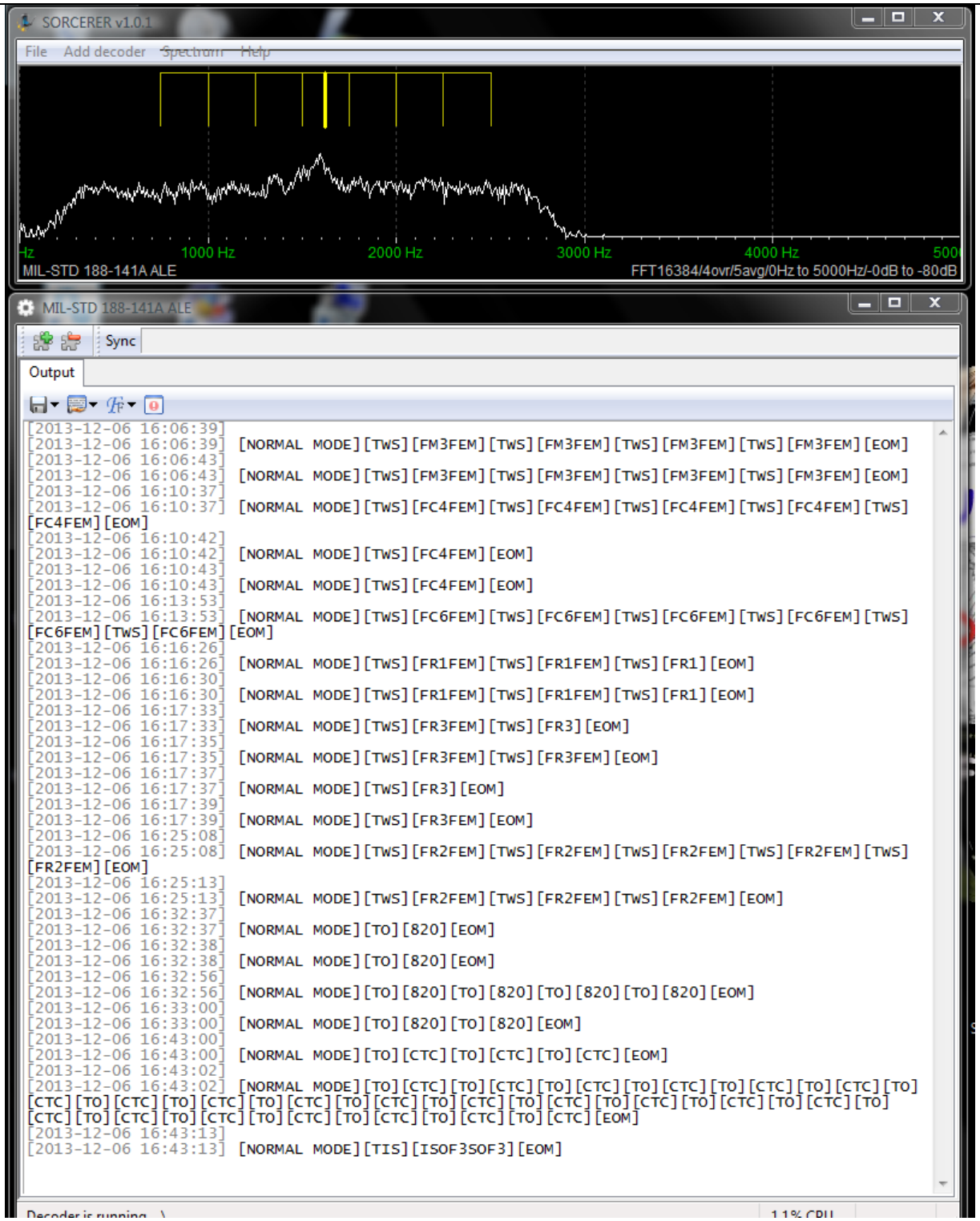
SORCERER INSTALLATION AND OPERATION

By N0SYA December 6th, 2013



Preface

This paper is intended to provide information on the installation and use of Sorcerer, a software multimode decoder. It was written following the theory that certain aspects of the tool such as features, optional settings, and tuning routines are the functional equivalent of those found in other decoding tools. More or less it's just those things I have noticed in the tool so far and would like to point them out for those who might have missed them or not understood them at least to the degree I may. In the end they simply represent my opinion. Error in the paper is to be expected. Reading the user manuals for other decoding tools may give further insight into the use of this tool and is suggested reading. This paper will also address some common receiver issues that could be considered when using software decoding tools. This paper assumes that a user has working receiver/antennae, pc, interface, and these are connected and adjusted properly. The user should also be familiar with hf radio. "Ionosphere and You" primer included at no charge.

Use of this paper constitutes agreement with the following;

- It is for information only.
- The olivia decoder crashes the tool.
- Other decoders may infrequently crash the tool.
- The tool has been reported by some to contain malware.
- By installing and/or using software you accept all risk involved.
- The user accepts full and sole responsibility for his or her actions.

What is Sorcerer?

Per the installation manual;
"SORCERER is a collection of decoders for modes found in the ELF-SHF range. These work in tandem with proprietary intelligent bit parsers automatically identifying targets of interest .(ie - country and specific service as well as identifying data link protocols, compression schemes, file formats, and cryptographic formats in use.

These feature:

- No proprietary hardware
- The most comprehensive collection of current, on-air modes
- Superb demodulation, decoding and parsing of ELF-SHF modes
- Run multiple decoders simultaneously
- Unmatched decoder performance in weak/poor conditions
- Hundreds of parsers always available - run multiple per decoder
- High-speed constellation display
- Offline or Online Analysis
- Flexible variety of outputs to support cryptanalysis
- Continuous development - new modes added throughout the year
- Custom demodulators, decoders and parsers available upon request
- The decode modules are selected based on the requirements of Avonlea Services' customer requirements and the realities of what is actually currently on air in these spectra. It is Avonlea Services' goal to provide a collection of decoders and parsers simply not found in any product offered by competitive manufacturers. Customization and Prioritization of decode
- modules in currently in progress in possible and to this end Users should contact Avonlea Services for details of special contracts.

System Requirements
The following minimum system requirements are recommended:

- Pentium-class CPU, 1.0 GHz+
- 128MB+ RAM
- Standard AC97 soundcard
- OS - Microsoft Windows 98, 98SE, 2000, XP(with sp1/sp2/sp3)

Tool Footprint
The tool takes about 1 meg of space on disk and in operation creates 6 threads while taking up about 13 megs ram (or less) with one S4285 decoder running. A performance increase may result from use on multiple cpu systems as the tool is multithreaded and adds another thread for each decoder running. With 33 decoders (cw, all fsk and mfsk modes, and about half the psk modes) running I was warned about too many windows open. In this state the tool used about 50 percent cpu, 27mb ram, and had 37 threads running. It runs about 12 percent cpu decoding a single instance of S4285. Cpu time the tool uses will vary from system to system due to processor characteristics and loads. With no decoder running the tool uses little to no cpu time. What all this means is the tool is very lightweight in disk space and ram taken and is not cpu intensive in most instances, it should run well on newer systems and many older systems that do not quite come up to the specs suggested for the tool. The pc system used for testing was a Intel 2.13GHz C2d machine, 4gb ram, 32bit Vista os.

Tool Capabilities
Some program features such as non-standard bit parsers, automated mode identification, automated decode parameter setup, and signal database may not be present - if they are I did not find them. The downloads available consist of the main program of the tool; a FFT Spectrum Display window from wich to call up decoders and their parsers, and a manual. Not all the decoders were checked for decode function as not every type of signal was present when needed. All named decoders executed when called and did not crash the tool in this instance- with the exception of Olivia and sometimes but not often other decoders. These random crashes - always when the decoder was activated not in the middle of a session - may be attributed to application uptime, the longer the app is running the more neurotic it may be.

Decoders
Decoders are programs that take coded input and process it (hopefully) into a less coded form. For example, many codes employed on hf are very highly structered and complex in the sense of forward error correction, interleaving, and synchronisation and that's besides any intentional encryption. These encodings are meant to ensure message delivery by reduncancy of bits in most cases. The decoder understands these paradigms and tries to make them into something the average pc can output/display in a meaningful sense to a user or another program. One might view decoders and parsers as interpreters of bits.

Decoders available
CW

FSK:
ACARS, ARQ E, Async FSK, AX.25HF/VHF/9600Bd, CIS-11, Cosmos Navdata, EFR, GTOR, GlobeWireless FSK, IRA ARQ, ITA2 FSK, IVSU, Linea SITOR A/B, M823DGPS, MD674, Pactor1, SITOR A/B, STANAG4481, Sync FSK.

MFSK:
CIS MFSK-16/20, Coquelet 8/13, Olivia(crashes tool), Piccolo MK6.

PSK:
ARINC 635, GlobeWireless PSK, HAM BPSK/QPSK modes, MilStd188-110A, MilStd188-110A App.A, MilStd188-110B, Pactor II/III, STANAG4285, STANAG4529(sometimes crashes tool).

SELCALL:
ALIS, BARRET Selcall, CODAN CALM ChirpCall, CV-786, Datron S3, GMDSS HF/VHF DSC, HARRIS RF-3560,

JENAL/SHUEMPERLIN SC2 BARRET/CODAN, JENAL/SHUEMPERLIN SC3 BARRET/CODAN, MilStd188-141A ALE, Motorola MDC-1200, NECODE 321/322ARX Selcall, QMAC, RSX.25, SGC BARRET/CODAN, SPECTRATEK SR-3 CODAN/BARRET, Thales HF950, VERTEX, WA2 Selcall, Tone Selcalls (ICAO, CTCSS, PL, etc).

FAX;
AM, FM Greyscale, FM Black&White.

Parsers
A parser takes the output of the selected decoder and tries to further place it into some sense a person or program can use, such as text, graphical bitstream, or raw bitstream; 1s and 0s. Most decoders will automagically bring up one or more appropriate parsers, such as "Ascii" or "ITA-2". Sadly I did't see an XOR parser, wich could be handy for certain fsk signals. Another parser inherent to the tool but is only available in certain decoders is "Bitstream-VisualBits. VisualBits provides a graphical representation of bit patterns and in doing so increases cpu load noticeably, but not so much as to hinder tool performance in a single instance. Such bit parsers are typically used to allow a user to note sequences and visualy locate the start position of a frame in a bit stream.

A faster decoder rate (such as 1200L in S4285) using the VisualBits parser may result in rather high cpu usage. This additional cpu usage may stem from video card driver overhead due to the VisualBits parser running and the video card processing the image to be displayed. To best save a VisualBits image intact use the "save file as unicode" save option.

Other parsers may be inherent to the tool depending upon decoder and you can add these. After adding a decoder you can call up further parsers by clicking on the + button in the upper left corner of the decoder. To remove a parser simply click the colocated - button while viewing the parser window to be closed. Testing to see if the decoder can employ a 3rd party parser was not done. I assume one would add these to the tool as dll files.

Parsers available;
Ascii. ITA-2, , Bitstream, Bitstream-VisualBits, KG84C Crypto Parser

These parsers may have options to themslves. Only certain parsers are available in every decoder.

TCP IP Servers;
This option is called up by the unlabled Start Server button located just to the right of the Save File button on the decoder. It offers two TCP server types; ANSI and UNICODE, and asks for the port number to employ for the server. I assume the tool uses the default IP address of the host pc. This functionality was not further explored at time of writing.

Why use Sorcerer?
Having tried many other freely available decoding tools, followed their install and setup directions to the letter, simply no decoding tool worked as well. The Sorcerer gui is very intuitive and non-intimidating. There is no .dat file to be replaced every few months to keep the tool running nor need to change the current date in the pc just to enable the tool. No intimidating gui filled with tiny controls that are in turn filled with tiny fonts, or demanding and involved installation and setup that places bits of the tool here and there in a hard drive. It just works well where, sadly, the others often did not. That is not to say other tools are not worthy of consideration. The others simply do not come close to this tools usefulness and ease of operation in my case. The only decoder featured in the tool that crashed in testing is the olivia fsk mode. This mode crashes the tool and has been reported to activate malware but I've only noted the tool crash with no other effects on the pc. There are other freely available tools that decode olivia, wich is an infrequently found amateur radio mode.

The following is diagnostic output of an olivia decoder crash;
Problem signature:

Problem Event Name:	APPCRASH
Application Name:	sorcerer-v1.0.1.exe
Application Version:	0.0.0.0
Application Timestamp:	49bc5109
Fault Module Name:	StackHash_fd00
Fault Module Version:	0.0.0.0
Fault Module Timestamp:	00000000
Exception Code:	c0000005
Exception Offset:	00007a48
OS Version:	6.0.6002.2.2.0.768.2
Locale ID:	1033
Additional Information 1:	fd00
Additional Information 2:	ea6f5fe8924aaa756324d57f87834160
Additional Information 3:	fd00
Additional Information 4:	ea6f5fe8924aaa756324d57f87834160

Pre Installation/Operation Suggested Practices

Installation:
Determine wich Sorcerer download link you wish to use and download Sorcerer if you have not. Once you have your copy simply open the zip file and copy the exe intact to a folder named appropriately from where you will be using the tool.

For example: C:\RadioApps\Decoding\Sorcerer

You may include the original Sorcerer installation pdf file in the same folder if you wish. The installation pdf file provides info on the full version install procedure. It also offers some hints at what the tool is capable of especially with regards to radio control.

Note on Root Folders:
Vista and later MS os require programs that are in the "Program Files" or "Program Files (x86)" folders to write data to the "ProgramData" folder.
Thusly, in Vista and Win7 do not install the tool to the C:\Programs folder as that may limit its ability to make changes to the contents of that folder such as logs the tool can save automatically, and may have other issues with regards to optional settings being saved. Installing it to its own distinct parent folder should ensure desired permission levels and program function. This applies to any exe, not just Sorcerer. Other os may not have such issues and one may install the tool anywhere.

Shortcuts
Left click on the Sorcerer exe in your folder and set a startup icon on the desktop or in the startup menu by pinning the link in the startup menu. Once you have your shortcut, right click on the link and select properties. Select maximised window if desired, via the "shortcut" tab menu. Under the "advanced" tab of the same property sheet, select "run as administrator" if that option is available and desired. If you use the Aero (or other) Windows gui as opposed to explorer it may help to use some of the compatibility options found in the shortcut compatibility menu tab. If there are visual anomalies in the tool related to the gui, experiment with these and see if they help. Some guis can make apps not specifically written to run under said gui look "wrong" such as missing or corrupted fonts or controls or other visual issues. I have had no issue with gui in the case of Sorcerer on Vista with Aero disabled other than the tool windows not always minimising/restoring with a single click.

So now you should have the tool installed and a means to execute it without going into its folder each time.

Tool input selection
This tool can accept wav files, live audio from a sound card, or I/Q input. Only sound card input was used for this paper.

Interfaces
An radio interface is typically used with most any radio not having an I/Q output. If you have an sdr radio you can use its I/Q output to feed the tool and thusly avoid the need for an interface. Interfaces can be bought or built, and range from cheap to expensive. One can always just run a patch cable from radio audio out to pc audio in but a decent interface will have isolation transformers and level adjustments that can be very beneficial to decoder performance. For example, there's often an impedence and level missmatch between the line input on a soundcard and the impedence and level of a radio line level output. In such a case isolation transformers can be of benefit for matching impedences. They can also reduce ground loop caused hum and other noises. Often an interface provides some audio bandwidth limiting, and as long as it doesn't limit the desired frequencies this should be of benefit. I suggest interfaces with isolation over simple patch cables.

Sound card properties
Sound cards come in various levels of quality, wich is often reflected by their price. Some onboard soundcards are full of system noise and are not going to do very well used as an input to the tool, other onboard soundcards may offer excellent audio reproduction. External soundcards may or may not be superior to onboard soundcards. Try what you have and see how well it does. If it seems that the sound card is keeping you from good decodes try another.

Windows Sound Settings
I used the tool with audio input not I/Q input thusly have no suggestions as to using I/Q input to the tool. I run the soundcard input and output at full volume and use the external interface to control levels between the radio and pc. However, use whatever means and settings you feel inclined. Try to adjust settings for sound cards in windows before you run the tool. Changing sound card settings in windows after a tool is running and already using the sound card may cause the tool to be disconnected from the sound card even if momentarily, and may cause the tool to not run properly afterwards. In such case shut the tool down and then restart it after sound settings have been made.

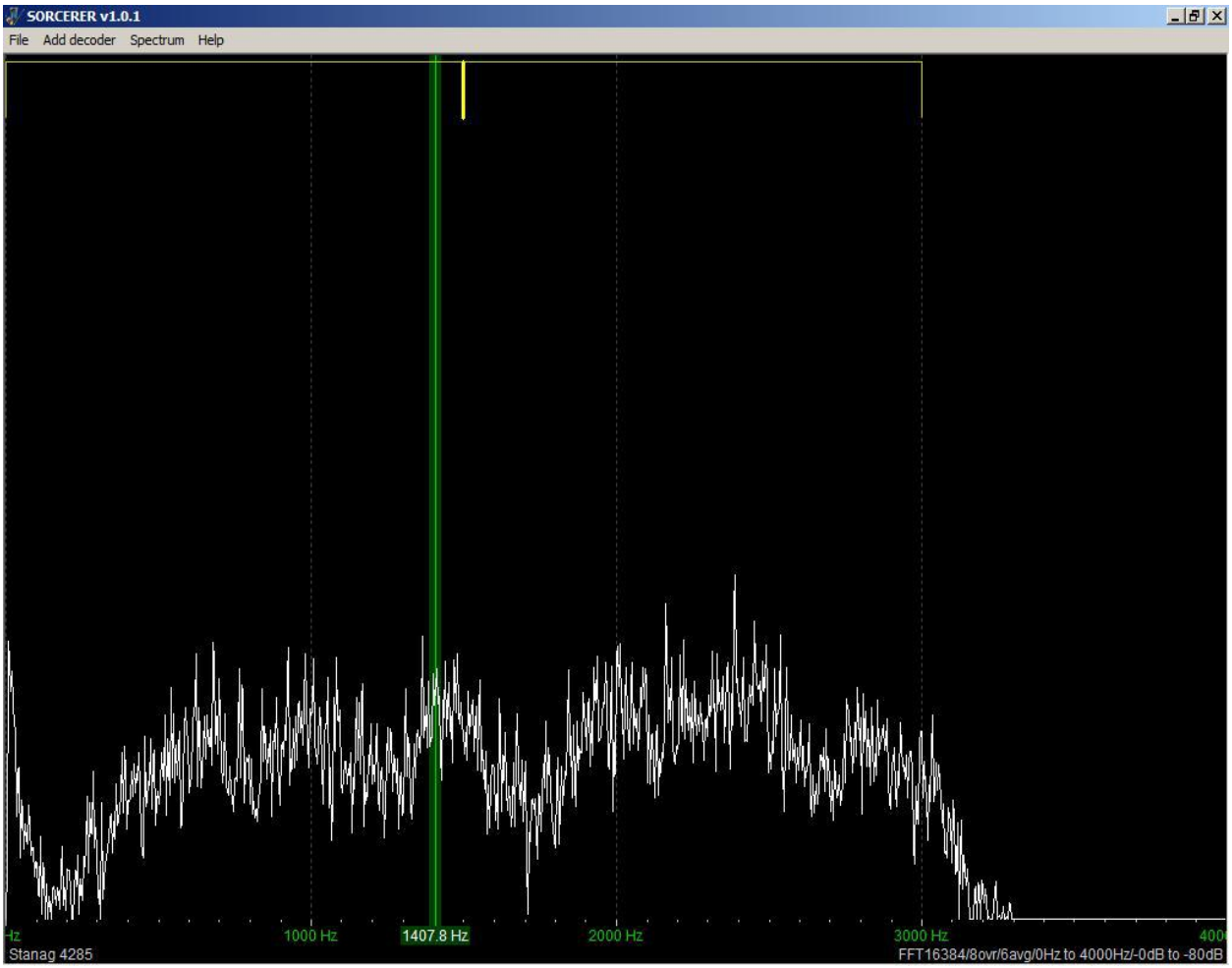
Tool Sound Settings
It may be wise to run a tool with the least audio input that gets the job done. This means a sufficient signal for the tool to decode successfuly and no more so as to maximise dynamic range of the tool. Very few decoding apps have great input dynamic range and are almost too easily overdriven, resulting in decode failure.

In testing the tool by deliberately increased input level to the maximum level of the interface and in the os itself, the tool still decoded. Many decoding tools fail this test at much lower input levels, yet the tool is sensitive enough to decode or at least detect or sync signals at the noise floor of the receiver at normal tool input levels. Often to get a large input dynamic range a tool must be coded to be insensitive so as to tolerate high level input signals at the cost of low level signals being lost in the noise. This is not the case with this tool. This may indicate the tool is very robust and has a wide dynamic range for input signals presented to it.

Sound Card Sample Rates under Windows
I run the soundcard at the highest sample rate the card will run at. This rate will vary for different sound cards. The highest rate may or may not be best for all systems and all tools. This setting for input and output both will be under the soundcard properties sheet in windows. The tool as well as others may or may not run the sound devices at the rated speed and may select their own rate often below the sound cards maximum, regardless of that selected in windows.

Initial Operation and Setup

Double click your startup link or tab and the tool should execute. If not, right click on the shortcut and select run as administrator and try again. If you don't see the app on the desktop after executing it, check the system tray or task bar. If it's minimised, click on it and maximise or restore it. If you don't see the tool, you have other issues beyond the scope of this paper. If your av detects the tool as a virus and prevents it from executing it may be a virus or it may be a false positive. You will have to determine wich is the case as that is beyond the scope and purpose of this paper. With a running tool now on the desktop you should see this screen



Here we see the FFT (Fast Fourier Transform, a dsp algorithm) Spectrum Display screen where a x/y plot of frequency versus amplitude is displayed. On the lower right corner you'll see information on the current FFT Spectrum Display settings of the tool. If you have audio of sufficient level coming into the tool it will show up on the screen here. If you know the tool should be hearing audio but it isn't, you need to look into signal levels in your sound device feeding the tool or if the sound device is enabled. Often other sound using apps set sound card properties to their likings and the next tool to use the soundcard is left with those same settings wich may or may not work for that tool. Must have input before you can do any decoding.

Click on the "file" menu tab in the upper left corner of the tool and note the tabs for "Recording", "Options", and "Exit".

In the "Recording" menu tab you will find "Show Settings' tab with a "Sample Rate" option you can select if you know the rate of your sound device and wish to do some recordings. If the rate is unknown leave it at default value. You can also input the directory where recordings will be saved by the tool. Recording was not attempted for this paper.

Under "Options" note "sample rate correction" and sound card enumeration such as "default (SoundMapper)", or other

options if available such as "USB Audio Codec". Leave the sample rate timing correction at 1.0000 for now. If you do know your sound cards timing error, input it now. If not, leave this control alone. If you have a specific sound device that shows up as a selectable option in the menu and you wish to use it, select it by clicking on it in the drop down property sheet. Leave "Use DirectSound" checked if it is checked. Otherwise leave the tool as installed and attempt to run it at default sound settings. Then if you aren't getting sound input to the tool alter the settings and try again. Leave the other settings in this menu at defaults unless you wish to experiment with rig control. If sound is still not making it into the tool, try different sound card settings in the windows sound control panel.

The Exit tab will cause the tool to exit.

FFT Spectrum Display Options
These are under the "Spectrum" menu tab on the FFT Spectrum Display of the tool. Note that these options should have no bearing on the decoding ability of the tool, only on the properties of the FFT spectrum display itself.
Keep in mind that most of these options will interact, altering FFT spectrum display performance and/or information level.

Size
The FFT length in which the signal is processed and displayed. To obtain a higher resolution of the displayed frequency range, increase the FFT length. Set it to your liking. If you want to view maximum detail on a signal, set this control to max wich is 65536.

Averaging
The spectrum is displayed in an exponential average of several spectrums sampled by the tool. The change in the spectrum will be a average of the spectrum over time. Set this to your liking or leave at default.

Window Overlap
The FFT algorithm is used for the calculation of the spectrum. This algorithm, however, shows inaccuracies in the amplitude (attenuation) as well as in the bandwidth (expansion) of a signal due to the finite signal probe. Adjusting this control from one extreme to the other will show you the tradeoffs. These inaccuracies can be reduced using windowing however for a high bandwidth accuracy you give up amplitude accuracy and vice versa. Set this control to your liking or leave it alone.

Frequency Offset
Changes the zero beat or imaginary carrier or leftmost baseline of the tool. If you set it to say 1500 the baseline starts the FFT spectrum display at 1500Hz rather than 0Hz at the left edge of the tool. This can be of help in some experiments on signals.

Frequency Range
The frequency range represents the bandwidth of audio input on screen. I set it to 4KHz. A wider range can be of benefit for experimentation.

Dynamic Offset
Sets the offset or zero of the dynamic range (bottom of screen aka noise floor) of the FFT display with respect to the input level and dynamic range setting of the display. Zero is at the bottom of the screen, increasing it raises the baseline above zero.

Dynamic Range
The unit of the spectrum may be dBFS ie deciBels of Full Scale, wich is pretty arbitrary. This refers to the gain of the signal as displayed on the screen. 0 dB means full scale and –100 dB means 100 dB below full gain. Set this to your liking or leave at default.

Spectrum setup I settled on;
Size; 4096
Averaging; 40
Overlap; 4x
Frequency offset; 0
Frequency range; 4kHz
Dynamic offset; 0
Dynamic range; 100

This completes the Install/Setup procedure that should cover all modes. The next section covers some but not all available decoder types and their options. Only some of the available decoders will be expounded upon as many decoders offer the same options.

Adding Decoders
This is the part you've been waiting for. We ignored the "Add decoder" menu button so we could get the tool set up for operation, now that we have done that we'll try some decoding.

But first a word on receiver IF center frequency offset and filtering. Just what you wanted to read.

This tool was written for Professionals and these Professionals are expected to use radios for Professionals that have appropriate IF filter bandwidths and IF filter frequency centers of known and generaly agreed upon Professional characteristic. And these Professional filters will have very good (meaning low) group delay, a desireable feature. The tool was written taking these Professional attributes into consideration and thusly is expecting them in every case but few hobbyists have such radios. And that presents problems for the hobyist.

However, one can run the tool with the radio as it is and see if it decodes properly, if so, fine and good. If not, or if you just want to see if you can improve decoding performance, there are some measures that can be taken to increase the chance of success.

Unlike some tools for the same marketplace this tool is flexible on IF filter center. This is a saving grace for us hobbyists as some of our radios often employ as standard a nominaly 2.8KHz wide ssb filter centered not on the tools expected 1800Hz (in the case of S4285 decoding) but 1500Hz. This filter will often display a different passband from USB to LSB. And this hobbyist filter will typically have very poor group delay especially at each end of the filter passband. You could always try to use PBT and IF Shift to align IF center but that may or may not work better. Employing PBT and IF Shift to make up for the center frequency differences may create compromises in IF filtering quality, especialy in radios that have more than one filtered IF conversion. PBT and IF Shift can only go so far and are tedious in this day of digital automation as far as I am concerned. One way to test using IF Shift or PBT to reduce offset issues is to view the signal in the FFT Spectrum Display window and try to set the center of the filter over the signal by varying IF Shift or PBT.

In one hobbyist case, IF filters are at 1500Hz centers for ssb use and 600Hz center for cw/rtty narrow filters, and 1500Hz for voice modes and 800Hz for cw/narrow modes in a similar radio. So how do we deal with these issues? Some don't deal with the issues and then wonder why they don't have much success at decoding.

After you have selected the mode to be decoded you can simply left click on the FFT Spectrum Display screen, placing the green line - wich represents the center frequency the decoder will use - where the offset should be in relation to the frequency readout in the FFT Spectrum Display window. Also in some decoders display window you are given the option to set the offset numerically in the "Center" input box. Right and left mouse clicks raise and lower these if you hover the cursor over the number to be changed.

You will have to do this alignment for every mode decoded if need be. Also keep in mind the tool resets to hard-coded default "Center" values on each decoder. Fax mode will decode just fine at the tool default 1900Hz since fax doesn't have much bandwidth anyway. Most hobbyist ssb filters pass hf fax easily without moving the tools center frequency. This

green marker line is also handy to determine the frequency of interesting spectra on the FFT Spectrum Display, you read off the frequency as you superimpose the marker on the point of interest.

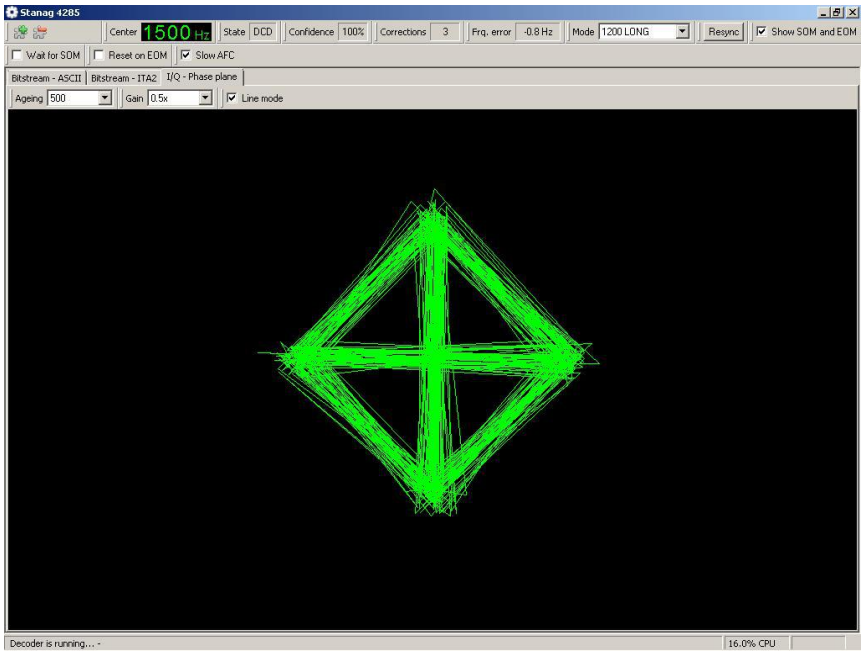
The standard 1800Hz offset expected by most professional decoding tools results from industry standard, typically milspec rated Professional filters that pass 3.3KHz centered on 1800Hz. The Professional ssb filter passes audio from 300Hz to 3600Hz, with 1800Hz being the center of the filter.

Here's how to get around these limitations; In this example you're not a Professional but a hobbyist and want to decode a STANAG4285 signal with this tool. Your non adjustable (meaning non dsp filtering) hobbyist-quality IF filter passes about 2800Hz, from 100Hz to 2900Hz centered on 1500Hz. Obviously this isn't going to work well when you are using an 1800Hz IF center in the decoder as that would lop off some 200Hz of the desired signal to be decoded. This can hinder copy. Also, the far ends of the hobbyist-quality filter are normaly where one finds the worst group delay. Well, that's true of most any analog filter, even Professional grade. So with the hobbyist receiver at 1500Hz IF center, 2.8KHz filter width, and a decoding tool with a 1800Hz center you're lopping off 200Hz minimum of desired S4285 signal and likely more due really bad group delay when the radio is tuned such that the tool decodes at 1800Hz center.

Group delay is where the signal passed in, say, the middle of the filter arrive "sooner" (usualy this is the case) than the signal passed near the ends of the filter, thusly distorting the output. And it gets worse, the filter will likely have different group delay at each end of the filter passband. Humans deal with this distortion with no trouble and usualy don't notice it at all. A voice signal can have loads of group delay yet still be understood by people, it mostly goes unnoticed.

The digital world, however, expects a flat group delay for any input; from one end of the filter passband to the other they want the same group delay if any is present. It's bad enough we're passing digital signals via the analog ionosphere wich does all sorts of crazy analog things to any signal and here a digital device is really expecting perfect digital input signals. If that digital device had emotions it just might be disapointed with this situation.

Being locked into a specific IF center and having undesired group delay due to poor filters is a more or less analog radio problem that doesn't or needn't apply to dsp radios. We can still get the best out of analog radios with some effort, by making some simple changes in the tool rather than the radio. If you have a dsp or sdr radio they can go a long way to reducing or eliminating group delay and often can have their IF centers adjusted to the expected 1800Hz easily. Sdr or dsp IF filters are created in software and are typically designed for minimum group delay, maximum symmetry and pass band flatness, and can often adjust the filter center frequency and its bandwidth to suit. Some analog radios also have a means to vary bandwidth, but these often simply increase group delay and distortion as the passband is altered from alignment.



Above we see a properly tuned STANAG4285 signal running at 1200L with the tool center at 1500Hz. The filter in the radio is set to 2.5Khz width, and passes a bit more than 1200Hz each side of 1500Hz center. Always want filters to be just a bit wider than the signal to allow it to slip past the walls of the filter without rubbing, thusly not passing any more band noise than needed. Note that 2.5KHz bandwidth does provide about 50Hz of excess either side of the desired signal as a STANAG4285 signal, at least the parts of it we're interested in, is about 2.4KHz wide according to Harry Nyquist.

Considering the qualities of hobbyist class filters, it is usualy going to be a benefit to use a filter a good deal wider than suggested by the Nyquist criterion in an analog radio. For example, a S4285 signal can pass - without signal degradation - a 2.4KHz wide filter, but that 2.4KHz filter had better be perfect in all its ways - meaning no group delay and absolute passband symmettry. Digital filters come close enough to perfect to be considered as such. Analog hobbyist class filters, especially those of the ceramic variety, will display their best traits in the middle of the passband at least as far as group delay goes. Thusly a wider filter may help in such cases, by keeping the desired signal within that part of a filter that passes the signal more faithfully. If your 2.8kHz wide filter sucks, try a 4kHz wide filter. Also if you selected a 4kHz wide filter for S4285 decoding you wouldn't have to bother with changing IF center. However, copying a 2.4kHz wide signal in a 4kHz bandwidth lets in a lot of noise with that signal.

So you now see why a (close to ideal) 2.5KHz wide filter works for this mode and we don't always need a 3.3KHz filter. It'll work far better if that 2.5kHz filter is a dsp filter than an analog filter, but if that analog filter is a high quality filter it may do the job well. Older Professional radios will likely have a 3.3KHz ssb mode filter as that is/was a common spec for military/government/commercial hf radios, and this is changing.

With the advent of COTS sweeping governments worldwide we may be seeing a lot less distinction between what is considered professional and what is considered amateur or hobbyist. Commercial Off The Shelf means no military/government specification need fulfilled for an agency to buy and use commercial, store bought consumer products. This likely means fewer and fewer analog filters will be designed/produced for a 3.3KHz width (and 1800Hz centers) even for Professional use as a 3KHz or narrower ssb filter becomes the Professional ssb norm. Today, 3kHz is considered the de facto voice bandwidth on hf, but in the past many government and commercial radios came with 3.3kHz filters anyway. Considering the increased occurance of wideband hf signals with some high speed hf modems covering 24KHz or more - usualy in steps of 3KHz, we should see 3kHz wide ssb filters become standard even if created by dsp and inherently unlimited in configuration.

The decline in analog filter manufacturing is being offset/caused by the increase in the use of dsp filters, wich can be designed to be superior in every way to their analog counterpart. Hardware filters may in time become a hobbyist only item save for as IF "roofing" filters in commercial products. Roofing filters don't really contribute to or determine final IF bandwidth, they're used to simply limit the spectrum seen by the adc - analog to digital converter, so the adc isn't overloaded by off frequency signals.

Improving S4285 (and other) signal decode with narrow filters;
One simple way to field test if a signal is helped or harmed by a filter is to tune to a weak signal using a wide filter and let the tool sync. Once sync is stable simply select the various narrower filter bandwidths and note their effects upon the signal, allowing time for the decoder to settle down between filter changes. If there's no change or at least not an apparent negative change, the filter is suited for that mode and is probably of benefit since it reduces band noise the decoder would otherwise have to deal with, even if only a few hundred Herz of noise. If you note decreased "Confidence" and increased "Corrections" you know the filter is a detriment to that signal. Keep in mind that with narrow filters you should take note of your frequency error, too much error on a narrow filter and you may start lopping off signal instead of just noise.

To really do this filter testing the scientific way you'd have to set up a ionospheric simulator and use the same signal over again on each filter through the various noise, doppler, multipath, and fading regimes. But live on the air signals have the appeal of being;
1. Real world.
2. There when you need them.

3. Cheap.
4. No setup time much longer than turning the radio and pc on.
5. More fun.

So I feel better now we have filters and group delay and center frequencies and so on covered.

Lets decode something already.

PSK STANAG4285
I'm in STANAG4285 mode as you can tell so we'll begin there. So you know, STANAG stands for STANdardised AGreement, a term coined by NATO to wich they all agree to use the same design criteria for whatever is going to be standardised; weapon ammunition, socks, hf modem protocols, you name it.
If you've never seen or heard a S4285 signal you first need to know what a S4285 signal sounds like and where to find them. If you don't know what they sound like, just google some examples on youtube or wherever. For a S4285 signal we should preset the receiver for USB mode, fast agc, 3KHz bandwidth, and account for the filter center in the tool if required. Tuning in 10Hz steps as a fine stepping will usualy work in any decoder. The tool will account for slight mistuning on its own. The idea is to align IF filter center with the decoder center, and then tune this combination as one via the vfo to the signal.

Then we need to find some S4285 on the air, wich won't be a problem as it's all over hf. Literally 24/7 even. Mainly because all of NATO uses it. Pick out a good clean strong S4285 to roll the dial onto. Doesn't matter if it's encrypted or not, you just want to practice tuning a live signal. Once you find a clean strong suspected S4285 signal you may find it easier to tune off a KHz or so to one side or the other and roll onto the target from above or below. This tuning method may seem time consuming but if you try to tune by attempting to center the signal in your filter as depicted by the FFT Spectrum Display you may take more time tuning back and forth trying to find the sweet spot than if you tune from one end to the center.

First make sure the tool is running and hears band noise, select PSK from the "Add decoder" menu, and scroll to S4285. For STANAG4285 mode ensure "slow afc", "Wait for SOM", and "Reset on EOM" are unchecked in the Bitstream-ITA2 parser window. Then you simply need to tune the radio slowly towards the center of the signal in 10Hz steps or finer untill the "Confidence" field and the "Corrections" field start getting some numbers - any numbers are fine at this point. Then stop when you do. If you're looking at the "I/Q Phase plane" of the STANAG4285 decoder window when you hit the sweet spot you will either see some green dots start moving on the black background, wich dots represent bits in some phase displays, or tangled green lines moving about if the lines option has been selected.
The "Frequency Error" box will show you wether you're above or below the center of the signal. Staying within +/-30Hz may be a good idea. With experience you may find yourself tuning by sound alone. To me a tuned in S4285 signal sounds almost like an old steam train chugging along the tracks.

By design, a good S4285 decoder - meaning written to the actual STANAG4285 military specification - will lock onto the signal from plus or minus 75Hz of the center of any decodable S4285 signal, so when you get that close to the signal center you should expect the tool to do something. Another neat trivia tidbit about S4285 is the protocol basically is coded so that there's a 1 in 2 billion chance that the tool will sync on noise.

If "Wait for SOM" and "Reset on EOM" are checked it will inhibit text copy as those signals are only sent at the beginning and end of any transmission, wether that transmission is an idle/channel marker signal that lasts for hours or a short duration qso with a ship. Also if they're enabled before you sync up you'll have to disable them to verify those stations that are broadcasting in the clear. Then after clear text is verified you may try enabling SOM/EOM so you don't end up with 500 miles of "ry's", "sg's", and "testing" to sort through to read the desired message traffic logs.
Something to keep in mind is it may pay to leave the tool tuned 30Hz or so off one way or the other of any S4285 signal for long term monitoring or in a noisy signal environment. This seems to aid in keeping the tool synced for hours at a time.

The S4285 decoder in Sorcerer defaults to 600L rate/interleave wich is a fine place to start. Most S4285 hf signals are long interleave, indicated in the decoder "Mode" list by the presence or absence of L or S following the rate. L is for long, S for short, no letter means no interleave. Currently on hf either 300L or 600L data rate are most common, with a few 1200L broadcasts here and there. Shame S4285 has no built in protocol for announcing rate and interleave, you have to sort that out on your own.

The "Confidence" figures box on the decoder indicate the viterbi decoder outputs that say how likely or not they think you're tuned to a S4285 signal. The "Corrections" field shows how many errors were corrected by the tool per the fec/interleaver in the signal. Google for viterbi decoder and/or fec error correction and interleaving if you want to know more. There are multitudes of papers written about the S4285 and other STANAG protocols one may download if interested in the working parts.

As a second must pass for short interleave signals and 10 seconds for long, remember to tune slowly, only a few tens of Hz at a time, 20 or 30Hz, and give about 10 seconds between tuning steps as the decoder won't sync and display meaningful results untill the interleave length time period has passed after any frequency change. You may have to roll the dial back a few tens of Hz and wait for the interleaver to catch up if you roll into and past sync while tuning. If you bump the tuning dial or hit the "Resync" button don't expect sync to stabilise instantly. After you've tuned S4285 a few times it's easy and you may even start to enjoy the challenge.

With any luck you tuned to within 75Hz or less of the S4285 signal center and you've got numbers in both fields. At first while the tool is syncing up the numbers may be all over the place and that is good, the tool is working. However, the numbers we always work towards are "Confidence" 100 and "Corrections" 0. Always and under any circumstances. The closest you can come to those usualy indicates the "right" settings for that specific S4285 signal with one caveat - the rate and interleave agree with the phase display. Channel noise and multipath and doppler often work against us getting a syncable signal or cause us to not get the steady numbers we want, but we can make do with what we get because this is a really good tool and you know what you're doing.

Question: Ok so within a few dozen Hz of signal center per the tool, you've got a highish "Confidence" (average above 60) and a lowish "Corrections" level (about 20 or less) but say it's not a stable 100 and 0. So what can we look at to tell us what the true nature of our S4285 signal is and account for it?

Answer; Look at the decoders "Phase plane" display tab. Lines or dot blobs in a more or less horizontal plane indicate 600 or slower rate, lines or dots in a diamond shape indicate 1200 or faster rate.

So now that you're thinking in the right direction the next step is to determine the exact data rate, and that will be the one that gives us 0 "Corrections" in the best case, the lowest attainable in the worst case. Step through the rates till you find the one that results in "Confidence 100" and "Corrections 0" and ensure the rate selected is correct per the phase display. Don't be surprised if just about any rate we select may result in 100 percent "Confidence" for an S4285 sig, keep in mind we wish to see 0 "Corrections". Try the various rates, starting with the L interleaves, untill the lowest "Corrections" are seen, then you have done all you can.

If the phase dots are a giant glob in the center of the screen, or in line mode the lines are a huge tangled mess, it may be a weak, fading, or multipath-ridden 1200 or faster modem. At certain times even slower rates will also make a mess of the phase display but these usualy clear up with patience and settle down to their normal horizontal selves. Strong 1200 rate signals will almost immediately form an obvious diamond shape phase display no matter what the rate and interleaver is set to, the phase display is independent of the rate selected. I've yet to see a rate faster than 1200 on the air but S4285 is capable of faster rates and these rates are available in the decoder.

Other radio decoding softwares may also show the phase plane of a signal, and may display 8 dots or phase lines for a given S4285 signal as seen at the decoder input whereas this tool shows the phase plane of the decoder output.

Another help to determining rate and so on with a S4285 signal is by watching the output of the Ascii or ITA-2 parser

window. If the signal is plain text, unencrypted, the Ascii or ITA-2 window will show gibberish on a signal that is not being decoded properly, but will show much the same gibberish repeatedly. Thusly we suspect there's a plain text signal in there, we just have to find the right rate/interleave. If the signal were encrypted the Ascii, ITA-2, and VisualBits parsers will simply fill with random data at all settings. You could always just call the station up and ask what rate they're sending at.

Decode Product;
So what do you get for all this time and painstaking adjustment of pc and radio to intercept a S4285 signal?

Not much! :D

Seriously though you should be proud of having successfully tuned in a STANAG4285 signal! How many people outside signals intelligence and the utility radio hobby do you know can do that? I think you should consider yourself of the elite. Surely this skillset affords bragging rights.

As most S4285 traffic is encrypted you'll consequently most often get gibberish. However, some signals are in the clear and you can follow along when they have traffic. Which traffic mostly consists of ships sending to the shore station on another frequency and the shore station acknowleging the traffic on one of their fleet broadcast/channel marker frequencies ... that you're tuned to since it is broadcasting in plain text. A fleet broadcast is a signal all surface ships of a fleet monitor, a channel marker is a signal that pretty much just keeps others from using that frequency at that time. Normaly, a fleet broadcast will be encrypted. You can bet that many of those encrypted S4285 signals you come across on the bands are just that, however in an emergency you might rationally expect to see interesting traffic on channel marker broadcasts. When not encrypted S4285 traffic is usualy decoded into plain text in the "Bitstream-ITA2" parser of the S4285 decoder, 5N1 Framing, everything else unchecked. Never seen anything plain text sent "Bitstream-Ascii".

You didn't really waste all this time for gibberish. Say you've been sitting on a plain text S4285 signal sending the same few phrases over and over for hours and it suddenly goes off the air. Don't tune away in bored disappointment just yet, go back to whatever you were doing while waiting for traffic, there's a chance that shore station is receiving ship traffic on another frequency and will shortly resume transmitting on the frequency you're tuned to, wich again is likely a fleet broadcast/channel marker frequency. Their reply to the ship should be forthcoming if so.
The ship (and likely entire surface fleet) listens to the broadcast of the shore station you're tuned to while the shore station typically listens out for ships on discrete frequencies. Sometimes the Fleet Broadcast/Channel Marker abruptly changes the idle signal sound pattern noticeably, and this is also an indication traffic of interest may follow. You'll know this signal because instead of the rythmic chugging of a S4285 signal, it makes an NNNNNT! sound.

If you were somehow monitoring the ship frequency you may have copied the message it sent if it wasn't encrypted and/or wasn't in a different mode, wich are more than possibilities. I feel that we should expect this ship to shore traffic to be encrypted as it is a military message. For that matter I wonder why the channel markers are in plain text, must be some overriding reason they're not. The ship side of the two way exchange will be brief and you'll be lucky to find it as the frequencies may change daily or hourly. As a rule, warships generally don't transmit unless they must and only for long enough to pass the traffic. Keying a radio on the high seas (or anywhere) is an invitation for direction finding and further signals intelligence scrutiny, especially in the case of warships. For example, Germany lost a good number of their UBoot fleet in WWII due primarily to HF direction finding done on land and at sea. An exception to be considered is Link11/SLEW, wich is a encrypted NATO warship broadcast often found on hf. Its use is more or less line of sight limited as far as net participants go. Yet Link11 can be heard hundreds or thousands of miles away. It's a digital signal allowing network members to share data and display sonar and radar tracks of interest to the entire task force. Since a Carrier Battle Group is kinda obvious on the high seas, it doesn't mind giving away its position with Link11 and other transmissions - everyone interested already knows they are there.

That being said, many warships carry efficient non-directional vertical monopole and wire antennas for hf use and can transmit with rather high power, so theoreticaly they can indeed be monitored as their signals should propagate quite efficiently over the expanses of salt water they sail. It stands to reason we should hear the ships perhaps even better

than we hear the shore stations, wich shore stations may use directional antennas with gain and even higher power than the warships. Then again the ship may send in HF FH/AJ (Frequency Hopping/Anti Jam) mode where the transmission changes frequencies many times per second. Or via satelite perhaps, and was responded to by the shore station on hf, thus making ship to shore difficult to intercept for a hobbyist. One can always attempt it.

I suspect that the shore station stops sending on the broadcast/channel marker frequency so the absence of the signal alerts ships monitoring the fleet broadcast/channel marker that the shore station's currently handling traffic, possibly unavailable for any other traffic. I also suspect that this traffic could be entirely automated on both sides of the contact, with humans inputting a message to be sent and machines handling it from then on untill it gets to the addressee. I am at odds with the idea of full automation since I have intercepted traffic that may be considered opchat (operator chatter) to an extent, so a mixture of automation and human intervention is likely here.

All following decode was done with tool set to 1500Hz center, receiver set for USB mode, 3KHz filter width, fast agc time constant.

Example traffic; shore station sending to ship;

"[SOM]
OVFR
FR EDCNBB ODTE3
%73'0') 4 19:671+ ,9= 13MJJE
KKKKI
FR FR FR
DE FUE FUE FUE
QSL R 190020Z NOV 13
TIME 0046Z
KKKKILO
DFF
[EOM]"

In the above traffic example, shore station "FUE" is rogering for traffic it accepted with the following line;

"QSL R 190020Z NOV 13TIME 0046Z"

QSL means traffic was copied, R may mean "Routine" message precedence as sent by the message originator or it may be R for "Rogering" (accepting) the traffic or some other signal. When a mil/gov (typically naval) station "rogers" for traffic it is then legaly responsible for that message and bound to deliver that message according to regulations. The figures give time and date of message creation in Zulu/UTC time. SOM is Start Of Message and EOM is End Of Message, which are signals built into the S4285 protocol that will be sent to inform radio operators of traffic so they don't have to sit and look at hours of decoded idle text looking for interesting traffic like some hobbyists do.

The ship may then send more message traffic if it has any to send and the shore station will acknowlege it. There is also a measure of noise generated gibberish in the above example. It happens.

You may also see traffic like this as the shore station bids good journey to the ship it has just handled traffic for;

"[SOM]
VFS FS FS FS FS
DE FUE   FUE
MCI
BONNE JOURNEE
AR   AR   AR   AR

DFF
[EOM]"

In the above traffic the two letter code "FS" may mean the callsign of the ship. "DE" means "from" so you know.

Then, after traffic is passed, the shore stations go back to idle transmission, wich produces (hours of) copy such as;

"OVV
ZCZC
ABC001
ALM DE FUE ALL DE FUE ALL DE FUE
TESTING TESTING TESTING
RYRYRYRYRYRYRYRYRYRYRYRYRYRY
SGSGSGSGSGSGSGSGSGSGSGSGSGSG
0 9 8 7 6 5 4 3 2 1
0 1 2 3 4 5 6 7 8 9
INT ZBZ INT ZBZ INT ZBZ
NNNN"

After a successful decode one might justifiably be inclined to exclaim "Ha ha! We're in your net, listening to your dudes!" or somesuch.

There are people who say no one sends or uses "SOM" and "EOM" messages, well, if it's a S4285 signal, it's going to have "SOM" and "EOM" messages and you can use them to your advantage.
When the fleet broadcast/channel marker goes back to idle after you've copied traffic, "SOM" and "EOM" boxes can be checked in the decoder, then hit the "Resync" button so the decoder doesn't buffer hours of the idle message. Then hit save to save the traffic if desired and then hit erase buttons in the "Bitstream-ITA2" and "Bitstream-Ascii" and "VisualBits" windows if present. The next time traffic comes along the "SOM" message, which the shore station will broadcast, will cause the tool to begin copying actual traffic. Otherwise expect miles of idle message copy if you leave "SOM" and "EOM" boxes unchecked. This has to be done after any non-idle signals unless you want those miles of idle decode.

Other S4285 idle signals may produce output such as this;

"IDR02I(0)/IDR21 /IDR22 /IDR03I(0)/IDR01I(0)/IDR23 /IDR02I(0)/IDR21 /IDR22
/IDR03I(0)/IDR01I(0)/IDR23 /IDR02I(0)/IDR21 /IDR22 /IDR03I(0)/IDR01I(0)/IDR23 /)
3&3,$-:
O CANALE OCCUPATO
V CANALE OCCUPATO DA UTENTE NON IDENTIFICATOE
C ZUJ LISTE CHIAVI
U QSY
K QRV
M IMI(01-99) IMI PAGE...
AS AS
R QSL
N(2-9)
ZUJ RIGA...
IDR02I(0)/IDR21 /IDR22 /IDR03I(0)/IDR01I(0)/IDR23 /IDR02I(0)/IDR21 /IDR22
/IDR03I(0)/IDR01I(0)/IDR23 /IDR02I(0)/IDR21 /IDR22 /IDR03I(0)/IDR01I(0)/IDR23 /"

Assumed Italian navy.

And another idle signal decoded;

"//NSS2I(0)/NSSHGI(0)/NSS4I(0)/NSS5I(0)//
LEGEND:
I(N) IDLE
B BUSY
BQ BUSY (ARQ)
U UNREADABLE
K TRANSMIT
M REPEAT
N(01-99) RETRANSMIT
AS WAIT
R RECEIVED
C(2-16) CHECK
//NSS2I(0)/NSS3I(0)/NSS4I(0)/NSS5I(0)//"

Assumed Canadian navy.

The above two intercepts reveal traffic handling codes as well as the calls of what I assume are afloat units, individual or task groups, along with the shore stations own calls. I assume these types of intercepts are always fleet broadcast/channel marker shore stations.

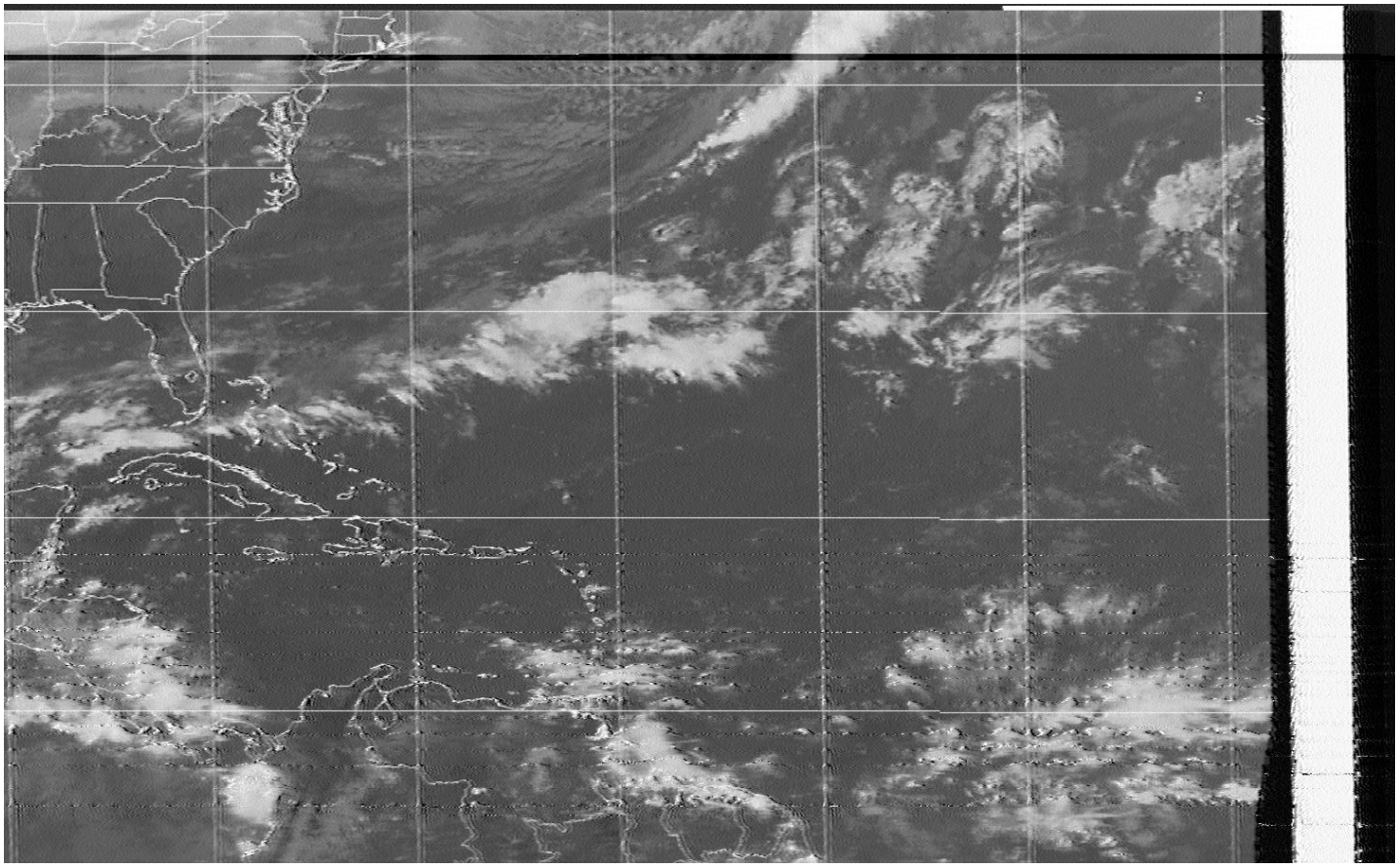
And one idle signal I found odd as I'm unsure of the language;

"AIT HBH
AIT HBH
AIT HBH
PPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPP
VFNNAC,,-:)3 @(22@(22@(22
TEZTAIG TEZTAIG
SYSYSYSYSYSYSYSYSJSYSYSYSYSYSYSYSYSYSYSY
ZGZGZGZGZGZGZGZGZGZGZZGZGZGZGZGZGZGZGZGZGZ
P N A U Y T S E W
KNYEH KNUZ DE BSACAUEAT FCO J EQAAIE PSEZ LU GSAL WRIJ
AIT HBH
AIT HBH
AIT HBH"

My guess for the above copy is Greek Navy fleet broadcast.

So that should get you up and running on S4285.

HF Fax
To decode HF Fax you must know what a fax signal sounds like and/or where to find them. Adjust the receiver for USB mode, fast agc, and get the tool up and running. Once prepared to copy fax with the tool select "Add decoder" then "Image" and then "FAX". Tune your receiver to a on air fax signal or to a frequency where you know fax to be broadcast. Keep in mind some fax frequencies are whole kilohertz, some are not. Hf fax all seem to run on a 1.9KHz offset from suppressed carrier frequency. The tool sets a decoding center frequency of 1900Hz wich can be left at default and most hf receivers will pass the fax signal easily when set to their default ssb bandwidth. HF Fax decoding works very well in the tool as does autosaving.



The tool offers various options for fax decode mode such as;
"FM Greyscale" "FM Black&White" "AM"

Note that the "FM" modes set the decoder center to 1900Hz while "AM" mode sets the decoder center to 2400Hz.

For hf use I find leaving the tool set to "FM Greyscale" works well even though not every fax needs greyscale shading, the satelite images relayed via hf fax will. If set to greyscale the decode results in more "noise" on the image than if it was decoded in black and white mode when copying fax that are black and white. If set to "FM Black&White" you will get a much cleaner decode of black and white fax but no greyscale image will be possible. You might want to know the schedule of a fax station so you can set the decoder to the right mode for each type of transmission at the right times.

As to image formatting, most hf fax are sent at a "LPM" of 120 and a "IOC" of 576, wich are defaults of the decoder for FM modes. Not all nations resort to those LPM and IOC conventions however, especially Russia and North Korea, so keep that in mind when you run across a fax signal.

If the tool is copying a fax signal and the image is not aligned where it should be, simply click on the margin wherever it is in the screen and the tool will justify the image for you. If the image shows tilt it indicates receiver or transmitter drift or soundcard error that could be accounted for if you took the time to adjust it out. You need a means to find the error, if any, wich is a topic for another paper. Then you would input the error figure into the box provided at the top of the fax decoder tool. Or you could enter the sound card correction globaly for all modes via the soundcard rate error option provided by the FFT Spectrum Display window "option" tabs.

Fax copy, due to it being an "amplitude" mode even if decoded via an fm demodulation scheme, can be performed under very low signal levels, even to the noise floor if one is unconcerned for the image quality such low signal levels generate. The tool simply works well at fax, and there's not much more to decoding hf fax with this tool than starting the fax decoder and tuning to a fax transmission.

When saving images, the tool will ask you for a directory to save to when you click the save button. The tool can also be set to save automatically, and will save to the same directory the tool was set to save to in the initial setup. When saved the tool will name the file with a date and time, a nice feature. It will save the images as .bmp files. When autosave is enabled, the tool will save when the next fax starts and sends the prepare to copy/clear screen signal. Clicking on the "Clear" button erases the image from the screen.

FSK SITOR-B

Once again you must know what a SITOR signal looks/sounds like before you can tune to and decode it, so google it if you don't. SITOR is a two tone FSK mode and uses forward error correction to impart a redundancy to the signal resulting in fewer errors on reception. These signals are often used to transmit weather reports to mariners and are still fairly common on hf for such an old mode. They can normaly be found amongst most other maritime HF signals such as fax and may have easily found schedules.

Preset your receiver to USB or RTTY/FSK mode, fast agc, and a filter bandwidth appropriate for the mode, in this case 200Hz or so if possible. A filter just wider than the signal of interest maximises desired signal power and minimises noise power for the decoder.

To decode SITOR traffic select FSK from the "Add decoder" menu and then SITOR-B. This will bring up a SITOR decoder. The next step is to tune the receiver to the signal, placing it well in the filter. If your receiver has a reception mode especially for "Rtty" or "FSK" use them if possible and adjust for any decoder center offset via the FFT Spectrum Display by clicking the center indication between the peaks of the FSK signal. There will be a pronounced null between the peaks and this null is where you want to place the decoder center. The decoder does well in obtaining and maintaining sync then.
Some features of the SITOR decoder;

- A force sync button is provided.
- The decoder has invert and unshift on space controls.
- The decoder is insensitive to the bfo sense of the signal - wether USB or LSB - and will automatically determine wich sense and adjust itself to it.
- The decoder will display its decode sense and sync status in the "Status" line. The decoder displays suspected errors in red font on the screen.

Here is some example SITOR traffic;

"FAOM CAMSPAC PT. REYES:
13 THE U.S. COAST GUARD HAS TE~MDNATED HF RADIOTELEX
(~8594) SERVICES AT THE FOLLOWING LOCATINS:
COMMUNINATIONS AREA MASTER STATION ATLANTIC (CAMSLANT NMN)
COMMUNICATIONS STATION KODIAK (NOJ)
COMMUNICATIONS AREA MASTER STATION PACIFC (CAMNPAC NMM/NMO)

2. COMMUNICATIONS STATION GKAM (NRV) WILT CONTINUE TO COLLECT
AMVER SHIP POSITION REPORTS AND OF METEOROLOGICAL OBSERVATION
MESSAGES UNTIL 31MAR2012 +359Z.

3. AMVER AND NOAA MELOOROLOGICAL REPORTS WILL CONTINUE TO BE
RECEIVED AT NO CHARGE THRU SHIPCOM/W O HF RALIOTELEX
SERVICE OND NOAA SHIPBOARD ENVIROAMENTAL DCQA ACQIISITION
SYSTEM (SEAS) PROGRAM THRU INMARSAT-C. AMVERRTEPORTS MAY
ALSO BE SENT AT NO CHARGE THRU GLOBE WIREESS.

?5

,.: &.$'' '8594 %3: ?49-$:-'5

16806.5 KHZ

TIMES: 001$ AND 1735 UTC

NOTE: CARRIER OR DIAL FREQUESCY IS LOCATED 1700 HZ BELOW THE AESIGNED FREQUENCY (-1.7 KHZ).

IF THERE ARE ANY IUESTIONSOOR COMMENTS REGARDING
SERVICE PROVIDED BY THIS STATION, PLEASE WRITE TO:

COMMANDING OFFICER
U.S. COAAT GUARD COMMUNICATION AREA MASTER STATIOI PACIFIC
P.O. BOX 560
PT RETES STATION, CA 9~94~+3/~~
USA

UNITAT STATES COAST GUARD COMMUNICATIONS AREA MASTER STATION
IACIFIC NOW HAS A TOLL FREE 24 HOUR INFORMATION TELEPHONE LINE,
THE NUMBERIIS 877-662-4636 (877-NMC-INFO).

PHONE: (415) 669-2047
FAX: (415) 669-2096
BT
DE NMC VAJJJJ:~~~~3~#/-'~~8=/~@~"

The tool is quite satisfactory at decoding SITOR traffic.

BPSK31

BPSK31 mode is a Bi-Phase Shift Keying mode commonly used by amateur radio operators consisting of a carrier that shifts between two 180 degree phases. It somewhat rivals cw and baudot for popularity in amateur radio circles. It can be as narrow as 31Hz in bandwidth so is very spectrum efficient. It provides for good copy at very low signal levels. It has no error correction (however there are narrow band psk amateur modes that do have error correction and detection) so unwanted energy in the input may result in "copy" of random noise generated gibberish on the screen. The tool is very sensitive and will copy signals down to the noise floor.

As usual one must know what a psk31 signal sounds like before decoding so google it if you dont. To decode BPSK31 and the other modes this decoder offers, click "Add decoder" and select "PSK" and then "HAM BPSK/QPSK modes". In the HAM BPSK decoder there are few options, not even a phase display. A more important option that is present is the psk mode selection option where you can select various amateur psk modes from the drop down list. Once again one must know beforehand what psk signal type is to be decoded unless willing to try the modes till copy results. With experience one knows what they are by their sound and look in the FFT Spectrum Display.

Set the receiver for USB, fast agc, and about as narrow a filter as you can select, even a 50Hz filter will maximise decoder performance once you have the signal tuned in. Tune to a PSK31 signal. Use the center feature on the FFT Spectrum Display to center the decoder in the filter's passband wich should be tuned directly on the signal. Copy then should proceed if you have selected the right mode of psk. The "Status" window will tell you what the decoder is doing. Save, erase, and so on work as in the other decoders. The copy is often messy with band noise but the decoder works nonetheless.

Example traffic with noise;

"o niEt
1
tnx fer QSO chris, 73, God bless.
11/25/2013 02:34Z N8EWX de KB2WXI sk
nreo
 i
oeCmd dF* toua e- a o EraeUL eB e * "

CW

CW (Morse) mode is the oldest form of man-made radio emission, starting out as a broad banded spark emission, then progressing to longer range and more efficient CW emissions. CW consists of merely emitting a carrier and regulating the time on and off the air to transmit information. The tool has a CW decoder, and I have to say I am impressed with it. Most decoder tools are not very good at decoding a CW signal at all. Most fail utterly. This one is not too shabby at all. it seems to thrive on faster sent CW, and those CW operators who use a keyer rather than a straight key are probably partialy to blame for this decoders success at CW decoding. If a machine is used to generate and send CW signals a machine usualy stands a much better chance of accurate copy than if the CW is hand sent by a human with a straight key. Machines send with digital precision whereas humans send a bit sloppier in comparison.

To copy CW simply click on "Add decoder" and select CW. Tune the receiver to a decent sounding CW signal and select a narrow filter if possible. The decoder offers little in the way of options other than to save copy and to manualy set decoding speed rather than allow the decoder to do so automatically. When using the CW decoder, in the FFT Spectrum Display window simply place the center indicator onto the signal of choice and observe the copy resulting. Using a very narrow filter seems to help in decoding. The decoder will indicate the sending speed of the CW signal it is tuned to.

Example hand sent CW;

"TMLDED AP ALSO USE OPEN WE FOR MAKING UP SOME LERGTH BUT TH5LONG WE IS 8 4FT LONG WITH COUNTERPOISE WE UP 25 FT MAKES FOR NICE SIE ANTENX = SOWXHR NOW 60F EXPECSNG COOLF TEM OVF NIGHT S BEEN VERY MINDY HR TODAY NEVF T ABE 70F SO WONT HOLDU JUST H U C AND TO RLYTOU HE THANKS G 5VING UOUES URS NOW GB 73 L SK AA 8 VDE WB3AAI/4 S KEE E"

A experienced CW operator would have no trouble understanding the above even with the added noise caused letters. The decoder is capable of better performance, this example was hand sent in a noisy/weak signal environment.

ARINC 635

ARINC 635-3 aka HFDL aka GlobeLink/HF is based on a number of interconnected ground stations. Each ground station transmits a frame called a Squitter every 32 seconds. The Squitter frame informs aircraft of the system status, provides a timing reference and provides protocol control. Each ground station has a time offset for its Squitters. This allows aircraft when trying to log on to jump between ground stations finding the best one as fast as possible. When passing traffic Time Division Multiplexing (TDMA) is used. This prevents two aircraft transmitting at the same time causing radio collisions.

This mode is called up in the tool via the "Add decoder", PSK, ARINC 635 menu. And as usual, one must know what an Acars signal sounds like and where to find them on hf or vhf for successful decoding. All hf acars signals I have monitored fall on a whole kiloHerz frequency. Use USB mode, fast agc, and a ssb voice bandwidth filter to best copy ARINC 635.

What do the check boxes mean ?

PREAM Displays received preamble information.
SPDU Displays Squitter Protocol Data Units.
MPDU Displays Media Access Protocol Data Units.
LPDU Displays Link Protocol Data Units.
BDU Displays Basic Data Units (Segmented messages fragments).
Verbose Displays very detailed output.
HFNPDU Displays Network Data Units; probably most interest.

The decoder offers individual windows for "Output", "Squitters", and "Acars".

Example intercepted HFDL traffic;

"Preamble 300 bps 1.8 sec Interleaver FREQ ERR 8.483709 Hz Errors 0
[MPDU 03:33:56 GND SLOT 1 300 BPS]
Ground station ID CANARY ISLE - SPAIN SYNCHED
NR AIR CALLS 3
AIR CALL 0 = LOG-ON
LPDUS = 1
Max Bit rate 300 bps
AIR CALL 1 = LOG-ON
LPDUS = 1
Max Bit rate 300 bps
AIR CALL 2 = CB
LPDUS = 1
Max Bit rate 300 bps
[LPDU LOG ON CONFIRM]
ICAO 1BAB61 ID CC TXW = 0 D(R) = 0 D(R)vect = 0
[LPDU LOG ON CONFIRM]
ICAO 1DEEE5 ID CD TXW = 0 D(R) = 0 D(R)vect = 0
[LPDU UNNUMBERED DATA FM GND TO AIR CB]
HACARS mode: 2 Aircraft reg: .A7-ADZ
Message label: _☐Block id: L [Uplink]
Message content:-"

I found the tool to decode HFDL better at low signal strengths than other tools I have used.

In Summation
Sorcerer is a formidable decoding tool, especially considering the price and effort needed to get set up. It offers hobbyists a taste of that class of "high priced because it's worth it" tools the pros use. It seemingly excels at what modes it does copy. Wish the full version, even if slightly dated and missing certain functions, was made available to hobbyists at a moderate cost. Thanks for reading this paper, I had fun writing it while exploring the tool and hope you found items of interest within it.

73, and good hunting.