

building a cyber range in GCP

- and -

the magic of 10 meter ham radio



**IF YOU GET KIDS INTERESTED IN
AMATEUR RADIO**



**THEY WILL NEVER HAVE MONEY
FOR ALCOHOL OR DRUGS**

Tom Costello

@kd9cpb@infosec.exchange

he/him/his

kd9cpb.com

Panckakescon3 backup speaker, Pancakescon4 actual speaker!

Slides at github.com/kd9cpb/slides

Who's this dude and what is a cyber range?

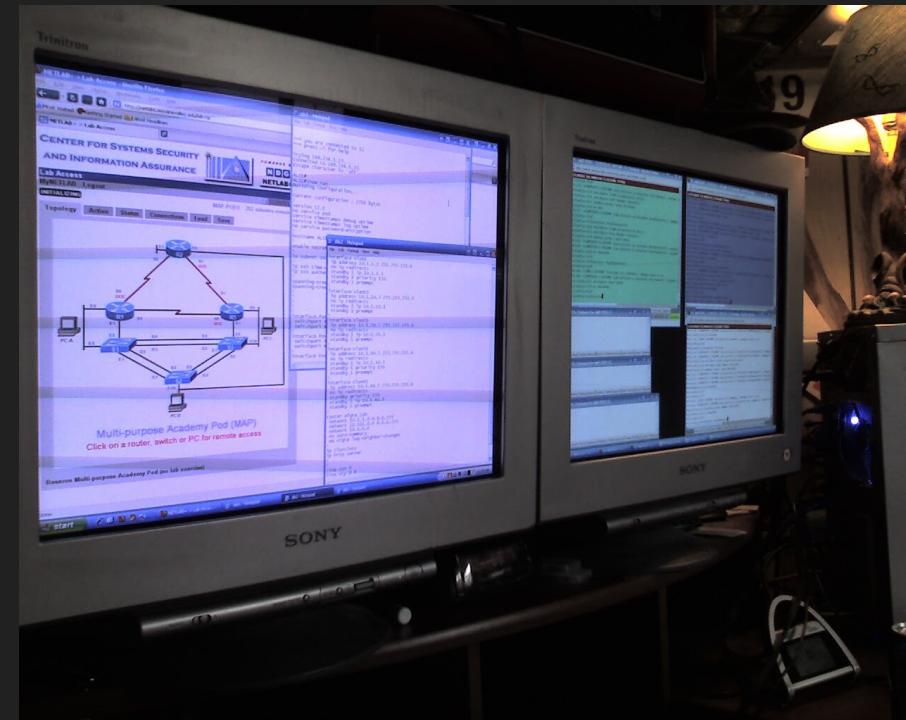


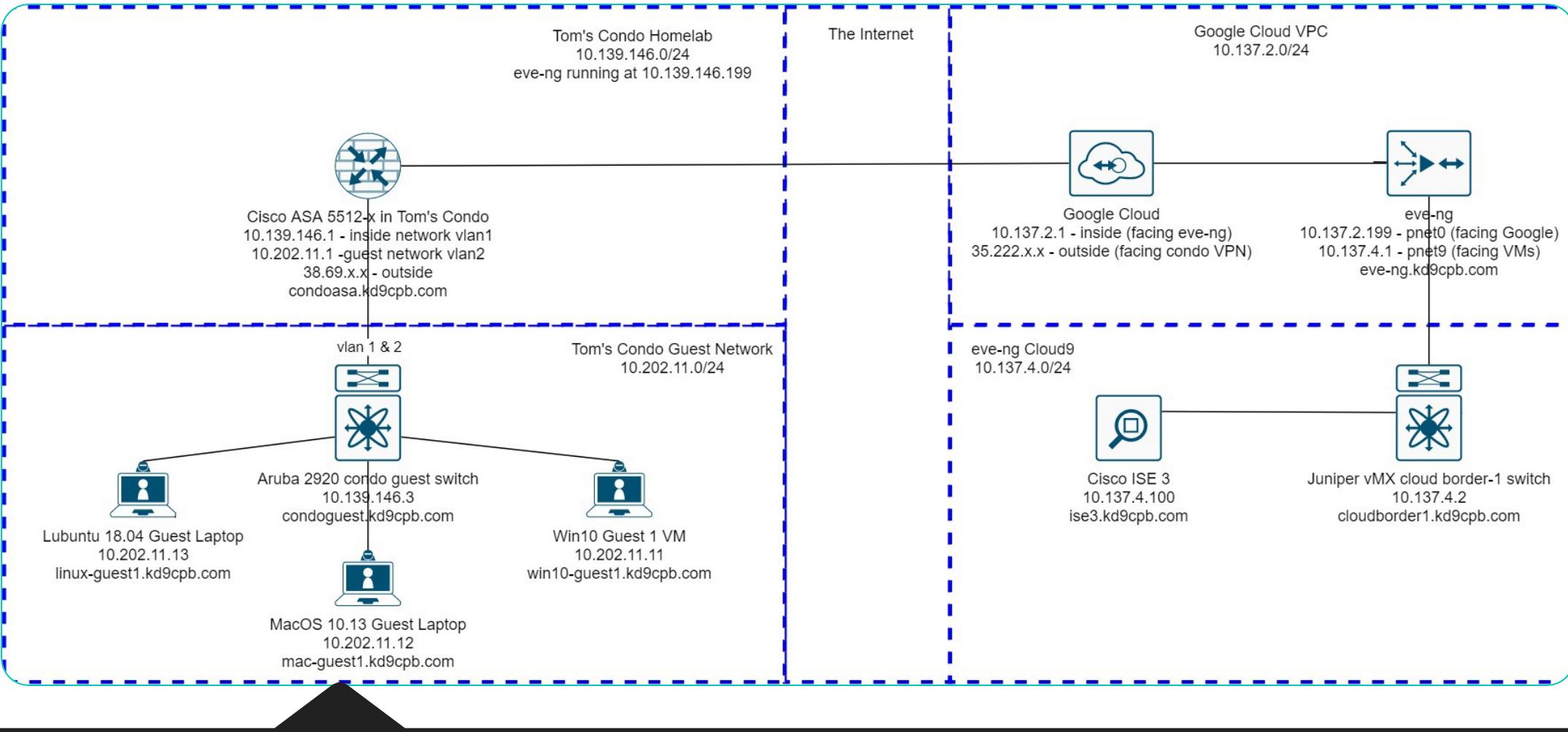
- Been into network security since DC14 + BackTrack Linux days
- Blue Team FTW
- Boring "views & opinions" disclaimer goes here

- “A cyber range is a controlled, interactive technology environment where up-and-coming cybersecurity professionals can learn how to detect and mitigate cyber attacks using the same kind of equipment they will have on the job.”
- cybersecurityguide.org

Humble Cyber Range Beginnings

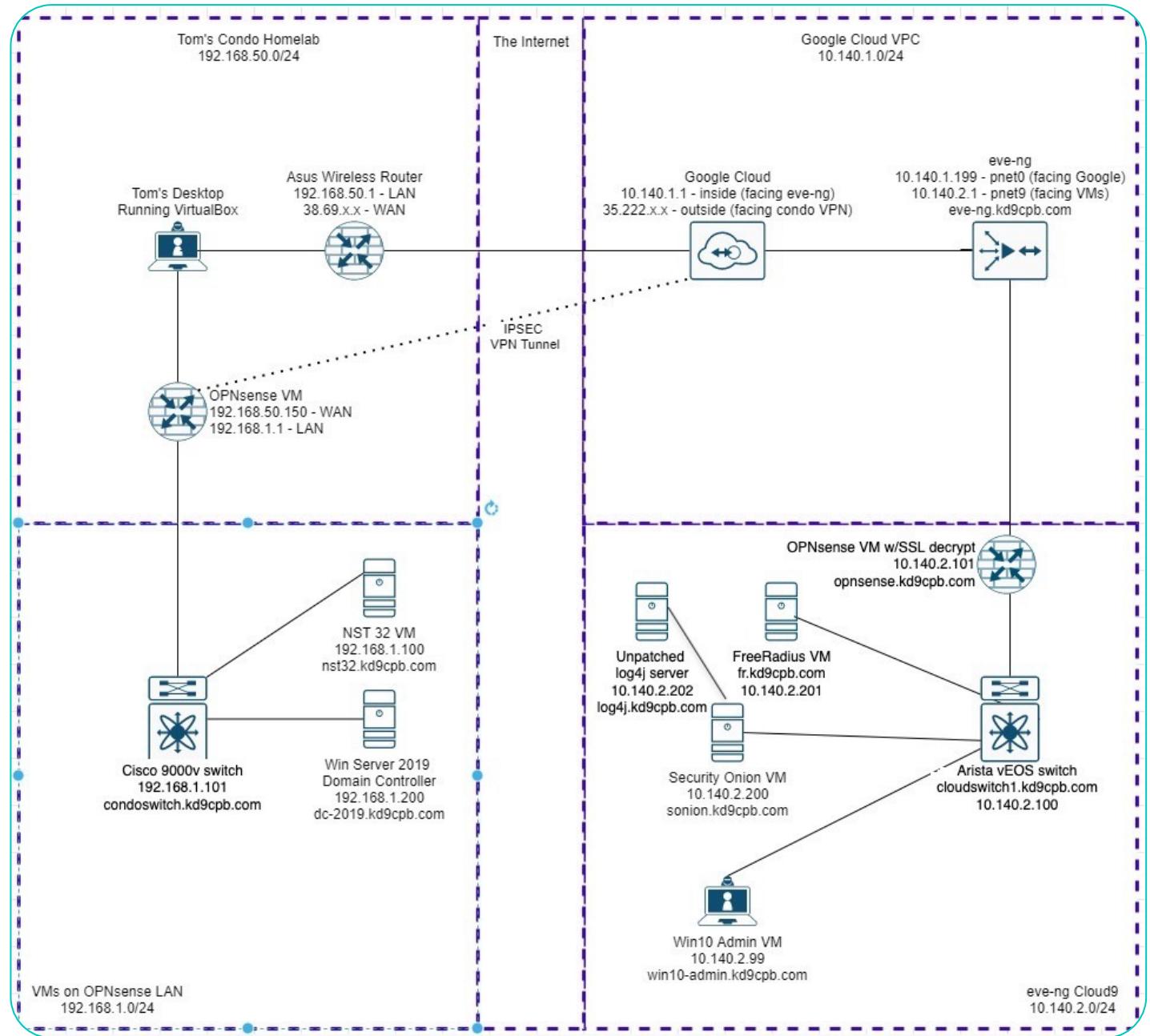
- I've been doing network security homelabs since mid-2000's, they aren't super exciting





A GCP cyber range is born

- Thanks to new gig in Summer 2020, found out about eve-ng in GCP as cyber range
- This is exciting! Can add things to home wifi that can access things in cyber range
- \$300 Google Cloud New Customer Credit FTW



Doing it with free-ish stuff only

2 ways to connect btwn home & cyber range



2 different ways to BYO GCP cyberrange

- Option 1: Tony E's videos at
<https://youtu.be/aiATWfvyJmE>
- Best if you want to get running ASAP
- Just works out of the box, no messy tunneling
- This is the blue pill
- Option 2: my blog at
<https://kd9cpb.com/opnsense-eve-gcp>
- Best if you want to really learn GCP networking
- It's messy, but you will learn a ton about cloud networks & OPNsense firewall
- This is the red pill



So you built a GCP cyber range, now what?

- Write your own Python/Ansible automation to do your work for you per <https://kd9cpb.com/automate-gcp-eve>
- See if your favorite NGFW/IDS actually detects vulns log4j, Bluekeep, etc. on an unpatched system in range
- Try different network vendor's stuff for free per <https://ethancbanks.com/free-networking-lab-images-from-arista-cisco-nvidia-cumulus/>
- Test if an ACL or security policy change breaks stuff without breaking things in the real-world
- Eve-ng isn't the only game in town; check out containerlab or gns3 too

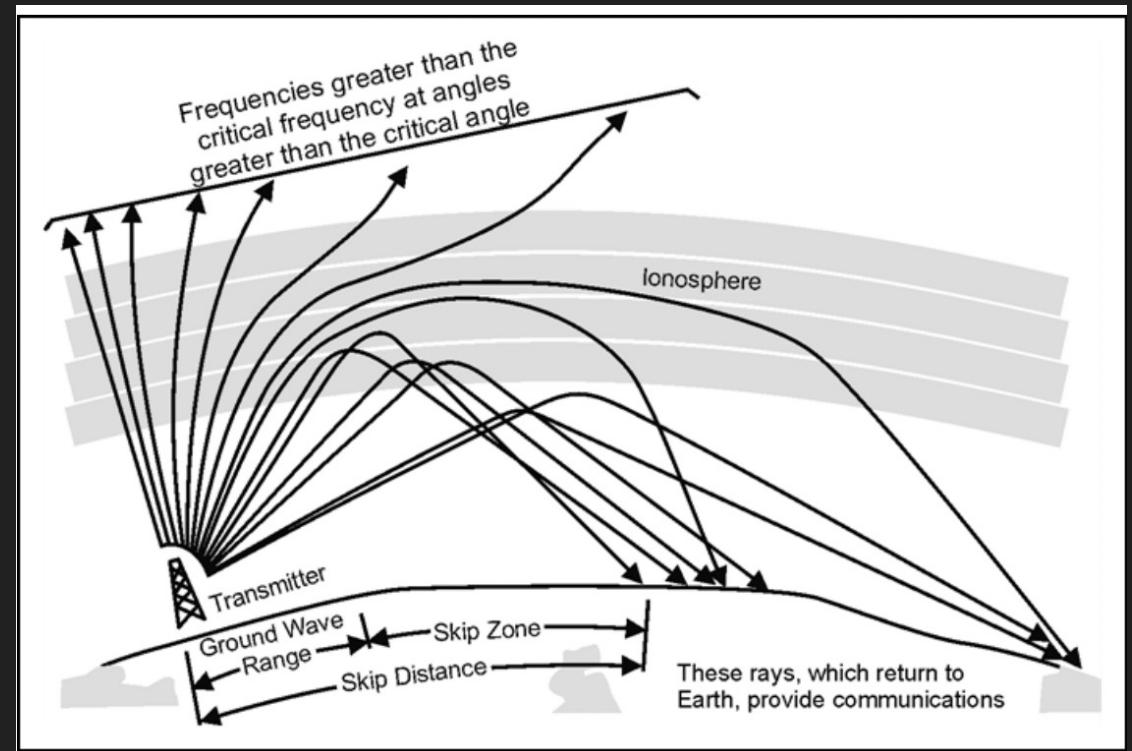




Please type
cyberrange
Questions
into Slack
now before
we go into
radio fun!

The magical 10 meter band in ham radio

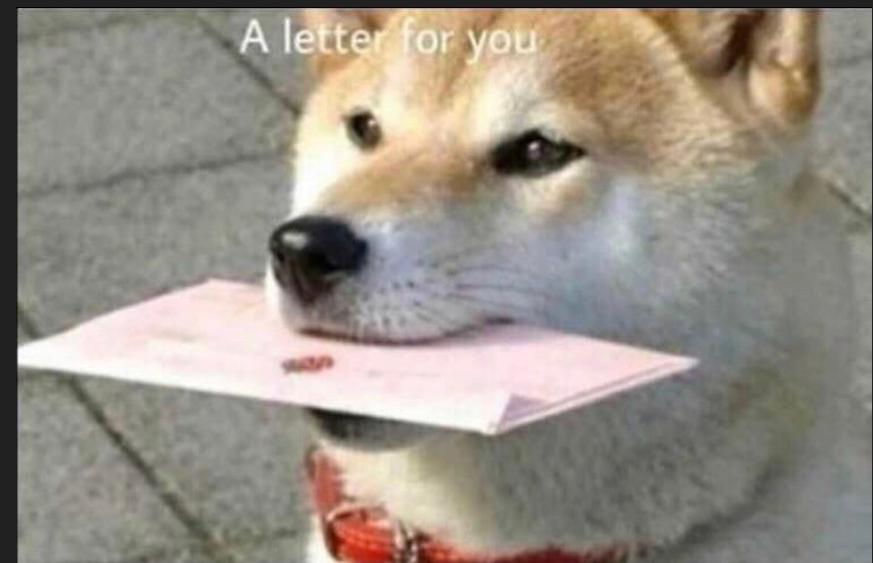
- Full story of why HF is awesome at
https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN20819_ATP_6-02x53_FINAL_WEB.pdf



How do I start blasting RF into the ionosphere?

- Step 1: Get a ham radio license
- Step 2: Get a radio, antenna and adapters
- Step 3 (optional): Get WSJT-X working on your computer
- Step 4 (optional): Get QSL cards or electronic logbook

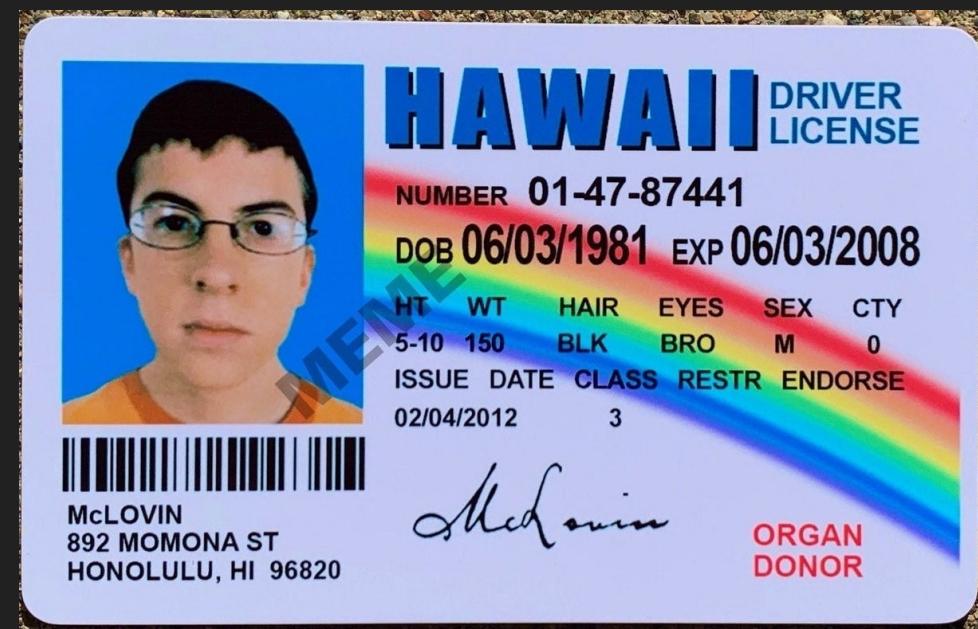
If you just want to take a listen for now, buy an SDR dongle (should be less than \$50, search rtl-sdr or nooelec smart)



**RF is
just
wiggly air**

Step 1: Getting a license

- Either web search for “Chicago ham radio volunteer examiner” (substituting out Chicago for your town, unless you are in Chicago)
- Or do it online (proctored) via orgs like <https://kl7aa.org/vec/> and <https://www.w5yi.org/>
- Use hamstudy.org (or similar) to memorize technician question pool



Step 2: Get a radio, antenna, adapters

- Option 1: Go cheap and get a 10 meter ham radio
- <https://kd9cpb.com/10m-ft8> blabs about this, it'll cost between \$150 – 450
- If you don't like it, you can put it all back on eBay at a small loss
- This is the blue pill



- Option 2: Go fancy with an expensive all-band HF ham radio with a tuner
- <https://kd9cpb.com/g90> has my all-band setup if you're curious, \$500+ to get started
- "Buy once, cry once" if you get General level license (way more studying)
- This is the red pill



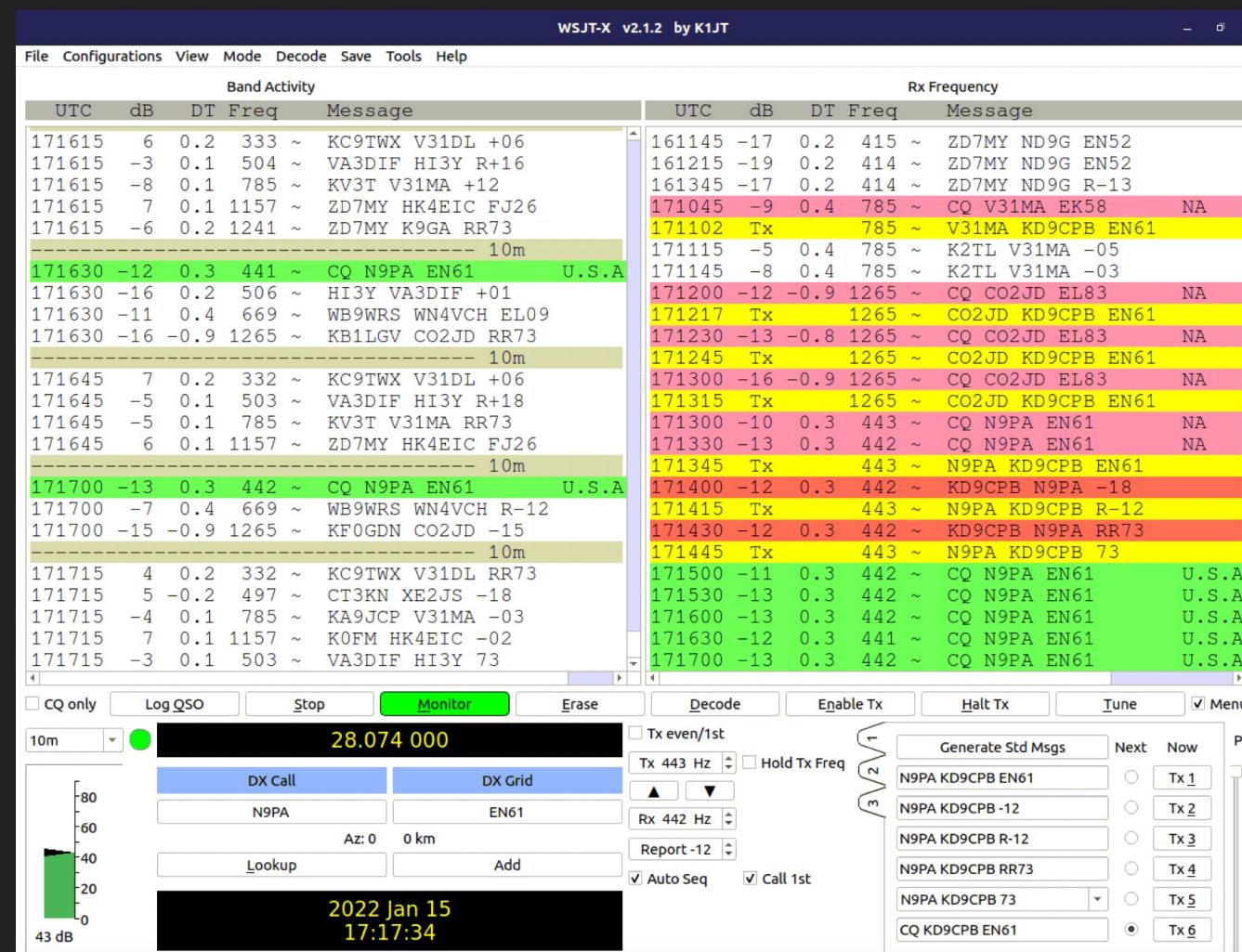
Step 3: WSJT-X

- Makes magical bagpipe noises from your computer's mic jack
- Listens for magical bagpipe noises from around the world
- When you send and receive noises, it counts as a QSO!
- Similar programs like JS8call exist to have actual conversations with the world
- No morse code required
- YouTube Tutorials are your friend

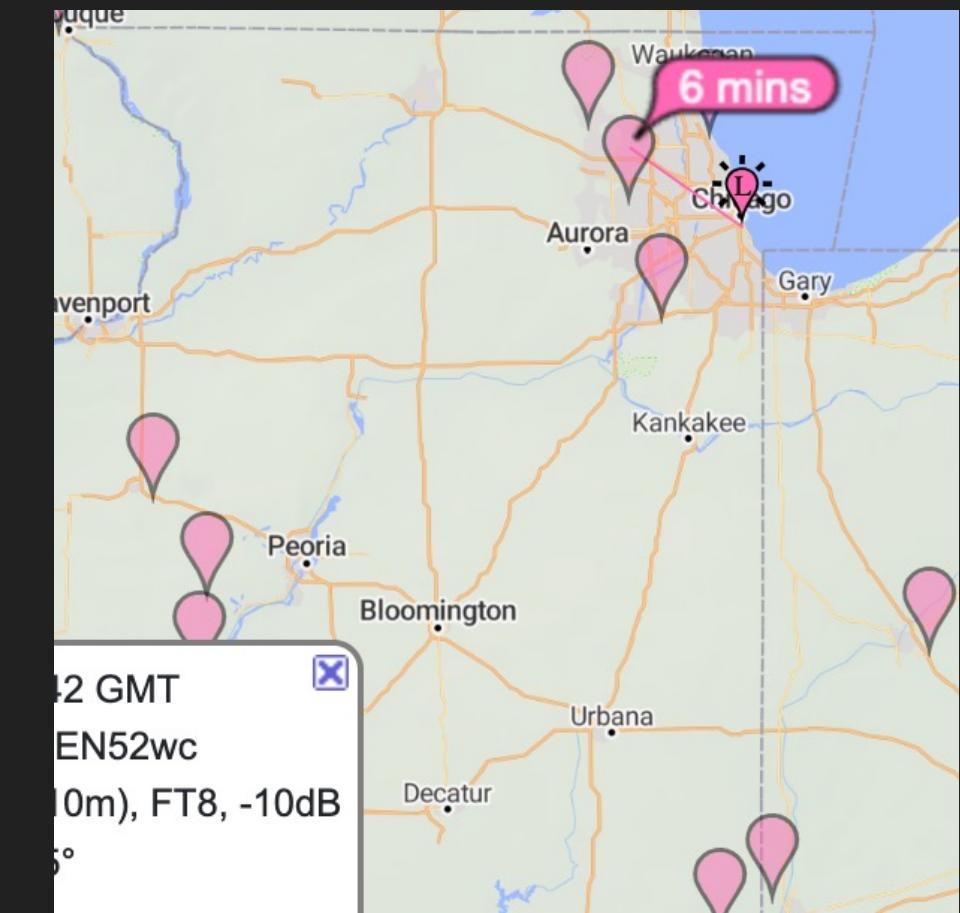
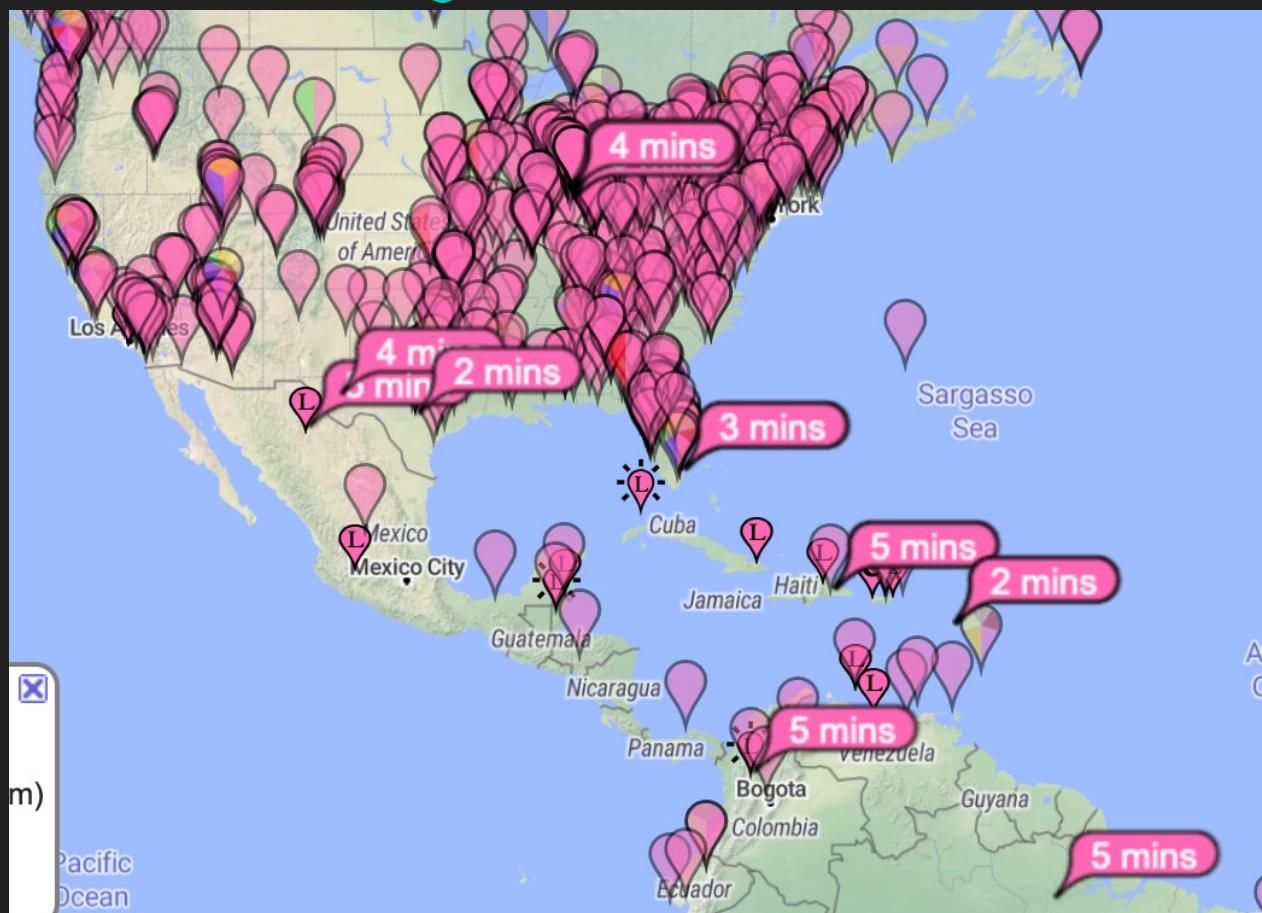


| | | |
|-----------|-----------|-------------|
| A ● - | J ● - - - | S ● ● ● |
| B - ● ● ● | K - ● - | T - |
| C - ● - ● | L ● - ● ● | U ● ● - |
| D - ● ● | M - - | V ● ● ● - |
| E ● | N - ● | W ● - - |
| F ● ● - - | O - - - | X - ● ● - |
| G - - ● | P ● - - ● | Y - ● - - |
| H ● ● ● ● | Q - - - ● | Z - - - ● ● |
| I ● ● | R ● - - ● | |

What a good 10 meter FT8 QSO looks like



Your 10 meter milage may vary



Step 4: QSL cards or electronic logging

- QSL cards are a fun hobby but not ideal for privacy
- eQSL services like QRZ, LoTW and eQSL.cc are very popular, no postage!



| | | | | |
|----------------|--|---|-------------------------|-------------------------|
| Serial | 687446856 | Log Date | 2021-10-30 20:48:16 UTC | |
| QSO Start | 2021-10-30 17:45:00 UTC | Confirmed | 2021-10-30 20:15:02 UTC | |
| QSO End | 2021-10-30 17:45:00 UTC | Contest | n/a | |
| Serial | 0 | Serial | 0 | |
| Station Class | |  | | |
| QSL-TO | QSL-FROM | | | |
| Station | VP2EIH | KD9CPB | | |
| Op | IRA HARRIS | Thomas M Costello | | |
| QTH | PO BOX 1206 THE VALLEY, ANGUILLA British West Indies | Chicago | | |
| State | | IL | | |
| Country (DXCC) | Anguilla | USA | | |
| Frequency | 28.074 MHz | 28.074 MHz | Mode | FT8 |
| Power | 0 W | 10 W | Mode | FT8 |
| RST Rcvd | -15 | RST Sent | -12 | |
| Coordinates | 18.229351 N, -63.047791 W | 41.713314 N, -87.756652 W | | |
| Grid | FK881f | EN61cr91 | Distance | 3507km (2179 mi) @ 311° |
| Distance | 3507km (2179 mi) @ 131° | Distance | 3507km (2179 mi) @ 311° | |

Last slide I promise

- Thanks for watching! Slides at github.com/kd9cpb/slides
- Seriously after Pancakescon consider spending your \$300 free GCP credit on building a cyberrange
- Then spend \$300ish real money on 10 meter ham radio gear after the GCP credit runs dry 😊
- Hit me up @kd9cpb@infosec.exchange or qrz.com
- Have a nice day!

