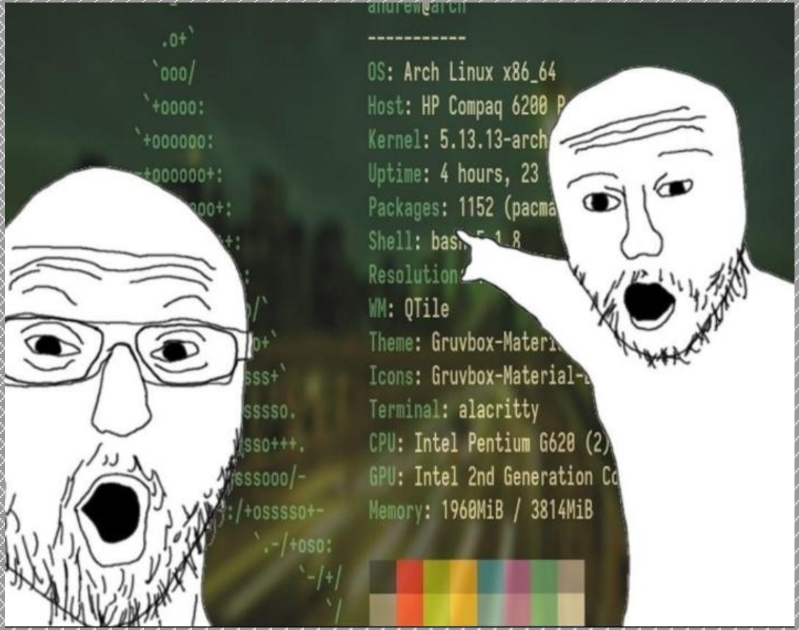
Drinking from the OSINT Firehose

~$ whoami

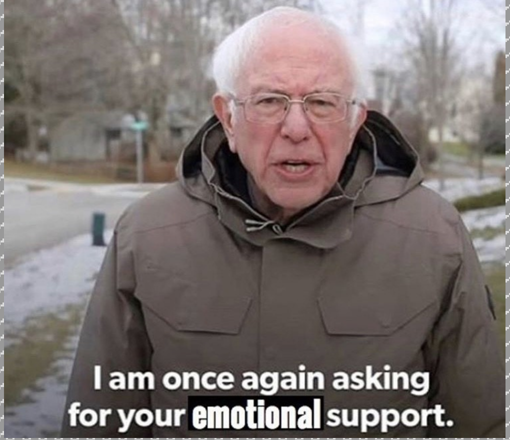
- SFDC Admin
- Linux hobbyist
- Studier of osint
- Aspiring security practicioner



```
                       andrew@arch
       .o+`            -----------
      `ooo/            OS: Arch Linux x86_64
     `+oooo:           Host: HP Compaq 6200 P
    `+oooooo:          Kernel: 5.13.13-arch
    -+oooooo+:         Uptime: 4 hours, 23
        ooo+:          Packages: 1152 (pacma
           +:          Shell: bas   5.1.8
            :          Resolution
           /`          WM: QTile
           o+`         Theme: Gruvbox-Materi
          sss+`        Icons: Gruvbox-Material-
         sssso.        Terminal: alacritty
         sso+++.       CPU: Intel Pentium G620 (2)
        sssooo/-       GPU: Intel 2nd Generation Co
     :/+osssso+-       Memory: 1960MiB / 3814MiB
        `.-/+oso:
             `-/+/
                `/
```

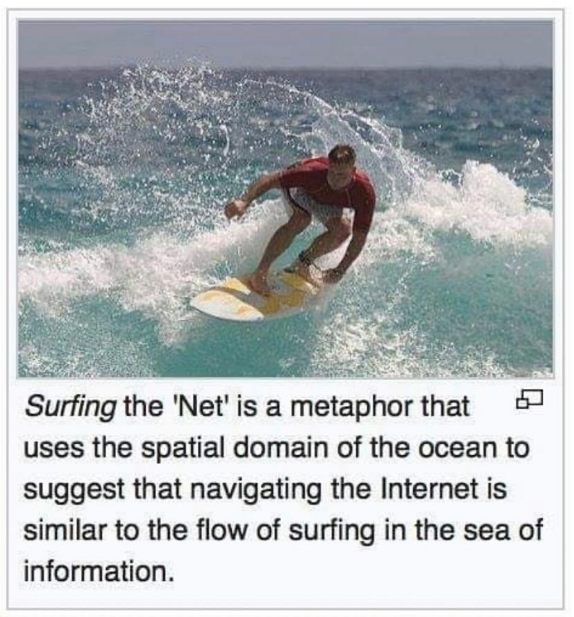
A word on Mental Health..

- Cyberspace 🄯 | Meatspace ®
- Blue Blockers 4 eye health (Ra Optics)
- Sleep / water
- Kids/family/work/divorce/separation/addiction
- Nuclear war ⚛️



Agenda

- whoami
- A word on mental health
- OSINT
- Building an OSINT VM
  - Options & considerations
  - Config and scripts
- TTPs
  - Firefox
    - Critical extensions
  - Some tools I prefer
    - LF (uberzug)
    - PCManFM



Surfing the 'Net' is a metaphor that uses the spatial domain of the ocean to suggest that navigating the Internet is similar to the flow of surfing in the sea of information.

Building an OSINT VM

Goals:

- Replicability
- Independence
- Ease of use
- Preferred tools
- Compartmentalization
- Chaos

Operating Systems & Pre-Configured Options

1) Host system
2) Windows VM
3) Ubuntu VM
4) Kali VM
5) TraceLabs preconfig OSINT VM
6) ???

Hybrid Approach: Bazzell’s tools + my own shenanigans

THE MOST DANGEROUS PHRASE IN THE LANGUAGE IS
1 (800) NEW-WAYZ
UNLEARN
RELEARN
UNDO
REDO
“WE’VE ALWAYS DONE IT THIS WAY.”

- Ubuntu → Debian 11 Bullseye Install
- OSINT book tools – options laid out with commands
- Unique requirements to a pentesting distro:
  - fewer network/script tools, more browser/media focused + reporting (LaTeX and/or Office Suite
  - Templates | templates | templates

Setup

- Download Debian image; VirtualBox
- Manual install of tools
- GUI tweaks
- Update, update
- Reboot, reboot some more
- Save & snapshot
- Add my own tools

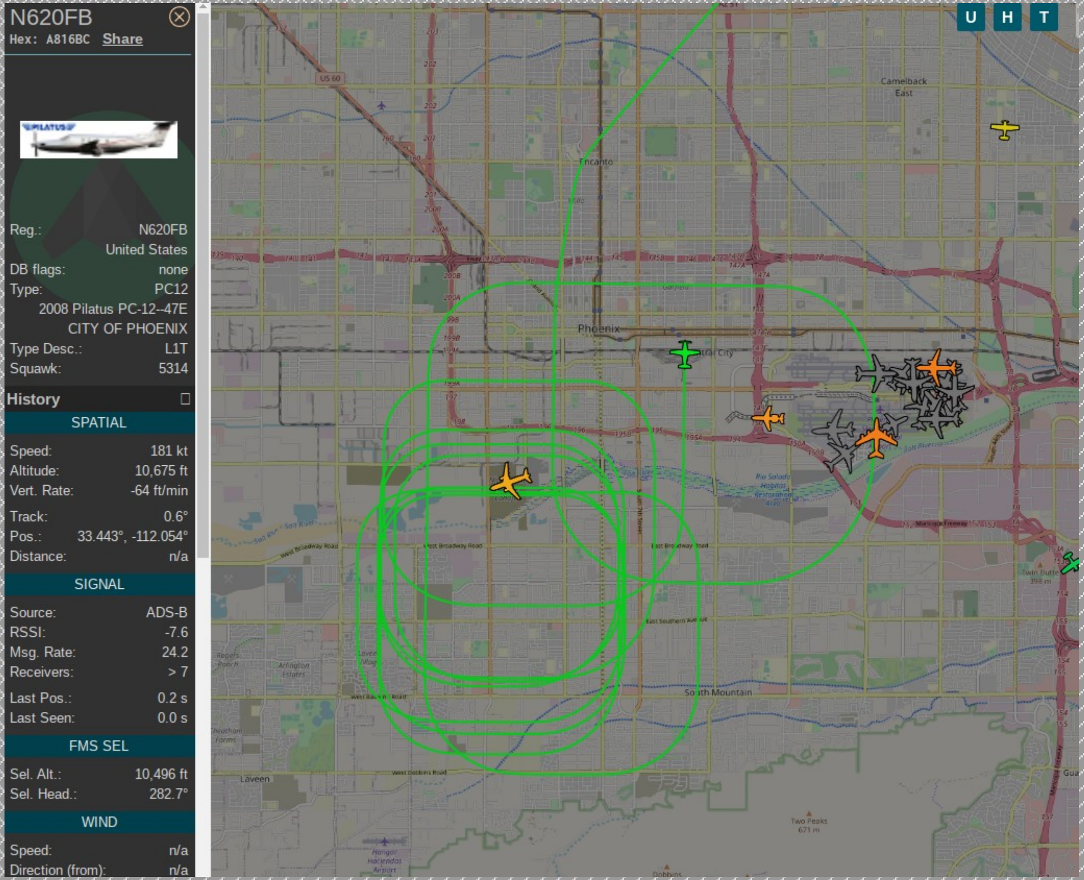
WAITING FOR THE VM TO BOOT
WAITING FOR DEBIAN UPDATES
WAITING FOR YOUR TOOLS TO LOAD

Stumbles and lessons learned

- Not what tool you use but how you use it
- Building your own tools teaches you more tho
- Back up
- Experiment with things
- Try something you wouldn’t normally do

Aircraft OSINT

- ADSB Exchange
- Flightradar24
- SDR
- Google Dorks
-



N620FB

Hex: A816BC Share

Reg.: N620FB

United States

DB flags: none

Type: PC12

2008 Pilatus PC-12--47E

CITY OF PHOENIX

Type Desc.: L1T

Squawk: 5314

History

SPATIAL

Speed: 181 kt

Altitude: 10,675 ft

Vert. Rate: -64 ft/min

Track: 0.6°

Pos.: 33.443°, -112.054°

Distance: n/a

SIGNAL

Source: ADS-B

RSSI: -7.6

Msg. Rate: 24.2

Receivers: > 7

Last Pos.: 0.2 s

Last Seen: 0.0 s

FMS SEL

Sel. Alt.: 10,496 ft

Sel. Head.: 282.7°

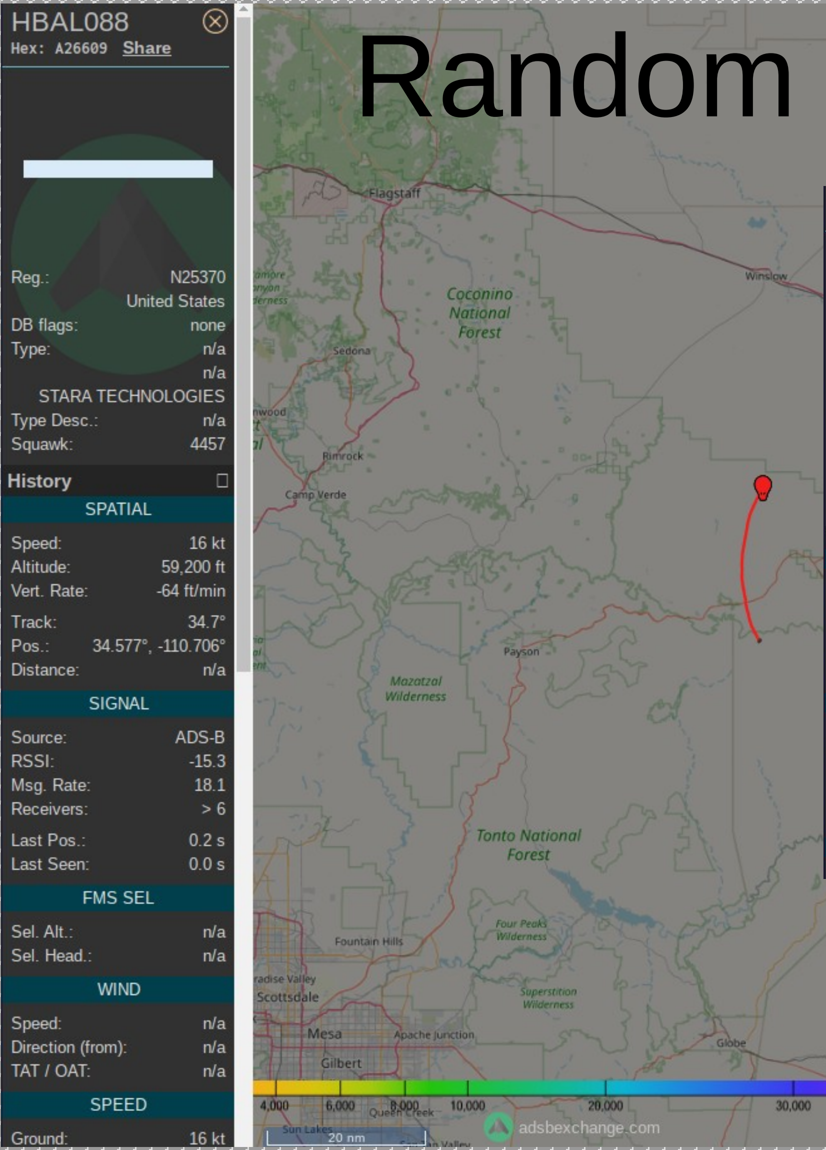
WIND

Speed: n/a

Direction (from): n/a

FAA Docs (74 pgs)

Random things we’ve seen



HBAL088

Hex: A26609 Share

Reg.: N25370
United States
DB flags: none
Type: n/a
n/a
STARA TECHNOLOGIES
Type Desc.: n/a
Squawk: 4457

History

SPATIAL

Speed: 16 kt
Altitude: 59,200 ft
Vert. Rate: -64 ft/min
Track: 34.7°
Pos.: 34.577°, -110.706°
Distance: n/a

SIGNAL

Source: ADS-B
RSSI: -15.3
Msg. Rate: 18.1
Receivers: > 6
Last Pos.: 0.2 s
Last Seen: 0.0 s

FMS SEL

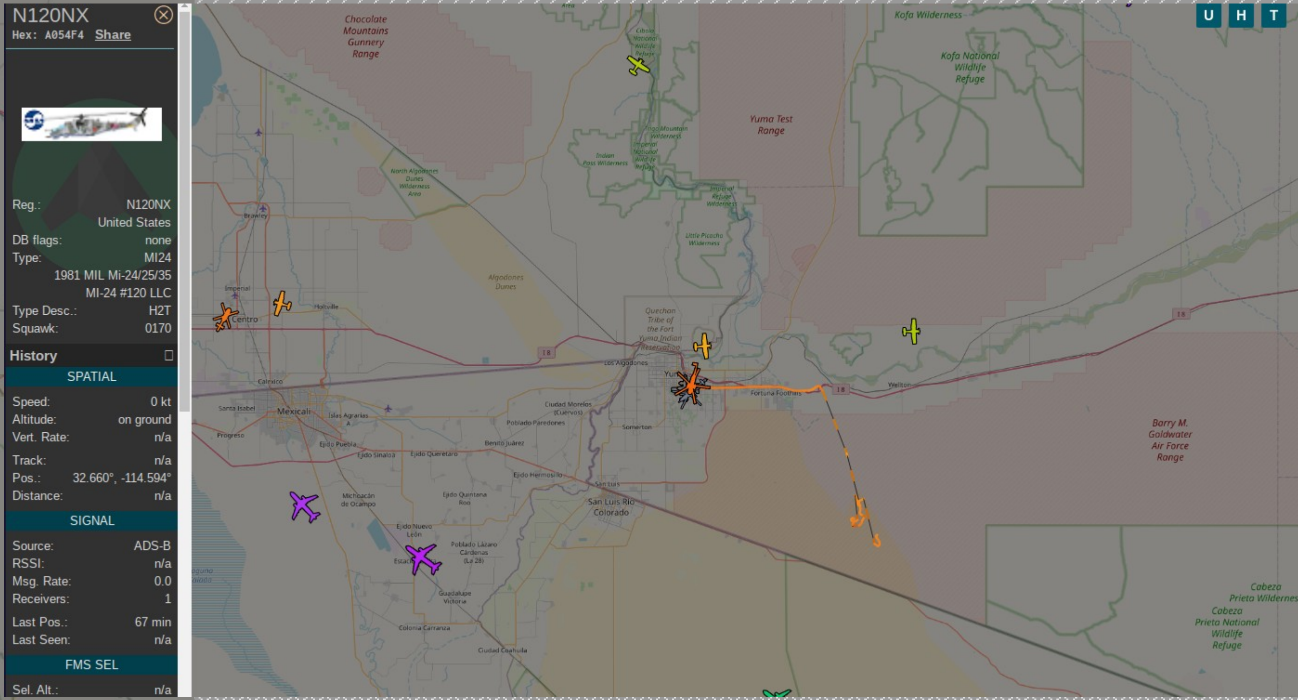
Sel. Alt.: n/a
Sel. Head.: n/a

WIND

Speed: n/a
Direction (from): n/a
TAT / OAT: n/a

SPEED

Ground: 16 kt



N120NX

Hex: A054F4 Share

Reg.: N120NX
United States
DB flags: none
Type: MI24
1981 MIL Mi-24/25/35
MI-24 #120 LLC
Type Desc.: H2T
Squawk: 0170

History

SPATIAL

Speed: 0 kt
Altitude: on ground
Vert. Rate: n/a
Track: n/a
Pos.: 32.660°, -114.594°
Distance: n/a

SIGNAL

Source: ADS-B
RSSI: n/a
Msg. Rate: 0.0
Receivers: 1
Last Pos.: 67 min
Last Seen: n/a

FMS SEL

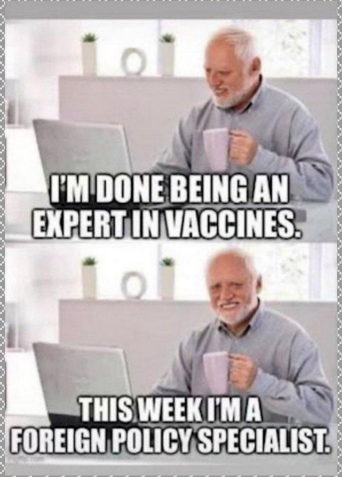
Sel. Alt.: n/a

U
H
T
Chocolate Mountains Gunnery Range
Kofa Wilderness
Kofa National Wildlife Refuge
Yuma Test Range
Algodones Dunes
Imperial
El Centro
Calexico
Mexicali
Wellton
Somerton
San Luis Rio Colorado
Barry M. Goldwater Air Force Range
Cabeza Prieta National Wildlife Refuge

What’s going on in Ukraine?

I lied, I don't have netflix
7780.00
AM
Take off your shoes, we're gonna listen to Russian numbers stations on shortwave radio

Stuff


I'M DONE BEING AN EXPERT IN VACCINES.
THIS WEEK I'M A FOREIGN POLICY SPECIALIST.

- Ukraine Marshal Law
- Russia invades Ukraine
- Air traffic restricted in Ukraine
- India goes over no-fly zone
- Russian Radio comms intercepted on web SDR
- Luxembourg Radar planes
- Threat of nuclear war

Future talk ideas

Ethics of OSINT