some *Ham* for hunting eggs...

Ham - 469

PoliCTF 2017

by cr0c0

#Recon - pt. 1

- General

```
$ file ham.wav
RIFF (little-endian) data, WAVE audio, Microsoft PCM,
16 bit, stereo
```

- Looks like it's uncompressed at first glance...

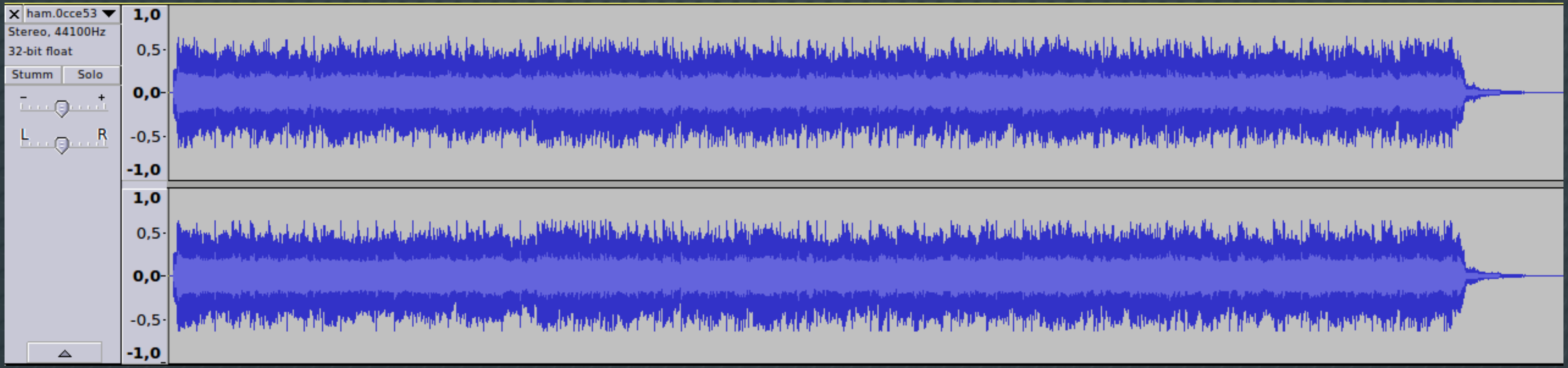
#Recon - pt. 2

- Anything in meta/tags ?

```
$ ffprobe ham.wav
Input #0, wav, from 'ham.wav':
  Metadata:
    title           : Free Software Song (CTF-edited)
    artist          : Bino
    date            : 2012
    genre           : FreeMusic
  Duration: 00:00:31.16, bitrate: 1411 kb/s
    Stream #0:0: Audio: pcm_s16le ([1][0][0][0] / 0x0001),
```

#Recon - pt. 3

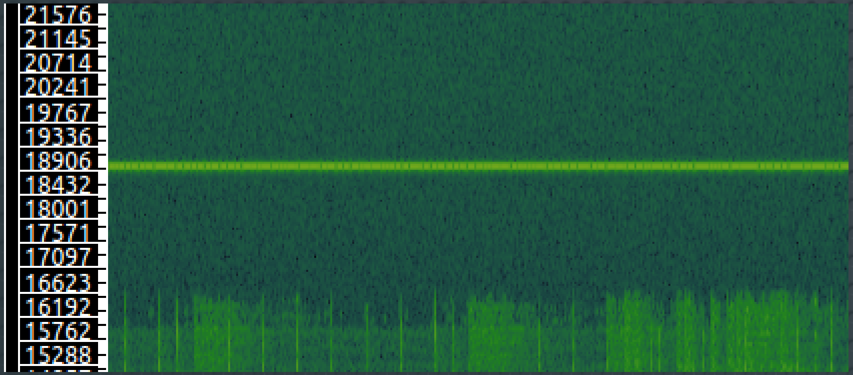
waveform



by cr0c0

#Recon - pt. 4

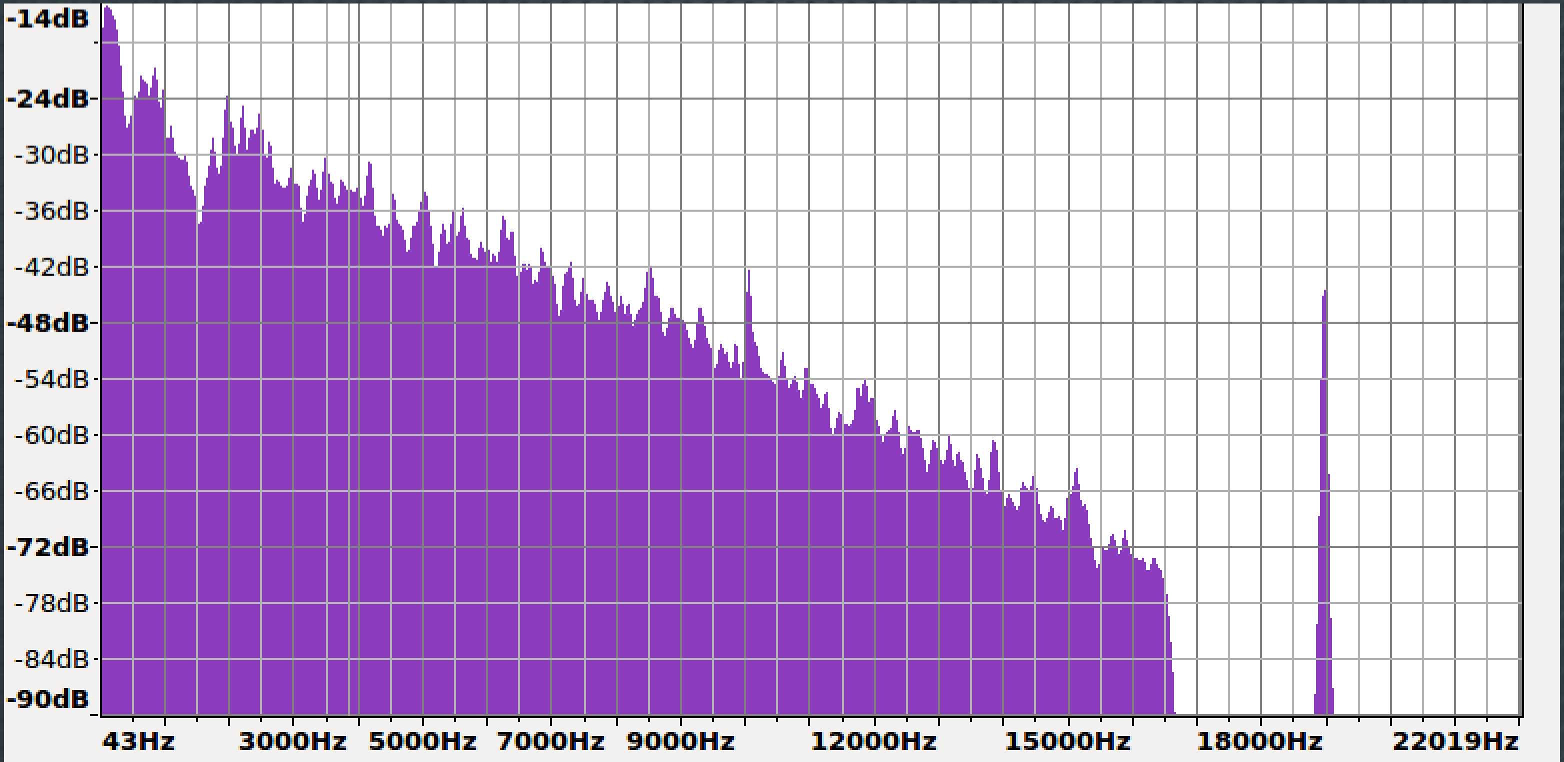
spectrogram



- Some small-band signal around 18 kHz constantly
- Signal-To-Noise Ratio ?

#Recon - pt. 5

spectrum



- Quite weak with attenuation of -48 dB

by cr0c0

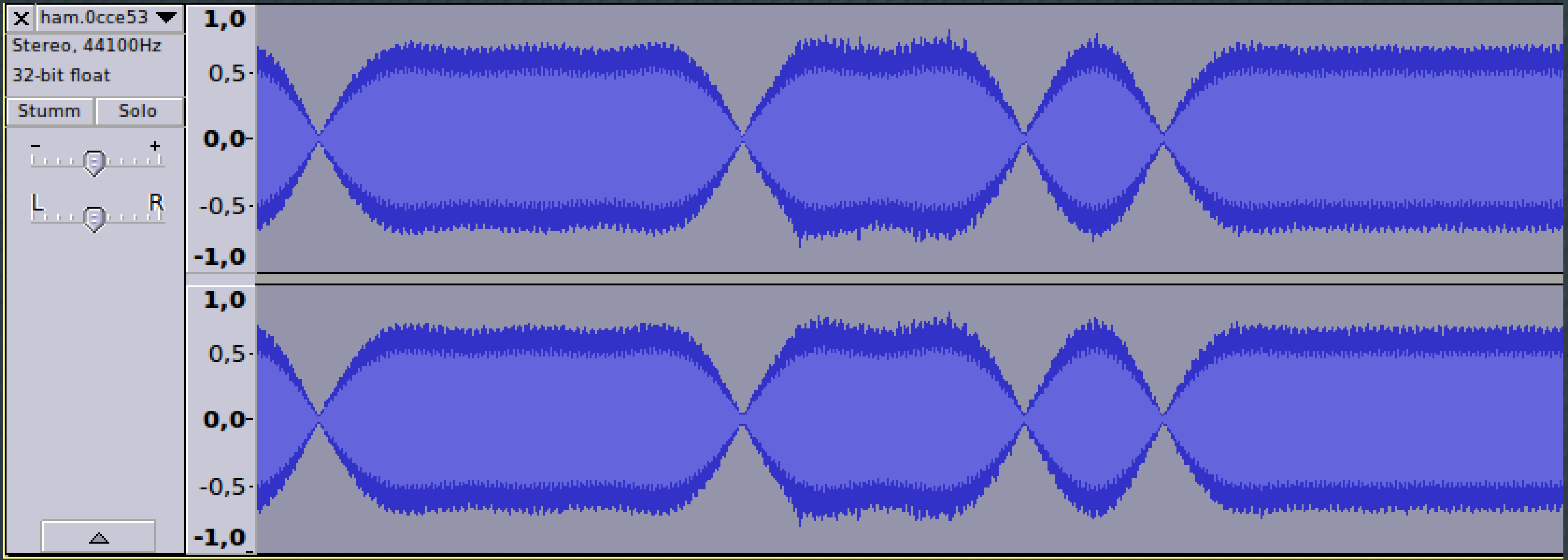
???

THAT'S NOT ENOUGH
WE HAVE TO GO DEEPER
memegen.com

#Extracting

#Extracting - pt. 1

- Reject start and end of track
- Apply high-pass (cutoff = 18 kHz)
- Amplify ~ 45 dB



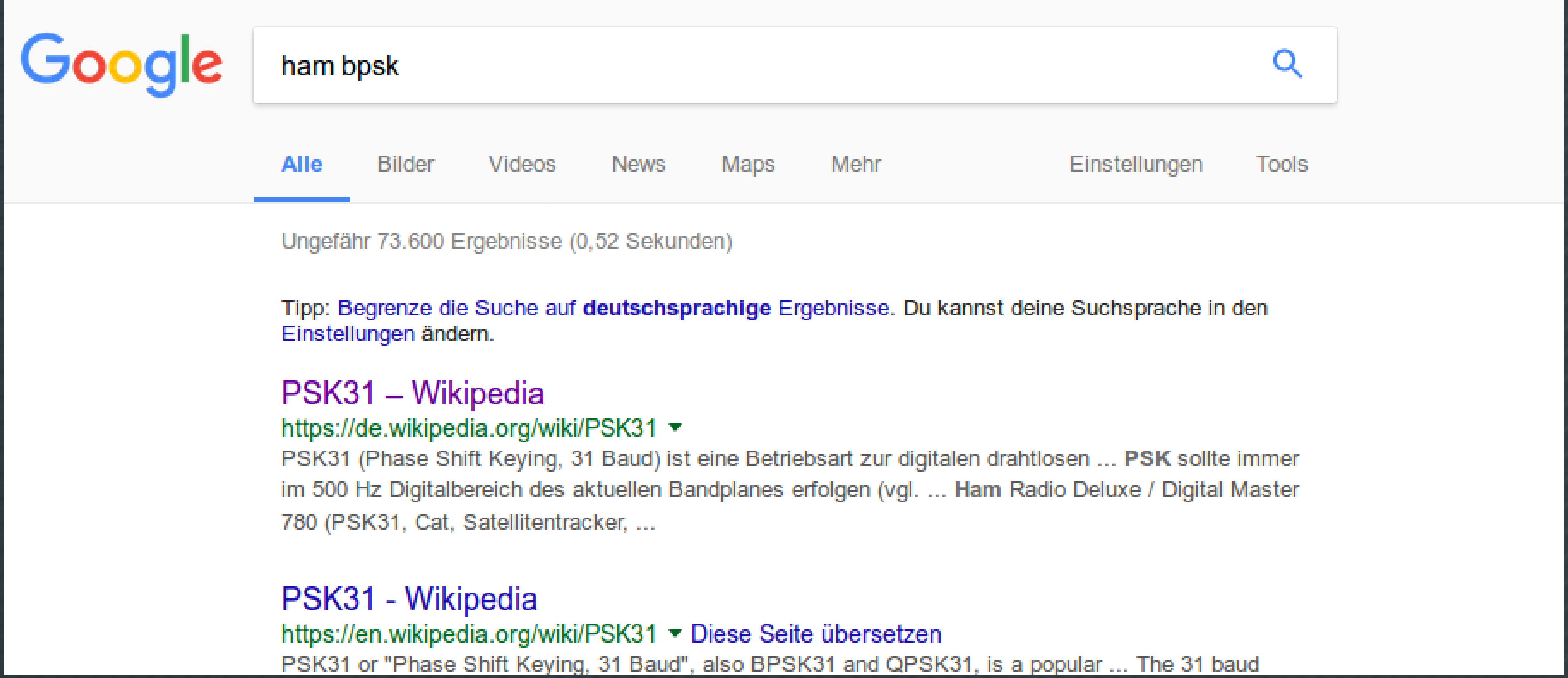
by cr0c0

#Extracting - pt. 2

- Some 2-symbol binary encoding: $a \in \{0, 1\}$
- Binary Phase Shift Keying (BPSK)
- Duration of 32 ms per symbol

#Extracting - pt. 2

- Maybe chall#s title tells us something



ham bpsk

Ungefähr 73.600 Ergebnisse (0,52 Sekunden)

Tipp: Begrenze die Suche auf **deutschsprachige** Ergebnisse. Du kannst deine Suchsprache in den Einstellungen ändern.

PSK31 – Wikipedia
https://de.wikipedia.org/wiki/PSK31 ▾
PSK31 (Phase Shift Keying, 31 Baud) ist eine Betriebsart zur digitalen drahtlosen ... **PSK** sollte immer im 500 Hz Digitalbereich des aktuellen Bandplanes erfolgen (vgl. ... **Ham** Radio Deluxe / Digital Master 780 (PSK31, Cat, Satellitentracker, ...

PSK31 - Wikipedia
https://en.wikipedia.org/wiki/PSK31 ▾ Diese Seite übersetzen
PSK31 or "Phase Shift Keying, 31 Baud", also BPSK31 and QPSK31, is a popular ... The 31 baud

by cr0c0

#Extracting - pt. 3

- Formerly called "Varicode", now PSK31
- Fano-Code
- No symbol is proper prefix of another one
- So it can be decoded quite easily...

#Flag

#Flag - pt. 1

```
from scipy.io import wavfile
import numpy as np

rate, data = wavfile.read("filtered.wav")

# select the second channel

data = data[:,1]
samples_per_symbol = int(rate / 1000.0 * 32)
data = data[:-(data.size % samples_per_symbol)]
symbols = np.mean(np.abs(data.reshape(-1, samples_per_symbo
symbols = symbols[symbols > (symbols[0] / 2)]
cutoff = np.mean([max(symbols), symbols[0]])

print ''.join(["1" if x else "0" for x in symbols > cutoff]
```

#Flag - pt. 2

- Extracting "varicode" binary information from audio track

```
python -W ignore decode.py
00000000000000000000000000000001010101010010110011101100100
```

- Thanks to github, there's a decoding table for varicode already as python dictionary

by cr0c0

#Flag - pt. 3

```
decode = {
    '1010101011' : '\x00',    '1011011011' : '\x01',
    '1011101101' : '\x02',    '1101110111' : '\x03',
    '1011101011' : '\x04',    '1101011111' : '\x05',
[...snip...]
   '11011111'    : 'x',        '1011101'     : 'y',
    '111010101'   : 'z',       '1010110111' : '{',
    '110111011'   : '|',       '1010110101' : '}',
'1011010111' : '~', '1110110101' : '\x7F' }
```

by cr0c0

#Flag - pt. 4

- Turning audio to flag gold

```
[...snip...]
data = data.lstrip("0").rstrip("1")
chars = data.split("00")
print ''.join([varicode[c] if c in varicode else "?" for c
```

> Ham radio amateurs are gradually in extinction nowadays :(-> flag{LookingForRainbowsInTheSpectrumMadeMeBlind}?

by cr0c0

#Questions ???