Intruder Watch: Monitoring, state of the art

Communications on HF has to obey specific international and national rules. On the highest level, we find the "Frequency Allocations" of ITU's "Radio Regulations".[1] They allocate specific frequency ranges to specific services (i.e. broadcast, maritime, aeronautical, amateur radio) on a worldwide or regional base to ensure interference-free communications.

Ham radio with its relatively small powers is especially endangered by so-called "intruders" which pirate their allocated bands and cause interference. To combat these intruders, IARU has set up an "Intruder Watch"[2], monitoring the amateur radio bands, dig up illegal transmissions by other services and deliver these information to their national authorities for further action.

Software-defined radio (SDR) now allow for a very efficient method of complying this task. With that, you can record a whole amateur radio band for hours or even days, visualize any activity graphically in a so-called sonagram (or: waterfall diagram) and spot even short-timed transmissions visually with a high reliability. Software like SDR-COM2 of Simon Brown[3] is an unique tool with some desired features for professional monitoring tasks. Above all, it includes a "click and listen" feature, plus making documentation very easy.

They are many station layouts to do monitoring. Below I will describe just one combination of Hardware and software (*Figure 1*), and one possible workflow (*Figure 2*). Both will provide some general information which may have to be adapted to your monitoring setup and your needs.

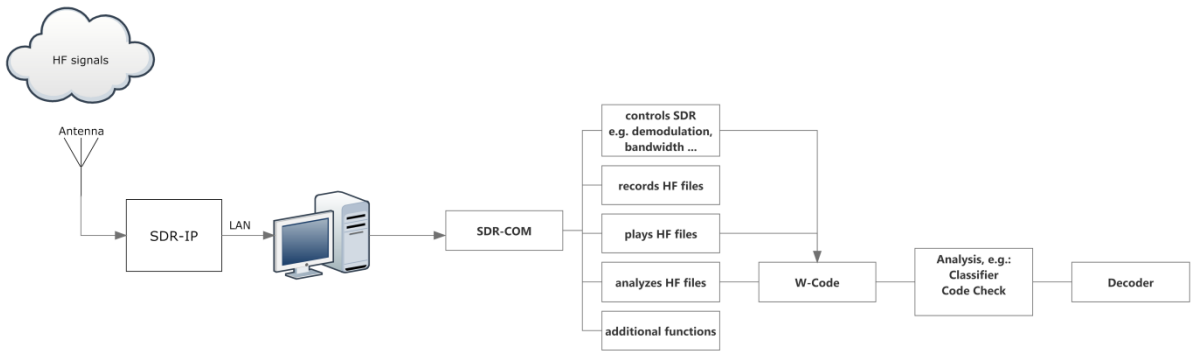

Figure 1: Example for a high-end receiving post. It consists of an SDR-IP from RFSpace[4] as receiver, locked to a GPS-driven frequency standard. The SDR is controlled by software SDR-COM2, and classification plus decoding of data transmission is done by software decoder W-Code of Wavecom[5].

[1] http://www.itu.int/pub/R-REG-RR-2012, Article 5, see pages 37 - 178. Can be downloaded free of charge.
[2] Region 1: www.iarums-r1.org, Region 2: www.iaru-r2.org/monitoring-system, Region 3: www.iaru-r3.org/ms/, ARRL Intruder Watch, Region 2: www.arrl.org/intruder-watch
[3] http://sdr-radio.com
[4] http://rfspace.com
[5] www.wavecom.ch

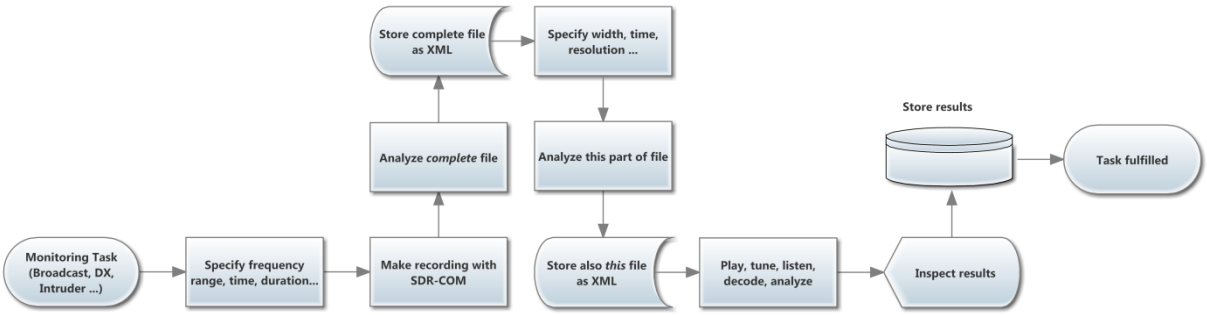

Figure 2: Generally, the process of systematic monitoring consists of these steps.

Your station may consist of smaller equipment in this or that respect; e.g. of a decoder free of charge like Sigmira[6] or under 50 US-$ like MultiPSK[7] or under 1000 US-$ like Code3-32P of Hoka[8]. You may have a bigger - congrats! - or smaller antenna than my 20 m loop. And you may use your SoftRock SDR, and drive it all with an ultrabook or Atom PC. Nevertheless, the station you run - you surely will get some new ideas from the following examples.

They are presented step by step from easy to a bit challenging. You can step in wherever you want. But if you are a mere newcomer to monitoring, you should start at start. For if you don't have some experience - which you get that fast! -, you will end in some disappointment by beginning somewhere in between.

Step 1: First, you must define the frequency (range and width) and the time, you want to record. Then you have to do the recording. Preferably, this should be done by the scheduler. It is easy to program, and it organizes all files of a scheduled recording in an automatically generated folder.

Step 2: After having concluded this recording, open it for inspection in the "SDR Data File Analyser". Instantaneously, the sonagram will build up. Depending on the amount of information and your PC power, this can take from a few seconds to many ten minutes. Store the completed sonagram as .XML file, so the next time this sonagram will build up in seconds!

As the 40 meter band seems to be prone most to regular intruders, I chose the range of 7.000 kHz to 7.200 kHz which is exclusively allocated to amateur radio on a worldwide base; with a few exceptions, or "footnotes" in ITU-speak. I made a recording over 24 hours, resulting in 50 files of 2 GB each. For a first look, they are presented completely as sonagram at a visual frequency resolution of 100 Hz and a visual time resolution of a bit better than 30 seconds. SDR-COM2 has a tool aboard, doing the automatic scrolling in either direction even on a small(er) display (*Figure 3*).

[6] http://www.saharlow.com/technology/sigmira/
[7] http://f6cte.free.fr/index_anglais.htm
[8] http://www.hoka.com/products/code3-32p.html

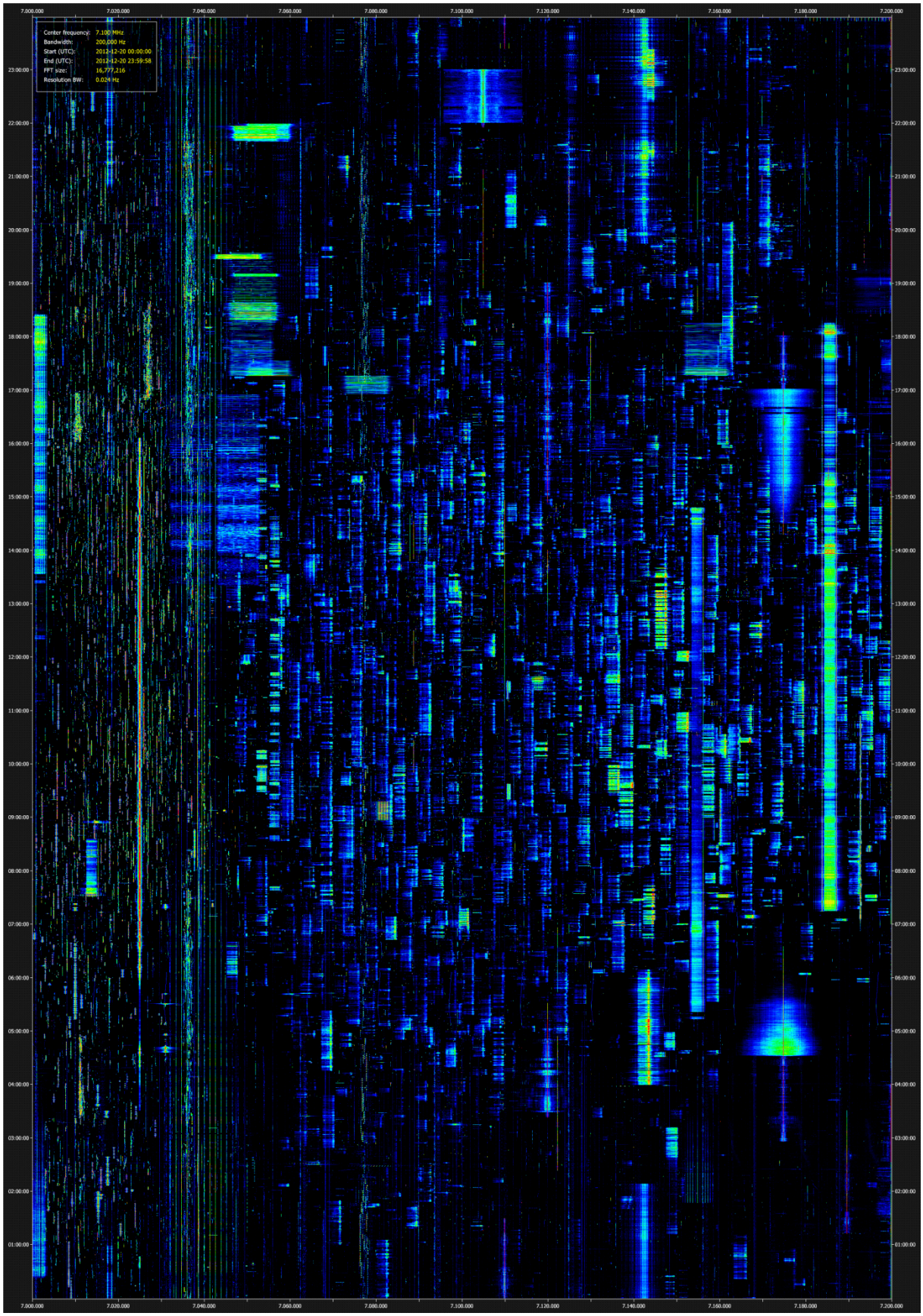

Figure 3: 7.000 to 7.2000 kHz from 00:00 to 23:59:58 UTC on December 20th, 2012. On the left you see CW and data, going into LSB.

Step 3: Start with digging up the broadcasters first, as they are quite easy to identify by their AM signals over some hours. *Figure 5* shows some examples.

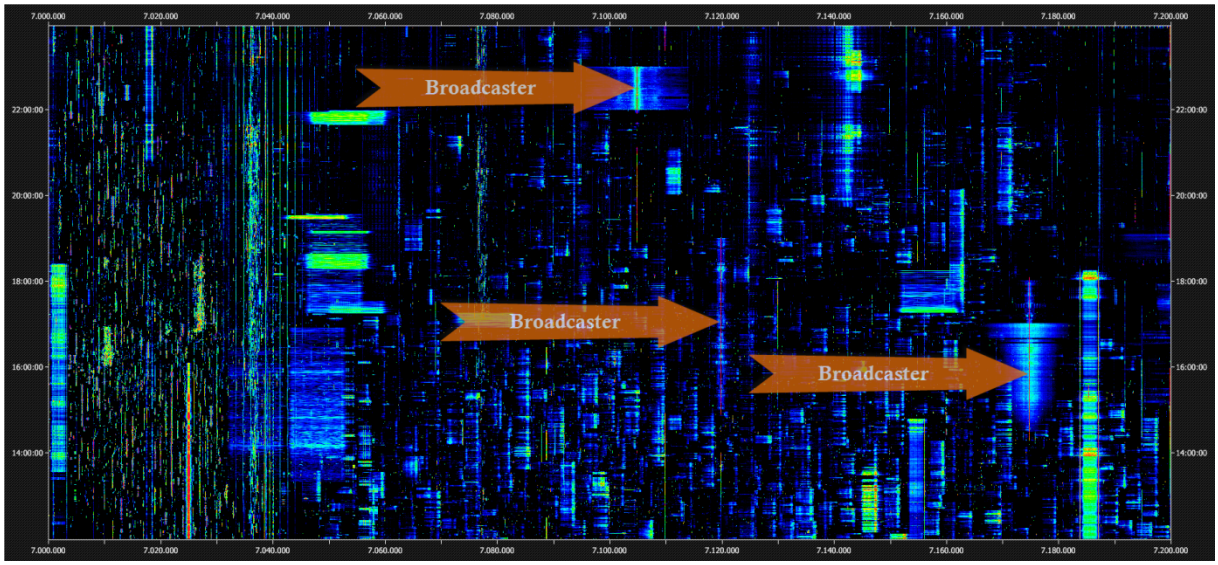

Figure 5: Carrier, symmetrical amplitude modulation and staying on the air at least for 30 minutes - these signals must be broadcasters.

Step 4: Listen and identify, analyze, document!

Example 1: Broadcast

The first task of this step is somewhat easy with broadcast stations, because literally each of them identifies itself by announcement at signing on/off, on the (half) hour, by national anthem etc. This method of identification should be preferred above all other - like matching frequency to published schedules or logs of other listeners. Nevertheless: if also you are not quite fluent in Amharic, Chinese or Sinhala, you should refer to the station identification printed in reference books like the "World Radio TV Handbook".[9]

Analyze the station by some technical parameter as sign on, sign off, development of signals strength and power of modulation. This "fingerprinting" should consist of several parameters, but for now I will concentrate simply on the carrier itself. Just zoom into the carrier with a bandwidth of 100 to 10 Hz. Figures 6 to 10 will give some examples and suggestions.

[9] http://www.wrth.com/

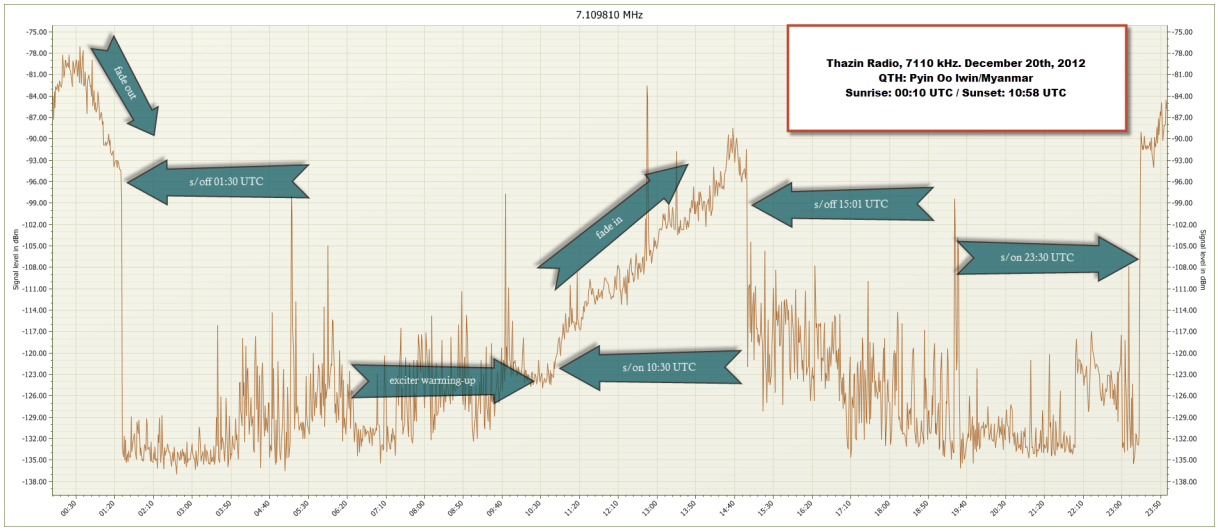

Figure 6: Signal history of Thazin Radio/Myanmar with s/on, s/off, fade-in and fade-out. This broadcaster of the Myanmar Army truly is an intruder to 40 m but may also an attractive DX opportunity to shortwave listeners.

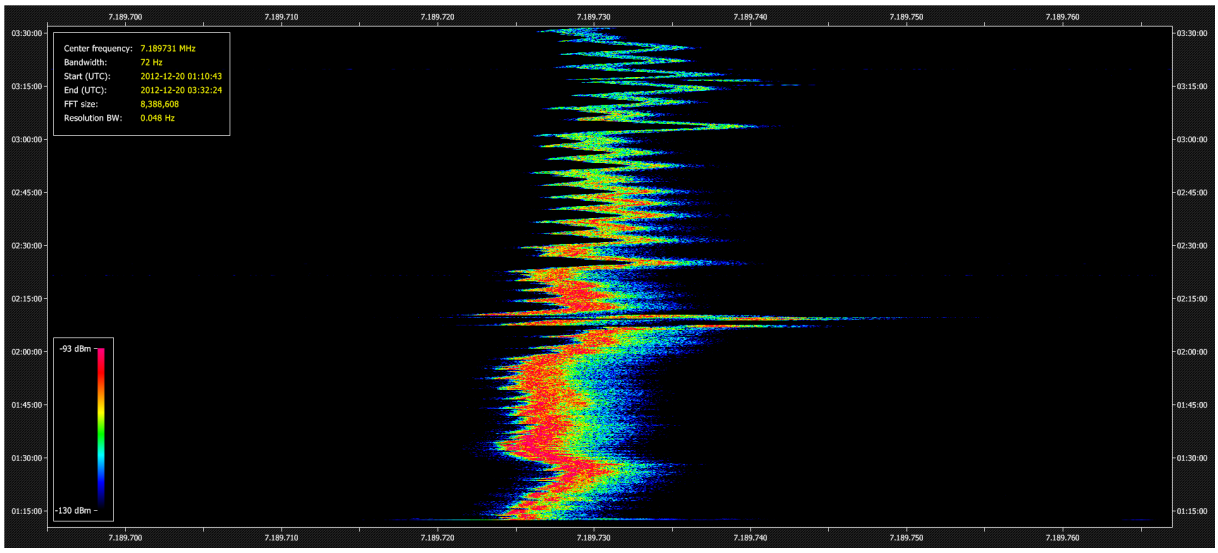

Figure 7: Under the microscope: In a window of 72 Hz width, the carrier of SLBC Ekala/Sri Lanka on 7190 kHz shows this behavior over 135 minutes at a frequency resolution of 0,048 Hz. As receiver's frequency is GPS-controlled, all variation are due to the transmitter's oscillator plus some Doppler spread.

Each signal has its own story to tell. Take the broadcasting signal of 7105 kHz. In fact, it consists of two stations: Falun Gong-related Sound of Hope Radio International from Tanshui/Taiwan and a transmitter from Chinese mainland, most obviously meant to jam it. *Figure 8* not only reveals their slightly different schedule and frequencies, but also a thickening of each carrier towards the end of their transmission. It becomes visible from around 22:33 UTC on the transmitter from Taiwan and from 22:48 UTC from that of the Chinese mainland. The first time almost exactly coincides with the sunrise at Tanshui at 22:34 UTC - see *Figure 9*[10]. Around sunrise the ionosphere undergoes dramatic changes, resulting in some Doppler spread from the moving layers and subsequently a thickening of the carrier. If we apply this observation also for the mainland transmitter, we can locate that roughly on a line between Shanghai and Hong Kong - see *Figure 10*.

[10] Made with DXAtlas: http://www.dxatlas.com/

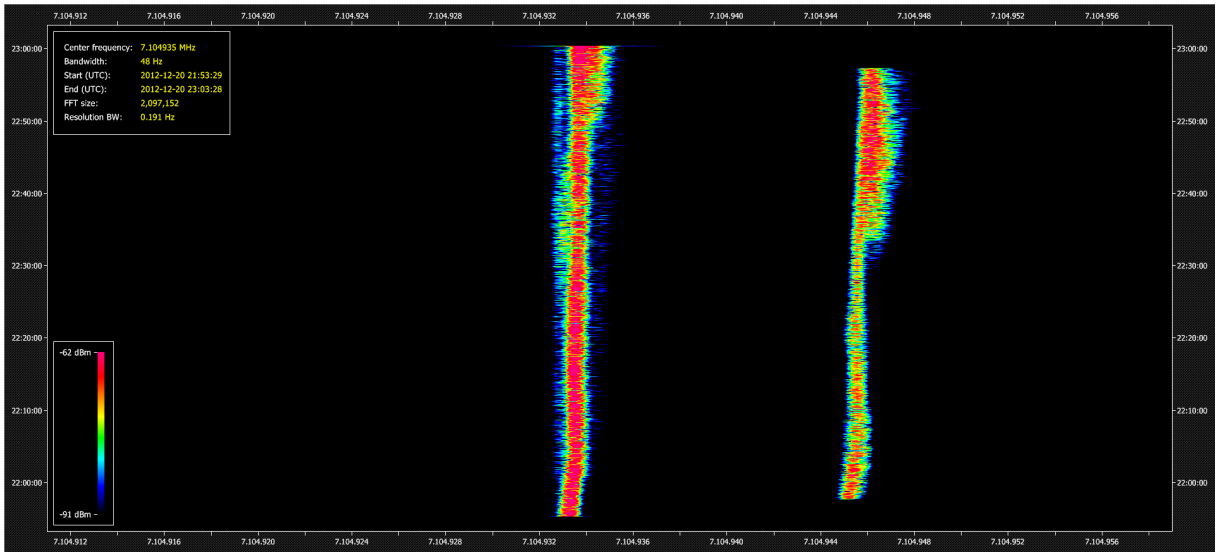

Figure 8: On the right you see the carrier of "Sound of Hope" from Tanshui/Taiwan, on the left and 12 Hz below that of a station from the Chinese mainland. See text for explaining the thickening of the carrier towards signing off.

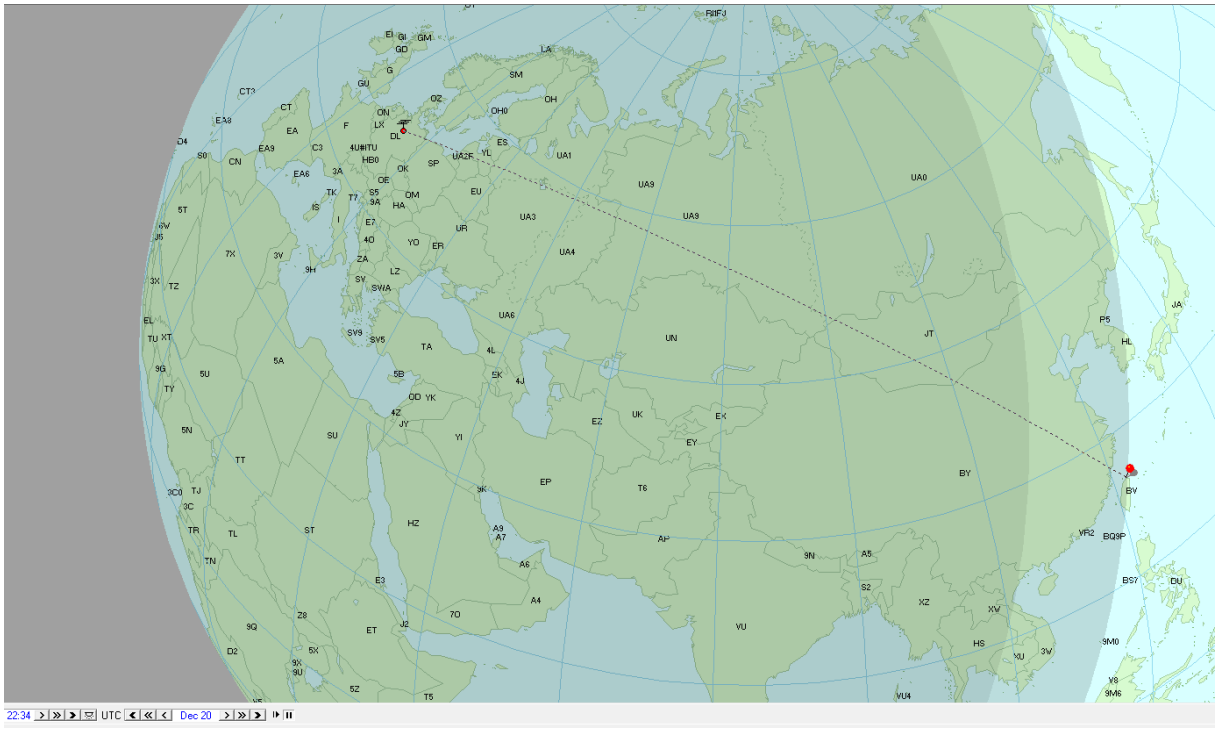

Figure 9: Zones of night, day and dawn on 20th of December, 22:34 UTC at sunrise at Tanshui (red pin), as seen by the DXAtlas.

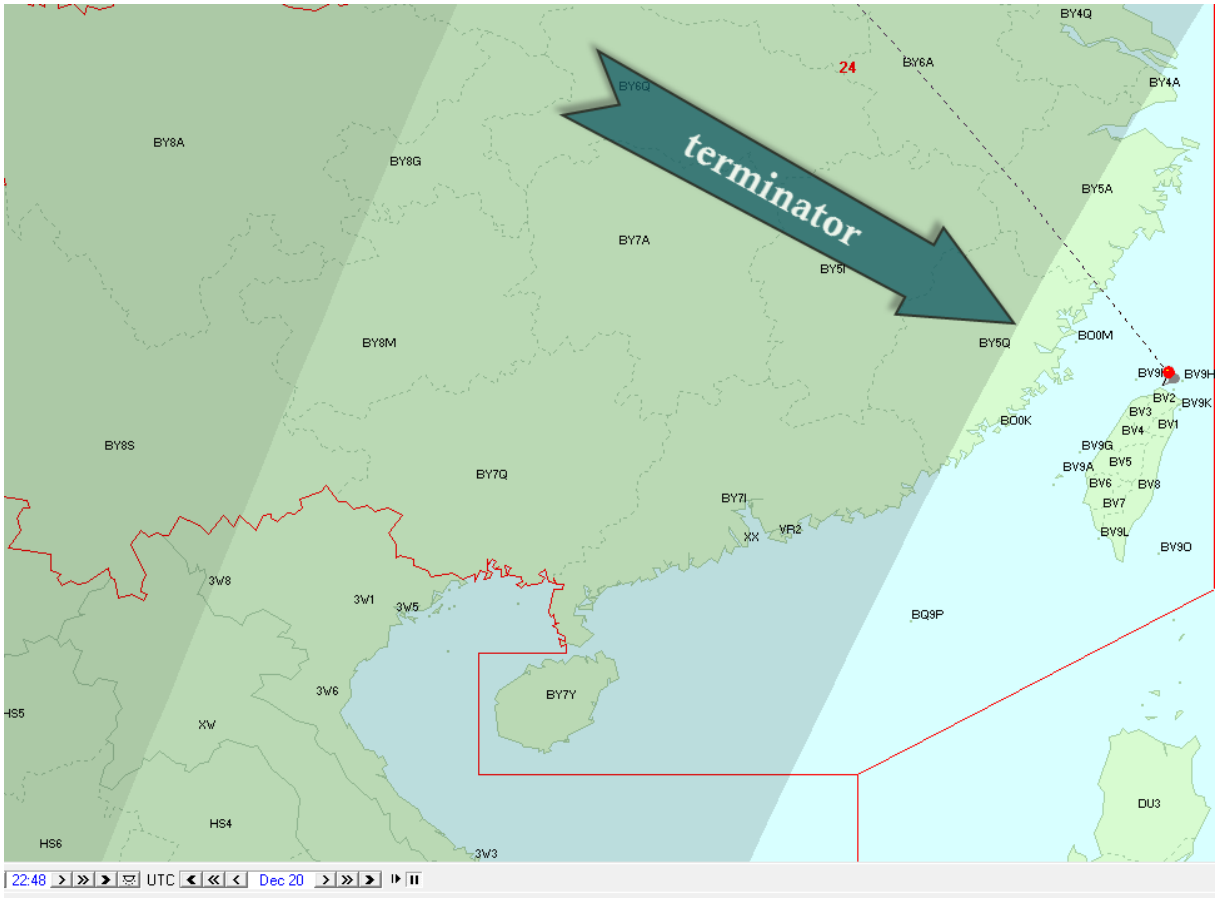

Figure 10: Applying the Doppler spread of a known location from Figure 8, the jamming station should be located on Chinese mainland along the "terminator".

Example 2: Beacons

For years, a beacon cluster with one-letter "callsigns" works within a bandwidth of 700 Hz around 7039,050 kHz. They span Russia from the north east ("S", Severomorsk) to the far east ("K", Kamchatka), including Sevastopol/Ukraine ("D"), the latter with many spurii. They are as fascinating for propagations studies along the terminator as well as annoying; see *Figures 11* and *12*.

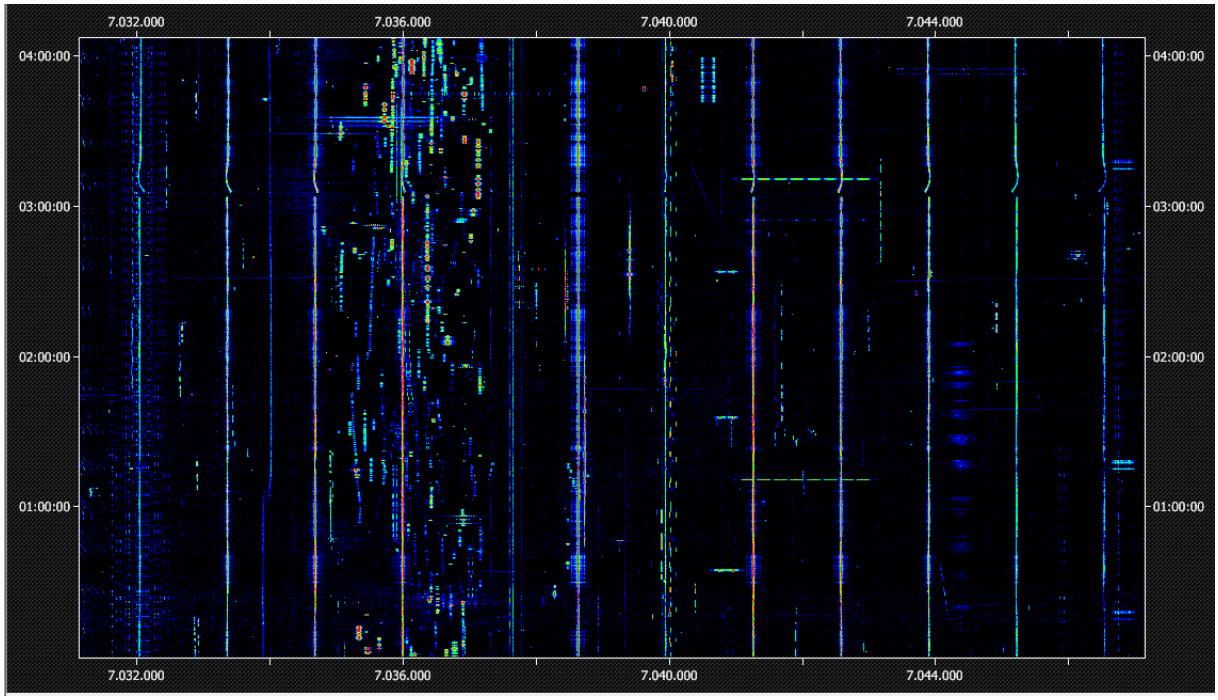

Figure 11: 13 vertical bars represent eight beacons plus some spurii of one of them.

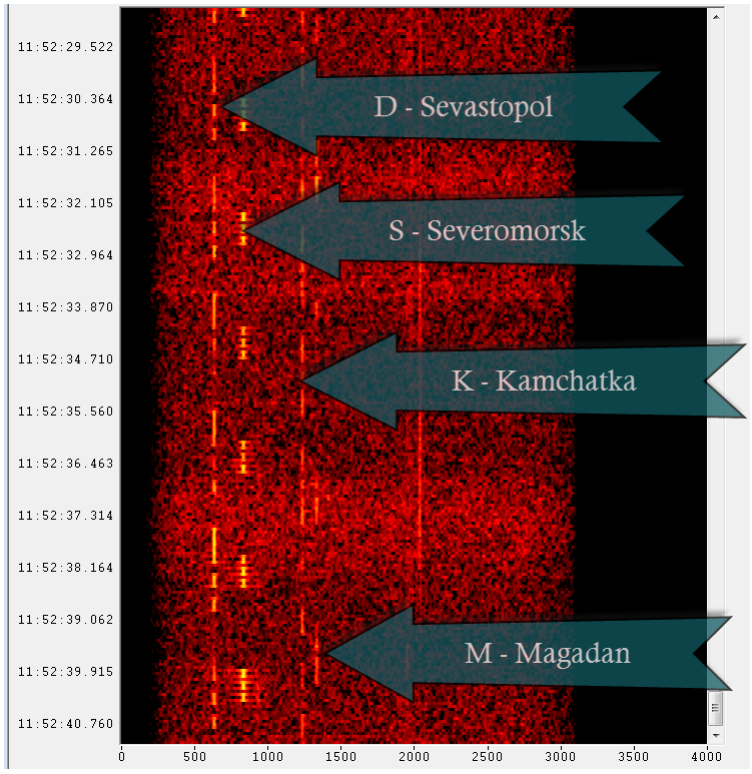

Figure 12: Beacons are annoying but provides also information for propagation. Kamachatka and Magadan are about 7000 km away from DK8OK showing reception over this difficult high latitude path.

Example 3: Chirp Signals

Chirp transmitters are often found on 40 m. They may provide an HF radar or ionospheric experiments or even communications. At least, we can document some parameters of these stations. That at *Figure 13* e.g. consist of frequency-modulated chirps of 15 milliseconds each which will result

in carriers of a distance of 66,7 Hz (15 ms x 66,7 = 1 s), see *Figure 13*. Each of the transmissions consists of 250 such chirps, lasting for 3,75 seconds.

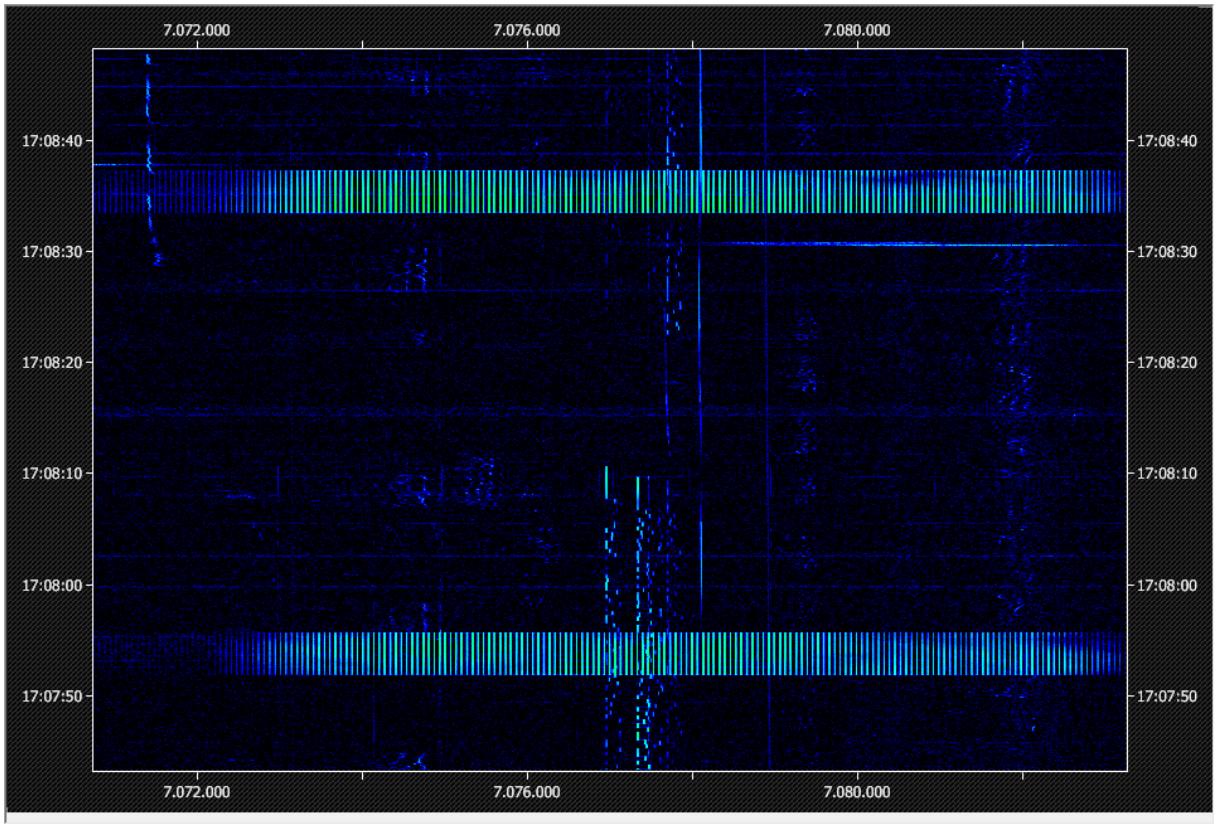

Figure 13: The two blocks of carriers are 3,75 seconds long and consist of carriers with a distance of 66,67 Hz.

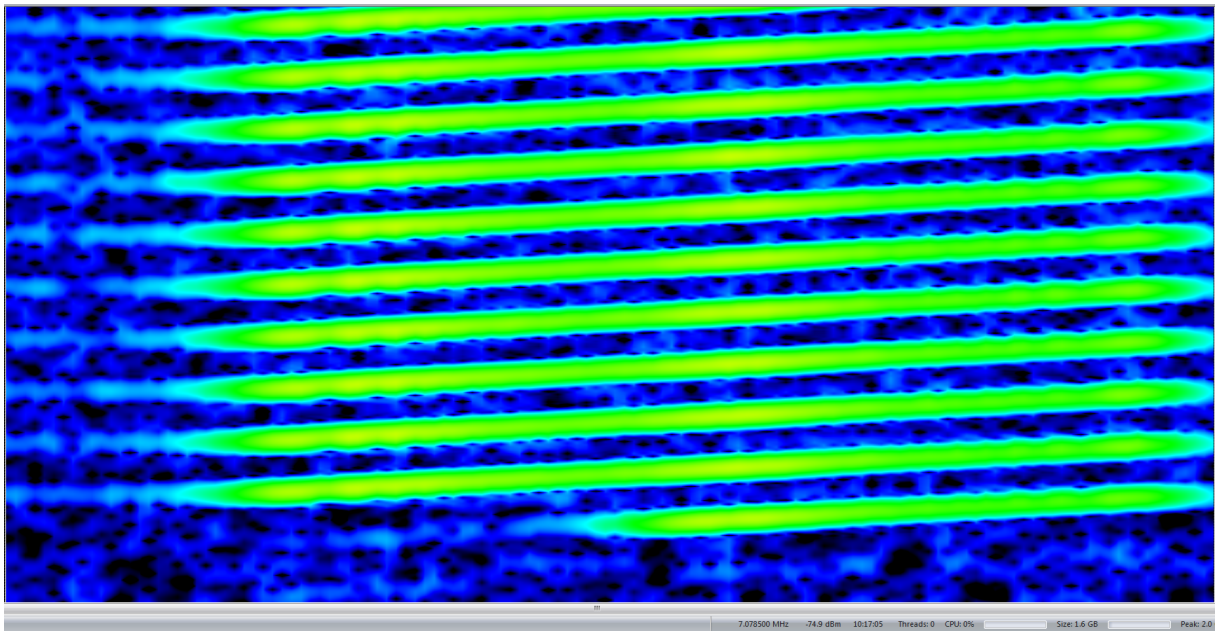

Figure 14: A detailed look shows frequency-modulated chirps of 15 milliseconds duration each.

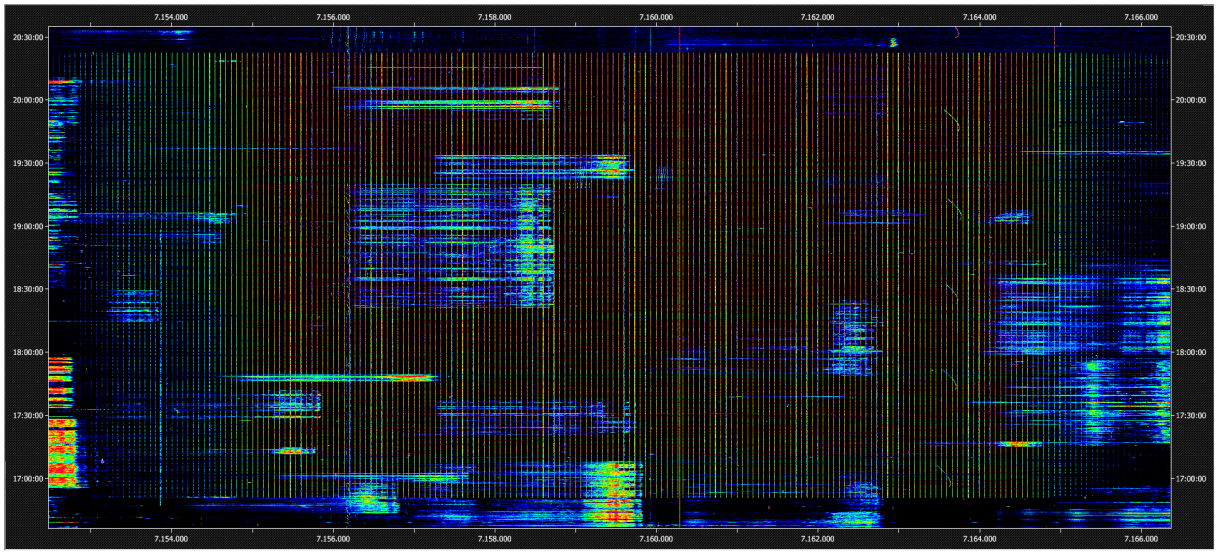

Figure 15: Amateur radio behind bars: A strong chirp transmitter covers some SSB conversation of hams around 7.160 kHz.

Example 4: Digimodes

Digimodes are widely found on shortwave, also among intruders.

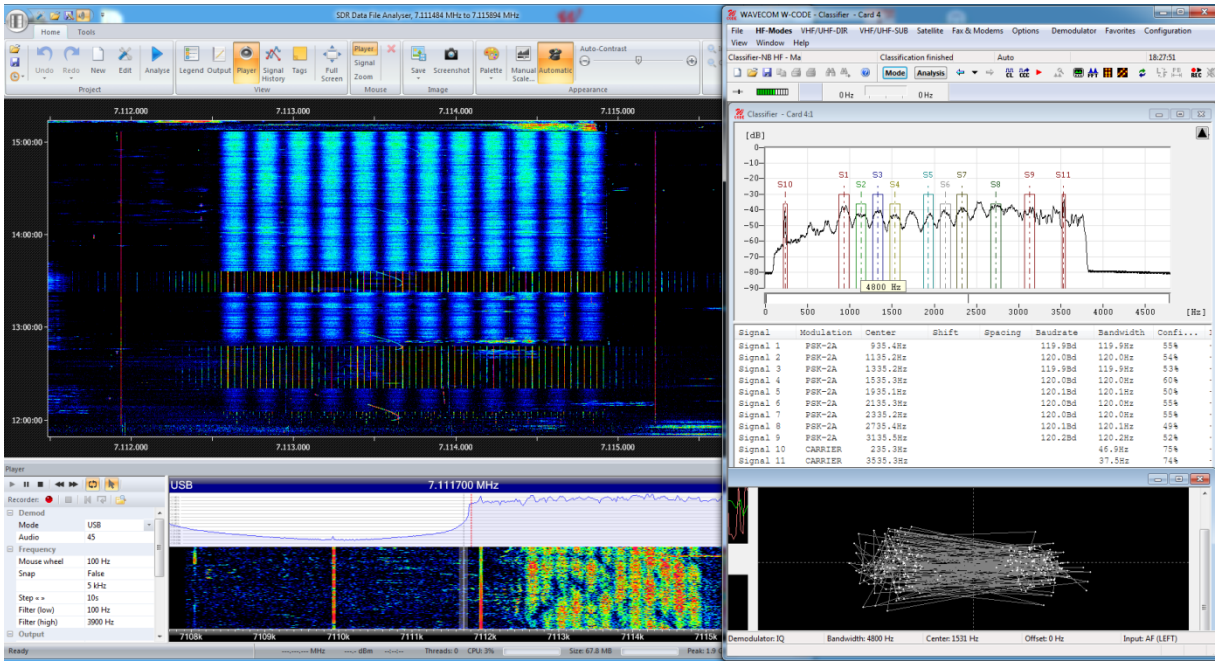

Figure 16: Here the OFDM-12 data signal around 7113,7 kHz (left, in the window of SDR-COM2) has been classified by Wavecom's W-Code (right). Due to some interference, the classifier got eleven channels of the signal. Below at the right you see the phase plane of the PSK-2A signal. This example shows also, that under interference you cannot rely completely just on automatic classification.

Friend or foe?

Increasingly, hams are using professional waveforms and protocols which had been long-time proven by e.g. the military. What started with simple RTTY with mechanical typewriters some 50 years ago, has now reached complex waveform like orthogonal frequency division multiplex (OFDM) with up to 57 phase modulated carriers in one SSB channel. This sibling of digital DRM broadcast is mostly used for SSTV transmission.[11] The many flavors of Pactor[12] up to Pactor-4 today, are widely used by professionals like NGOs, but also hams. And military standard ALE is also heard form hams.

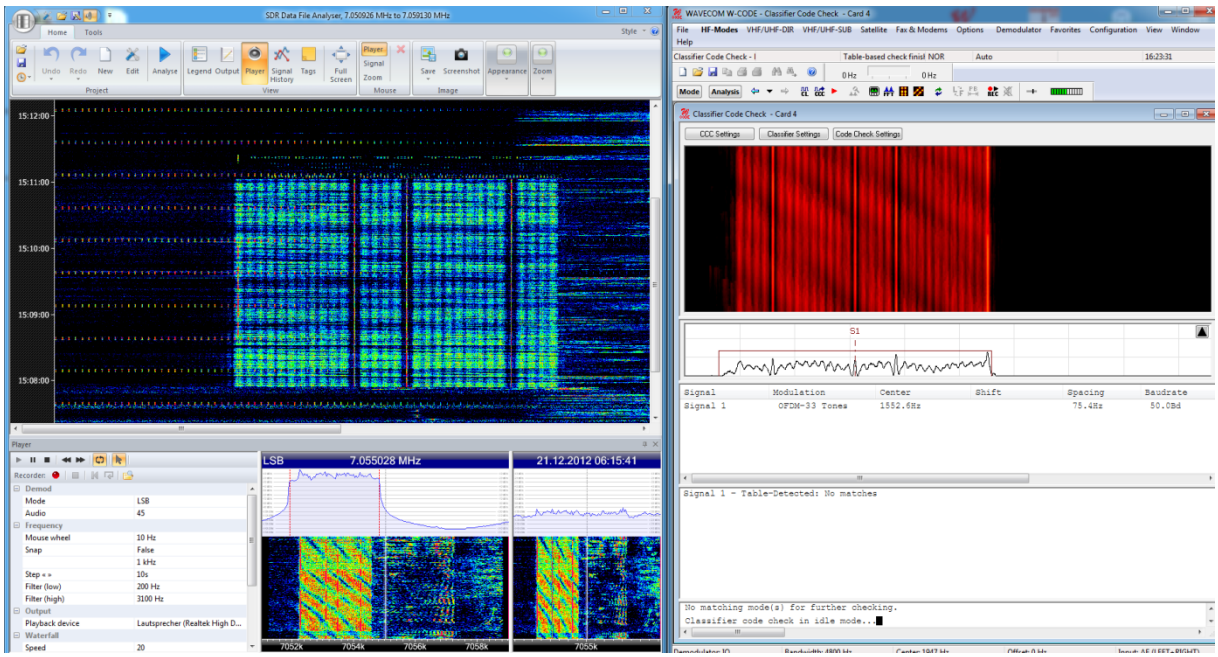

Figure 17: What sometimes had been considered an intruder thanks to its professional OFDM waveform …

[11] Software EasyPal by VK3EVL can be downloaded free of charge at:
http://www.vk3evl.com/index.php?option=com_content&view=article&id=46&Itemid=53
[12] http://www.scs-ptc.com/pactor/

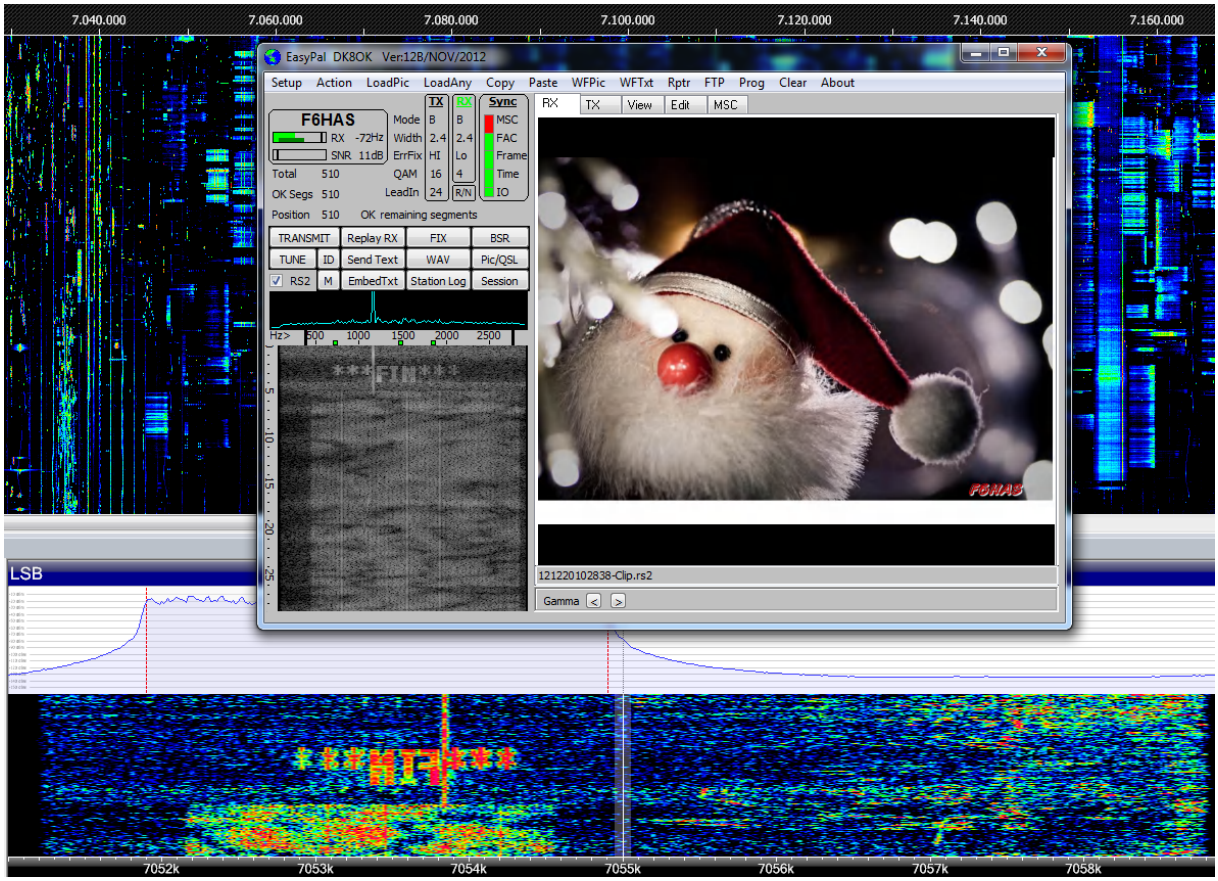

Figure 18: … turned out as Season Greetings by F6HAS in DRM - a legitimate user on 7055 kHz.

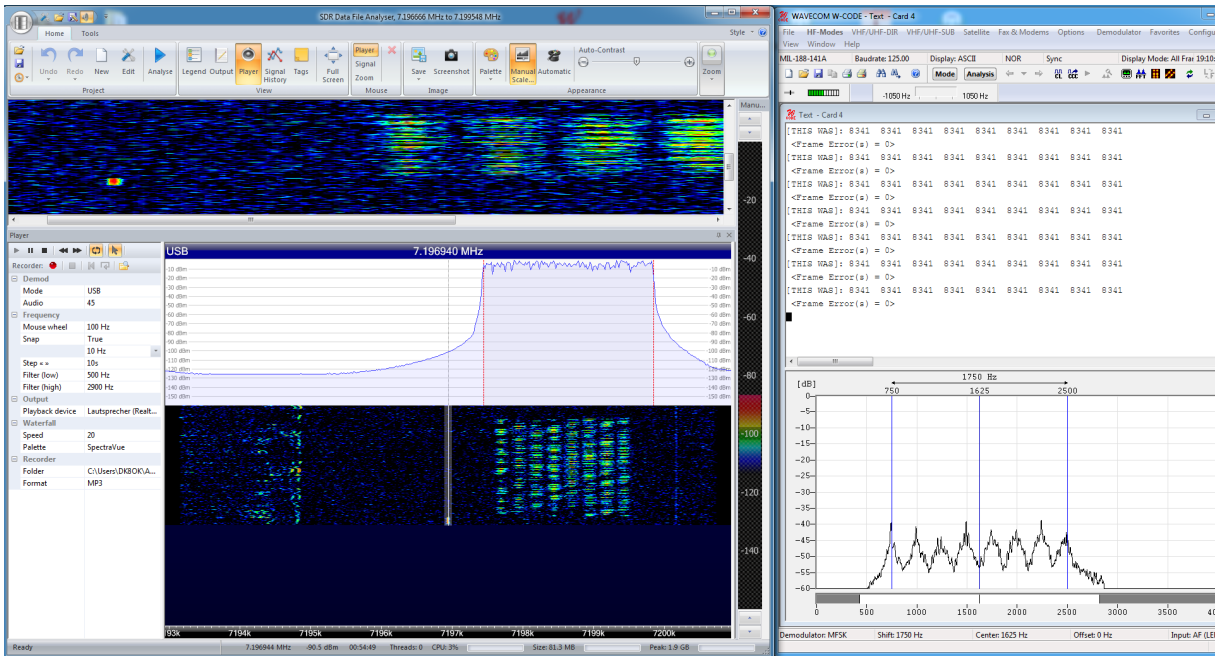

Figure 19: Turkish Civil Defence Network station "8341" on 7.196,940 kHz. This is part of a busy net consisting of many other Turkish agencies.

Sometimes even funny things can happen. As hams adopt some professional modes like automatic link establishment (more on that later), you can be trapped. See *Figure 20* for a ham (9A5EX) using ALE. On the other hand, “8341” (*Figure 19*) actually *is* an intruder. That's monitoring: You must scrutinize signal by signal.

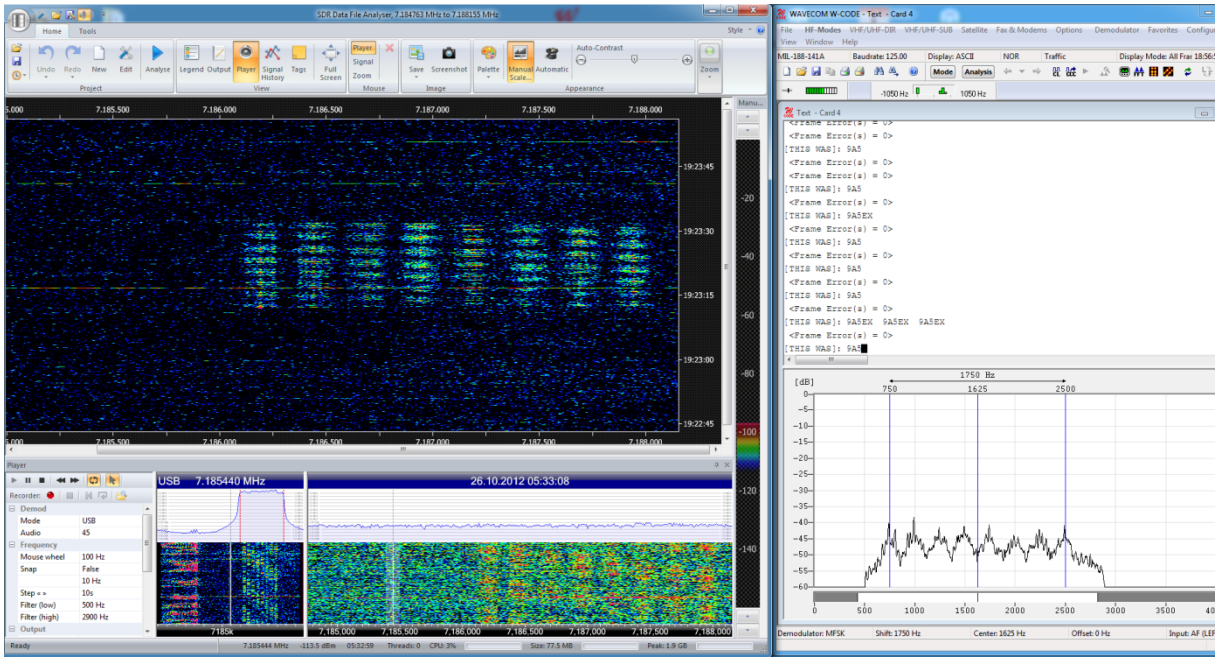

Figure 20: A legitimate user of ALE data on 7.184,440 kHz is 9A5EX, here with a faint signal which has been zoomed out. Zeljko Herman is coordinator for emergency coordination for Croatia within IARU.

ALE

Automatic Link Establishment, or ALE, is an efficient technique in automatically getting the best frequency out of a pool of channels at any given moment.

Therefore, each frequency of the pool is tested at specific intervals, e.g. 30 or 60 minutes. This "sounding" is received by the other stations of the network. The reception quality of each frequency is stored at each station of this pool. If a station wants to communicate in e.g. SSB or data, the link is established on the best frequency of the most recent "sounding".

ALE mainly isn't so much a means of communications by itself, but providing the best real-time frequency for establishing communications.

ALE signals of the second generation (2G) are very distinctive to ear and eye. Yet, with around ten seconds, each sounding is quite short. If each channel is tested each 60 minutes, it is occupied not even 0,3 % of time by each station.

This makes it an ideal candidate for I/Q file analysis.

Work in progress! To be continued.