

# HWIO\_2021\_CTS

## Signal5 (300pts) “quick” write-up

**B.VERNOUX 10 July 2021**

### Signal 5

**300 points**

**Welcome back to the 80s!**

In the 80s there was no such things like Signal or Telegram. We had different, ancient means to communicate. Sometimes even the physical layer of the communication stack was...unusual!

But you may not care, because you came for the flags! Come for the flags, stay for the hack! Right?

You see, we wish we could just plant a simple flag, but we thought...what a booring idea! So we decided to go a bit different for this challenge.

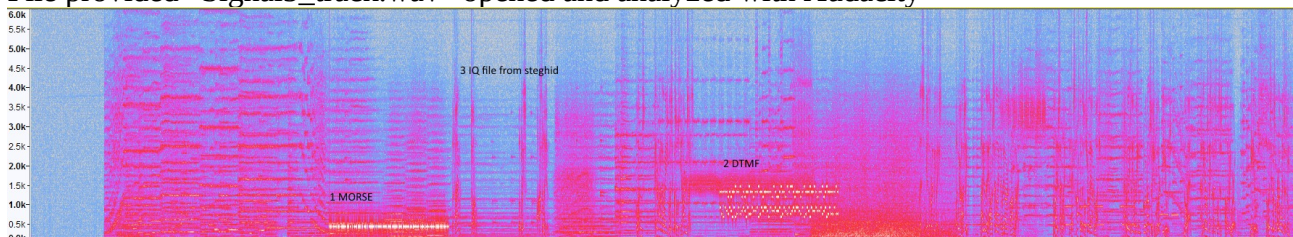
Instead of hiding the complete flag as is, we splitted it into many parts. Once you find all the parts, you must concatenate them sequentially using an underscore character "\_" as a separator.

The final flag will look like this:

```
TMCTF{part1_part2_..._partN}
```

We don't remember how many parts we hid in the challenge, sorry, so we can't really help: you just follow the leads and you'll find them all! :-)

File provided “Signal5\_track.wav” opened and analyzed with Audacity



1st part was in MORSE

2<sup>nd</sup> part was in DTMF

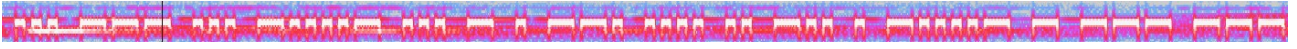
3rd part with 6 sub-part was in IQ file from steghide

The full track contain music with speech from WorldWar ... and it can be quite confusing as in some part (at start or after DTMF) it is like there is some other “MORSE code “hidden ... but it is fake just to loose time ...

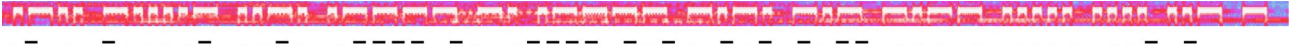
# 1 MORSE

<https://morsecode.world/international/translator.html>

Done partially manually to avoid errors when tested with filtered wav file.



... --- ... -....- ... - . --. .... .. -.. . -....- - --- ---  
SOS-STEGHIDE-TOO



.....- .....- ..- . - - - - . . - - - - ..... ..- -  
L-F1N1CKY5HUT

Flag reconstructed: **SOS-STEGHIDE-TOOL-F1N1CKY5HUT**

... --- ... -....- ... - . --. .... .. -.. . -....- - --- --- .-..  
-....- ..- . - - - - . . - - - - . . - . - - - - ..... ..- -

## 2 DTMF

DTMF extracted and filtered with Audacity (using HighPass & LowPass filter ...) =>  
Signal5\_track\_part2\_DTMF\_filtered.wav

- DTMF decoder python3  
<https://github.com/ribt/dtmf-decoder>  
user@ubuntu:~/dtmf-decoder\$ python3 dtmf.py  
'/media/sf\_\_CTS/HWIO\_2021\_CTS/Signal5/Signal5\_track\_part2\_DTMF\_filtered.wa  
v'

```
dtmf.py:26: WavFileWarning: Chunk (non-data) not understood, skipping it.  
  fps, data = wavfile.read(file)  
052080407203150670720650780350700820790770035*076060700840350830  
89078067035055065  
DTMF with errors ...
```

- DTMF-Decoder (Java) OK:  
<https://github.com/tino1b2be/DTMF-Decoder>

```
052084072035067072065078035070082079077035076069070084035083089  
078067035055065  
https://www.dcode.fr/ascii-code  
Result ASCII Converter => 4TH#CHAN#FROM#LEFT#SYNC#7A
```

## 3 steghid "iq-data.cfile"

Passphrase used: **F1N1CKY5HUT**

**steghide-0.5.1-win32 => KO:**

```
steghide.exe extract -sf Signal5_track.wav  
Enter passphrase:
```

```
steghide: assertion failed in WavPCMSampleValue.cc at line number 65.  
This means that you have found a bug. Please let me (shetzl@chello.at)  
know this if you have a way to reproduce the error.  
Steghide has to exit now. Sorry.
```

**Steghide-0.5.1 GNU/Linux => OK:**

```
user@ubuntu:~$ steghide info Signal5_track.wav  
"Signal5_track.wav":  
  format: wave audio, PCM encoding  
  capacity: 1.0 MB  
Try to get information about embedded data ? (y/n) y  
Enter passphrase:  
embedded file "iq-data.cfile":  
  size: 1023.9 KB  
  encrypted: rijndael-128, cbc  
  compressed: yes
```

```
user@ubuntu:~$ steghide extract -sf Signal5_track.wav  
Enter passphrase:  
wrote extracted data to "iq-data.cfile".
```

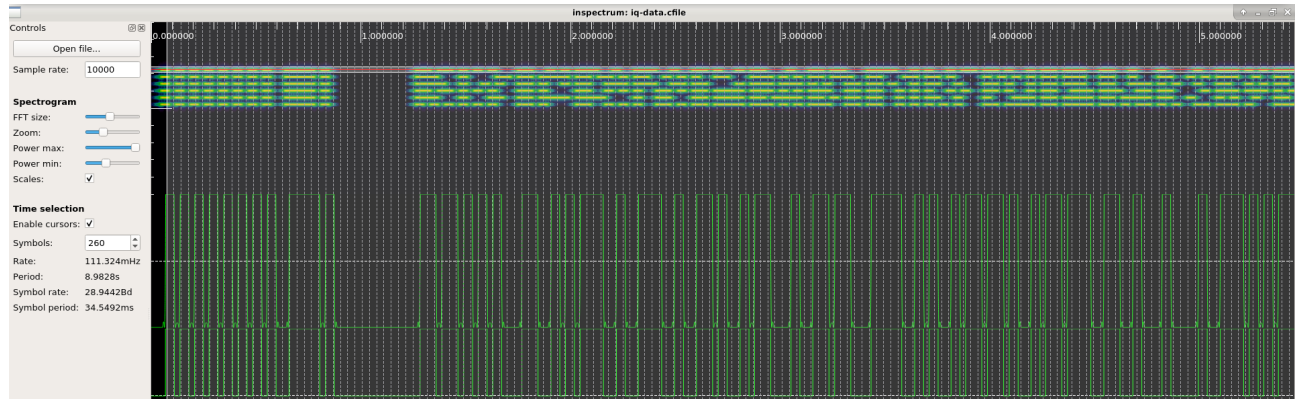
# 4 iq-data.cfile analysis/decoding with Inspectrum



6 channels to decode OOK Preamble 0xAA 0xAA SYNC 0x7A (hint from DTMF flag)

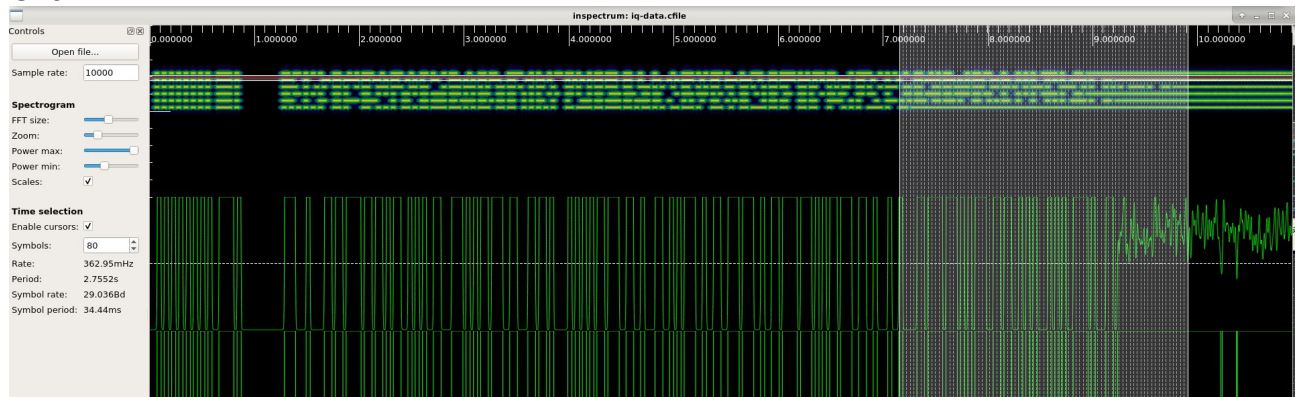
Just for fun I have decoded all 6 channels (even if only channel 4 was required for final flag)

## Chan1



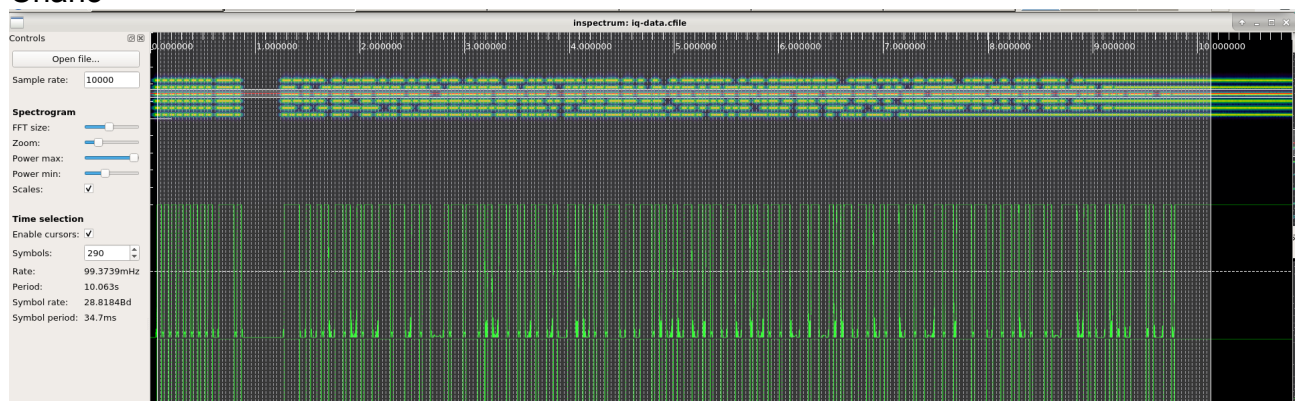
Hint: No need to resync when sized on at least 80 symbols (even better results with more)  
TerriblyKindButNoWayRealEOF

## Chan2



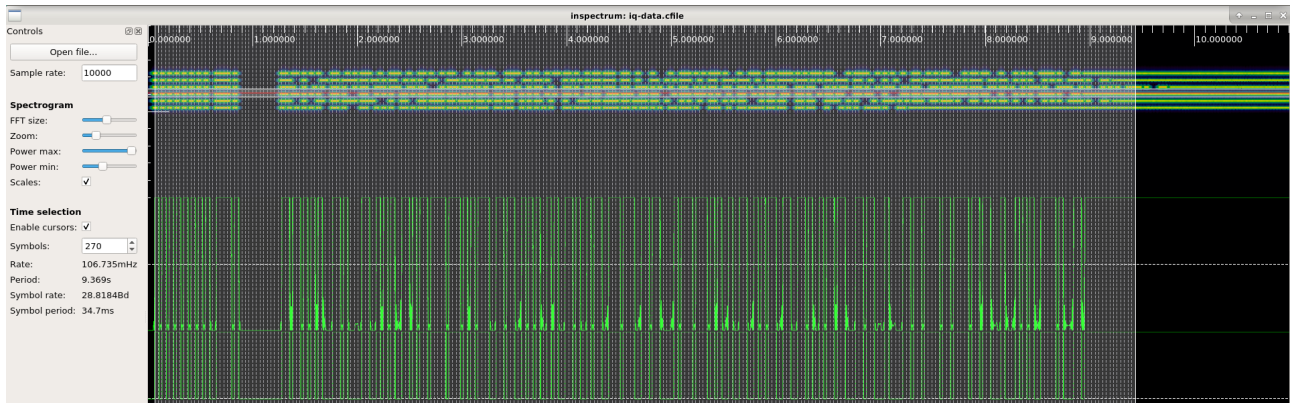
Hint: Reuse previous synchro  
ComeLunchUndergroundHouseEOF

## Chan3



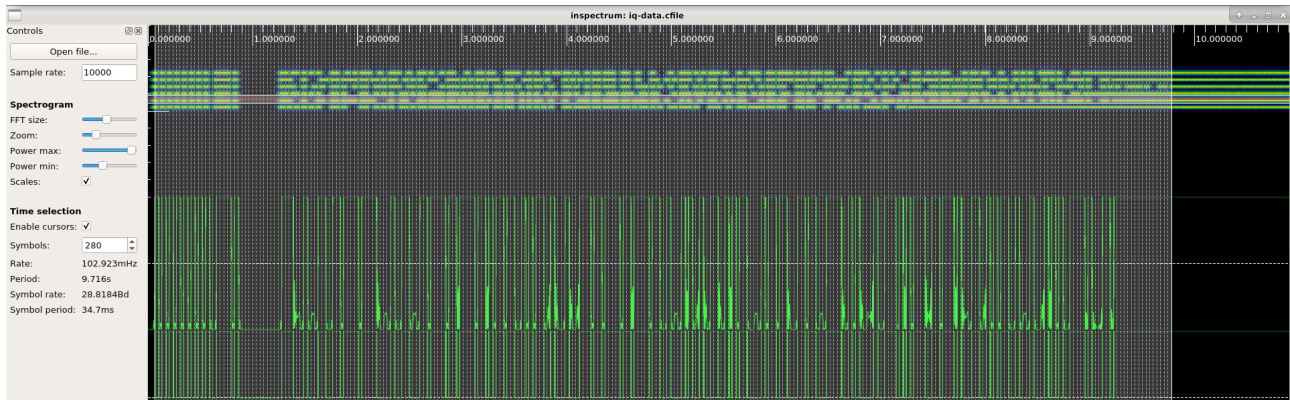
JigsawSidingRefillViscosityEOF

## Chan4



**Solution to use for final flag: TheMouseJigsawRefillCoolEOF**

## Chan5



**FoxLookedGoodReallyBustedEOF**

## Chan6

Same process as before...

**TheMouseTookStrollEOF**

Final Flag ?:

TMCTF{SOS-STEGHIDE-TOOL-

F1N1CKY5HUT\_4TH#CHAN#FROM#LEFT#SYNC#7A\_TheMouseJigsawRefillCoolEOF}

Flag not tested in time (too late)...