Visualizing RF

June 14th, 2011

Ryan Woodings

Chief Geek | MetaGeek LLC

Special Guest Trent Cutler

SHARKFEST '11

Stanford University

June 13-16, 2011

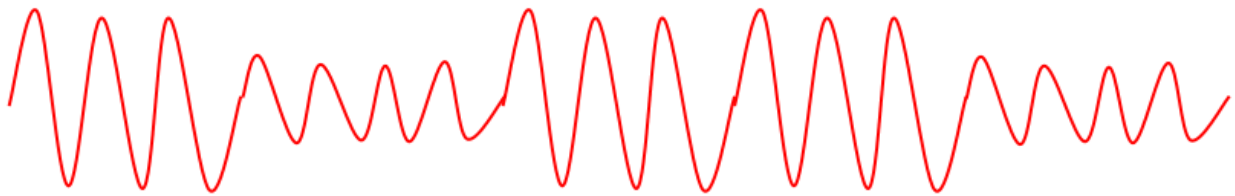
One Broadcast Beacon

```
0000   00 00 1a 00 6f 18 00 00   c3 a7 0f 05 00 00 00 00   ....o... ........
0010   10 0c 71 16 40 01 ca a8   00 22 80 00 00 00 ff ff   ..q.@... ."......
0020   ff ff ff ff 00 1f 5b 86   e1 a9 00 1f 5b 86 e1 a9   ......[. ....[...
0030   40 65 33 20 55 f1 6d 03   00 00 64 00 11 05 00 08   @e3 U.m. ..d.....
0040   4d 65 74 61 47 65 65 6b   01 08 8c 12 98 24 b0 48   MetaGeek .....$.H
0050   60 6c 03 01 95 05 04 01   03 00 00 07 1e 55 53 20   `l...... .....US
0060   24 01 0a 28 01 0a 2c 01   0a 30 01 0a 95 01 10 99   $..(..,. .0......
0070   01 10 9d 01 10 a1 01 10   a5 01 10 20 01 02 30 14   ........ ... ..0.
0080   01 00 00 0f ac 04 01 00   00 0f ac 04 01 00 00 0f   ........ ........
0090   ac 02 00 00 2d 1a 6e 02   17 ff ff 00 00 00 00 00   ....-.n. ........
00a0   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ........ ........
00b0   3d 16 95 05 00 00 00 00   00 00 00 00 00 00 00 00   =....... ........
00c0   00 00 00 00 00 00 00 00   dd 18 00 50 f2 02 01 01   ........ ...P....
00d0   07 00 03 a4 00 00 27 a4   00 00 42 43 5e 00 62 32   ......'. ..BC^.b2
00e0   2f 00 dd 1e 00 90 4c 33   6e 02 17 ff ff 00 00 00   /.....L3 n.......
00f0   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ........ ........
0100   00 00 dd 1a 00 90 4c 34   95 05 00 00 00 00 00 00   ......L4 ........
0110   00 00 00 00 00 00 00 00   00 00 00 00 00 00 dd 07   ........ ........
0120   00 03 93 01 6a 01 20 dd   0b 00 17 f2 01 00 01 01   ....j. . ........
0130   00 00 00 07 d1 f7 36 ab                             ......6.
```

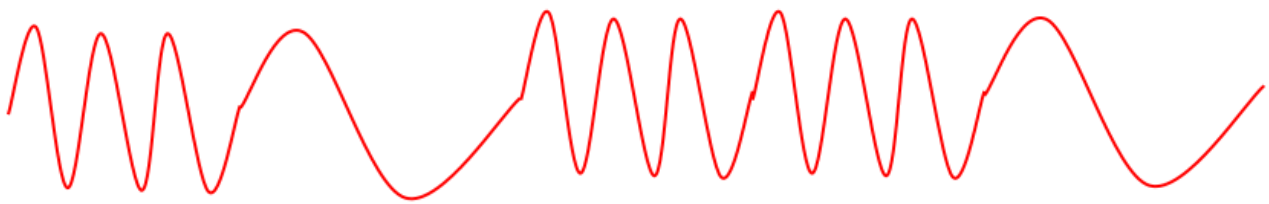
Where the 0s and 1s Come From

Modulation:

Amplitude

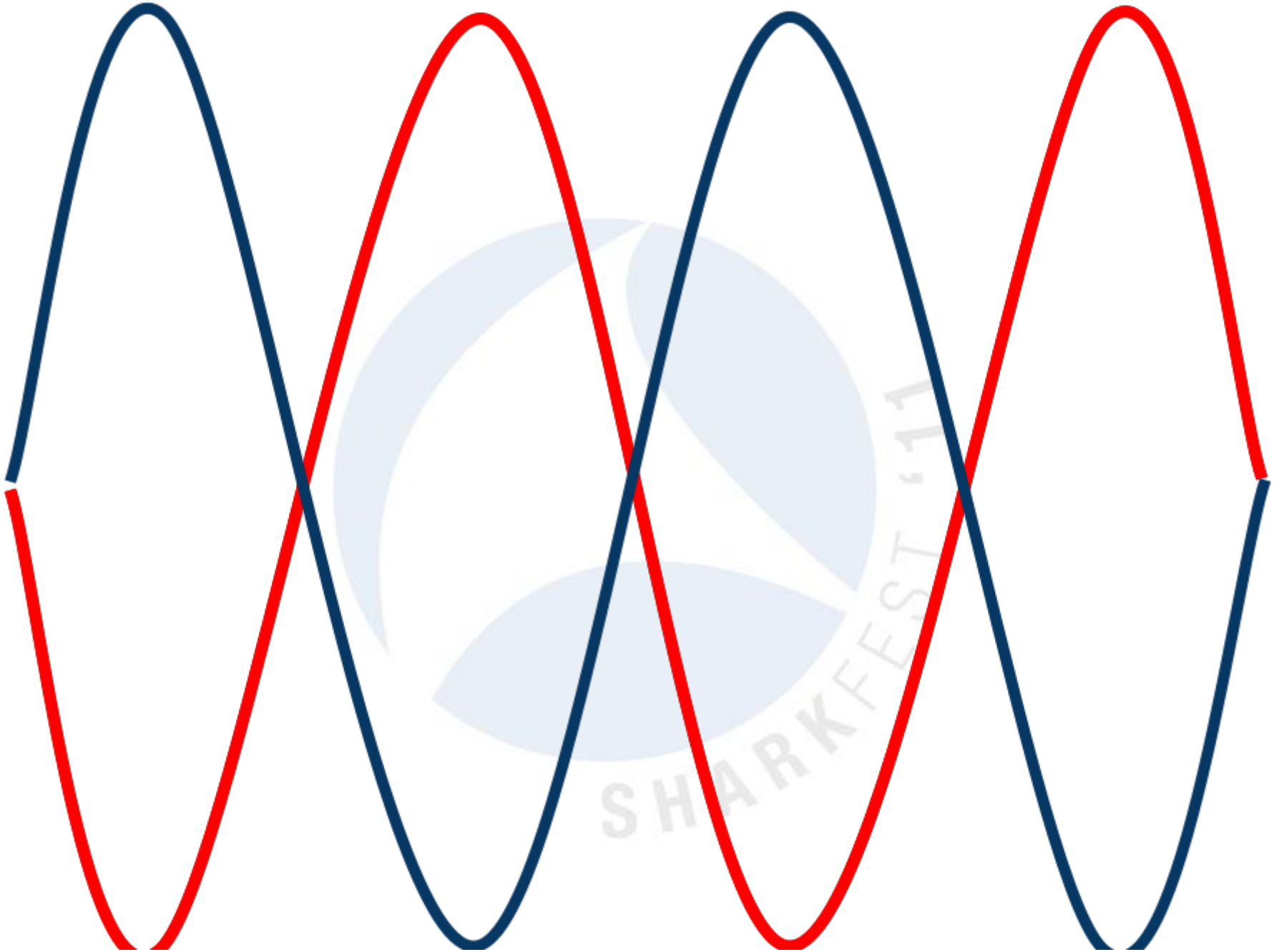


Frequency



Phase

Wireless Collisions

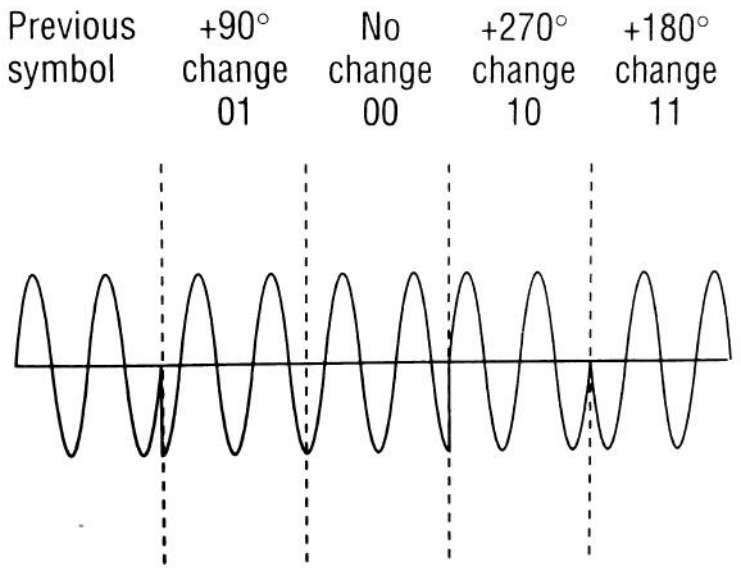


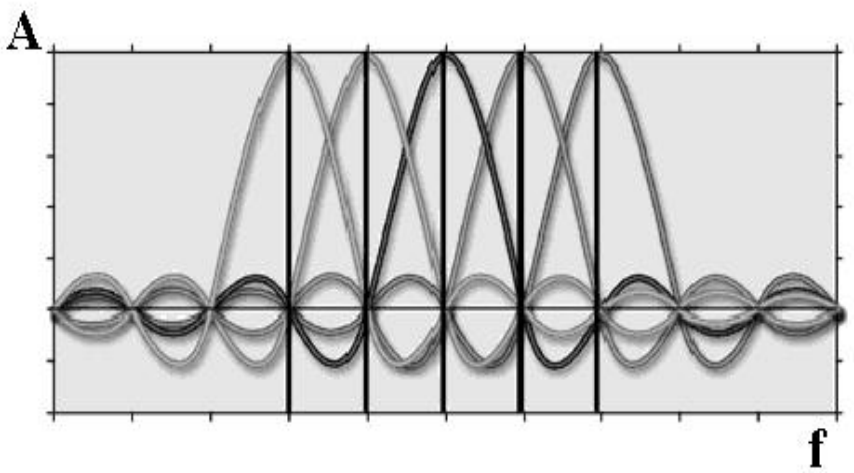
Wireless Collisions

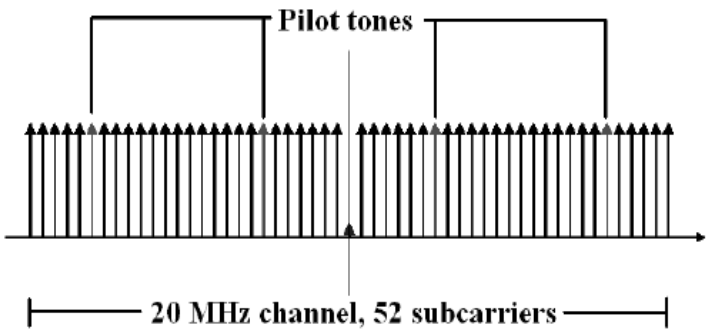
No Data.

RF Modulation

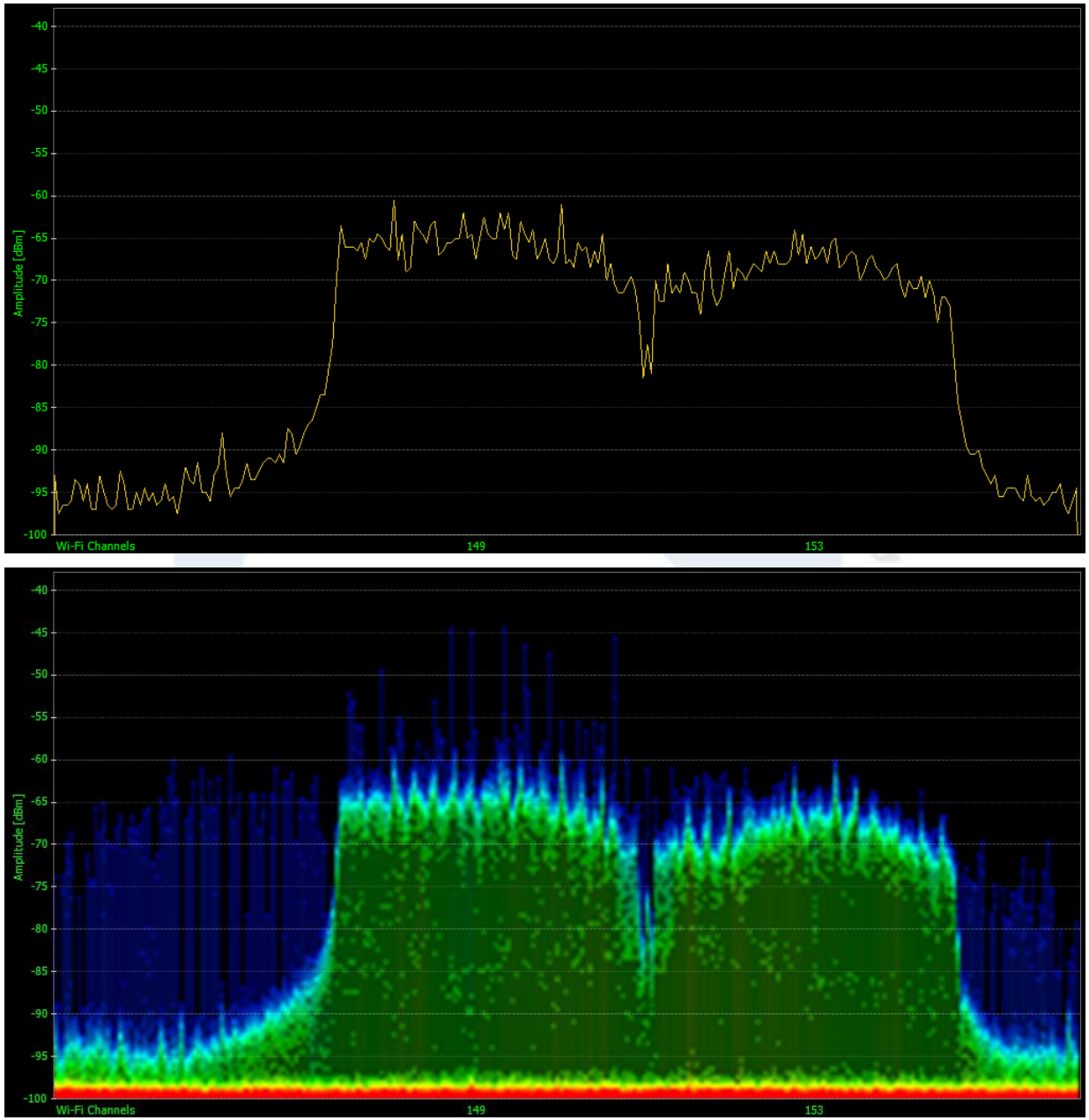
802.11a/g/n use Orthogonal Frequency-Division Multiplexing (OFDM)





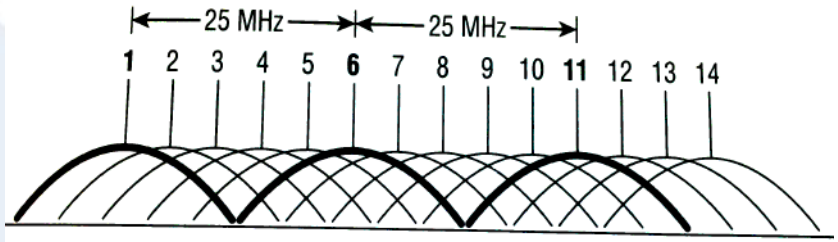


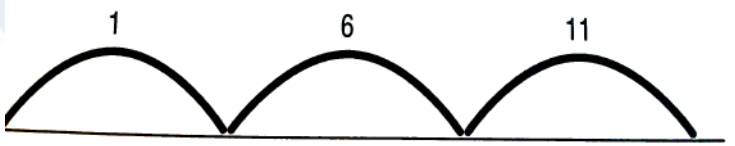
Spectrum Analysis



802.11b HR/DSSS PSK w/ CCK

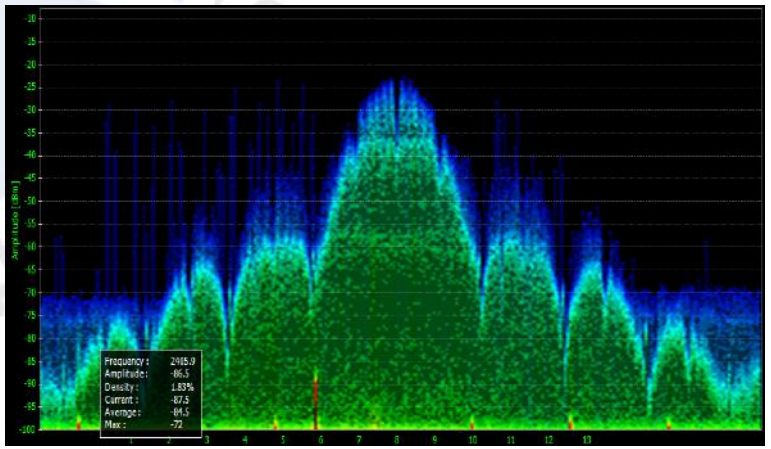
- 11Mbps
- 2.4 GHz
- 3 "non-overlapping" channels (US)





WireShark Filter:
ppi.80211-common.chan.type == 0x00a0

```
802.11-Common
    Field type: 802.11-Common (2)
    Field length: 20
    TSFT: 7470569556
  Flags: 0x0001
      .... .... .... ...1 = FCS present flag: Present
      .... .... .... ..0. = TSFT flag: microseconds
      .... .... .... .0.. = FCS validity: Valid
      .... .... .... 0... = PHY error flag: No errors
    Rate: 11.0 Mbps
    Channel frequency: 2437 [BG 6]
  Channel type: 802.11b (0x00a0)
      .... .... ...0 .... = Turbo: False
      .... .... ..1. .... = Complementary Code Keying (CCK): True
      .... .... .0.. .... = Orthogonal Frequency-Division Multiplexing (OFDM): False
      .... .... 1... .... = 2 GHz spectrum: True
      .... ...0 .... .... = 5 GHz spectrum: False
      .... ..0. .... .... = Passive: False
      .... .0.. .... .... = Dynamic CCK-OFDM: False
      .... 0... .... .... = Gaussian Frequency Shift Keying (GFSK): False
    FHSS hopset: 0x00
    FHSS pattern: 0x00
    dBm antenna signal: -43
    dBm antenna noise: -73
```

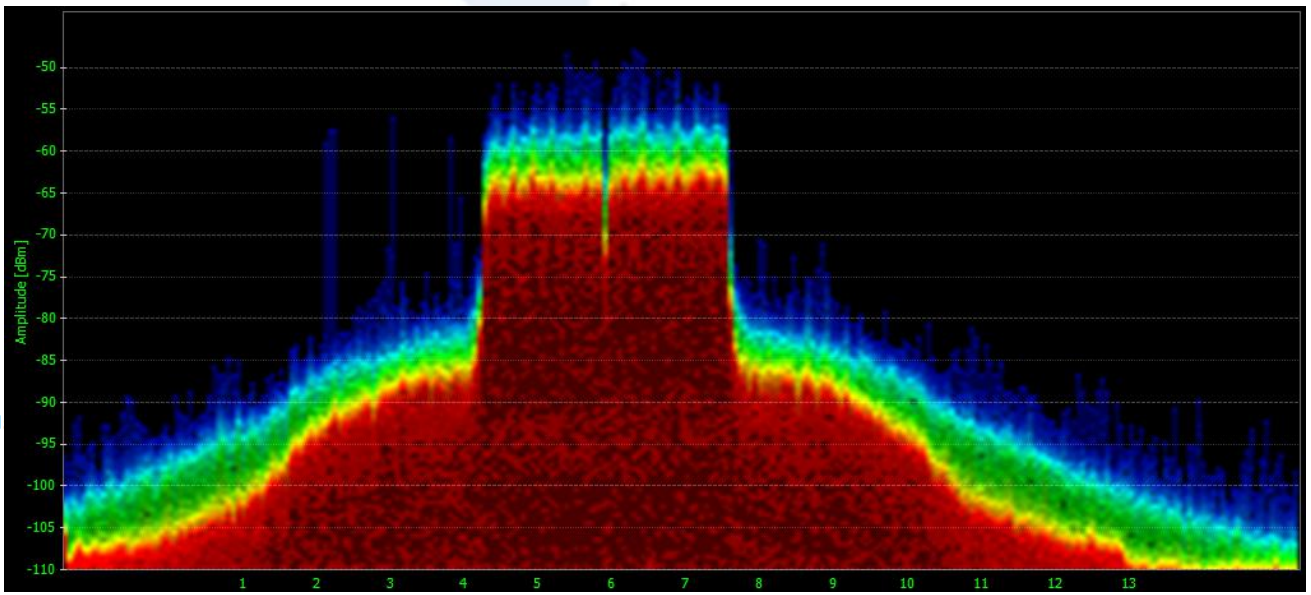


802.11g ERP-OFDM

- 54Mbps
- 2.4 GHz
- 3 non-overlapping channels (US)

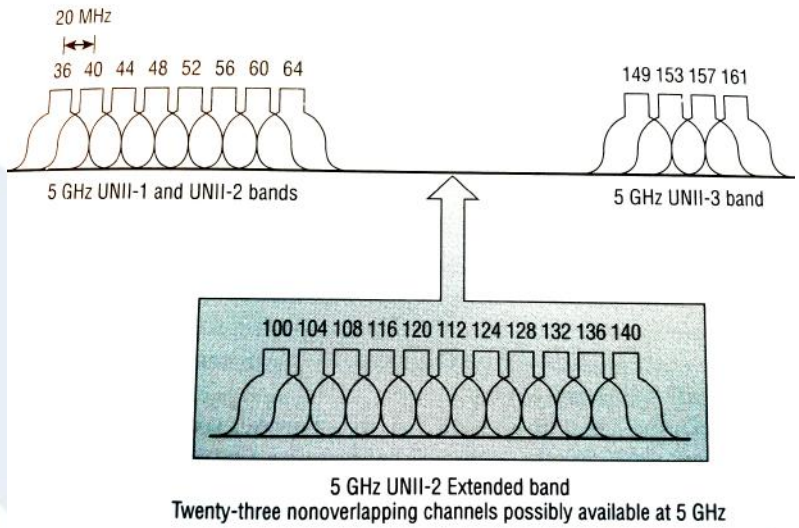
WireShark Filter:
ppi.80211-common.chan.type == 0x00c0

```
802.11-Common
    Field type: 802.11-Common (2)
    Field length: 20
    TSFT: 7470541392
  Flags: 0x0001
      .... .... .... ...1 = FCS present flag: Present
      .... .... .... ..0. = TSFT flag: microseconds
      .... .... .... .0.. = FCS validity: Valid
      .... .... .... 0... = PHY error flag: No errors
    Rate: 24.0 Mbps
    Channel frequency: 2437 [BG 6]
  Channel type: 802.11g (pure-g) (0x00c0)
      .... .... ...0 .... = Turbo: False
      .... .... ..0. .... = Complementary Code Keying (CCK): False
      .... .... .1.. .... = Orthogonal Frequency-Division Multiplexing
      .... .... 1... .... = 2 GHz spectrum: True
      .... ...0 .... .... = 5 GHz spectrum: False
      .... ..0. .... .... = Passive: False
      .... .0.. .... .... = Dynamic CCK-OFDM: False
      .... 0... .... .... = Gaussian Frequency Shift Keying (GFSK): Fal
    FHSS hopset: 0x00
    FHSS pattern: 0x00
    dBm antenna signal: -57
    dBm antenna noise: -73
```



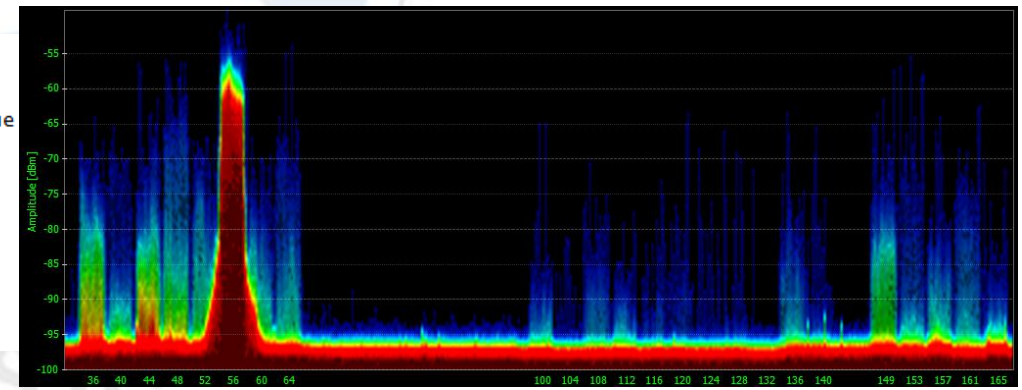
802.11a OFDM

- 54Mbps
- 5 GHz
- 20-23 non-overlapping channels (US)



WireShark filter
ppi.80211-common.chan.type == 0x0140

```
⊟ Channel type: 802.11a (0x0140)
    .... .... ...0 .... = Turbo: False
    .... .... ..0. .... = Complementary Code Keying (CCK): False
    .... .... .1.. .... = Orthogonal Frequency-Division Multiplexing (OFDM): True
    .... .... 0... .... = 2 GHz spectrum: False
    .... ...1 .... .... = 5 GHz spectrum: True
    .... ..0. .... .... = Passive: False
    .... .0.. .... .... = Dynamic CCK-OFDM: False
    .... 0... .... .... = Gaussian Frequency Shift Keying (GFSK): False
  FHSS hopset: 0x00
  FHSS pattern: 0x00
  dBm antenna signal: -44
  dBm antenna noise: -81
```

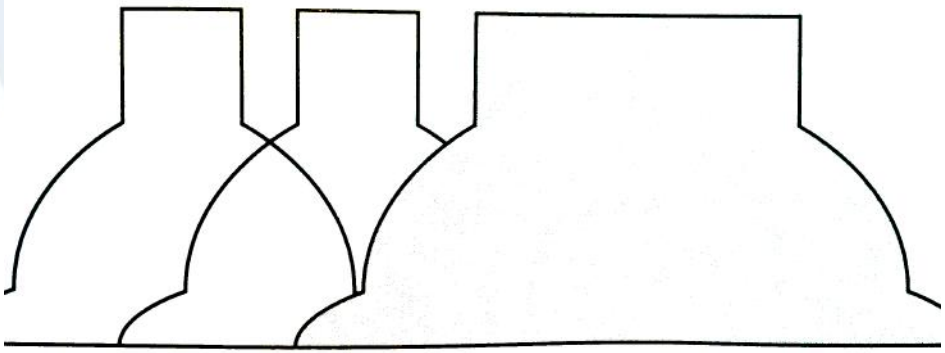


802.11n OFDM (40 MHz)

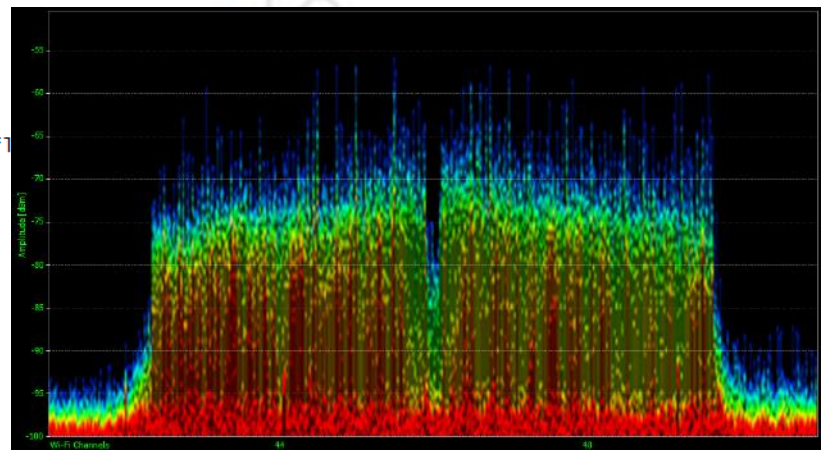
Channel Bonding (uses two Wi-Fi channels)

- Up to 450Mbps
- 2.4 & 5 GHz
- 1 non-overlapping channel in 2.4 GHz
- 11 non-overlapping in 5 GHz

WireShark Filter
ppi.field_len == 48
ppi.80211-common.rate > 54000

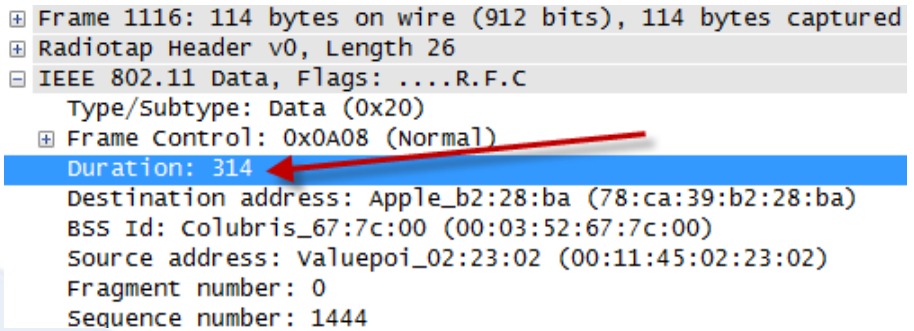


```
802.11n MAC+PHY
  Field type: 802.11n MAC+PHY Extensions (4)
  Field length: 48
  MAC flags: 0x00000000
    .... .... .... .... .... .... .... ...0 = Greenfield flag: False
    .... .... .... .... .... .... .... ..0. = HT20/HT40 flag: HT20
    .... .... .... .... .... .... .... .0.. = RX Short Guard Interval (SGI) flag: False
    .... .... .... .... .... .... .... 0... = Duplicate RX flag: False
    .... .... .... .... .... .... ...0 .... = Aggregate flag: False
    .... .... .... .... .... .... ..0. .... = More aggregates flag: False
    .... .... .... .... .... .... .0.. .... = A-MPDU Delimiter CRC error after this frame fl
  AMPDU-ID: 0x00000000
  Num-Delimiters: 0
  MCS: 2
  Number of spatial streams: 1
  RSSI combined: 31
  Antenna 0 control RSSI: 24
  Antenna 1 control RSSI: 255 [invalid]
  Antenna 2 control RSSI: 30
  Antenna 3 control RSSI: 255 [invalid]
  Antenna 0 extension RSSI: 6
  Antenna 1 extension RSSI: 255 [invalid]
  Antenna 2 extension RSSI: 4
  Antenna 3 extension RSSI: 255 [invalid]
  Ext. Channel frequency: 5765 [A 153]
```



Distributed Coordination Function

NAV - Network Allocation Vector



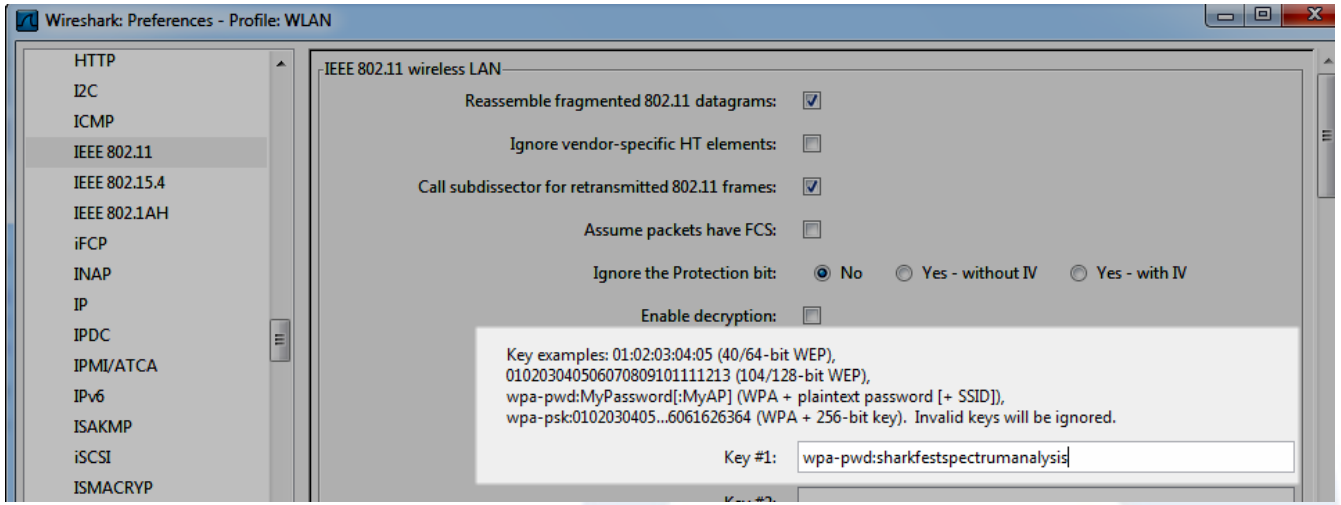
CCA - Clear Channel Assessment

DIFS - Distributed Coordination Function Interframe Space

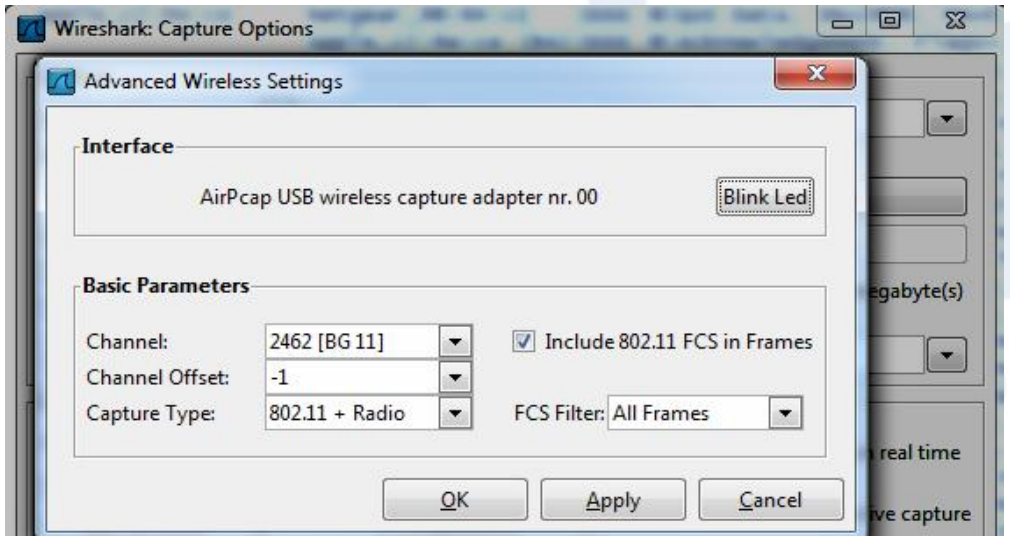
Slot Time - Backofftimer = random() x aSlotTime

Wireshark for the WLAN

Setting up Decryption



Monitoring a Wi-Fi Channel



Useful Filters

Filter Out Beacons
- !wlan.fc.type_subtype ==8

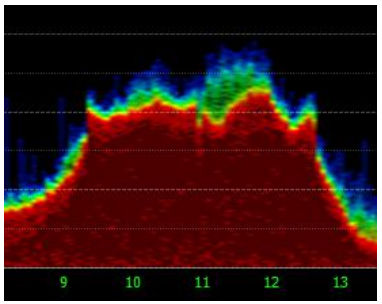
Retries
- wlan.fc.retry ==1

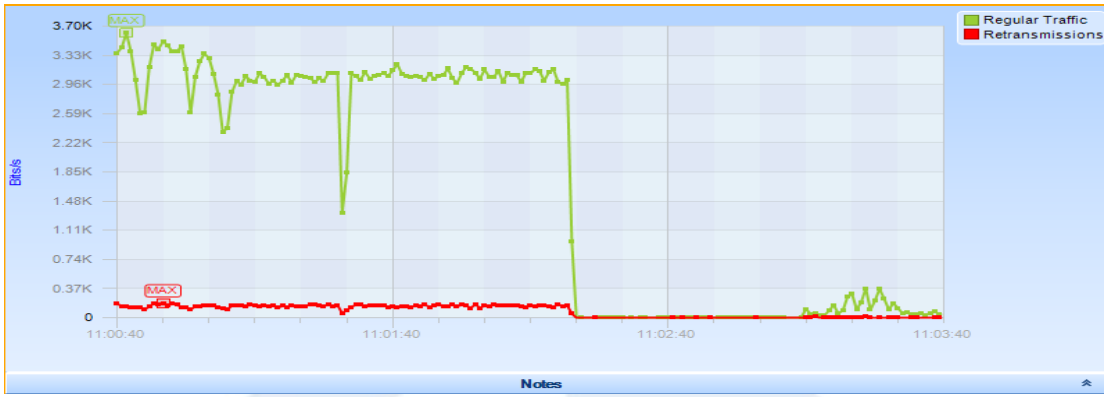
Disassociation
- wlan.fc.type_subtype ==10

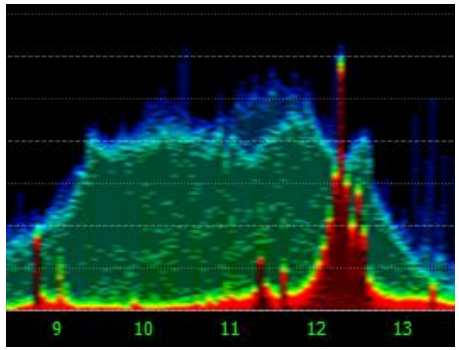
Probe Request/Response
- wlan.fc.type_subtype ==4 ||
  wlan.fc.type_subtype ==5

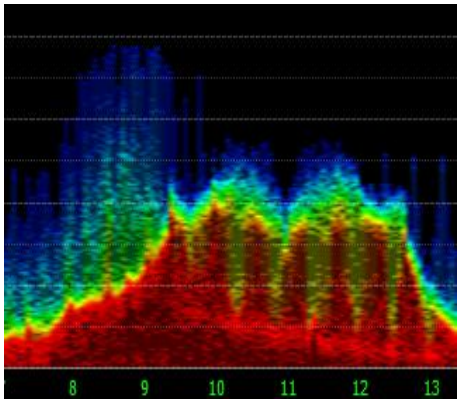
Roaming
- wlan.fc.type_subtype <= 0x03 ||
  wlan.fc.type_subtype == 0x0b || eapol

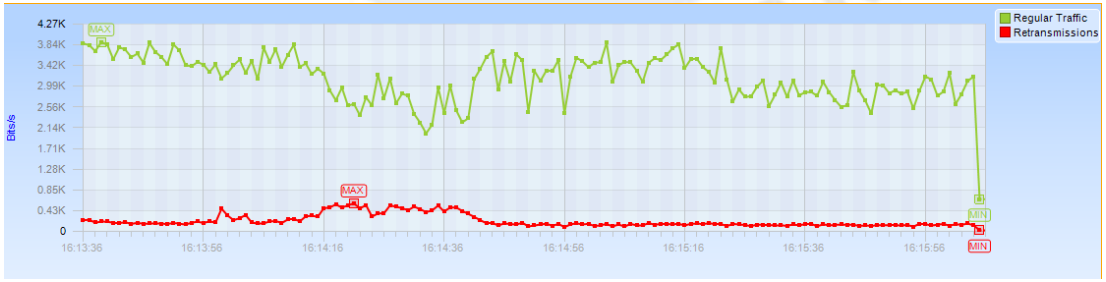
Symptoms of Interference

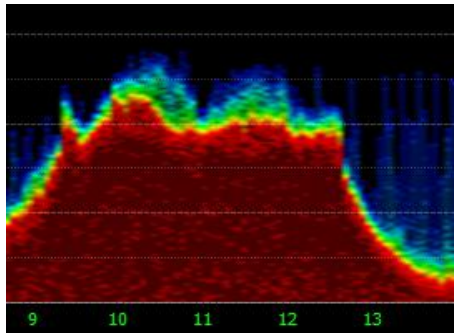






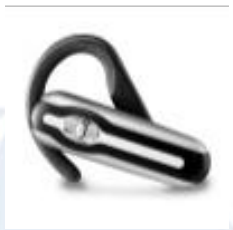






The Usual Suspects







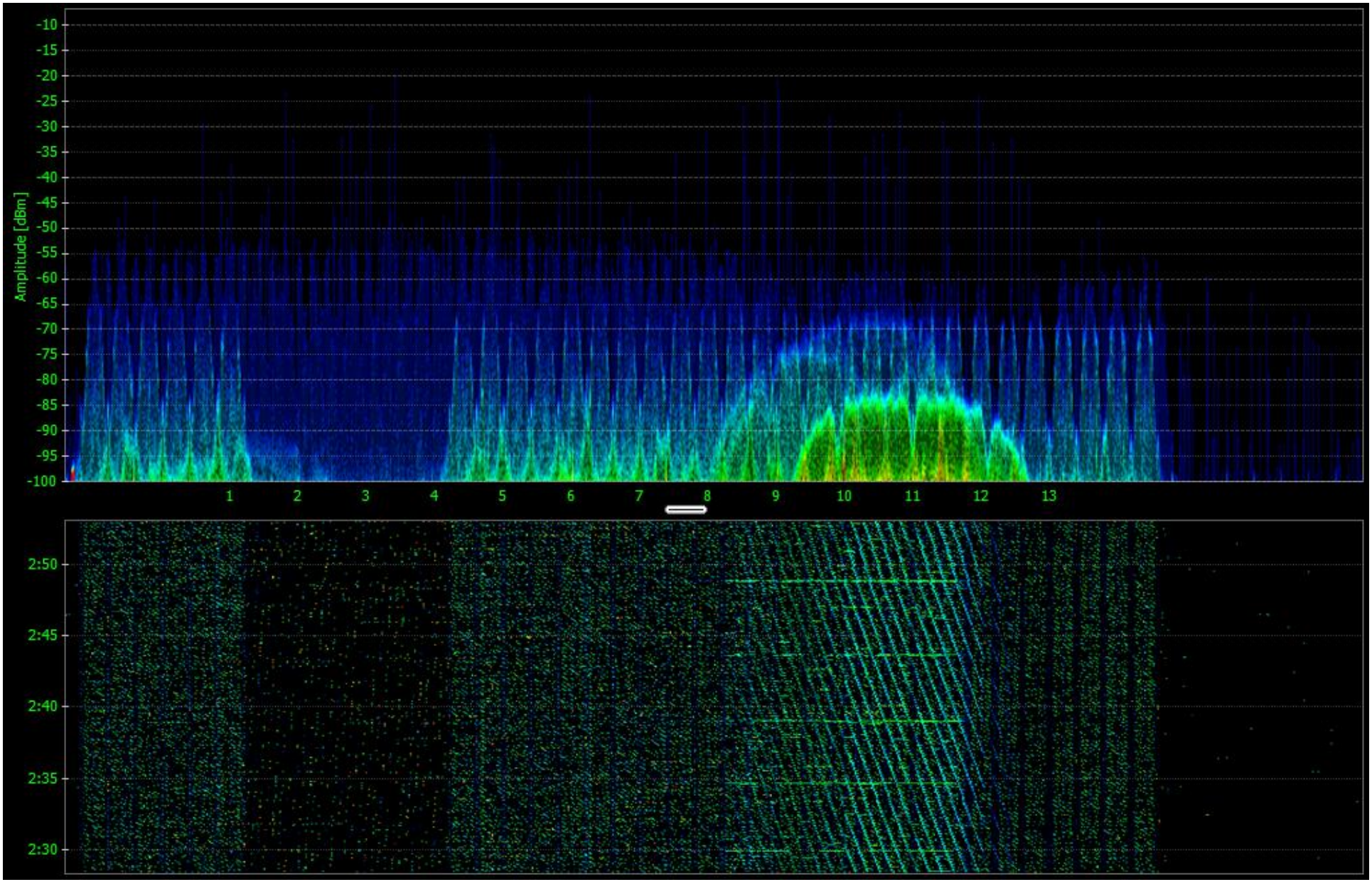




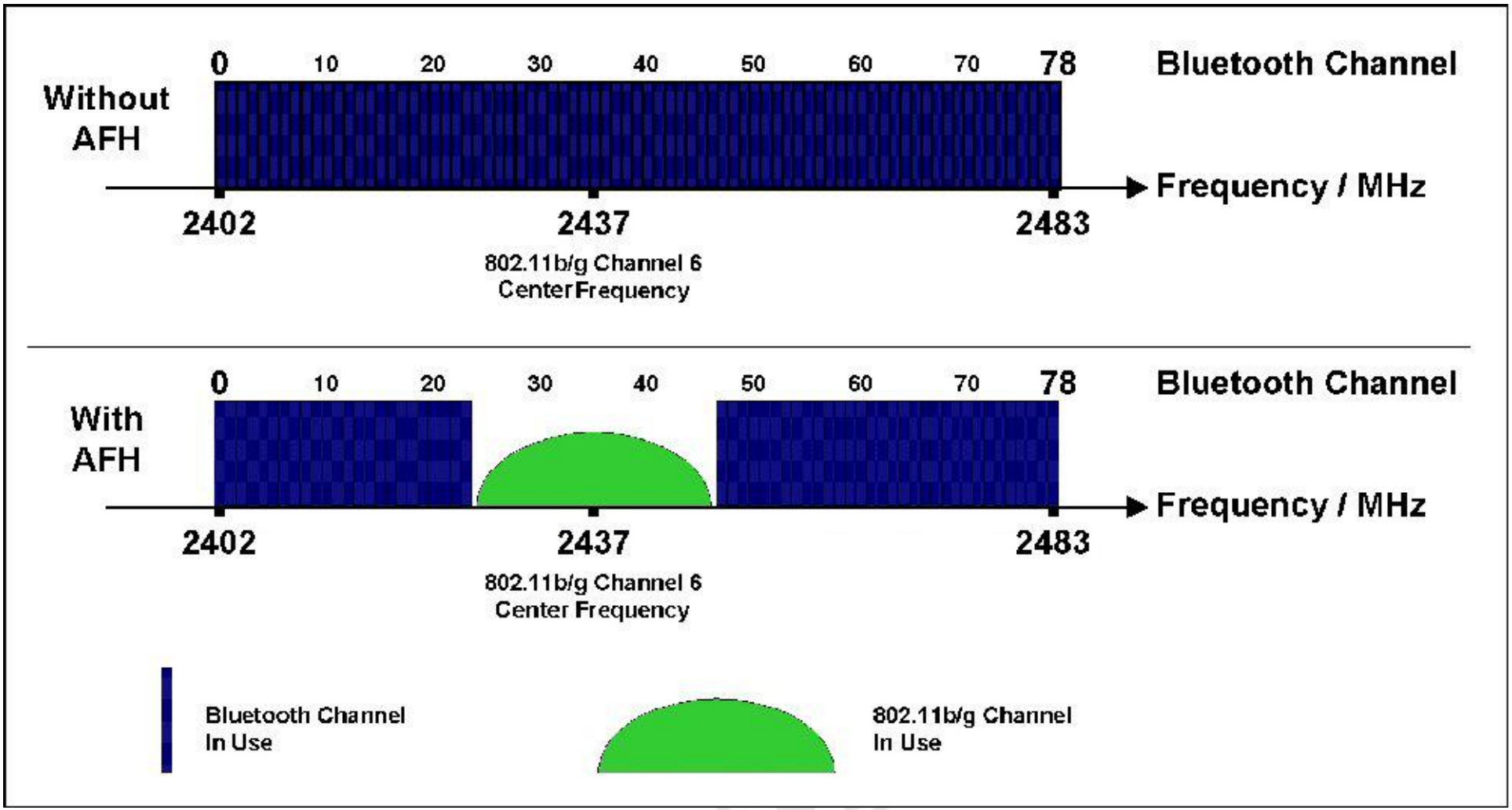


The Unusual Suspects

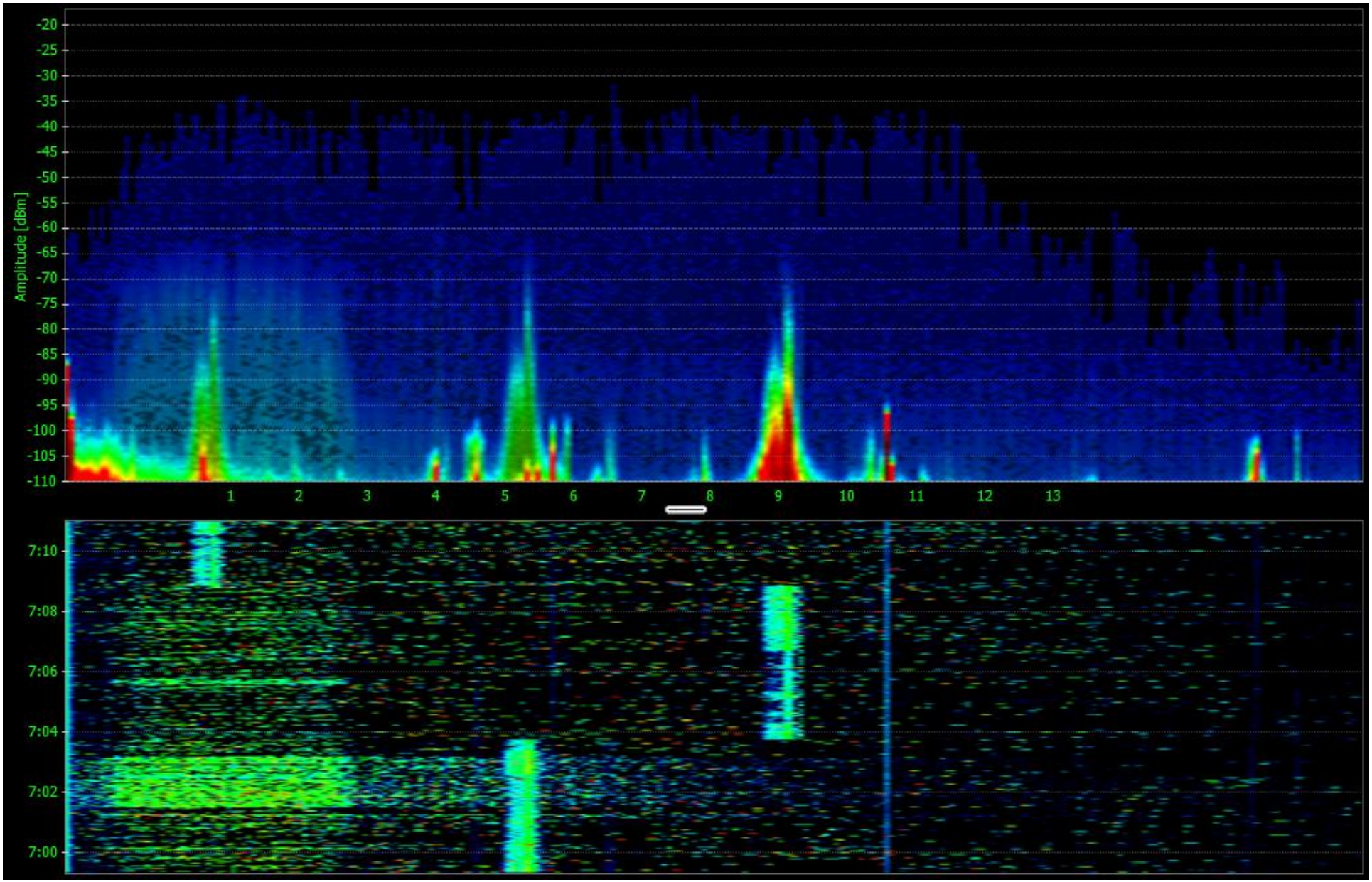
Bluetooth (Discovery)



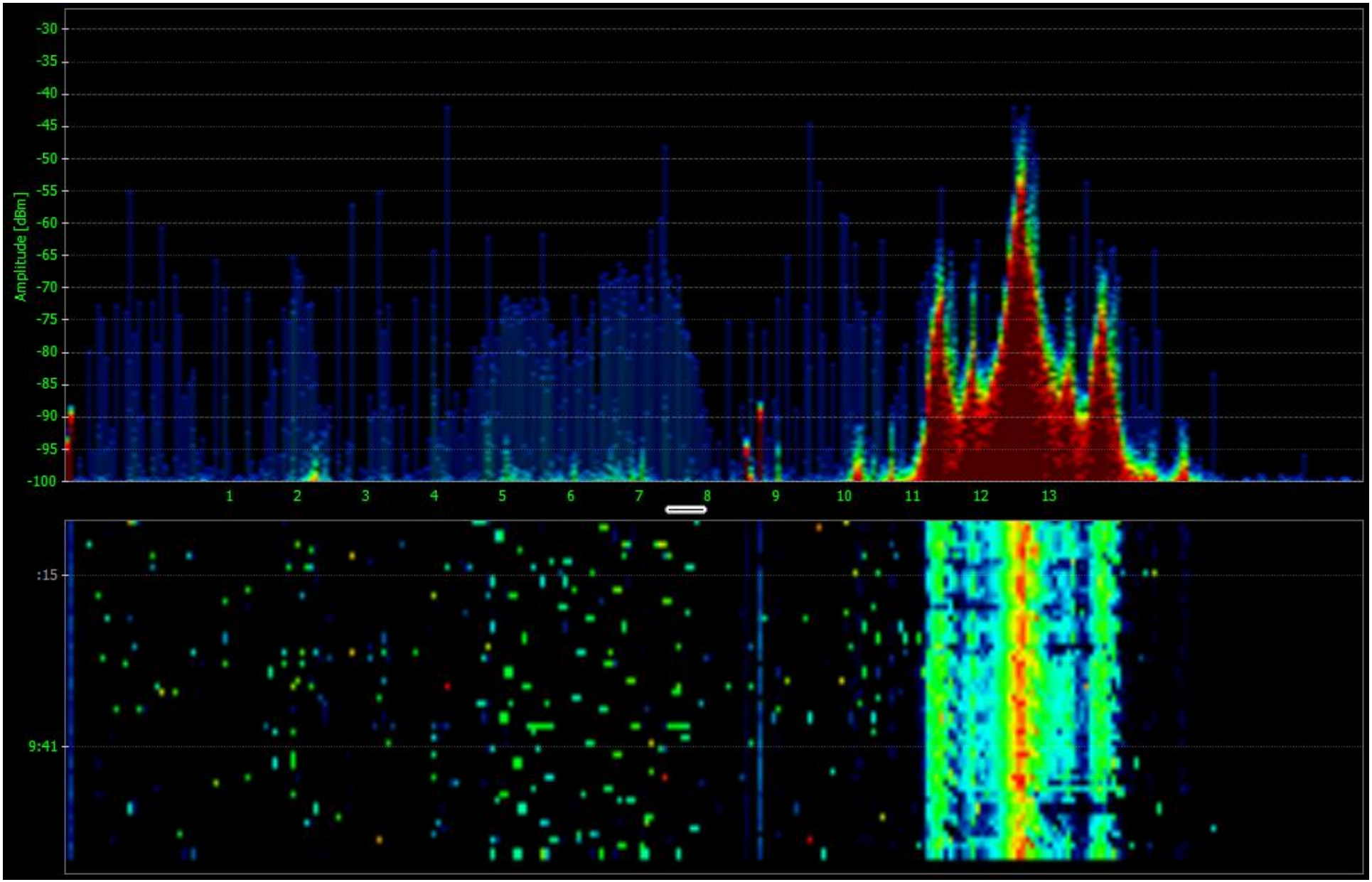
Bluetooth Adaptive Frequency Hopping



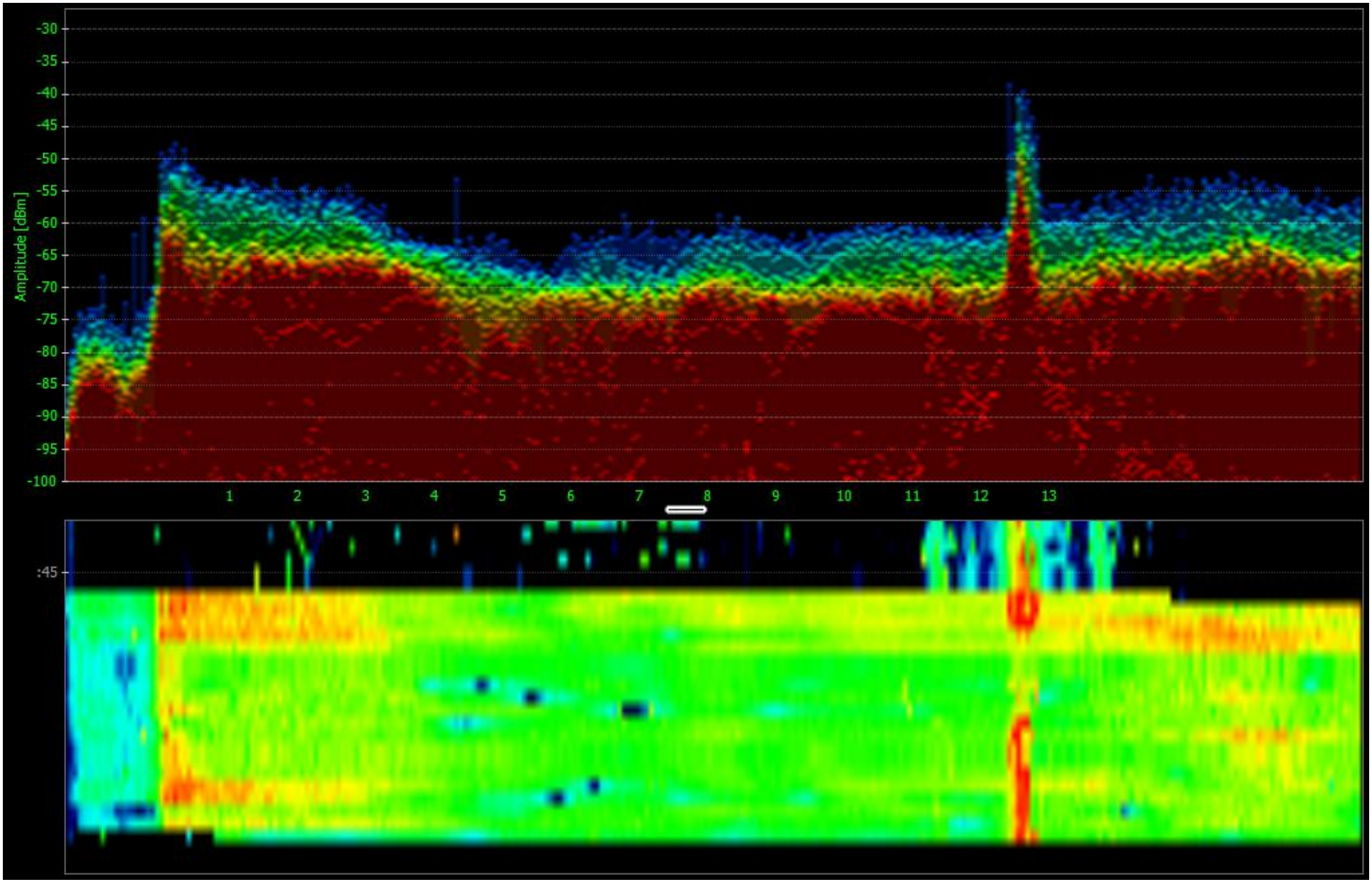
Baby Monitor



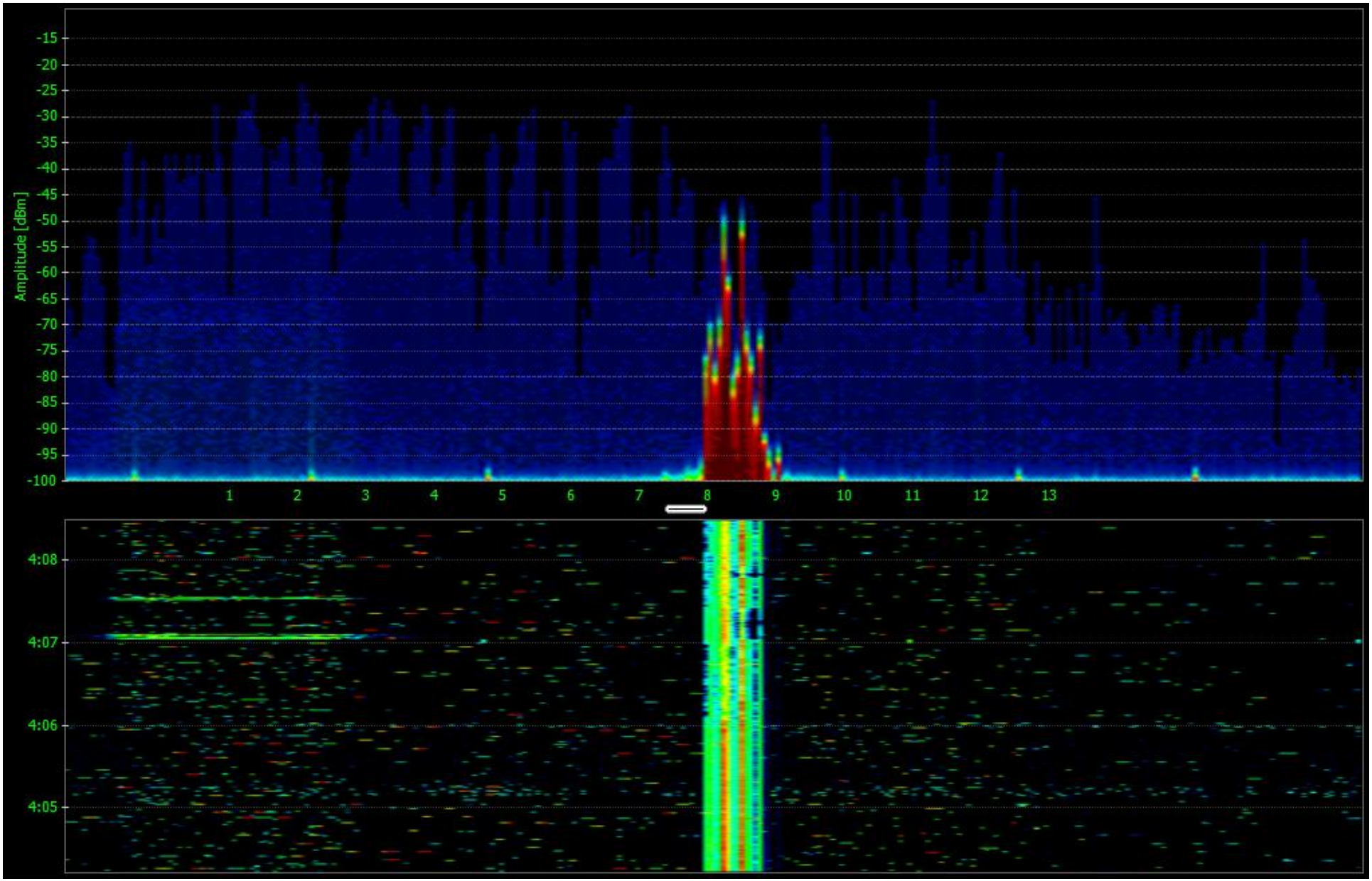
Analogue Video Transmitter



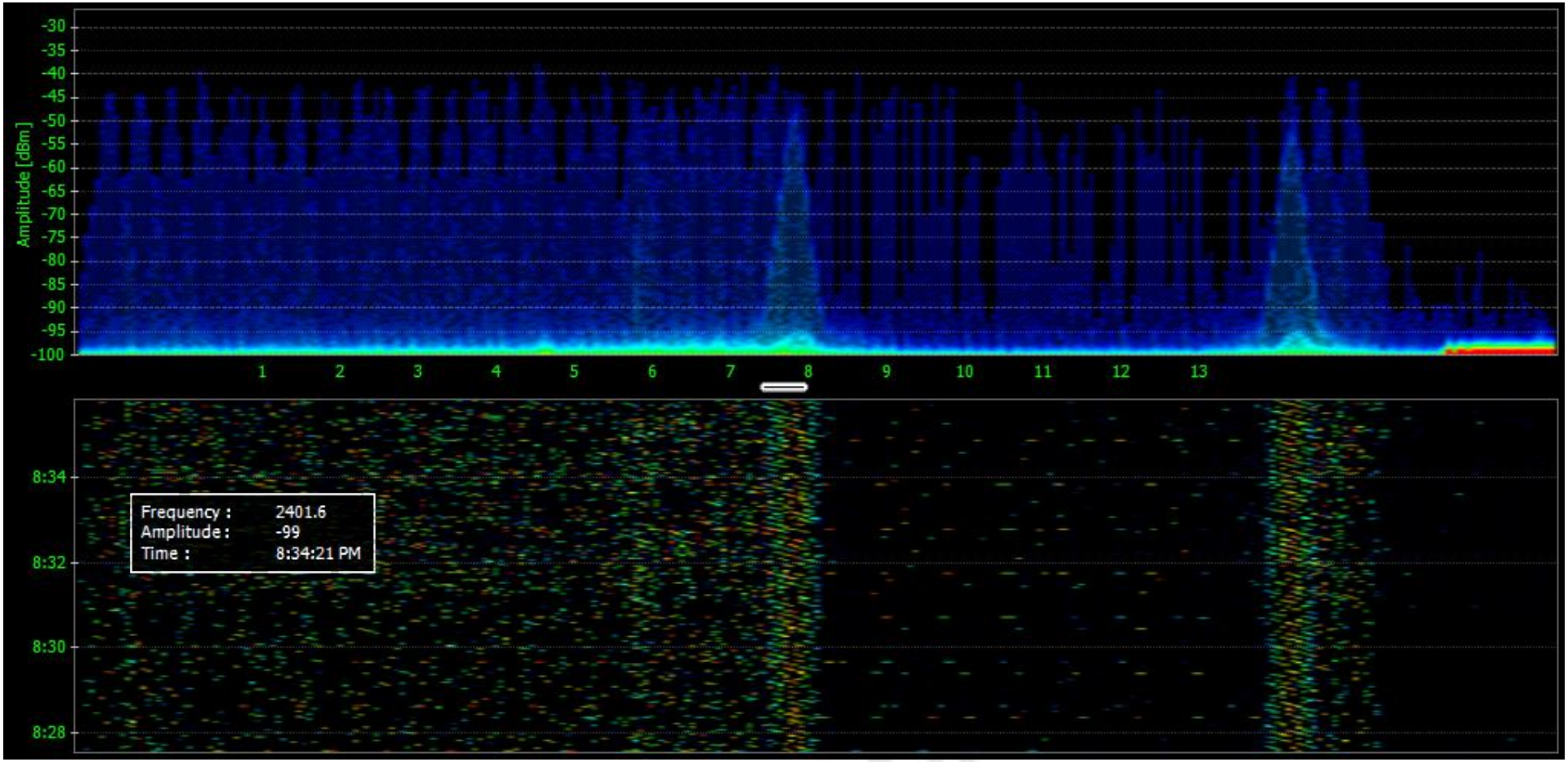
Wide Band Jammer



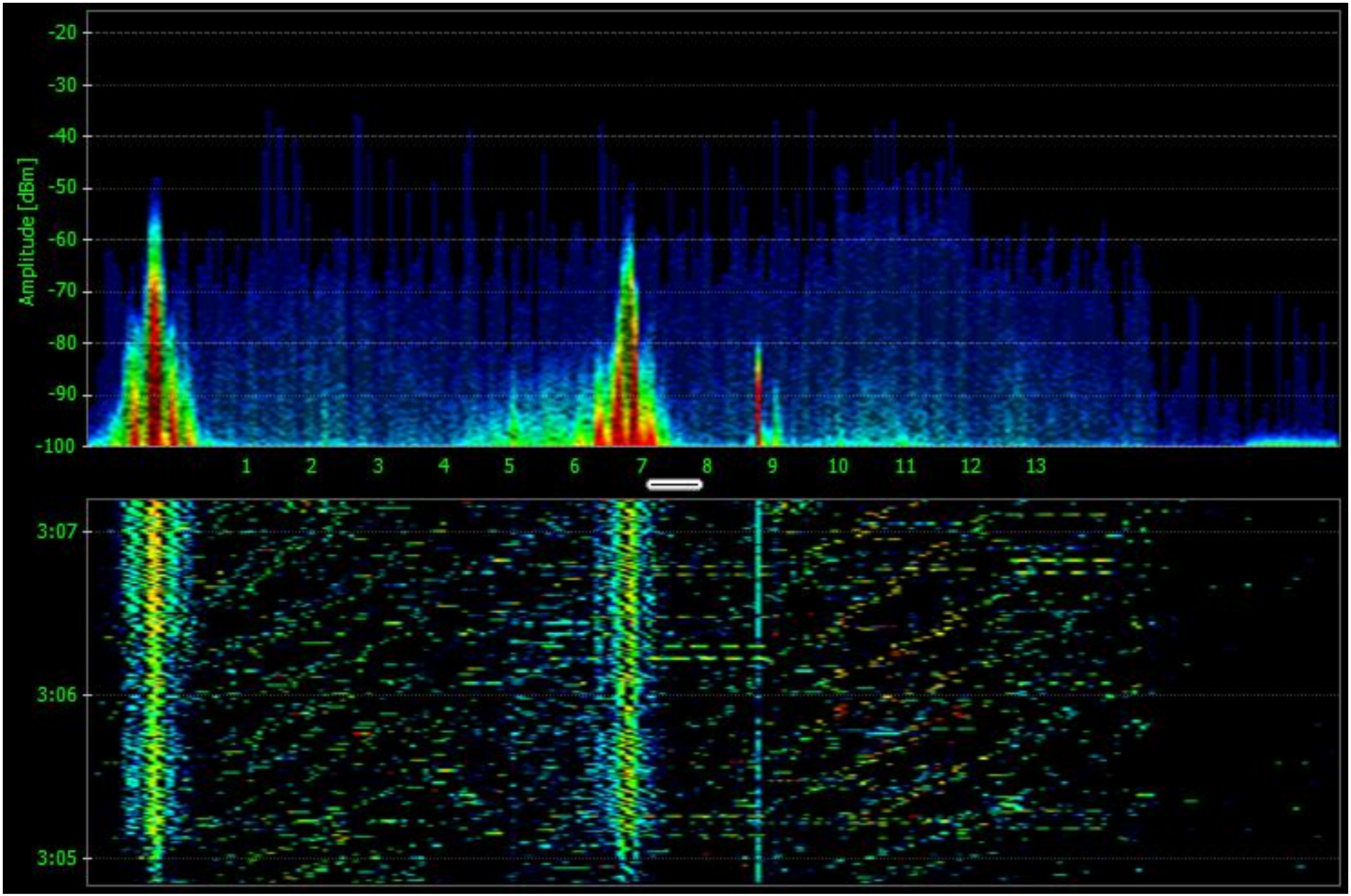
Motion Sensors



X-Box 360


Amplitude [dBm]
-30
-35
-40
-45
-50
-55
-60
-65
-70
-75
-80
-85
-90
-95
-100
1
2
3
4
5
6
7
8
9
10
11
12
13
8:34
8:32
8:30
8:28
Frequency : 2401.6
Amplitude : -99
Time : 8:34:21 PM

Wireless Headsets



Live Demo