - My understand is that planes are using single antennas

Other Research

- Lots of people have talked about this
- Haven’t seen research on attacking the ADS-B in hardware
- For a long time the aviation regulators said “don’t worry we know about this and we don’t see it as a real issue”

- In November 2017 there was finally a report from the aviation industry which mentioned risk, but no real mitigation for ADS-B issues other than MLAT or TCAS
    - No ADS-B v2 talk
    - ICAO and FAA have private lists of ADS-B security issues and mitigations
    - http://www.atlanticcouncil.org/images/Aviation_Cybersecurity_web_1107.pdf

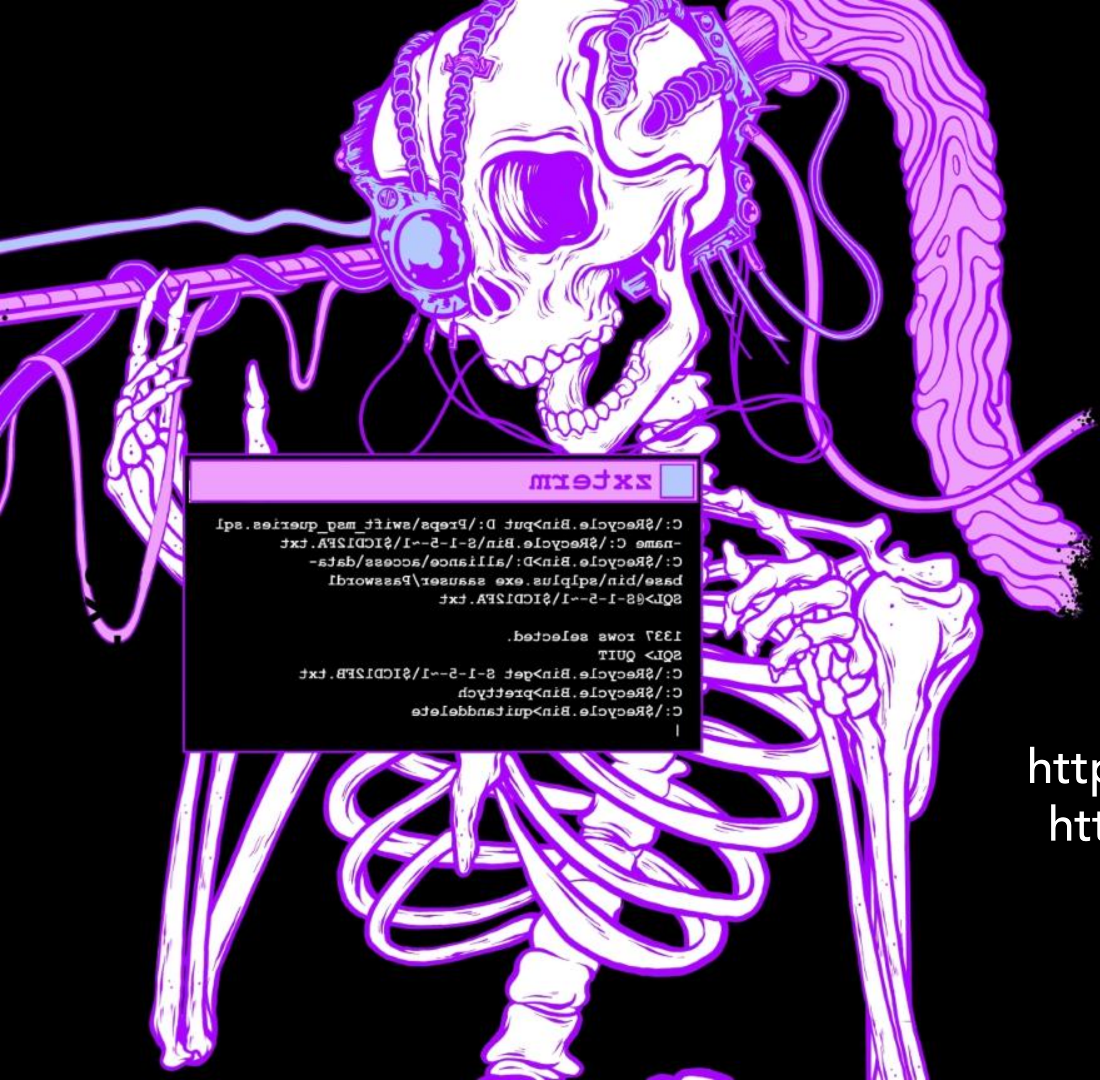
Further work for me

- Get a copy of ADS-B standard, which is behind a paywall ☹
- Extending Tool
  - More CSV
  - SoapySDR
- Getting hands on hardware
  - So I can test against actual hardware
- TCAS uses PPM as well so may be able to leverage the code base
  - Get standard
  - Get device
  - Find decoding software

- More than happy to talk and work with people on this

Takeaway

- You don’t have to understand SDR to a high level to think about and attack it
- It is fine to extend code that is available to make it more hacker friendly
  - You don’t only have to do research with a blank piece of paper



```
C:/$Recycle.Bin>put D:/Preps/swift_msg_queries.sql
-name C:/$Recycle.Bin/S-1-5--1/$ICD12FA.txt
C:/$Recycle.Bin>D:/alliance/access/data-
base/bin/sqlplus.exe saauser/Password1
SQL>@S-1-5--1/$ICD12FA.txt

1337 rows selected.
SQL> QUIT
C:/$Recycle.Bin>get S-1-5--1/$ICD12FB.txt
C:/$Recycle.Bin>prettych
C:/$Recycle.Bin>quitanddelete
|
```

End

Thanks
@nzkarit

https://github.com/nzkarit/ADSB-Out
https://github.com/nzkarit/tuskcon-2018-vm