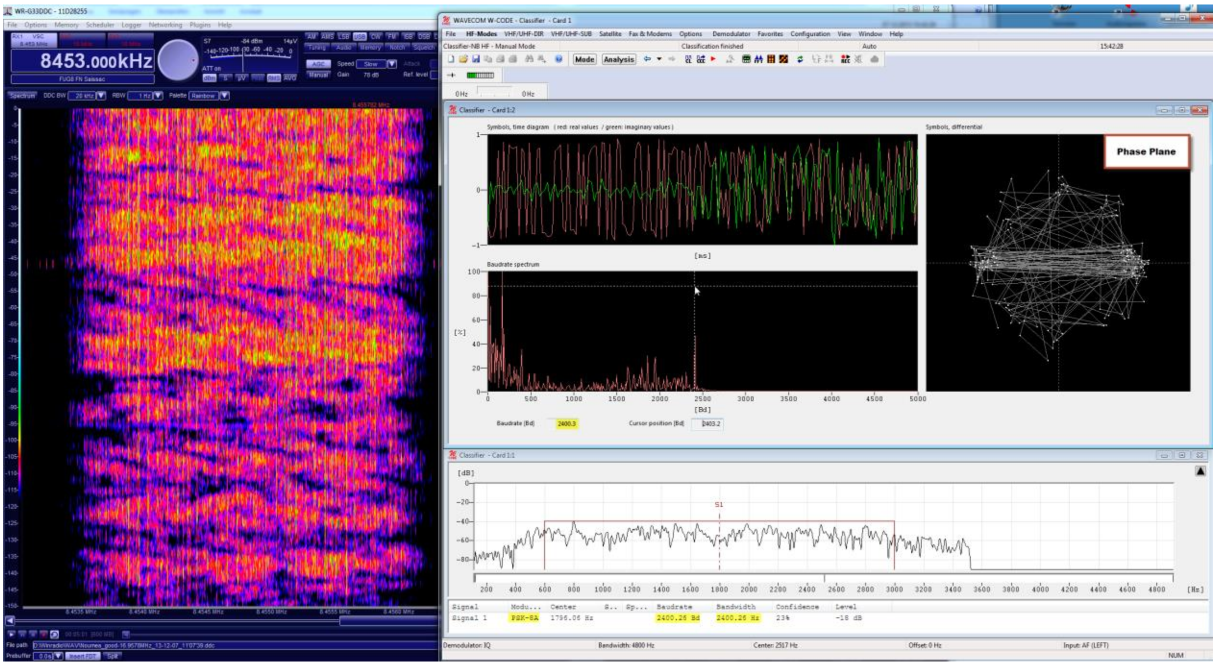
Some Notes on STANAG 4285 - A DXer’s View

STANAG 4285 is a single-tone modem, agreed upon by NATO member states in the 1980’s. The unclassified specification can be downloaded here. Until today, there are many NATO members, using this system - mostly enciphered. Please find below some hints from the DXer’s point of view.



Signal	Modu...	Center	S..	Sp...	Baudrate	Bandwidth	Confidence	Level
Signal 1	PSK-8A	1796.06 Hz			2400.26 Bd	2400.26 Hz	23%	-18 dB

Demodulator: IQ Bandwidth: 4800 Hz Center: 2517 Hz Offset: 0 Hz Input: AF (LEFT)

Figure 1: A strong STANG4285-signal in a fair-good quality, classified by Wavecom’s W-Code.

From Figure 1, you see all the important data. The speed is always 2.400 bps, the signal is 2.400 Hz wide and centers around 1.800 Hz. Thus, it covers around 600 Hz to 3.000 Hz in baseband.

There are several decoders around which cover STANAG 4285. Nevertheless, decoding can be somewhat frustrating. There are many reasons for that which you can’t avoid, namely a) encryption and b) decoders which would had needed a bit more work on this mode.

Fortunately enough, there a) some interesting transmissions with open text, and b) with Sigmira and Sorcerer you have two excellent decoders (not only) for this mode, and they are free.

Now for some points which you *can & should* avoid:

- The signals should be proper tuned. Try to tune them for 1.800 Hz center frequency as best as possible. Each 10 Hertz will count. According to specification, the difference between transmitter and receiver can be as large as ±75 Hz. Nevertheless, try to tune as much exact as possible!
- Don’t reduce the bandwidth of your receiver too much! You really need at least the range from 600 Hz to 3.000 Hz. If your receiver has only an SSB filter of e.g. 2,7 kHz width, you must use pass band tuning to get the whole signal into the pass band.
- Use a SDR as receiver! Only this type of receiver provides you with digital demodulation, plus digital filters. Try to avoid the AF part of any receiver as the soundcard of any PC. Use a “virtual soundcard” like VSC or VAC. Otherwise, you will produce additional distortion (level and phase) on which STANG4285 reacts quite sensible.

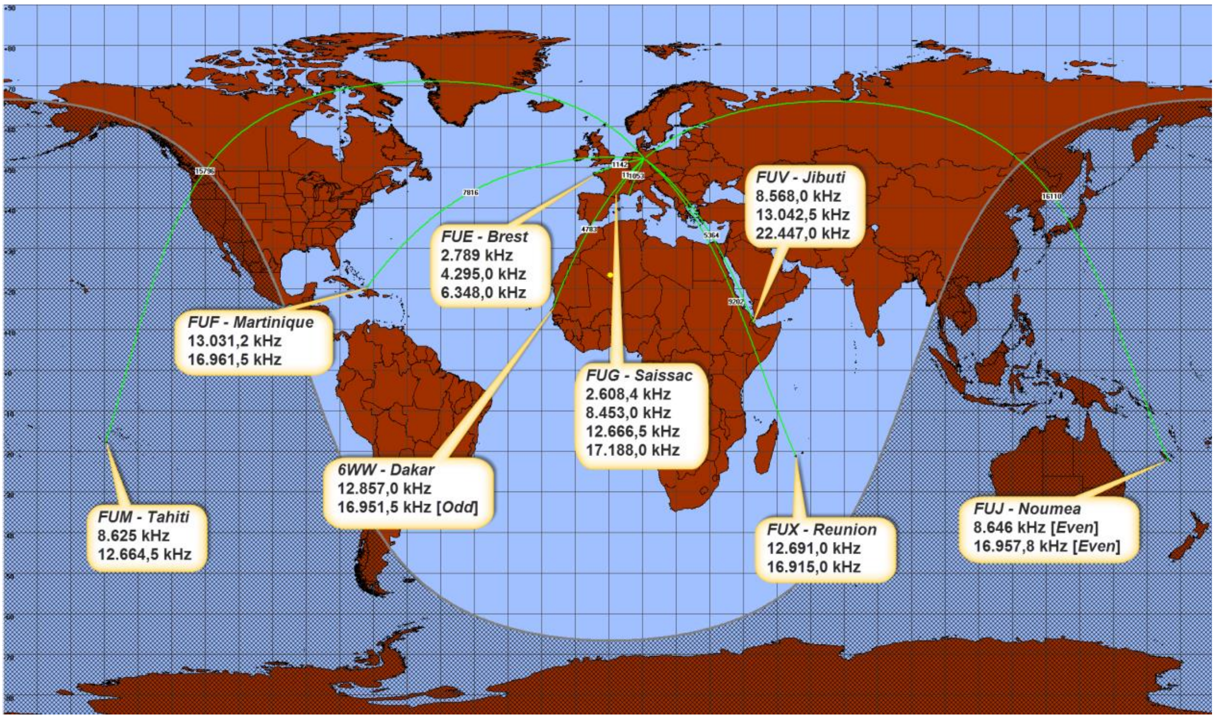
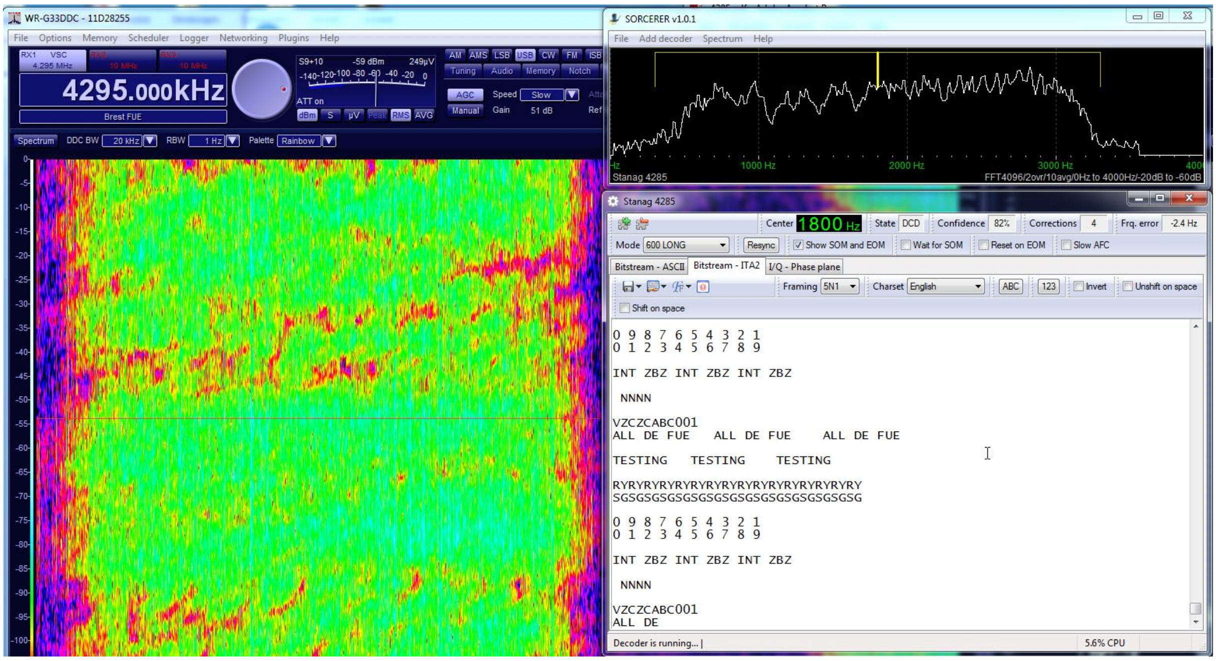


Figure 2: Some channels of the net of the French Navy, actually operated by DIRISI, proved a good starting point in receiving and decoding STANAG 4285 signals. Map made with PropLab 3.0.

First, try to tune (in SSB/USB) into one of the strongest signals of the map in *Figure 2*. In Europe, these are most probably located in Europe. Start your decoder (*Figure 3*).



Center 1800 Hz | State DCD | Confidence 82% | Corrections 4 | Frq. error -2.4 Hz

Mode 600 LONG | ☑ Show SOM and EOM | ☐ Wait for SOM | ☐ Reset on EOM | ☐ Slow AFC

Framing 5N1 | Charset English | ☐ Invert | ☐ Unshift on space | ☐ Shift on space

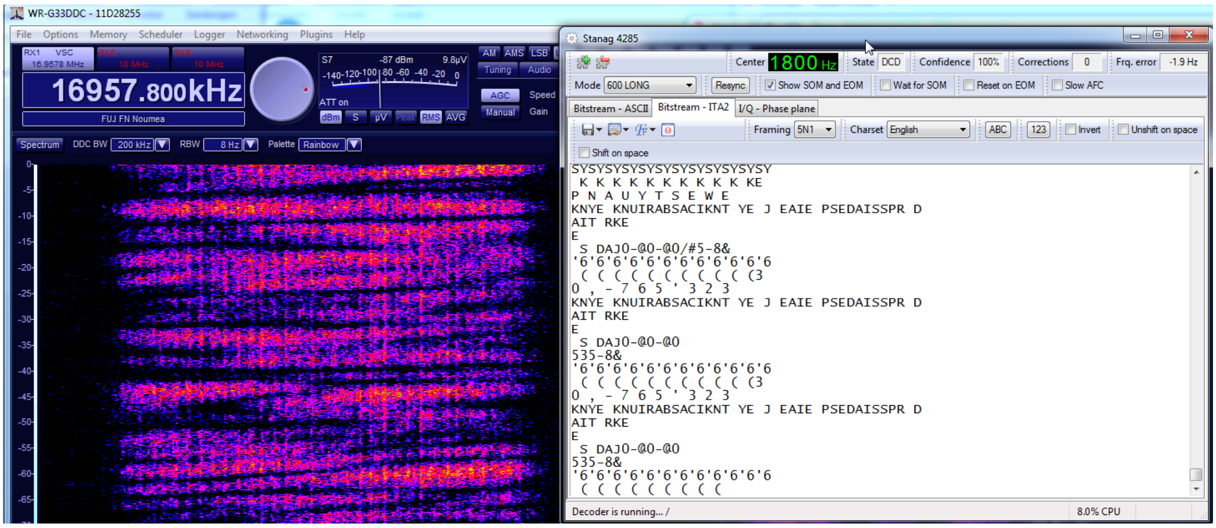
```
0 9 8 7 6 5 4 3 2 1
0 1 2 3 4 5 6 7 8 9

INT ZBZ INT ZBZ INT ZBZ

 NNNN

VZCZCABC001
ALL DE FUE   ALL DE FUE    ALL DE FUE

TESTING   TESTING    TESTING

RYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRY
SGSGSGSGSGSGSGSGSGSGSGSGSGSGSGSGSG

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

VZCZCABC001
ALL DE
```

Decoder is running... | 5.6% CPU

Figure 3: perfect decoding of FUE Brest on 4.295 kHz with “Sorcerer”: Center frequency 1.800 Hz, Mode “600 LONG”, Framing “5N1”. See following text on these values.

As said, the general speed of this single-tone modem is always 2.400 bps. The actual data rate can be set from 75 to 2.400 bps by the operator, according to the channel's quality. Usually, you will find 300, 600 and 1.200 bps. With open transmissions of the French Navy, 600 bps is the best bet.

STANAG4245 provides an interleaver, short or long. "600 LONG" is the best starting point for French Navy. "Data Format" (with "Sorcerer": "Framing") is another point, where the decoder must match the transmitter. Start with "5N1" (5 data bits, no parity, 1 stop bit).
"600 long" and "5N1" is the normal mode at *Figure 2*. Deviations from this rule occur at "parity", and has been added accordingly.

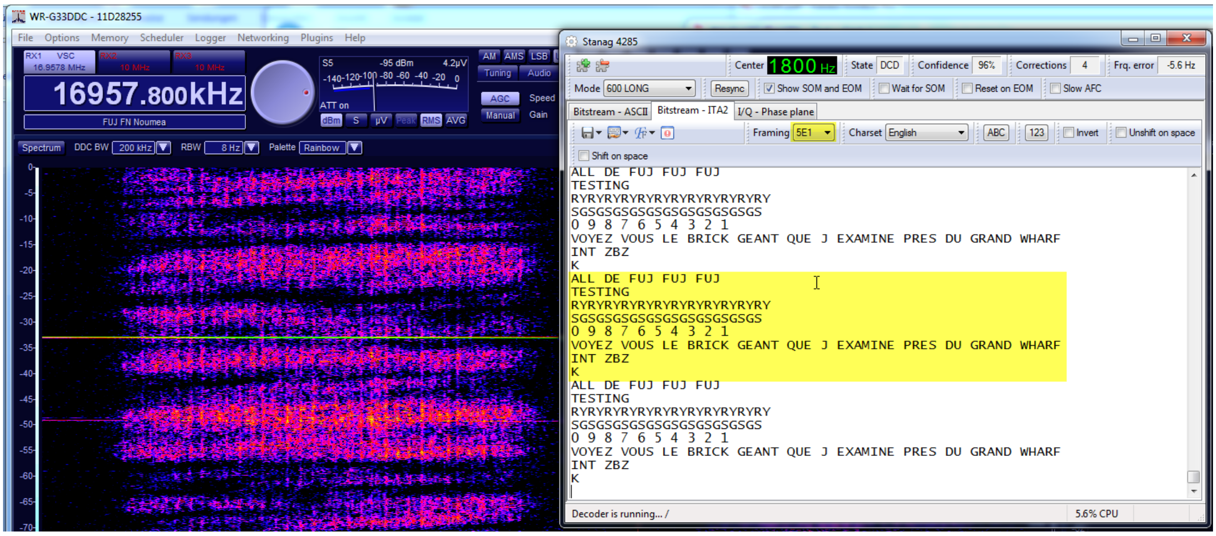


16957.800kHz
FUJ FN Noumea
Center 1800 Hz
State DCD
Confidence 100%
Corrections 0
Frq. error -1.9 Hz
Mode 600 LONG
☑ Show SOM and EOM
☐ Wait for SOM
☐ Reset on EOM
☐ Slow AFC
Framing 5N1
Charset English
☐ Invert
☐ Unshift on space
☐ Shift on space

```
SYSYSYSYSYSYSYSYSYSYSYSY
 K K K K K K K K K K KE
P N A U Y T S E W E
KNYE KNUIRABSACIKNT YE J EAIE PSEDAISSPR D
AIT RKE
E
 S DAJ0-@0-@0/#5-8&
'6'6'6'6'6'6'6'6'6'6'6'6
 ( ( ( ( ( ( ( ( ( ( (3
0 , - 7 6 5 ' 3 2 3
KNYE KNUIRABSACIKNT YE J EAIE PSEDAISSPR D
AIT RKE
E
 S DAJ0-@0-@0
535-8&
'6'6'6'6'6'6'6'6'6'6'6'6
 ( ( ( ( ( ( ( ( ( ( (3
0 , - 7 6 5 ' 3 2 3
KNYE KNUIRABSACIKNT YE J EAIE PSEDAISSPR D
AIT RKE
E
 S DAJ0-@0-@0
535-8&
'6'6'6'6'6'6'6'6'6'6'6'6
 ( ( ( ( ( ( ( ( (
```

Decoder is running... /
8.0% CPU

Figure 4: Obviously, something went wrong with this decoding of FN Noumea/New Caledonia. Enciphered, or is it just the "Framing 5N1"?

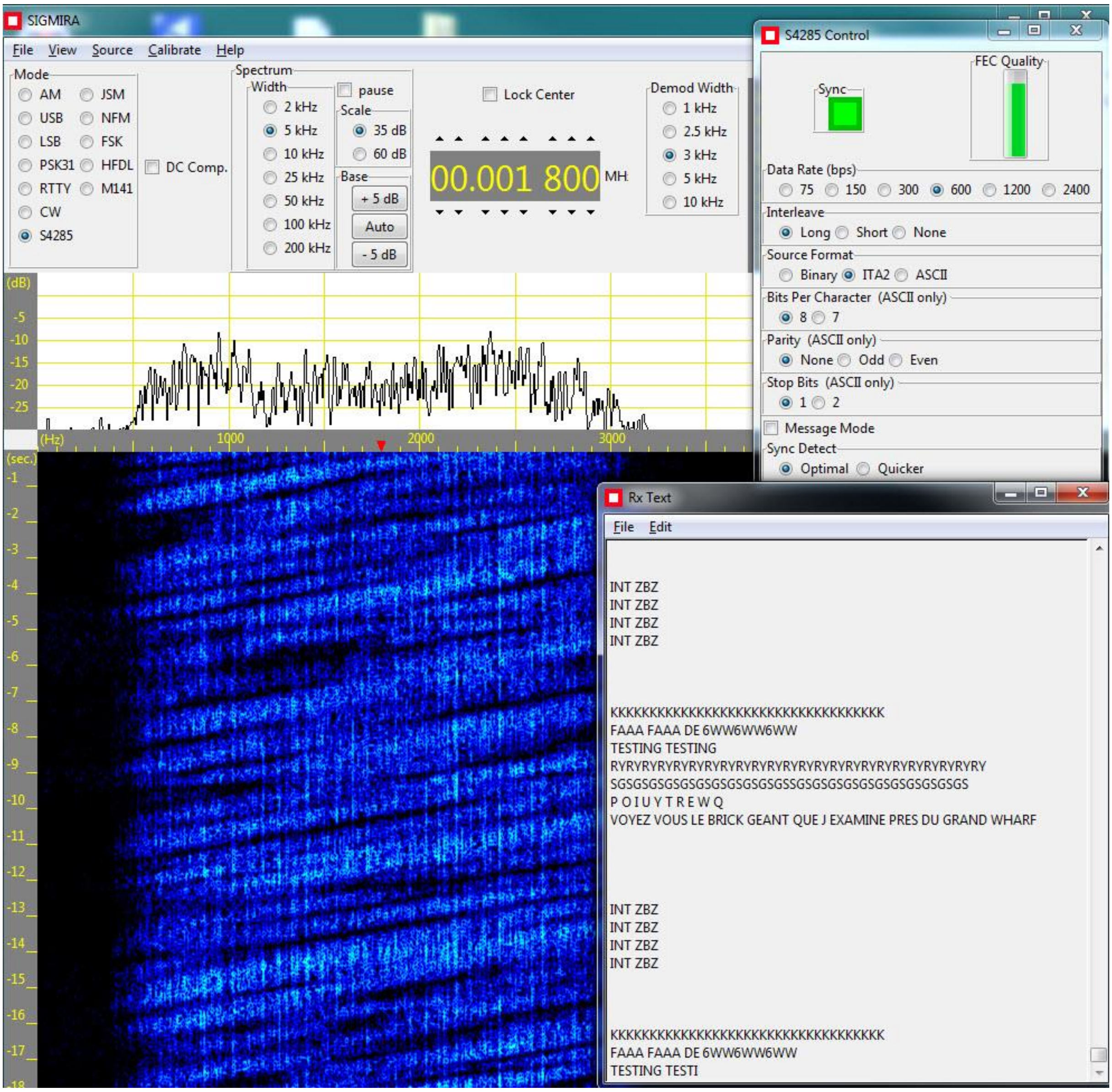


16957.800kHz
FUJ FN Noumea
Center 1800 Hz
State DCD
Confidence 96%
Corrections 4
Frq. error -5.6 Hz
Mode 600 LONG
☑ Show SOM and EOM
☐ Wait for SOM
☐ Reset on EOM
☐ Slow AFC
Framing 5E1
Charset English
☐ Invert
☐ Unshift on space
☐ Shift on space

```
ALL DE FUJ FUJ FUJ
TESTING
RYRYRYRYRYRYRYRYRYRYRYRY
SGSGSGSGSGSGSGSGSGSGSGS
0 9 8 7 6 5 4 3 2 1
VOYEZ VOUS LE BRICK GEANT QUE J EXAMINE PRES DU GRAND WHARF
INT ZBZ
K
ALL DE FUJ FUJ FUJ
TESTING
RYRYRYRYRYRYRYRYRYRYRYRY
SGSGSGSGSGSGSGSGSGSGSGS
0 9 8 7 6 5 4 3 2 1
VOYEZ VOUS LE BRICK GEANT QUE J EXAMINE PRES DU GRAND WHARF
INT ZBZ
K
ALL DE FUJ FUJ FUJ
TESTING
RYRYRYRYRYRYRYRYRYRYRYRY
SGSGSGSGSGSGSGSGSGSGSGS
0 9 8 7 6 5 4 3 2 1
VOYEZ VOUS LE BRICK GEANT QUE J EXAMINE PRES DU GRAND WHARF
INT ZBZ
K
```

Decoder is running... /
5.6% CPU

Figure 5: It's simply the "Framing"! If we switch to "5E1", we get the clear text.



Mode: ● S4285

Spectrum Width: ● 5 kHz

Scale: ● 35 dB

00.001 800 MH

Demod Width: ● 3 kHz

Data Rate (bps): ○ 75 ○ 150 ○ 300 ● 600 ○ 1200 ○ 2400

Interleave: ● Long ○ Short ○ None

Source Format: ○ Binary ● ITA2 ○ ASCII

Bits Per Character (ASCII only): ● 8 ○ 7

Parity (ASCII only): ● None ○ Odd ○ Even

Stop Bits (ASCII only): ● 1 ○ 2

☐ Message Mode

Sync Detect: ● Optimal ○ Quicker

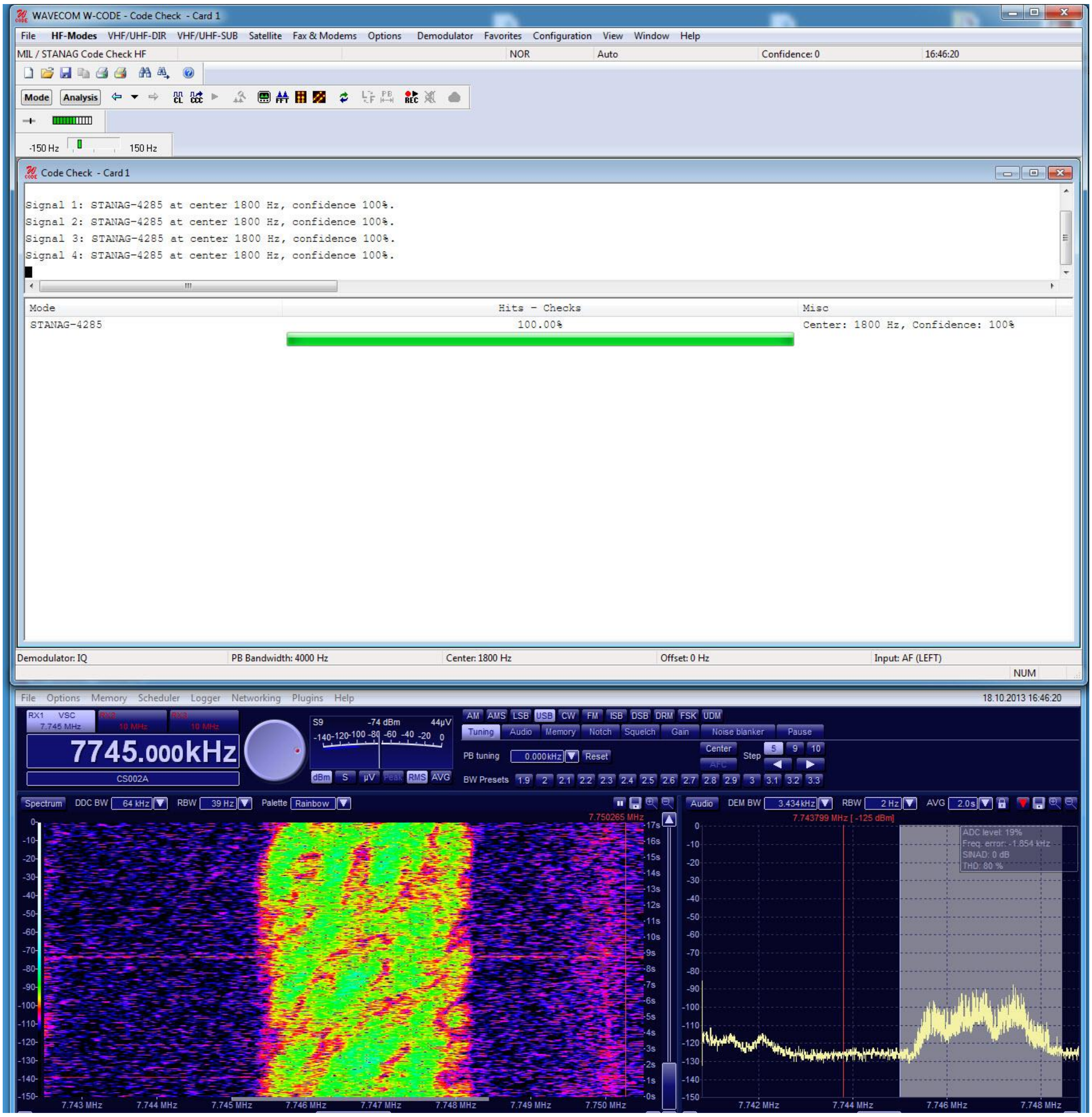
```
INT ZBZ
INT ZBZ
INT ZBZ
INT ZBZ



KKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKK
FAAA FAAA DE 6WW6WW6WW
TESTING TESTING
RYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRY
SGSGSGSGSGSGSGSGSGSGSGSSGSGSGSGSGSGSGSGSGSGSGS
P O I U Y T R E W Q
VOYEZ VOUS LE BRICK GEANT QUE J EXAMINE PRES DU GRAND WHARF



INT ZBZ
INT ZBZ
INT ZBZ
INT ZBZ



KKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKK
FAAA FAAA DE 6WW6WW6WW
TESTING TESTI
```

Figure 6: Sigmira also has an excellent performance in decoding STANG4285. If using the sound card as input, you must switch the "Center Frequency" to "00.001 800 MHz". Here FN Navy 6WW from Dakar/Senegal on 12.587 kHz.Sigmira always needs the latest "features.dat" file. So if Sigmira refuses to open, just get this file from the Sigmira homepage.

All said above works only if we know all data on the STANAG4285 transmission. *Figure 7* describes a more professional workflow of what to do, if you know nothing about data rate, interleaver etc.

Figure 7: A more professional approach of getting all important information of a STANAG4285 signal.

With free software decoder, your only chance is “brute force”: just try all possible combinations. Only with professional decoders, you are able to perform the workflow as shown in *Figure 7*. *Figures 8* to *13* will demonstrate just that at live examples.



MIL / STANAG Code Check HF NOR Auto Confidence: 0 16:46:20

```
Signal 1: STANAG-4285 at center 1800 Hz, confidence 100%.
Signal 2: STANAG-4285 at center 1800 Hz, confidence 100%.
Signal 3: STANAG-4285 at center 1800 Hz, confidence 100%.
Signal 4: STANAG-4285 at center 1800 Hz, confidence 100%.
```

```
Mode                 Hits - Checks        Misc
STANAG-4285          100.00%              Center: 1800 Hz, Confidence: 100%
```

Demodulator: IQ PB Bandwidth: 4000 Hz Center: 1800 Hz Offset: 0 Hz Input: AF (LEFT)

Figure 8: Is it a STANAG4285 signal? W-Code’s Classifier says “yes”, with 100% confidence. After classifying the signal, this decoder automatically changes to STANG4285 decoder.

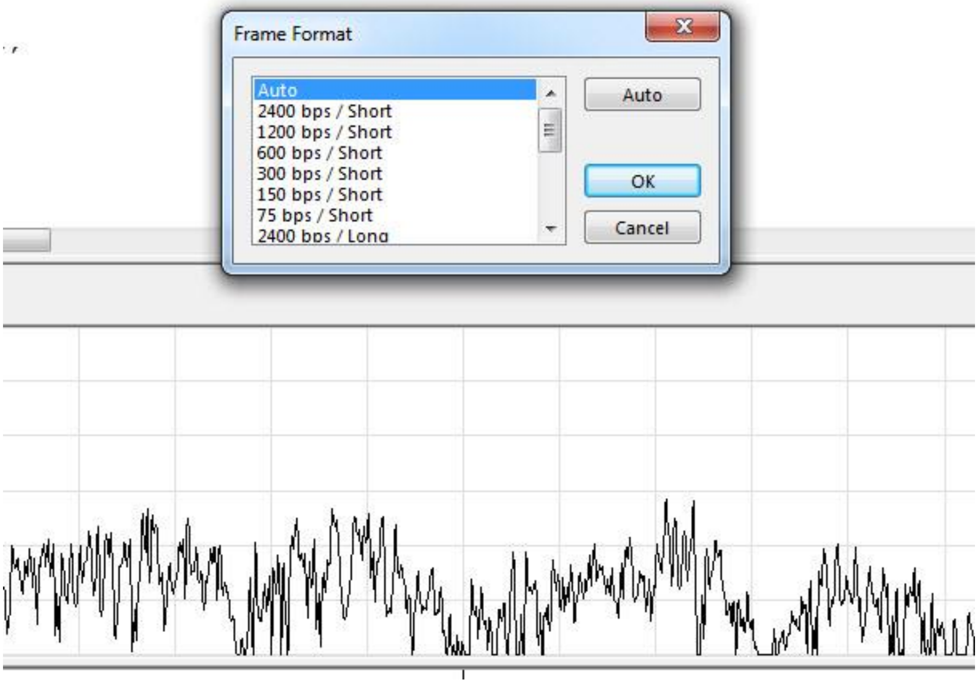
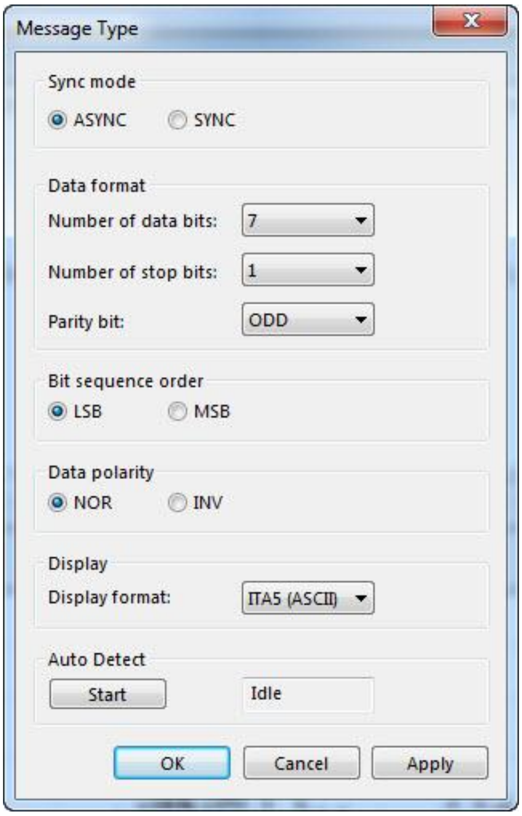


Figure 9: There we have to get the “Frame Format” first. “Auto” will measure that automatically.



Message Type

Sync mode
● ASYNC ○ SYNC

Data format
Number of data bits: 7
Number of stop bits: 1
Parity bit: ODD

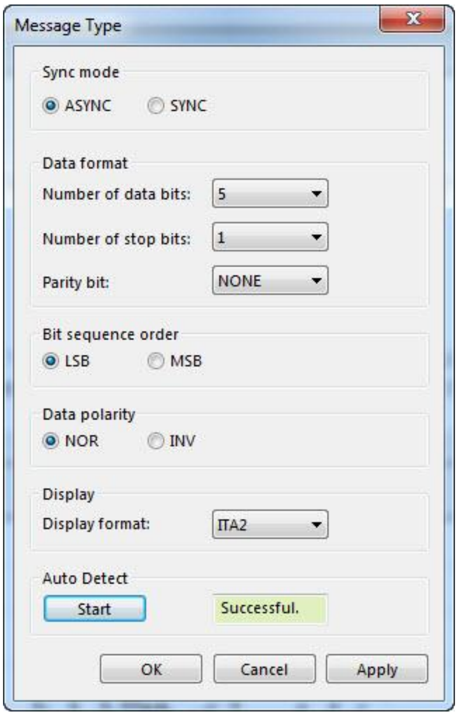
Bit sequence order
● LSB ○ MSB

Data polarity
● NOR ○ INV

Display
Display format: ITA5 (ASCII)

Auto Detect
Idle

Figure 10: Next step must answer the question: “Which message type?” W-Code does this by “Auto Detect”, click “Start”.



● ASYNC ○ SYNC

Number of data bits: 5

Number of stop bits: 1

Parity bit: NONE

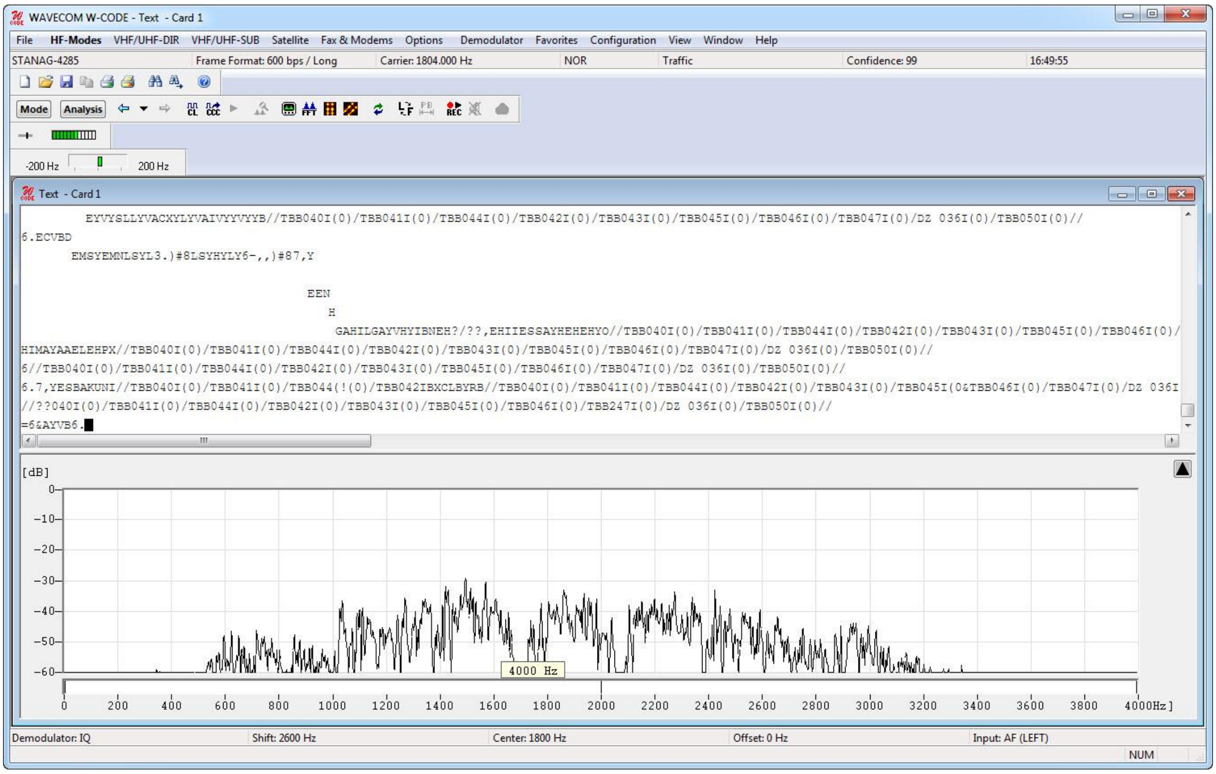
● LSB ○ MSB

● NOR ○ INV

Display format: ITA2

Successful.

Figure 11: Auto detection (from 7O1/ITA-ASCII from Figure 10 to the correct 5N1/ITA2 in this Figure) has been "Successful".



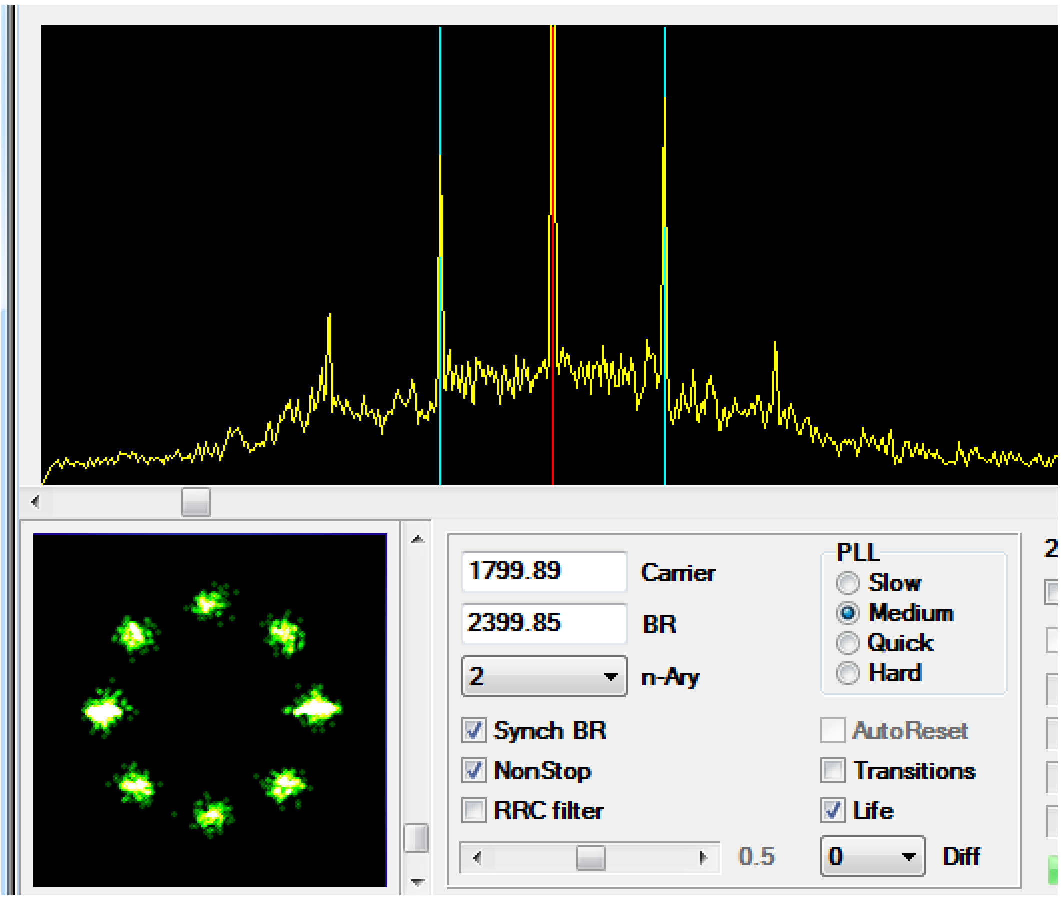
STANAG-4285 | Frame Format: 600 bps / Long | Carrier: 1804.000 Hz | NOR | Traffic | Confidence: 99 | 16:49:55

```
         EYVYSLLYVACXYLYVAIVYYVYYB//TBB040I(0)/TBB041I(0)/TBB044I(0)/TBB042I(0)/TBB043I(0)/TBB045I(0)/TBB046I(0)/TBB047I(0)/DZ 036I(0)/TBB050I(0)//
6.ECVBD
       EMSYEMNLSYL3.)#8LSYHYLY6-,,)#87,Y

                                         EEN
                                            H
                                             GAHILGAYVHYIBNEH?/??,EHIIESSAYHEHEHYO//TBB040I(0)/TBB041I(0)/TBB044I(0)/TBB042I(0)/TBB043I(0)/TBB045I(0)/TBB046I(0)/
HIMAYAAELEHPX//TBB040I(0)/TBB041I(0)/TBB044I(0)/TBB042I(0)/TBB043I(0)/TBB045I(0)/TBB046I(0)/TBB047I(0)/DZ 036I(0)/TBB050I(0)//
6//TBB040I(0)/TBB041I(0)/TBB044I(0)/TBB042I(0)/TBB043I(0)/TBB045I(0)/TBB046I(0)/TBB047I(0)/DZ 036I(0)/TBB050I(0)//
6.7,YESBAKUNI//TBB040I(0)/TBB041I(0)/TBB044(!(0)/TBB042IBXCLBYRB//TBB040I(0)/TBB041I(0)/TBB044I(0)/TBB042I(0)/TBB043I(0)/TBB045I(0&TBB046I(0)/TBB047I(0)/DZ 036I
//??040I(0)/TBB041I(0)/TBB044I(0)/TBB042I(0)/TBB043I(0)/TBB045I(0)/TBB046I(0)/TBB247I(0)/DZ 036I(0)/TBB050I(0)//
=6&AYVB6.
```

Demodulator: IQ | Shift: 2600 Hz | Center: 1800 Hz | Offset: 0 Hz | Input: AF (LEFT)

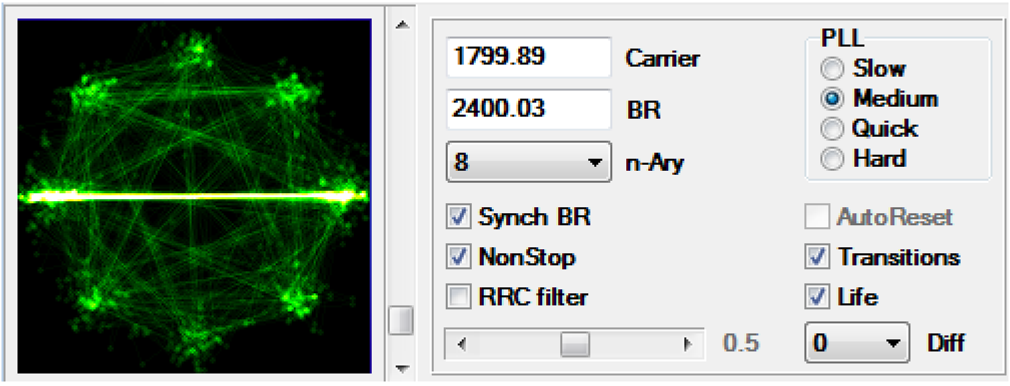
Figure 12: In the end of this workflow, we sometimes can read a decoded text (here: Turkish Navy).

Now a DXer’s view on the *modulation* of the signal. Obviously, we face 8-PSK, but there are phase states 0 and 4 seem “thicker” (Figure 13).



1799.89 Carrier
2399.85 BR
2 n-Ary
☑ Synch BR
☑ NonStop
☐ RRC filter
0.5
PLL
○ Slow
● Medium
○ Quick
○ Hard
☐ AutoReset
☐ Transitions
☑ Life
0 Diff

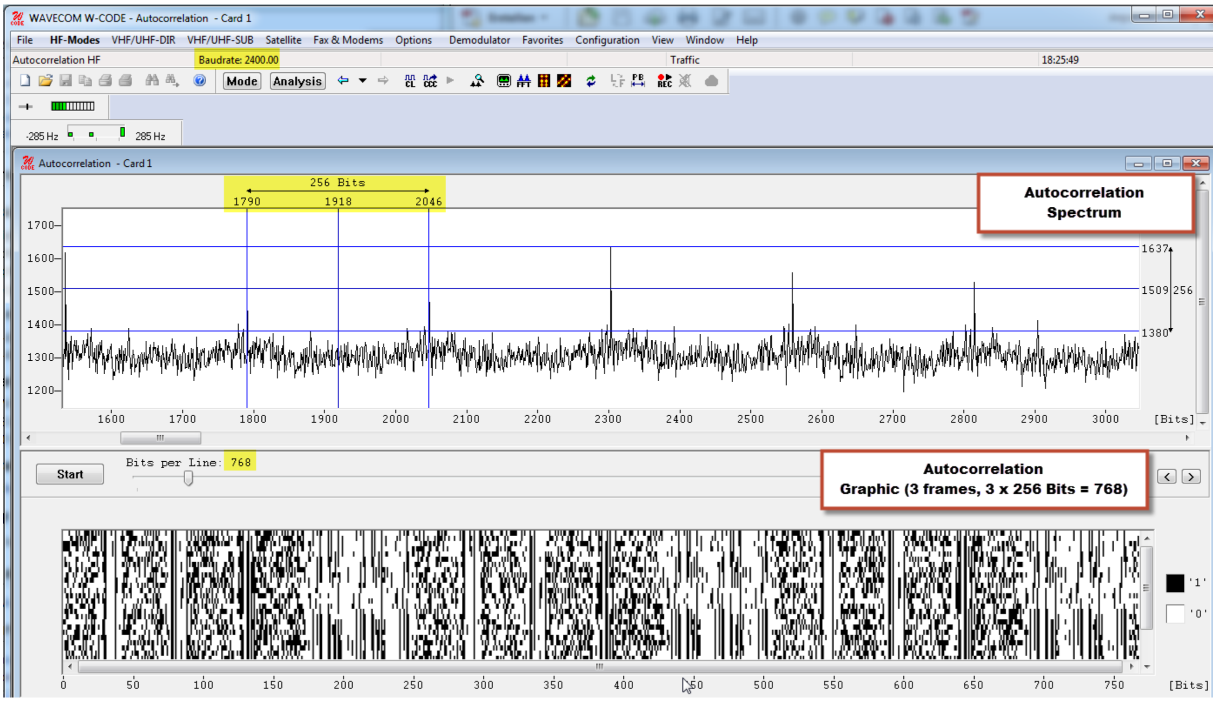
Figure 13: Phase plane of a STANAG4285 signal, as seen *by SignalsAnalyzer . Phase state (symbol) “0” and “4” are somewhat thicker, see next Figure.*



1799.89 Carrier
2400.03 BR
8 n-Ary
☑ Synch BR
☑ NonStop
☐ RRC filter
0.5
PLL
○ Slow
● Medium
○ Quick
○ Hard
☐ AutoReset
☑ Transitions
☑ Life
0 Diff

Figure 14: With “Transitions” activated, they reveal an additional 2-PSK (BPSK). By the way, “Sorcerer” is showing only this 2-PSK in its “Phase Plane”.

Now a DXer's view on the structure of the signal. A "frame" consists of 256 Bit of 106,667 ms length *Figures 15* to *17*).



Autocorrelation Spectrum

Autocorrelation Graphic (3 frames, 3 x 256 Bits = 768)

*Figure 15: "Autocorrelation" shows **three** repeating pattern as bit stream. The frames are measured to 256 Bit (spectrum, above). More on the smaller pattern (Graphic, below), later.*

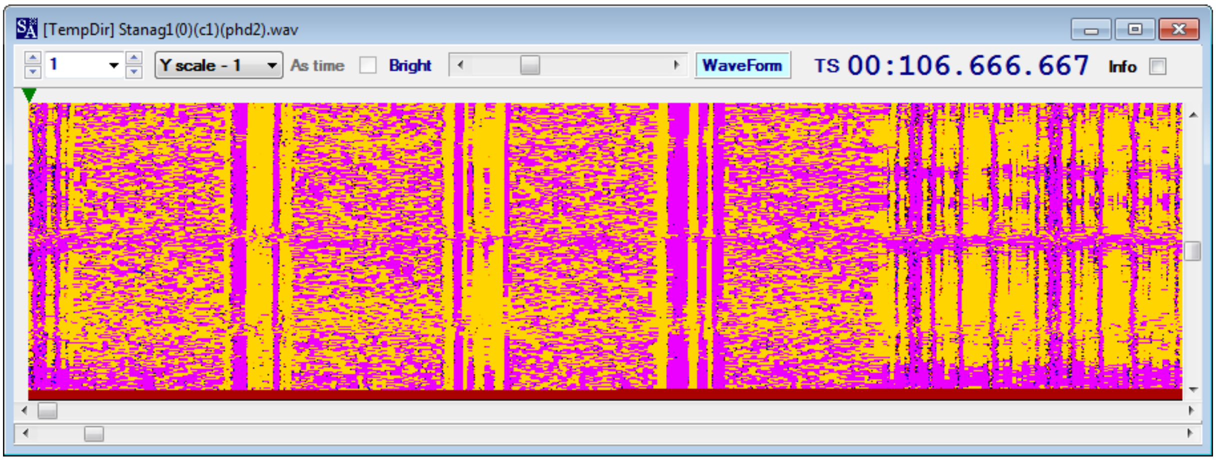


*Figure 16: Here we see **one** frame of 106,666667 ms length on a time scale, made by [SignalsAnalyzer](#).*

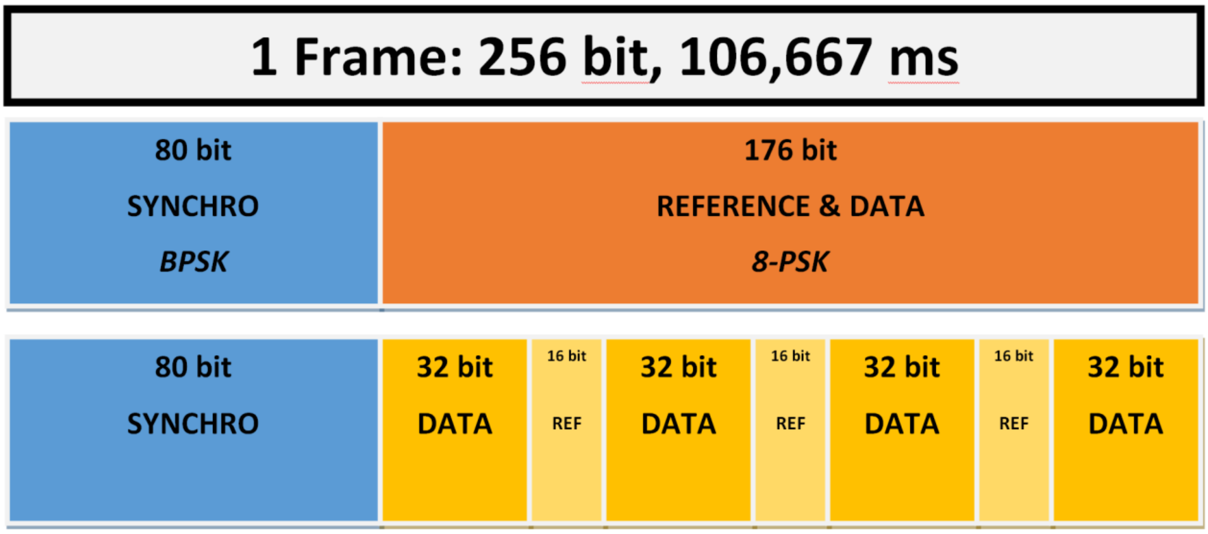
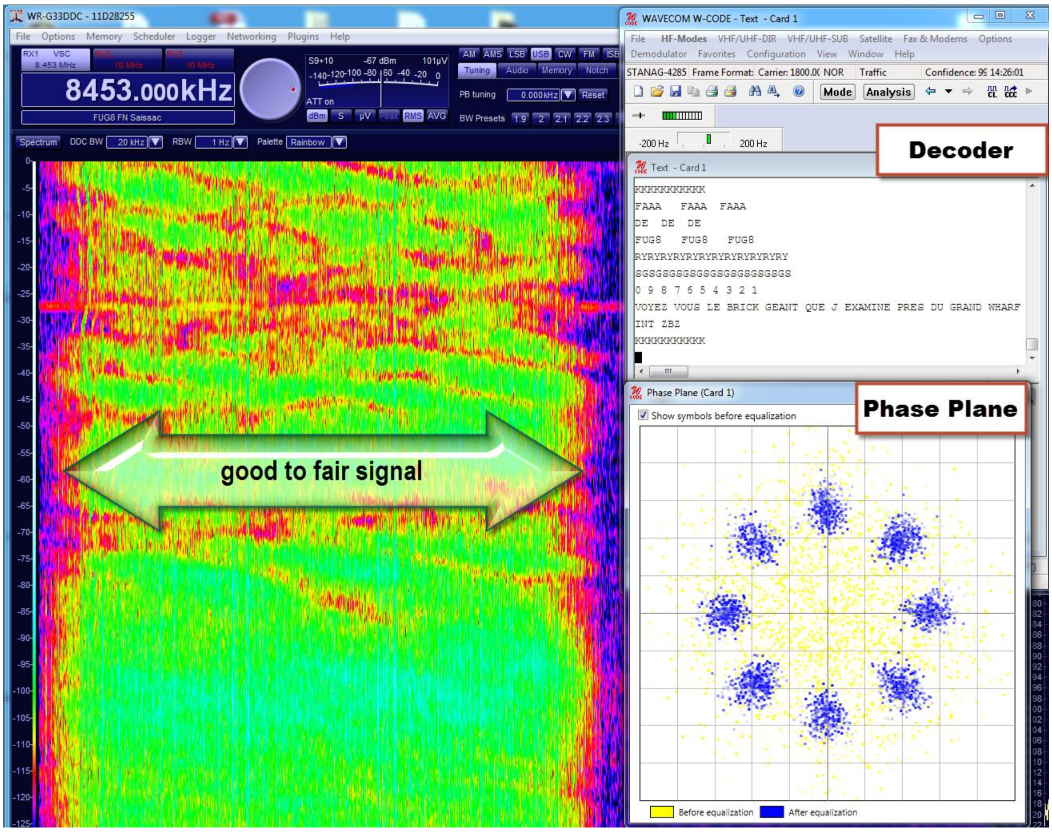


Figure 17: Structure of a STANAG4285-signal, according to specifications. It reveals that the BPSK in Figures 14/14 stem from the 80 bit synchro sub-frame in BPSK, whereas the 8-PSK comes from the 176 sub-frame of 4 x 32 data, separated by 3 x 16 bit reference (REF).

So far, so good. And if you have come to this point, you already are far beyond simple receiving and decoding. “Now for something completely different”: The synchro block of the first 80 bit is uses “*to detect the presence of the signal and for correction of the frequency shift resulting from the Doppler effect of the difference between the transmit and receive pilots, bit synchronization and either equalizer training in the case of equalization by recursive filtering or HF channel estimation in the case of detection according to the maximum likelihood method*”.

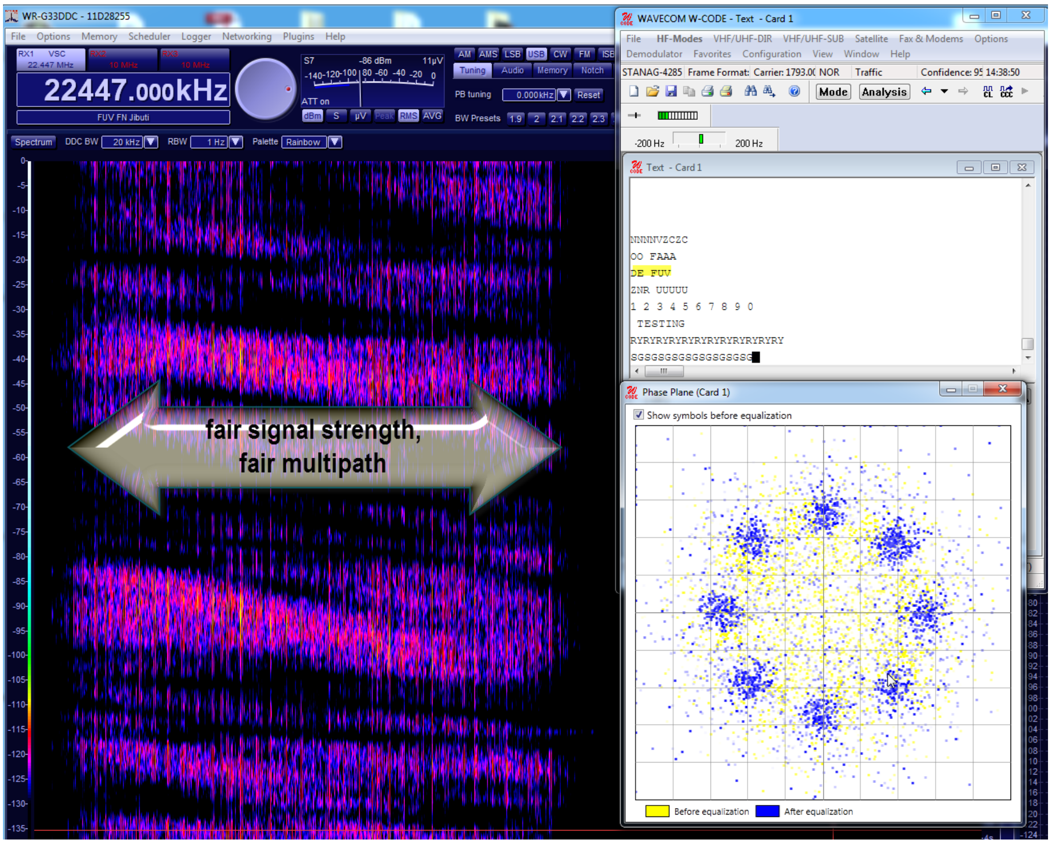
As far as I know, W-Code is the only software showing live the effect of “equalization”, see *Figures 18* and *21*. Of course, this software does also make use of this equalization.



STANAG-4285 Frame Format: Carrier: 1800.0(NOR Traffic Confidence: 9(14:26:01

```
KKKKKKKKKKK
FAAA  FAAA  FAAA
DE  DE  DE
FUG8  FUG8  FUG8
RYRYRYRYRYRYRYRYRYRYRYRY
SGSGSGSGSGSGSGSGSGSGSGSG
0 9 8 7 6 5 4 3 2 1
VOYEZ VOUS LE BRICK GEANT QUE J EXAMINE PRES DU GRAND WHARF
INT ZBZ
KKKKKKKKKKK
```

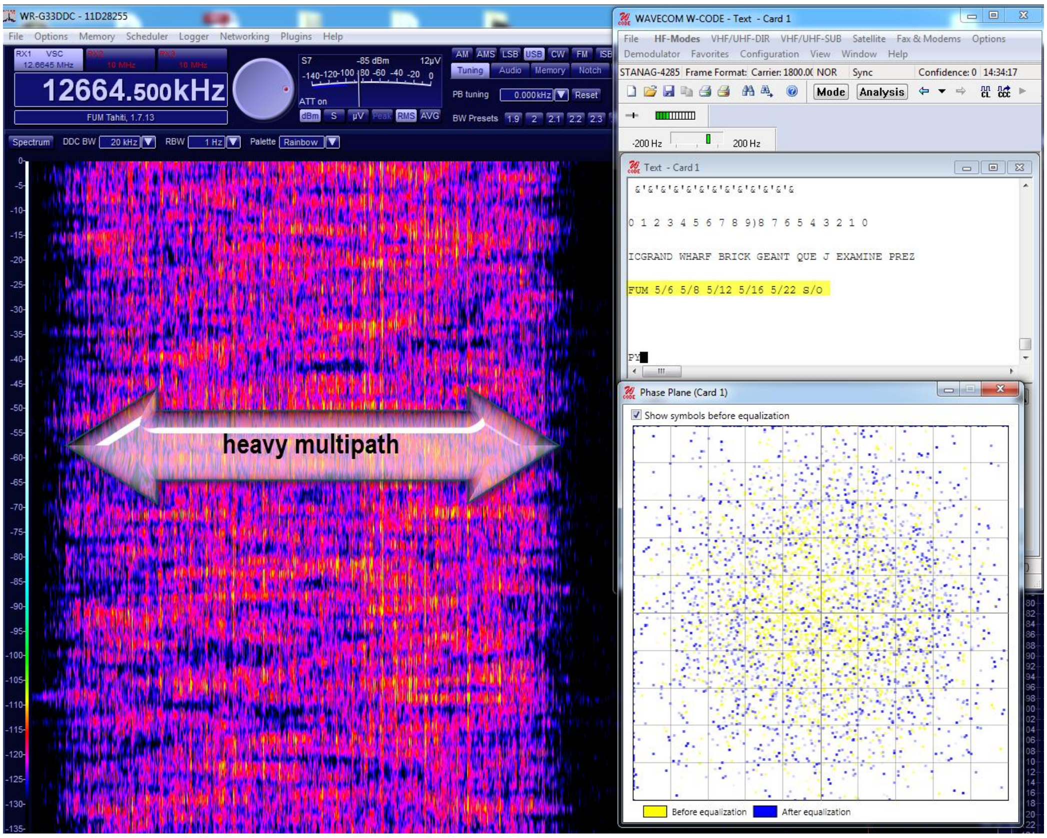
Figure 18: A fair to good signal re-produces the eight phases of the transmitted signal so that they can be clearly distinguished - by the software, and the human eye (FUG Saissac).



STANAG-4285 Frame Format: Carrier: 1793.0(NOR Traffic Confidence: 9(14:38:50

```
NNNNVZCZC
OO FAAA
DE FUV
ZNR UUUUU
1 2 3 4 5 6 7 8 9 0
 TESTING
RYRYRYRYRYRYRYRYRYRYRYRY
SGSGSGSGSGSGSGSGSG
```

Figure 19: Multipath and modest signal strength worsens the phase plane (FN Jibuti).



```
&'&'&'&'&'&'&'&'&'&'&'&'&

0 1 2 3 4 5 6 7 8 9)8 7 6 5 4 3 2 1 0

ICGRAND WHARF BRICK GEANT QUE J EXAMINE PREZ

FUM 5/6 5/8 5/12 5/16 5/22 s/o


PY
```

Figure 20: Heavy multipath limits decoding even more than just a modest signal (compare to Figure 19). The phase plane becomes that noisy that a human eye cannot distinguish the phases. But the software can - see the decoding of FN Tahiti/FUM.

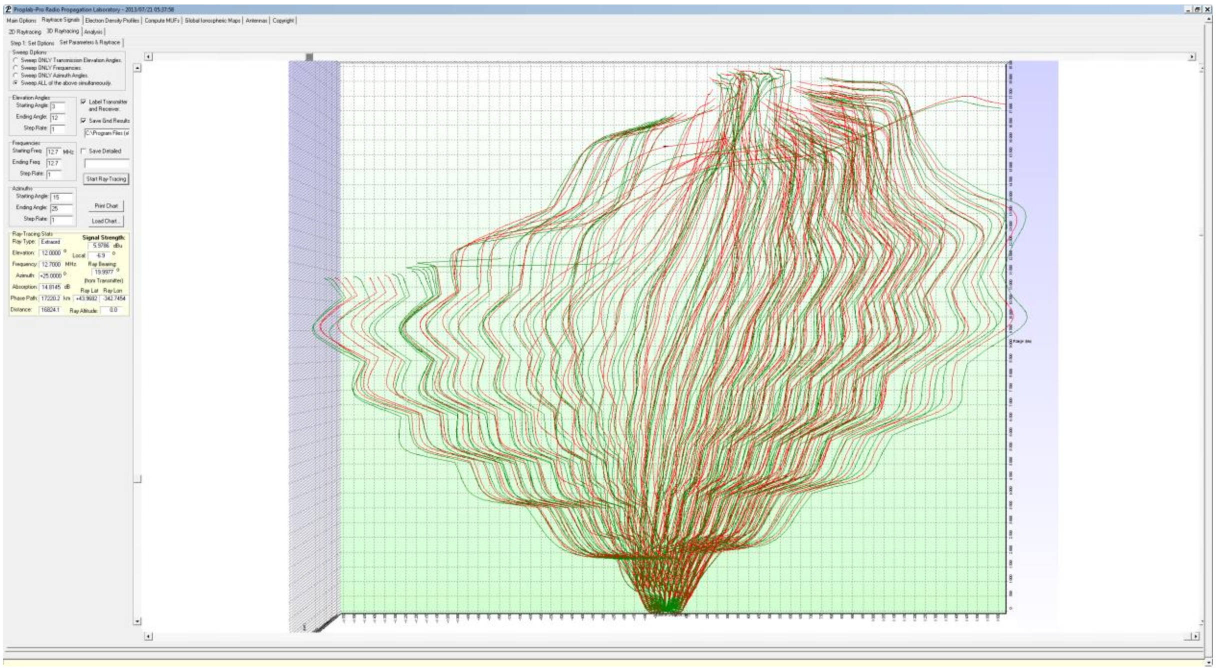
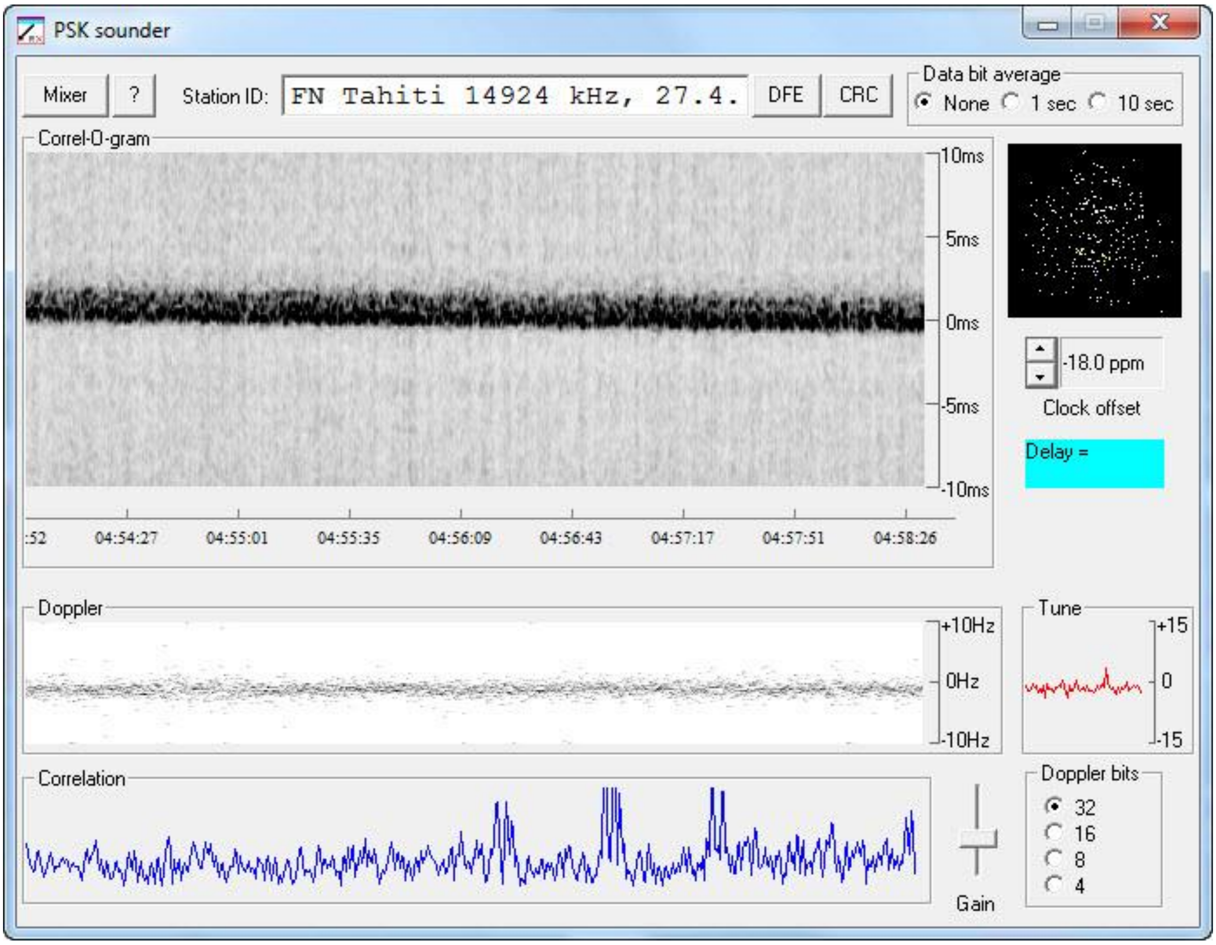


Figure 21: This 3D-ray-tracing simulation (seen from above) of the path between Tahiti and my location from the reception at Figure 20 shows, what multipath really is: a myriad of paths, each with different level, frequency (Doppler, because of the moving ionosphere), times of arrival and phases; heavy deviations from great circle propagation added. Simply a mess. This figure is screenshot of a simulation with PropLab 3.0 which took 36 hours on a 3.2 GHz quad core, 64 bit machine. It show how efficient coding as well as clever decoders can be.

Exact timing of STANAG4285-frames caused another clever idea: If multipath occurs, the time of arrival of the frames varies a bit according to variations in the ionosphere. The concept behind this idea is “cross-correlation”, or: When does the same structure repeats?

New Zealand hams Con Wassilief and Murray Greenman wrote a software PSKSounder which does not only measure these difference but put them into a graphic. This graphic shows relative delays of a specific cross correlation (vertical) versus time (horizontal). One can interpret this graphic as a cut through the ionosphere, showing just these layers where the signal is reflected. See *Figures 22* to *24*.



Station ID: FN Tahiti 14924 kHz, 27.4.

Data bit average: ● None ○ 1 sec ○ 10 sec

-18.0 ppm Clock offset

Delay =

Doppler bits: ● 32 ○ 16 ○ 8 ○ 4

Figure 22: PSKSounder in action, cross-correlating frames from Tahiti on 14.924 kHz. The “Correl-IO-gram” in the top do show a couple of differenc paths, but of only small time differences. In the middle you find in parallel a registration of the Doppler shift (“Doppler”). And at the bottom, you find the real-time correlation (“Correlation”). You have to click just in front of the strongest peak cluster, to zeroe the “Correl-O-gram”.

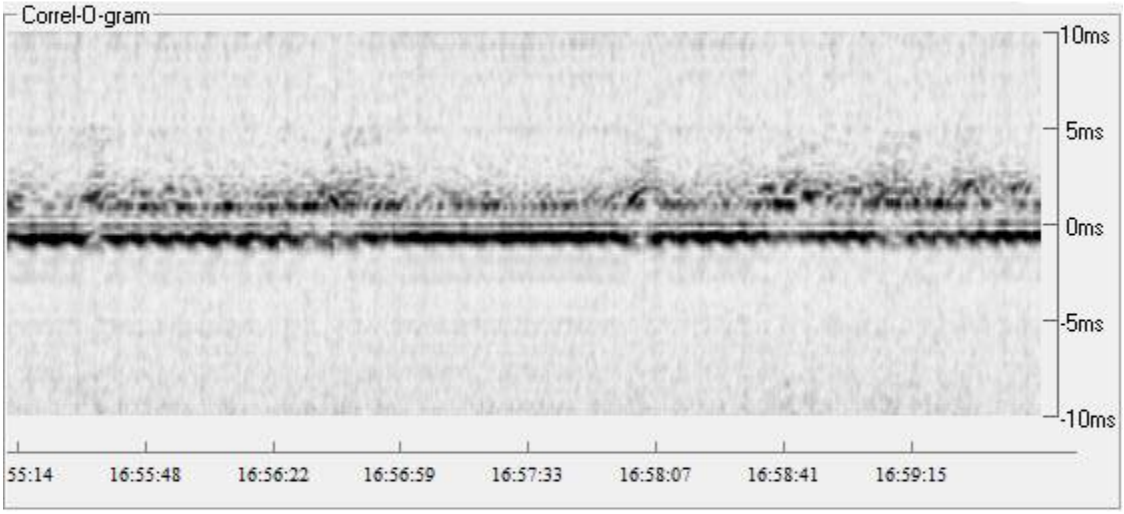


Figure 23: This graphic of a reception from Rome, 8.150 kHz, show one clearly dominating path. There are some much weaker paths with delays of up to three milliseconds.

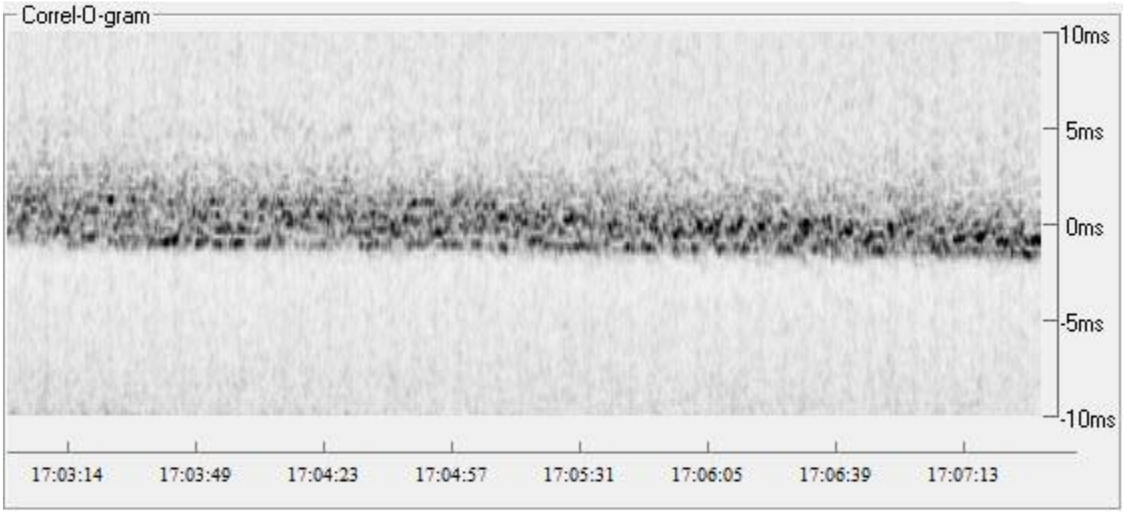


Figure 24: This signal from Jibuti on 8.568 kHz reveals at least four paths with quickly changing dominance. They seem to converge a bit at the end of the recording.