Automatic Identification System (AIS)

Gary C. Kessler, Ph.D., CISSP
Fathom5

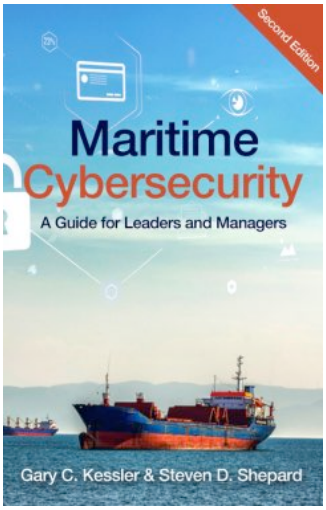
CyberBoat Challenge 2024
Beaufort, SC
December 2024

1

whoami

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

- Non-Resident Senior Fellow, Atlantic Council
- Board of Advisors, Cydome
- Principal Consultant, Fathom5
- Director/Co-Founder, Maritime Hacking Village
- Guest Faculty, USCG Academy
- Chief, Cybersecurity Prevention Operations Division, USCG Auxiliary (AUXCYBER)



50GT Master/Assistance Towing
Master SCUBA Diver Trainer

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

 2

2

Overview

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

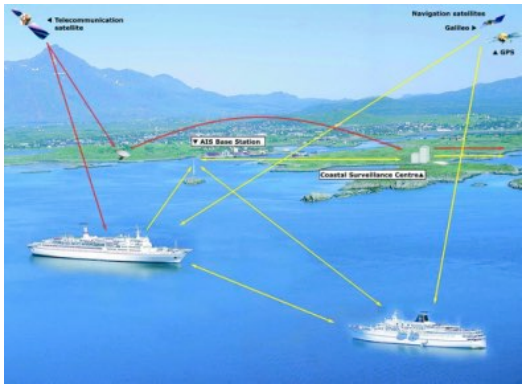
3

AIS Overview

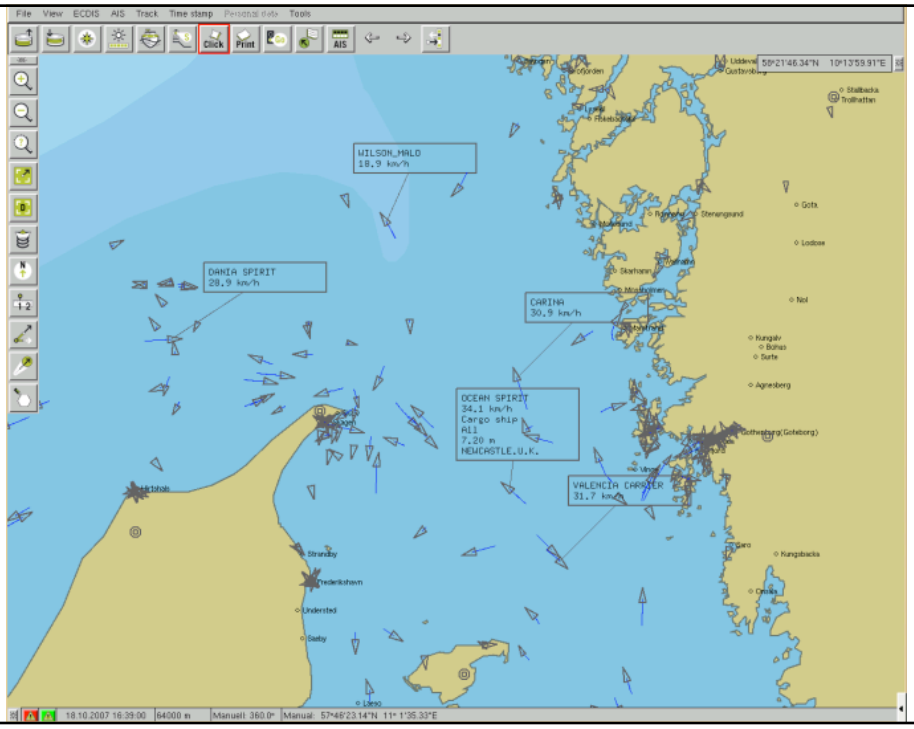
4

Automatic Identification System

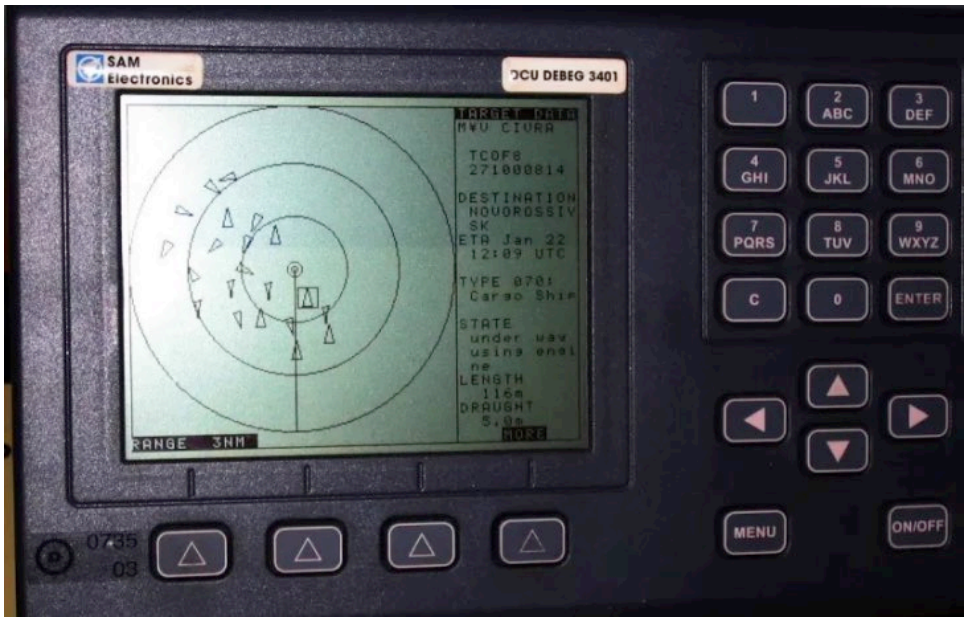
- AIS is a tracking system used by ships and VTMS
  - Provides a ship and maritime administration with situational awareness about area vessel traffic
- AIS provides sender's name, identifier, position, course, heading, speed, ROT, cargo, destination, and more
- Data can be displayed on a screen, ECDIS,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



5



6



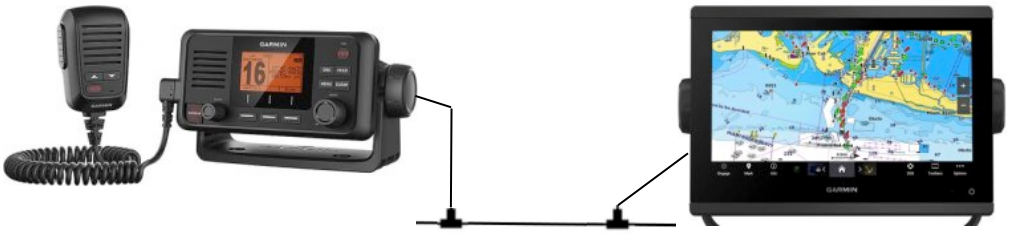
AIS transceiver shows the bearing/distance of nearby vessels in a radar-like display, plus additional vessel information.

7

Case Study: AIS Via VHF Radio

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

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

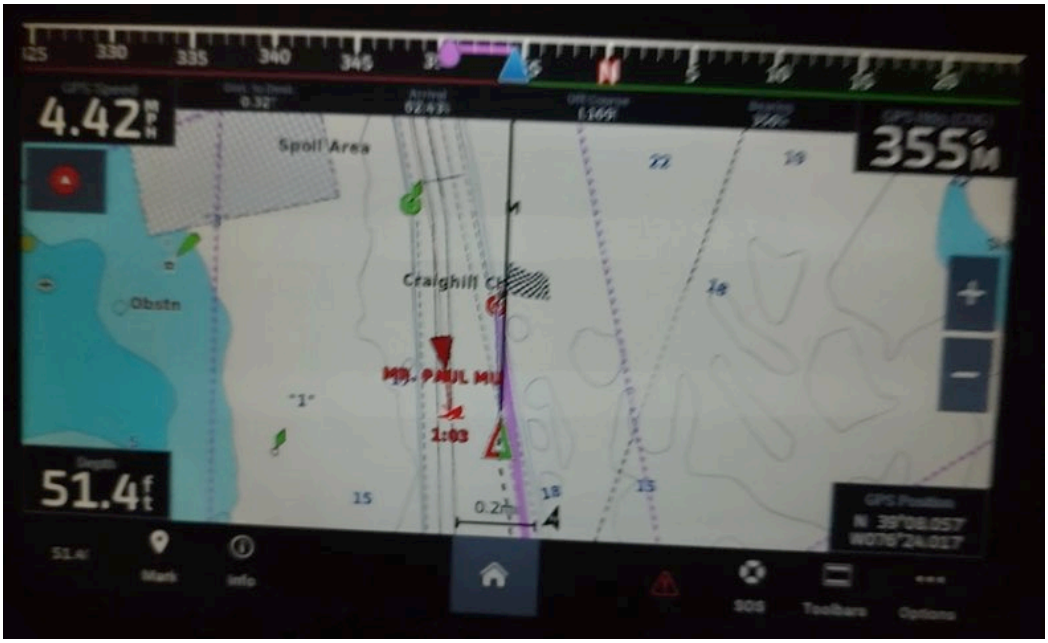


- AIS broadcasts are received by the radio and sent to the chartplotter via NMEA 0183/2000
- AIS targets and detailed information are displayed on the chartplotter.

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

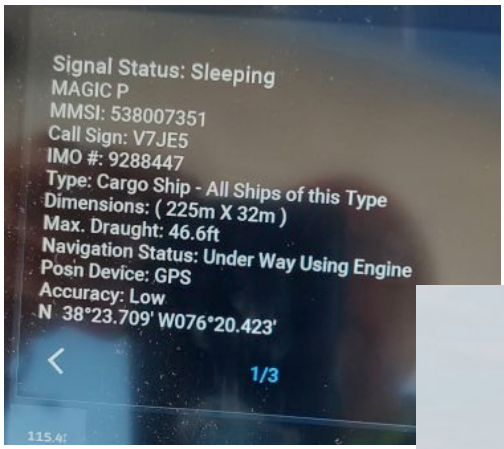
Configuration shown here for demonstration purposes only.
This is neither a product recommendation nor endorsement.

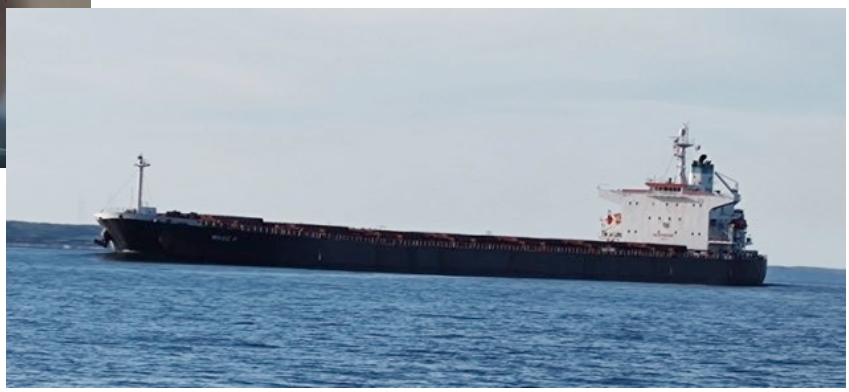
8



 9

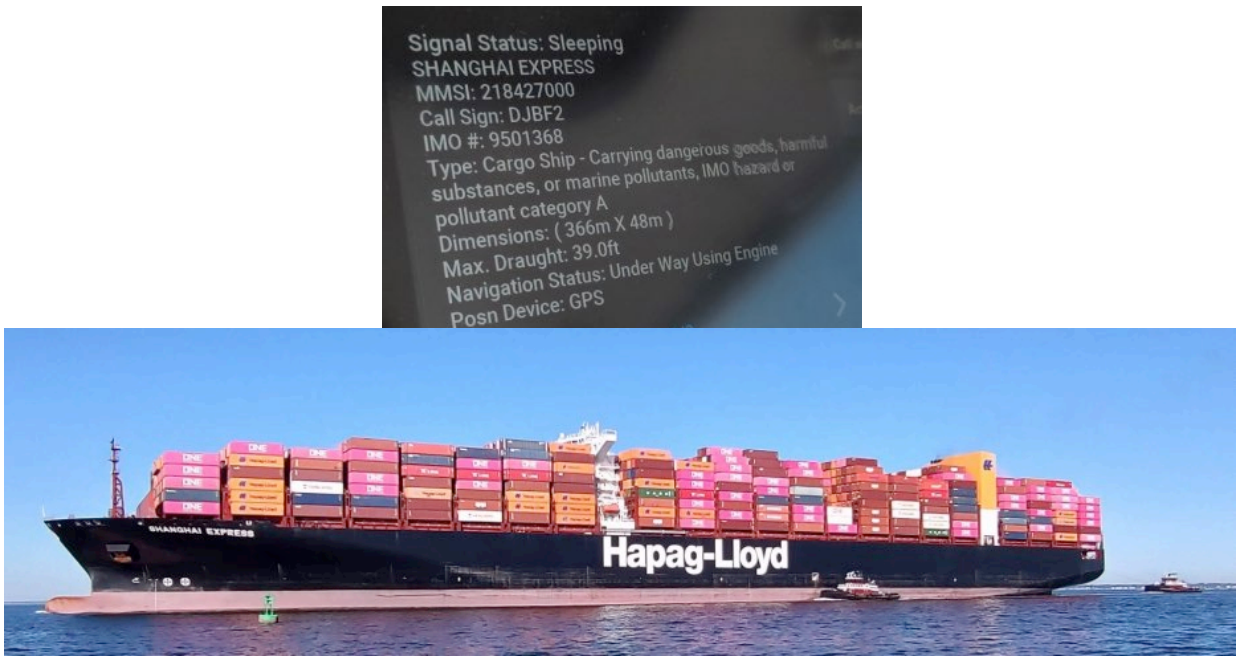
9





 10

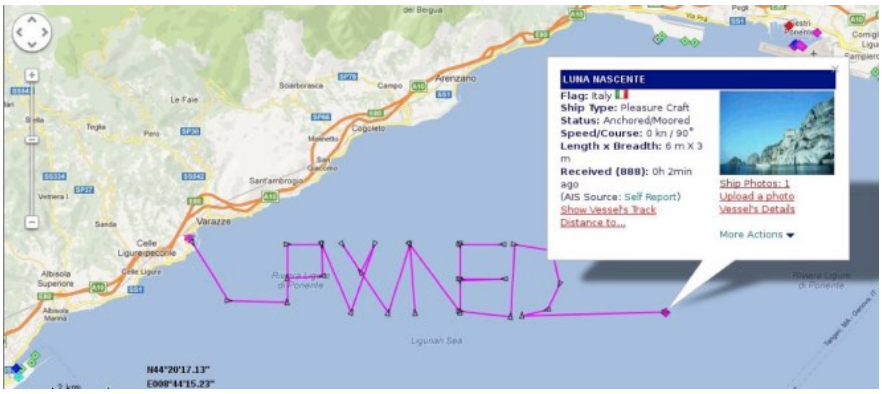
10



Side Note: AIS Requirements

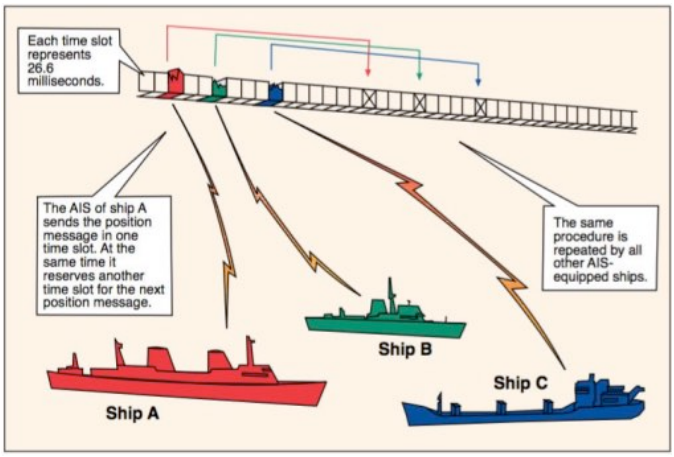
- Defined in 2002 SOLAS, Chapter V, Regulation 19 and, in U.S., 33 CFR 164.46
- In general, AIS is required on:
  - All vessels ≥300 gross tons travelling internationally
  - Commercial power vessels ≥65 ft (20 m)
  - Commercial towing vessels ≥26 ft (8 m) or >600 horsepower
  - Power vessels certified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

Communications Overview and Vulnerabilities



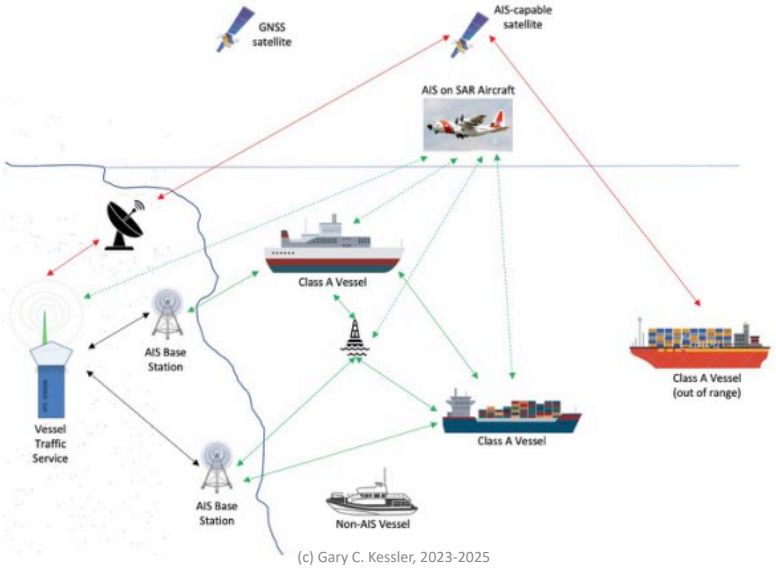
AIS Communication Protocol

- 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)

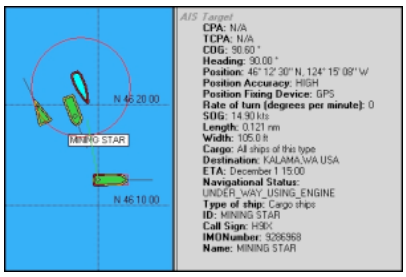
Elements of the AIS Network



15

AIS Security Weaknesses

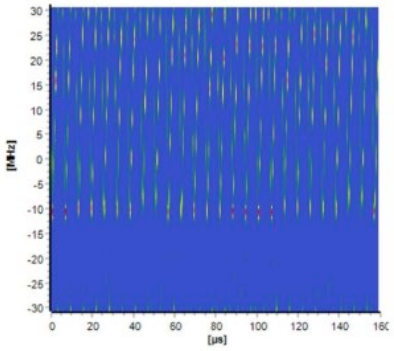
- TrendMicro (11/2013, 02/2017) reported a number of vulnerabilities in the AIS protocol
  - Lack of message integrity
  - Lack of timing integrity
  - Lack of authentication
  - Lack of validity
- VHF radio is also susceptible to jamming



16

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



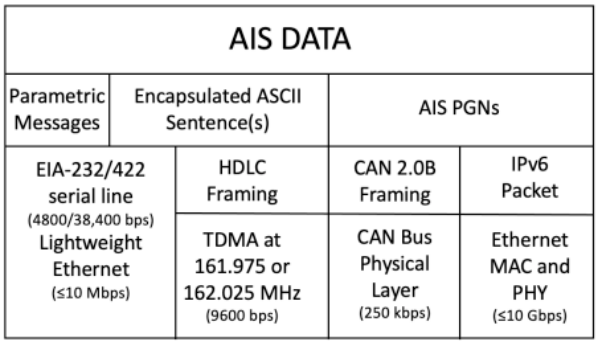
17

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 or ATON spoofing
- Data diddling
  - Sanction avoidance; IUU fishing, human trafficking, or other illegal activity; hide source of environmental impact; identity laundering; military pretext

18

Protocol Architecture and Standards



19

NMEA and ITU-R Protocols

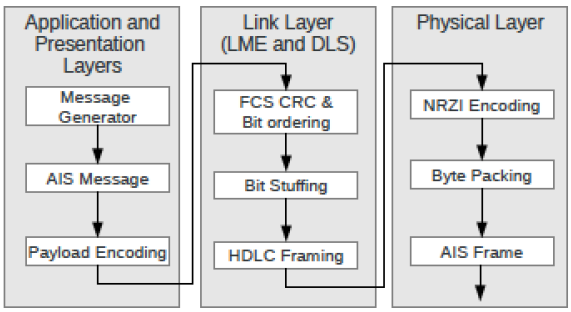
- NMEA standards describe inter-device communications onboard a vessel
  - *NMEA 0183 (1983; V4.30, 01/2024):* ASCII text messages over EIA-232/422 serial lines at 4,800 or 38,400 bps
    - Single-talker/multiple-listener: IEC 61162 Part 1 (NMEA 0183, low-speed), Part 2 (high-speed), and Part 450 (Lightweight 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

20

AIS Protocol Architecture

<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 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 on 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, -450</td><td>ITU Rec. M.1371</td><td>NMEA 2000
IEC 61162-3</td><td>NMEA OneNet</td></tr>
</table>

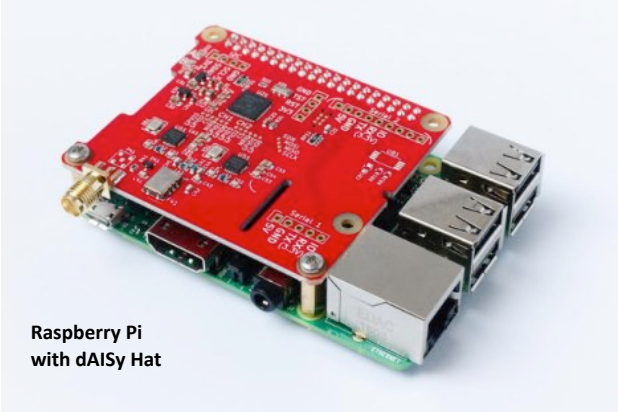
Side Note: ITU-R Rec. M.1371 Organization



Transmissions 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).

Build Your Own AIS Receiver…

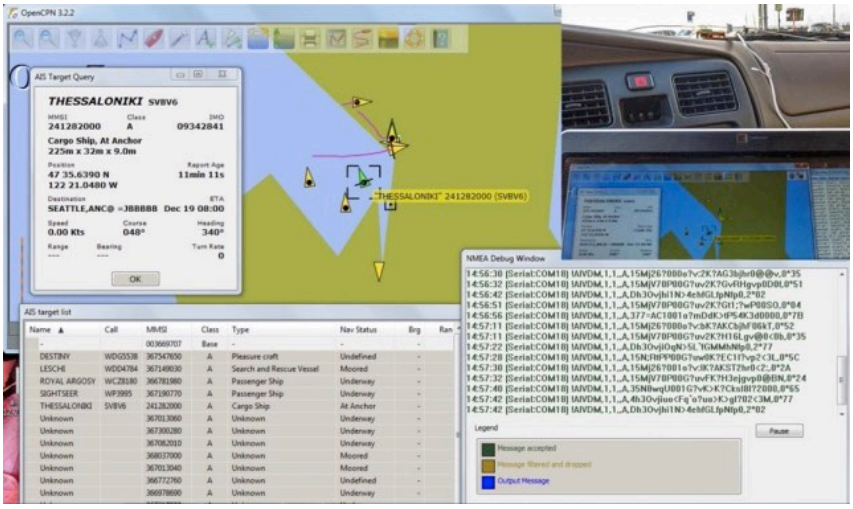
AIS Research Using a Raspberry Pi



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



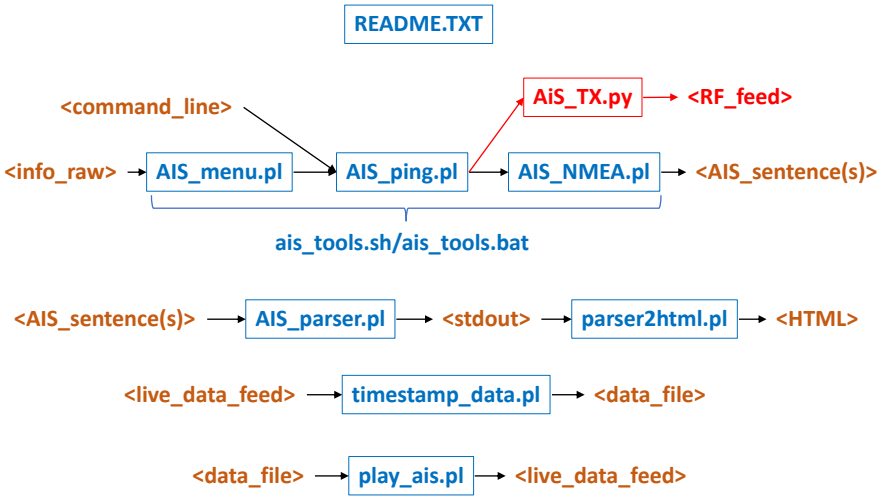
GCK's AIS Tools

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



28

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 NMEA 0183 AIS message types

```
AIS Sentence Preprocessor (Build: 04/11/2022 Version: 4.6.1)

MENU

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

X. Exit

Enter message type (1-24, 27) or 'X' to halt: 1
```


29

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=000001000001101011000010001011111001010000000000000111001100110100011001
100000011110000000100001110000101001010000001001111011000111100010011000000000000000000000000000 --ch
annel=A
```

AIS_NMEA.pl

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

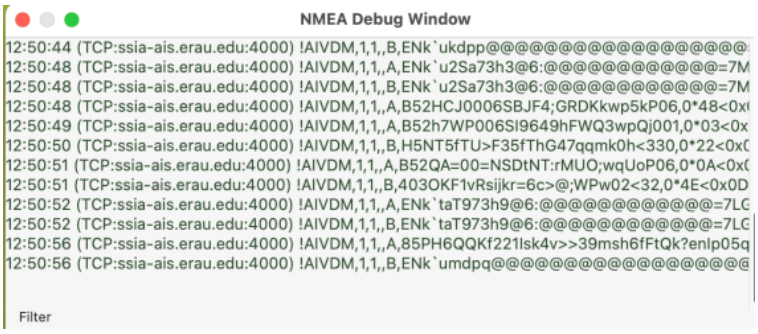
```
Moriarty:ais-prototype gck$ perl AIS_NMEA.pl --payload=000001000001101011000010001011111001010000000000000011100110011010001100110000001111000000100001110000101001010000001001111011000111100001001100000000000000000000000 --channel=A

***** 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: 000001000001101011000010001011111001010000000000000011100110011010001100110000001111000000100001110000101001010000001001111011000111100001001100000000000000000000000

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

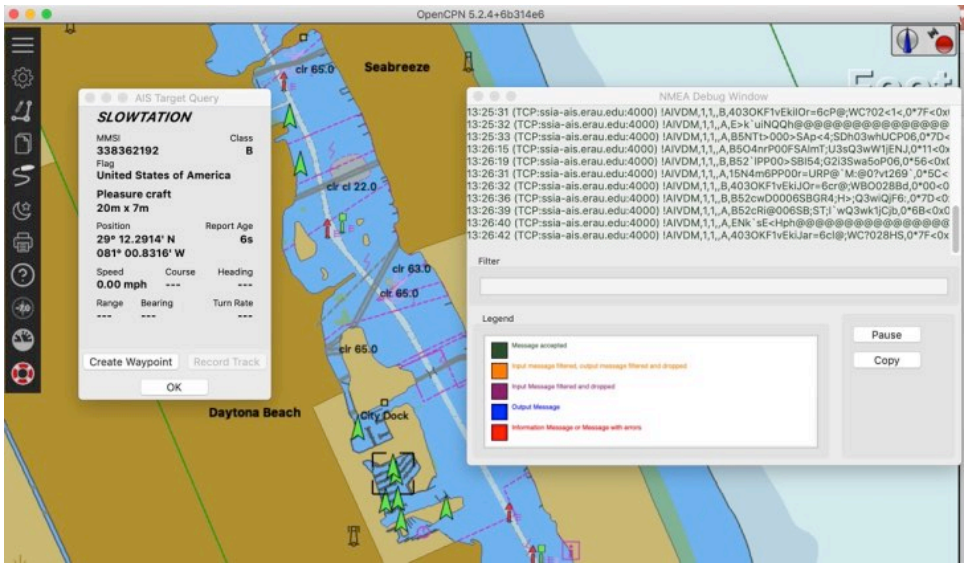
- Command line program accepts:
  - One AIS message binary string (from the command line or a file)
  - One AIS sentence on the command line
    - Requires use of "\" escape character on Unix/Linux systems
  - One or more AIS sentences, comprising one or more messages, from a file

```
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
111000010100101000000100111101100011110001001100000000000000000000000000

--- 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 ---
```

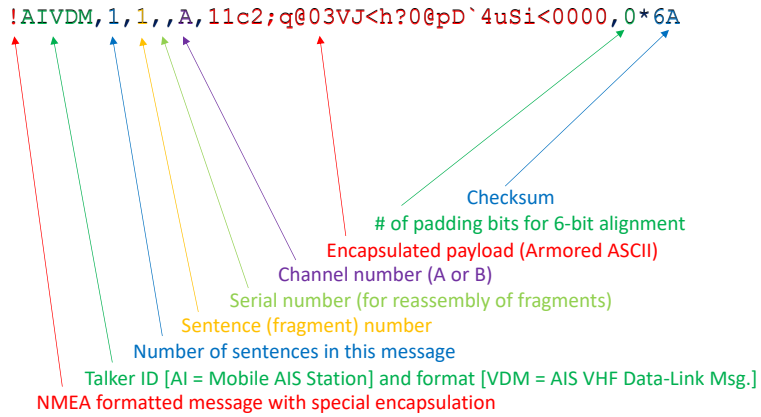

AIS Protocol Internals



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

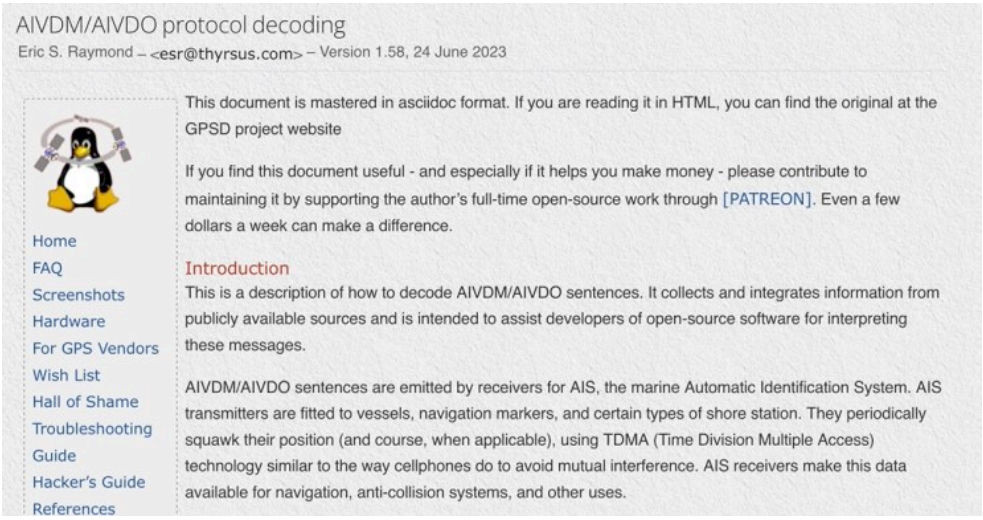


Encapsulated ASCII Sentence



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

The **BEST** Reference



AIVDM/AIVDO protocol decoding

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

Home
FAQ
Screenshots
Hardware
For GPS Vendors
Wish List
Hall of Shame
Troubleshooting Guide
Hacker's Guide
References

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

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)

48

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

49

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)

60

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)

61

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)

62

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)

63

Spare bits (bits 145-147)

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

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

BINARY OUTPUT
Spare [3] = 000

64

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)

65

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

```
000001000101100000001101100111000101010000000010010001001
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 0
00010010001001101101101000110110110101011 1
11011001000010100011101101101110001000110 0
00000111100100110000000000000000000000000 0
```

```
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

70

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

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 fragments: 1     Fragment number: 1     Serial number: <null>
 AIS channel: A
 Payload: 15P=W5@4RKJ=eGn@`sKR<1q<0000 (168 bits/28 6-bit words)
 Checksum: 0x71 (verified)
Binary payload (168 bits):
000001000101100000000110110011100010101000000010010001001101101101000110110110101011111011001000
101000111011011011100010001100000001111100100110000000000000000000000000000000

--- 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.fleetmon.com/vessels/?s=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°53.48'W)
Latitude = 29.079650°N (29°04.78'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 ---
```


71

Spoofing Example Overview

Example Deception

- GOAL: Spoof a tug on the Beaufort River
- EMILY ANNE MCALLISTER
  - MMSI: 366882560
  - Callsign: WDB3028
  - IMO number: 9291834
  - Length: 30.0 m (98.4 ft)
  - Beam: 14.0 m (45.9 ft)
  - Draft: 3.8 m (12.5 ft)
  - Gross tonnage: 280 tons
  - Owner: McAllister Towing New York

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

74

```
Bishop:ais-tools gck$ perl apate.pl

          Apate -- An AIS Spoofing Tool (Build: 11/17/2024 Version: 3.1.5)
                   [[Apate is the goddess of fraud and deception]]

Enter base name of file set (e.g., 'odyssey' or 'data/odyssey'): CB2024

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

Writing parameters to CB2024_parameters.txt...

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

Enter a description of this parameter file (<= 75 characters):
CyberBoat 2024

Enter MMSI (9 decimal digits, in range 200XXXXXX-799XXXXXX): 366882560

Enter vessel name (1-20 characters); Encoder default = NaN:
Emily Anne Mcalliste

Enter vessel call sign (0-7 characters):
WDB3028

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
 >>> 31

Enter distance from AIS antenna to bow (Dimension A), in meters (0-511, or null): 12

Enter distance from AIS antenna to stern (Dimension B), in meters (0-511, or null): 18

Enter distance from AIS antenna to port (Dimension C), in meters (0-63, or null): 6

Enter distance from AIS antenna to starboard (Dimension D), in meters (0-63, or null): 8
```


75

```
Enter draft, in meters in 0.1 m increments (0-25.5, or null); Default = 0: 3.8

Enter IMO Number (7 decimal digits or null): 9291834

Enter Destination (0-20 characters):
Beaufort SC

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: 20

Enter ETA hour, UTC (0-23 or 24 if not available, or null); Default = 24: 7

Enter ETA minute, UTC (0-59 or 60 if not available, or null); Default = 60: 30

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): 32.26

Enter longitude (-180 to 180): -80.65667

Enter display name for the initial point (<10 characters; <space> for no name;
 default = 'EMILY ANNE MCALLISTE')?
IP

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: 13.6

Enter course (0-359): 5

Enter length of leg, in nm (0.1-50): 3.3

Enter information for leg 2 ---

Enter speed, in knots (0 = moored; 0.1-50 is underway) or 'X' to stop: 13.6

Enter course (0-359): 342

Enter length of leg, in nm (0.1-50): 1.8
```

76

76

```
Enter information for leg 3 ---

Enter speed, in knots (0 = moored; 0.1-50 is underway) or 'X' to stop: 13.6

Enter course (0-359): 329

Enter length of leg, in nm (0.1-50): 1.4

Enter information for leg 4 ---

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): n

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

Reading parameters from CB2024_parameters.txt...
Writing Google Earth coordinates to CB2024_map.kml...

Writing route summary information to CB2024_summary.txt...


===== Summary information for vessel: 'EMILY ANNE MCALLISTE' (Apate V3.1.5) =====

MMSI: 366882560   =====   IMO number: 9291834   =====   Call sign:'WDB3028'
Vessel type: 31 (Towing ahead or alongside)
Length: 30.0 m (98.4 ft)   =====   Beam: 14.0 m (45.9 ft)   =====   Draft: 3.8 m (12.5 ft)

Start route at:
   32.260000°N ( 32°15.600'N)
  080.656670°W (080°39.400'W)

Information for leg 1...
   This leg ends at:
      32.314791°N ( 32°18.887'N)
     080.650998°W (080°39.060'W)
   The duration of this leg is 14.5588 minutes
   This leg ends 14.6 min (~874 sec) from the beginning of the route

Information for leg 2...
   This leg ends at:
      32.343322°N ( 32°20.599'N)
     080.661971°W (080°39.718'W)
   The duration of this leg is 7.9412 minutes
   This leg ends 22.5 min (~1,350 sec) from the beginning of the route
```

KML-only output

77

77

```
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 CB2024_parameters.txt...
Writing AIS_ping commands to CB2024_commands.sh...
Writing AIS synchronization information to CB2024_ais_sync.txt...
Writing Google Earth coordinates to CB2024_map.kml...

Writing route summary information to CB2024_summary.txt...


===== Summary information for vessel: 'EMILY ANNE MCALLISTE' (Apate V3.1.5) =====

Preparing AIS_ping Type 5 message...

MMSI: 366882560   =====   IMO number: 9291834   =====   Call sign:'WDB3028'
Vessel type: 31 (Towing ahead or alongside)
Length: 30.0 m (98.4 ft)   =====   Beam: 14.0 m (45.9 ft)   =====   Draft: 3.8 m (12.5 ft)

Start route at:
   32.260000°N ( 32°15.600'N)
  080.656670°W (080°39.400'W)

Information for leg 1...
   This leg ends at:
      32.314791°N ( 32°18.887'N)
     080.650998°W (080°39.060'W)
   Approx. course: 005°        Speed: 13 kn        Distance: 3.30 nm
   AIS Type 1 messages sent every 10 sec.   Duration of leg: 874 sec. (14.56 min)
   87 segments on this leg, each approx. 0.0379 nm (70.2 m)
   This leg ends 14.6 min (~874 sec) from the beginning of the route

Information for leg 2...
   This leg ends at:
      32.343322°N ( 32°20.599'N)
     080.661971°W (080°39.718'W)
   Approx. course: 342°        Speed: 13 kn        Distance: 1.80 nm
   AIS Type 1 messages sent every 10 sec.   Duration of leg: 476 sec. (7.94 min)
   47 segments on this leg, each approx. 0.0383 nm (70.9 m)
   This leg ends 22.5 min (~1,350 sec) from the beginning of the route

Information for leg 3...
   This leg ends at:
      32.363322°N ( 32°21.799'N)
     080.676198°W (080°40.572'W)
   Approx. course: 329°        Speed: 13 kn        Distance: 1.40 nm
```

KML+AIS output

78

78

```
Information for leg 3...
   This leg ends at:
      32.363322°N ( 32°21.799'N)
     080.676198°W (080°40.572'W)
   Approx. course: 329°        Speed: 13 kn        Distance: 1.40 nm
   AIS Type 1 messages sent every 10 sec.   Duration of leg: 371 sec. (6.18 min)
   37 segments on this leg, each approx. 0.0378 nm (70.1 m)
   This leg ends 28.7 min (~1,721 sec) from the beginning of the route

Course summary: Total distance: 6.50 nm
                Total time: 28.7 min
                Total number of AIS Type 1 messages: 171
                Total number of AIS Type 5 messages: 5
                Total number of AIVDM sentences: 181

The KML map file CB2024_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 CB2024_commands.sh
--> ./CB2024_commands.sh > CB2024_tmp.sh
--> chmod 755 CB2024_tmp.sh
--> ./CB2024_tmp.sh > CB2024_ais.txt
--> rm CB2024_tmp*

The AIS message file has been created.

The replay file CB2024_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=CB2024_replay.txt -s=- -ais=1 -time=0 -v

"Simplicity is the ultimate sophistication."

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

79

79

```
Bishop:ais-tools gck$ ls -la CB2024_*
-rw-r--r--  1 gck  staff   8773 Nov 21 15:47 CB2024_ais.txt
-rw-r--r--  1 gck  staff   1629 Nov 21 15:47 CB2024_ais_sync.txt
-rwxr-xr-x  1 gck  staff  36596 Nov 21 15:47 CB2024_commands.sh
-rw-r--r--  1 gck  staff    612 Nov 21 15:47 CB2024_map.kml
-rw-r--r--  1 gck  staff    532 Nov 21 15:37 CB2024_parameters.txt
-rw-r--r--  1 gck  staff   9557 Nov 21 15:47 CB2024_replay.txt
-rw-r--r--  1 gck  staff   1797 Nov 21 15:47 CB2024_summary.txt
```

```
Bishop:ais-tools gck$ cat CB2024_parameters.txt
#V2.3 -- This file is editable but be sure to maintain the block order and comment lines.
#Description: CyberBoat 2024
#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
366882560,'EMILY ANNE MCALLISTE','WDB3028',31,12,18,6,8,3.8,9291834,'BEAUFORT SC',12,20,7,30,1
#lat,long,leg_descriptor_type,label
32.26,-80.65667,C,IP
#leg,speed,course,distance || leg,0,mooring_duration,label || 0,<updated Type 5 information>
1,13.6,5,3.3
2,13.6,342,1.8
3,13.6,329,1.4
```

```
Bishop:ais-tools gck$ more CB2024_commands.sh
perl AIS_ping.pl --type=5 --mmsi=366882560 --vname='EMILY ANNE MCALLISTE' --callsign='WDB3028' --vtype=31
--vsize_a=12 --vsize_b=18 --vsize_c=6 --vsize_d=8 --draft=3.8 --imo=9291834 --dest='BEAUFORT SC' --month=1
2 --day=20 --hour=7 --minute=30 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=366882560 --navstat=0 --rot=0 --course=4.99999999998549 --heading=8 --spe
ed=12.1001130945687 --lat=32.26 --long=-80.65667 --ts=0 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=366882560 --navstat=0 --rot=0 --course=5.00003477851391 --heading=6 --spe
ed=12.3462130816706 --lat=32.2606297781987 --long=-80.6566048432151 --ts=10 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=366882560 --navstat=0 --rot=0 --course=5.00006955812494 --heading=5 --spe
ed=12.5818727724952 --lat=32.2612595563639 --long=-80.6565396855261 --ts=20 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=366882560 --navstat=0 --rot=0 --course=5.00010433882367 --heading=1 --spe
ed=11.0571297539766 --lat=32.2618893344957 --long=-80.6564745269329 --ts=30 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=366882560 --navstat=0 --rot=0 --course=5.00013912060929 --heading=5 --spe
ed=14.0791743849441 --lat=32.2625191125941 --long=-80.6564093674354 --ts=40 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=366882560 --navstat=0 --rot=0 --course=5.00017390348978 --heading=5 --spe
ed=14.5717555112616 --lat=32.263148890659 --long=-80.6563442070338 --ts=50 --nmea=A --batch --auto
perl AIS_ping.pl --type=1 --mmsi=366882560 --navstat=0 --rot=0 --course=5.00020868747333 --heading=6 --spe
ed=13.6299855315656 --lat=32.2637786686904 --long=-80.6562790457279 --ts=0 --nmea=A --batch --auto
```


80

```
Bishop:ais-tools gck$ more CB2024_replay.txt
0~!AIVDM,2,1,3,A,55Mpg082=j3aL@;?3;PDlTiV04ppF0l<4hhU=@D01PB683:7N9PQ@EASlU84,0*12
0~!AIVDM,2,2,3,A,hh000000008,2*2F
0~!AIVDM,1,1,,A,15Mpg0001qJ>j7LBMIH0<P@00000,0*4F
10~!AIVDM,1,1,,A,15Mpg0001sJ>j8dBMJn@<P<D0000,0*37
20~!AIVDM,1,1,,A,15Mpg0001vJ>j9rBMLDh<P:`0000,0*03
30~!AIVDM,1,1,,A,15Mpg0001gJ>j;8BMMk@<P2t0000,0*40
40~!AIVDM,1,1,,A,15Mpg0002=J>j<FBMOAh<P;@0000,0*5D
50~!AIVDM,1,1,,A,15Mpg0002BJ>j=TBMPh@<P;T0000,0*3B
60~!AIVDM,1,1,,A,15Mpg00028J>j>jBMR>h<P<00000,0*63
70~!AIVDM,1,1,,A,15Mpg0002AJ>j@0BMSe@<PBD0000,0*46
80~!AIVDM,1,1,,A,15Mpg0001fJ>jA>BMU;P<P:`0000,0*79
90~!AIVDM,1,1,,A,15Mpg0002@J>jBLBMVb0<P<t0000,0*05
100~!AIVDM,1,1,,A,15Mpg0002IJ>jCbBM`8P<P9@0000,0*1E
110~!AIVDM,1,1,,A,15Mpg0002=J>jDrBMaW0<P;T0000,0*65
120~!AIVDM,1,1,,A,15Mpg00029J>jF8BMc5P<P800000,0*4E
130~!AIVDM,1,1,,A,15Mpg0002@J>jGFBMdT0<P8D0000,0*3A
140~!AIVDM,1,1,,A,15Mpg0002?J>jHTBMf2P<P8`0000,0*78
150~!AIVDM,1,1,,A,15Mpg0002FJ>jIjBMgQ0<P:t0000,0*2A
160~!AIVDM,1,1,,A,15Mpg0002;J>jK0BMhw@<P?@0000,0*67
170~!AIVDM,1,1,,A,15Mpg0001eJ>jL>BMjMh<P7T0000,0*3F
180~!AIVDM,1,1,,A,15Mpg0001lJ>jMLBMkt@<P@00000,0*46
190~!AIVDM,1,1,,A,15Mpg0001tJ>jNbBMmJh<PBD0000,0*15
200~!AIVDM,1,1,,A,15Mpg00020J>jOpBMnq@<P@`0000,0*08
210~!AIVDM,1,1,,A,15Mpg0002=J>jQ8BMpGh<P4t0000,0*4C
220~!AIVDM,1,1,,A,15Mpg0001wJ>jRFBMqn@<PA@0000,0*39
230~!AIVDM,1,1,,A,15Mpg0001nJ>jSTBMsDP<P9T0000,0*67
240~!AIVDM,1,1,,A,15Mpg0002=J>jTjBMtk0<P<00000,0*27
250~!AIVDM,1,1,,A,15Mpg0002;J>jV0BMvAP<PBD0000,0*3B
260~!AIVDM,1,1,,A,15Mpg0002NJ>jW>BMwh0<P>`0000,0*51
270~!AIVDM,1,1,,A,15Mpg0002AJ>j`LBN1>P<P>t0000,0*7C
280~!AIVDM,1,1,,A,15Mpg0002GJ>jabBN2e0<P?@0000,0*58
290~!AIVDM,1,1,,A,15Mpg0001tJ>jbpBN4;P<P7T0000,0*5D
300~!AIVDM,1,1,,A,15Mpg0002:J>jd8BN5ah<P<00000,0*52
:
1640~!AIVDM,1,1,,A,15Mpg00029J>e;jBQ2bdnb:`0000,0*72
1650~!AIVDM,1,1,,A,15Mpg0002:J>e4TBQ3stnbBt0000,0*2C
1660~!AIVDM,1,1,,A,15Mpg0002OJ>duFBQ5<tnbI@0000,0*7D
1670~!AIVDM,1,1,,A,15Mpg0002QJ>dn:BQ6MtnbIT0000,0*62
1680~!AIVDM,1,1,,A,15Mpg0002FJ>dftBQ7g<nbF00000,0*3B
1690~!AIVDM,1,1,,A,15Mpg00023J>dWfBQ90<nbFD0000,0*40
1700~!AIVDM,1,1,,A,15Mpg00026J>dPPBQ:A<nb@`0000,0*24
```

28.7 minutes

81

```
Bishop:ais-tools gck$ perl play_ais.pl -f=CB2024_replay.txt -s=~ -ais=1 -time=0 -v -pro=tcp -port=8888

AIS Play (Version 2.4.4, Build date: 08/08/2024)
Connection success to 127.0.0.1:8888/tcp.
Reading file CB2024_replay.txt, using '\~' as a field separator.
Timestamps are in field 0 and AIS data in field 1.
Start at time 0 seconds.

Record 1 -- Timestamp = 0; waited 0 second(s) to send...
 !AIVDM,2,1,3,A,55Mpg082=j3aL@;?3;PDlTiV04ppF0l<4hhU=@DO1PB683:7N9PQ@EASlU84,0*12
Record 2 -- Timestamp = 0; waited 0 second(s) to send...
 !AIVDM,2,2,3,A,hh000000008,2*2F
Record 3 -- Timestamp = 0; waited 0 second(s) to send...
 !AIVDM,1,1,,A,15Mpg0001qJ>j7LBMIH0<P@00000,0*4F
Record 4 -- Timestamp = 10; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg0001sJ>j8dBMJn@<P<D0000,0*37
Record 5 -- Timestamp = 20; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg0001vJ>j9rBMLDh<P:`0000,0*03
Record 6 -- Timestamp = 30; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg0001gJ>j;8BMMk@<P2t0000,0*40
Record 7 -- Timestamp = 40; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg0002=J>j<FBMOAh<P;@0000,0*5D
Record 8 -- Timestamp = 50; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg0002BJ>j=TBMPh@<P;T0000,0*3B
Record 9 -- Timestamp = 60; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg00028J>j>jBMR>h<P<00000,0*63
Record 10 -- Timestamp = 70; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg0002AJ>j@0BMSe@<PBD0000,0*46
Record 11 -- Timestamp = 80; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg0001fJ>jA>BMU;P<P:`0000,0*79
Record 12 -- Timestamp = 90; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg0002@J>jBLBMVb0<P<t0000,0*05
Record 13 -- Timestamp = 100; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg0002IJ>jCbBM`8P<P9@0000,0*1E
Record 14 -- Timestamp = 110; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg0002=J>jDrBMaW0<P;T0000,0*65
```

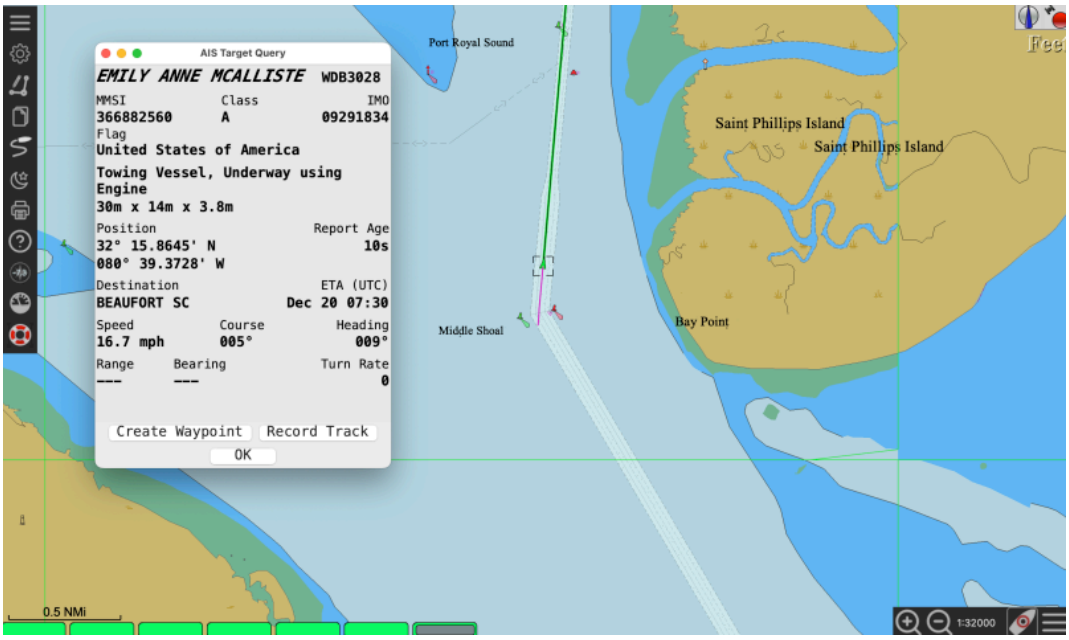
:
:

82

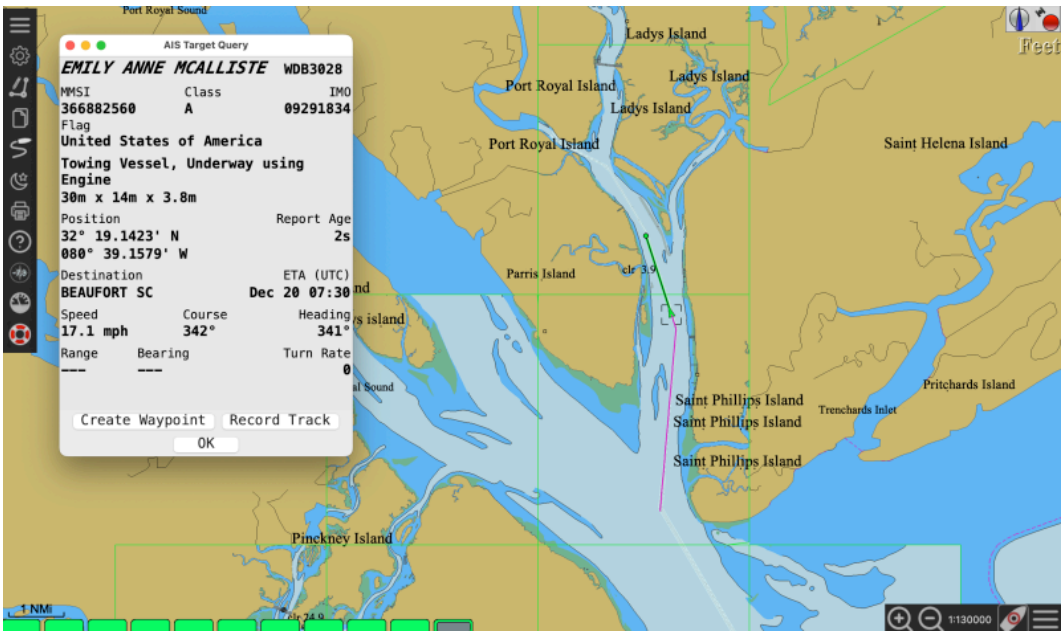
:
:

```
Record 168 -- Timestamp = 1570; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg00021J>ev@BPqk<nb@D0000,0*50
Record 169 -- Timestamp = 1580; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg00027J>eo2BPs4<nb@`0000,0*44
Record 170 -- Timestamp = 1590; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg00022J>egnBPtELnbFt0000,0*01
Record 171 -- Timestamp = 1600; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg0002IJ>e``BPuVLnb7@0000,0*2C
Record 172 -- Timestamp = 1610; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg0002NJ>eQJBPvoLnb;T0000,0*1A
Record 173 -- Timestamp = 1620; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg0002;J>eJ<BQ08dnb>00000,0*5B
Record 174 -- Timestamp = 1630; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg0001oJ>eC0BQ1Idnb<D0000,0*0F
Record 175 -- Timestamp = 1640; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg00029J>e;jBQ2bdnb:`0000,0*72
Record 176 -- Timestamp = 1650; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg0002:J>e4TBQ3stnbBt0000,0*2C
Record 177 -- Timestamp = 1660; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg0002OJ>duFBQ5<tnbI@0000,0*7D
Record 178 -- Timestamp = 1670; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg0002QJ>dn:BQ6MtnbIT0000,0*62
Record 179 -- Timestamp = 1680; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg0002FJ>dftBQ7g<nbF00000,0*3B
Record 180 -- Timestamp = 1690; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg00023J>dWfBQ90<nbFD0000,0*40
Record 181 -- Timestamp = 1700; waited 10 second(s) to send...
 !AIVDM,1,1,,A,15Mpg00026J>dPPBQ:A<nb@`0000,0*24

181 records sent

Bishop:ais-tools gck$
```

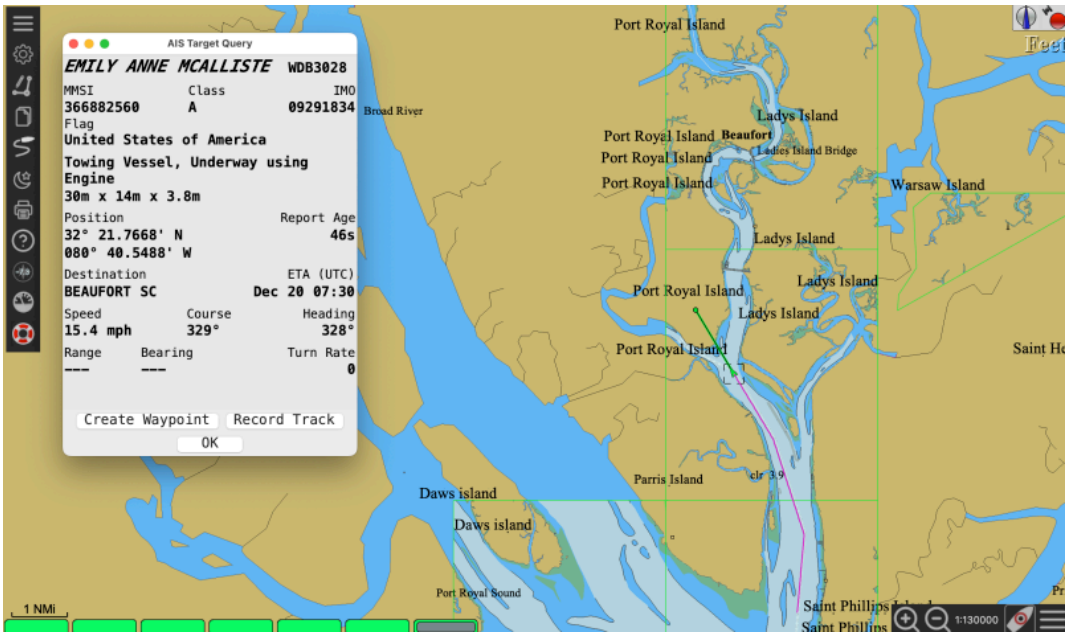

83


AIS Target Query
EMILY ANNE MCALLISTE WDB3028
MMSI 366882560
Class A
IMO 09291834
Flag
United States of America
Towing Vessel, Underway using Engine
30m x 14m x 3.8m
Position
32° 15.8645' N
080° 39.3728' W
Report Age 10s
Destination BEAUFORT SC
ETA (UTC) Dec 20 07:30
Speed 16.7 mph
Course 005°
Heading 009°
Range ---
Bearing ---
Turn Rate 0
Create Waypoint
Record Track
OK
Port Royal Sound
Saint Phillips Island
Saint Phillips Island
Middle Shoal
Bay Point
0.5 NMi
1:32000

84

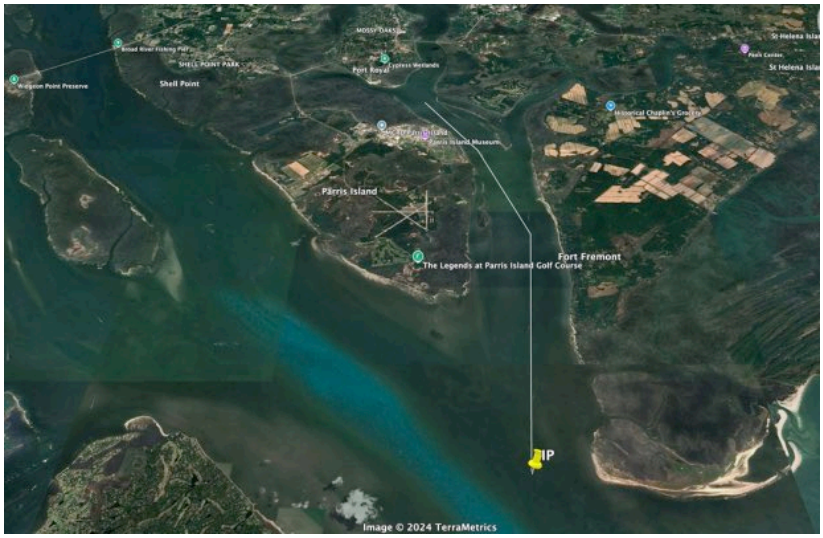

AIS Target Query
EMILY ANNE MCALLISTE WDB3028
MMSI 366882560
Class A
IMO 09291834
Flag
United States of America
Towing Vessel, Underway using Engine
30m x 14m x 3.8m
Position
32° 19.1423' N
080° 39.1579' W
Report Age 2s
Destination BEAUFORT SC
ETA (UTC) Dec 20 07:30
Speed 17.1 mph
Course 342°
Heading 341°
Range ---
Bearing ---
Turn Rate 0
Create Waypoint
Record Track
OK
Port Royal Sound
Ladys Island
Ladys Island
Port Royal Island
Ladys Island
Port Royal Island
Saint Helena Island
Parris Island
Saint Phillips Island
Saint Phillips Island
Saint Phillips Island
Trenchards Inlet
Pritchards Island
Pinckney Island
1 NMi
1:130000

85



86

Google Earth Rendition



87

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!!

88

Summary

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

89

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)
FCS	Frame Check Sequence
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)
LME	Link Management Entity
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
NRZI	Non-return-to-zero inverted
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
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. (2024, November 25). 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 International 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